CENG280, THE1 Solutions / Tuğberk

Q.1) Used proofs.

(I) The set $UC = \{0,1\}^*$ is countably infinite because countably infinite union of countable sets are countably infinite:

We can write $\{0,1\}^* = \bigcup_{k=0}^{\infty} S_k$

where $S_k = \{w \in \{0,1\}^* : |w| = k\}$

and for arbitrary $k \in \mathbb{N}$, $|S_k| = 2^k$, making S_k finite and consequently countable. Let $A_k = \{1, 2, \ldots, 2^k\}$ s.t. $|A_k| = |S_k|$. Thus, there exists a one-to-one function $f_k : A_k \to S_k$. Let $f_0(1) = e$.

Define, $f : \{0,1\}^* \to \mathbb{N}$ as

Note that f_k is defined for any $k \geq 0, k \in \mathbb{N}$.

$$\begin{cases} f(e) = f_0^{-1}(e) - 1. \\ f(w) = \sum_{i=0}^{|w|-1} |S_i| + f_{|w|}^{-1}(w) - 1, \quad w \neq e. \end{cases}$$

f is a bijection. Thus $\{0,1\}^*$ is countably infinite.

(II) The set $C = 2^{\{0,1\}^*}$ is uncountable as the set $2^{\mathbb{N}}$ is uncountable (proof on pg.28 of the book).

$\boxed{a.}$ $X = \{\{x\} : x \in (A_{280} \cup B\} \subseteq \{\{e\}, \{0\}, \{1\}, \{00\}, \{01\}, \{10\}, \{11\}, \ldots\}$

X is countable since, P_1: the set of single elements subsets of $\{0,1\}^*$: this set is countable since there exists a 1-to-1 function $f : \{0,1\}^* \to P_1$ s.t. $f(x) = \{x\}$.

C is uncountable.

Assume that $Y = C \setminus X$ is countable.

Then, $Y \cup X$ is also countable as union of two countable sets are countable.

Note that $C \subseteq Y \cup X$ as $C \subseteq (C \setminus X) \cup C$.

Then, C must be countable. However, C is clearly uncountable, and our assumption that Y is countable is wrong, i.e. Y is uncountable.

$\boxed{b.}$ $A_7 \cap B^* \cap C = \emptyset$ since C is the set of set of strings and A_7, B^* are sets of strings.

The set is finite with cardinality 0.

$\boxed{c.}$ U_C is countably infinite.

$A_2 \times B$ is also countably infinite since both $A_2 \subseteq U_C$ and $B \subseteq U_C$ are countably infinite sets and cartesian product of two countably infinite sets is also countably infinite.

$U_C \setminus A_2 \times B \subseteq U_C$ and thus is countably infinite.

$\boxed{d.}$ $U_C \cup \bigcup_{k=1}^{\infty} A_k = U_C$

$U_C \setminus \{0,1\}^* = \{\}$ and is finite with zero cardinality

Q.2) $\boxed{a.}$ $M = (K, \Sigma, \delta, s, F)$

K: 4, Σ: 2, fixed

$F \rightarrow$ any subset of K : $2^{|K|} = 2^4$

$s \rightarrow$ any $q \in K$ can be designated as s, $|K| = 4$.

$\delta : \underbrace{K \times \Sigma}_{8} \rightarrow \underbrace{K}_{4}$

how many functions? $|K|^{|K \times \Sigma|} = |K|^{|K| \times |\Sigma|} = 4^8$.

The number of selections $= 4^8 \times 4 \times 2^4 = 2^{22}$.

$\boxed{b.}$ $M = (K, \Sigma, \Delta, s, F)$

$F \rightarrow 2^{|K|} = 2^4$

$s \rightarrow |K| = 4$

$\Delta \subseteq K \times (\Sigma \cup \{e\}) \times K$

how many relations?

$2^{|K \times (\Sigma \cup \{e\}) \times K|} = 2^{|K| \times (|\Sigma|+1) \times |K|} = 2^{48}$

The number of NFA is $2^{48} \times 4 \times 2^4 = 2^{54}$.

$\boxed{\text{c.}}$ determinism vs nondeterminism

δ is a function $\qquad$ Δ is a relation

+

e-transitions are allowed.

$\boxed{\text{d.}}$ Regarding (a), some machines are equivalent, i.e. their languages are the same.

(b), some NFA will also be equivalent, each NFA would have eq. DFA having up to $2^{(|K|)}$ states; so these FA potentially recognize more distinct RL's than (a).

Also (a), min-state DFA can be found for each DFA, however some of those would be equivalent, too due to isomorphism.

Q.3)

$\boxed{\text{a.}}$ $\alpha_1 = (00(0(0 \cup 1) \cup 10) \cup 010(0 \cup 1) \cup 10(0(0 \cup 1) \cup 10))^*$

valid strings of all binary strings of length 4 + the empty string.

$\boxed{\text{b.}}$ $\alpha_2 = (0 \cup 1)(0(0 \cup 1))^*$

strings 0 and 1 are in L_2 as they trivially satisfy the constraints.

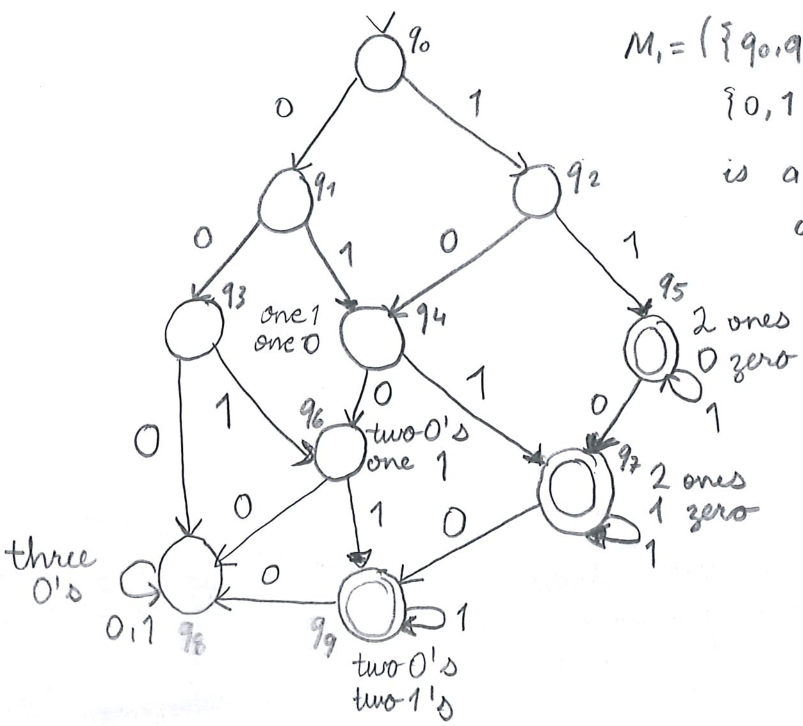
$\boxed{\text{c.}}$ $\alpha_3 = (1 \cup 01 \cup 00(1 \cup 01)^* 00)^*(0 \cup e)$

all strings with no occurrence of 00 : $(1 \cup 01)^*(0 \cup e)$

even non-overlapping occurrences of 00 : $(00(1 \cup 01)^* 00)^*$

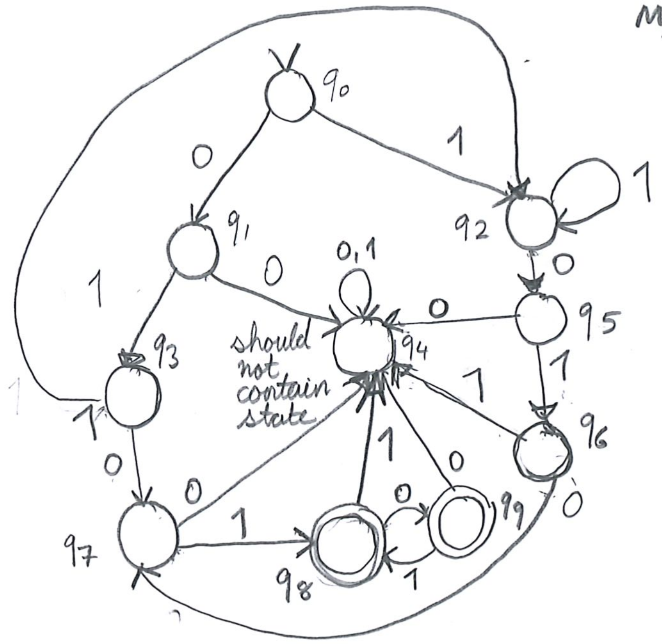
Q.4)

a.



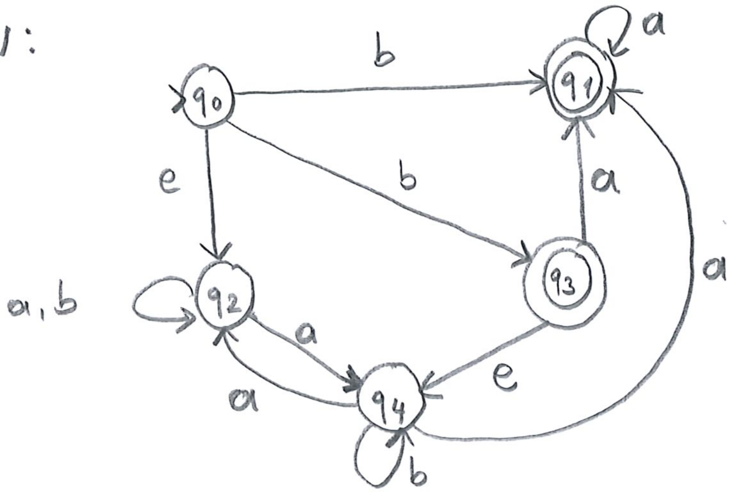
$M_1 = (\{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9\}, \{0,1\}, \delta_1, q_0, \{q_5, q_7, q_9\})$ is a DFA s.t. $L(M_1) = L_1$ and δ_1 is shown graphically on LHS.

b.



$M_2 = (\{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9\}, \{0,1\}, \delta_2, q_0, \{q_8, q_9\})$ is a DFA s.t. $L(M_2) = L_2$ and δ_2 is illustrated on LHS.

Q.5) N:



a. $(q_0, abaa) \vdash_N (q_2, abaa) \vdash_N (q_4, baa) \vdash_N (q_4, aa)$
$\vdash_N (q_1, a)$
$\vdash_N (q_1, e)$.

Since $(q_0, abaa) \vdash_N^* (q_1, e)$
and $q_1 \in F$, $abaa \in L(N)$.

b. Use a tree structure in which there is an edge between a parent and its child iff configuration at parent is related to config. at child via $\vdash_N$ relation, or list every case.

- $(q_0, babb)$
  - (q_1, abb)
    - (q_1, bb)
  - $(q_2, babb)$
    - (q_2, abb)
      - (q_2, bb)
        - (q_2, b)
          - (q_2, e)
      - (q_4, bb)
        - (q_4, b)
          - (q_4, e)
  - (q_3, abb)
    - (q_1, bb)
    - (q_4, abb)
      - (q_1, bb)
      - (q_2, bb)
        - (q_2, b)
          - (q_2, e)

Using reflexive-transitive closure of $\vdash_N$, we see that all possible cases include:

$(q_0, babb) \vdash_N^* (q_1, bb)$.

$(q_0, babb) \vdash_N^* (q_2, e)$.

$(q_0, babb) \vdash_N^* (q_4, e)$.

and $babb \notin L(N)$ since $q_2, q_4 \notin F$ and $bb \neq e$.

Q.6) $E(q_0) = \{q_0, q_2\}$.
$E(q_1) = \{q_1\}$.
$E(q_2) = \{q_2\}$.
$E(q_3) = \{q_3\}$.
$E(q_4) = \{q_3, q_4\}$.

Let $M = (K_M, \{a,b\}, \delta, s_M, F_M)$ be the constructed DFA.

$s_M = E(q_0) = \{q_0, q_2\}$.

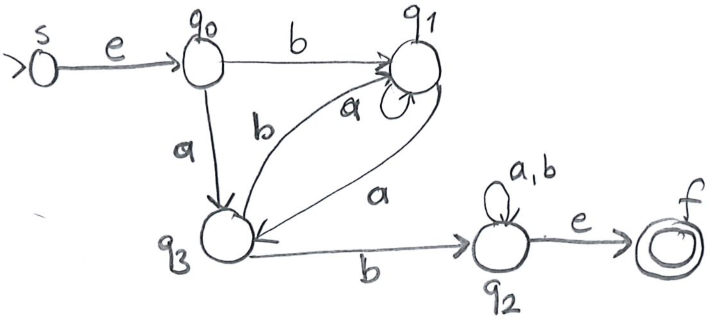
init $\delta(\{q_0,q_2\}, a) = E(q_0) = \{q_0, q_2\}$.
$\delta(\{q_0,q_2\}, b) = E(q_0) \cup E(q_1) \cup E(q_3) = \{q_0,q_1,q_2,q_3\}$. new state! ①
new① $\delta(\{q_0,q_1,q_2,q_3\}, a) = E(q_0) \cup E(q_4) = \{q_0,q_2,q_3,q_4\}$. new state! ②
$\delta(\{q_0,q_1,q_2,q_3\}, b) = E(q_0) \cup E(q_1) \cup E(q_3) = \{q_0,q_1,q_2,q_3\}$.
new② $\delta(\{q_0,q_2,q_3,q_4\}, a) = E(q_0) \cup E(q_4) = \{q_0,q_2,q_3,q_4\}$.
$\delta(\{q_0,q_2,q_3,q_4\}, b) = E(q_0) \cup E(q_1) \cup E(q_3) = \{q_0,q_1,q_2,q_3\}$.
no more new states → end.

Thus $K_M = \{\{q_0,q_2\}, \{q_0,q_1,q_2,q_3\}, \{q_0,q_2,q_3,q_4\}\}$

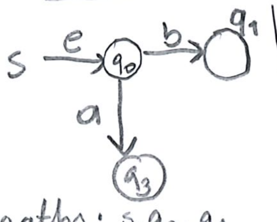
and $F_M = \{\{q_0,q_1,q_2,q_3\}, \{q_0,q_2,q_3,q_4\}\}$.

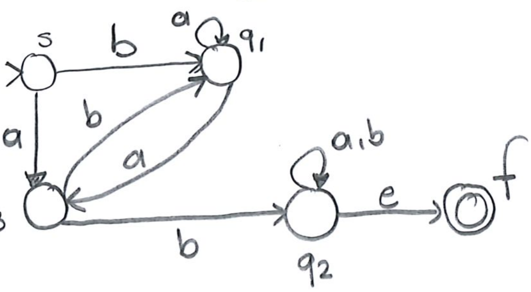
Q.7) GFA for N; $N' = (K \cup \{s,f\}, \{a,b\}, \Delta \cup \{(s,e,q_0), (q_2,e,f)\}, s, \{f\})$.

N':



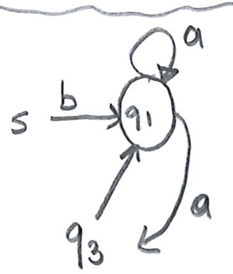
eliminate q_0:



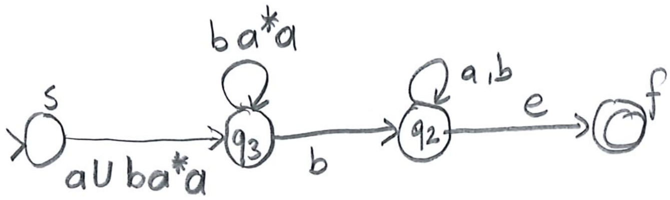


paths: s, q_0, q_1
s, q_0, q_3

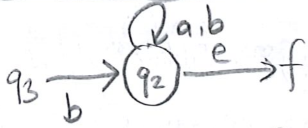
eliminate q_1:



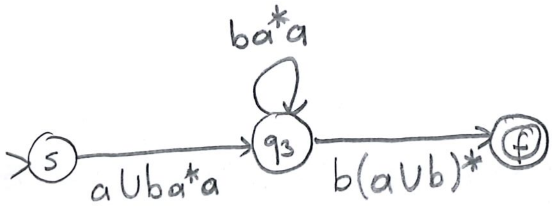
paths: s, q_1, q_3
q_3, q_1, q_3



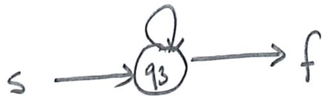
eliminate q_2:



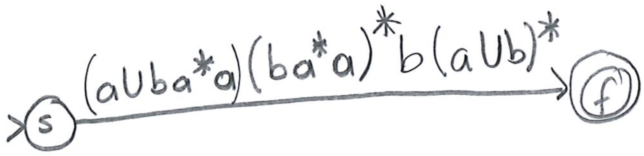
paths: q_3, q_2, f



eliminate q_3:



paths: s, q_3, f



Thus $L(N) = \mathcal{L}\left((a \cup ba^*a)(ba^*a)^* b(a \cup b)^*\right)$.

Q.8) Assume that L is regular.
Then, there is a DFA $M_L = (K_L, \Sigma_L, \delta_L, s_L, F_L)$ with $L(M_L) = L$.
Construct another DFA $M_H = (K_H, \Sigma_H, \delta_H, s_H, F_H)$ s.t.

$K_H = K_L$,
$\Sigma_H = \Sigma_L$,
$\delta_H = \delta_L$,
$s_H = q$ where $q \in K_L$ and $\delta_L(s_L, 0) = q$,
$F_H = \{q \in K_L : (q, 1, f) \in \delta_L$ for any $f \in F_L\}$.

We claim that $L(M_H) = H$. Prove it:

$L(M_H) = H$ iff $L(M_H) \subseteq H$ and $H \subseteq L(M_H)$.

proof by parts

I) $L(M_H) \subseteq H$: Assume that $w \in L(M_H)$.
Then, $(s_H, w) \vdash^*_{M_H} (f_H, e)$ for $f_H \in F_H$.
Since $\delta_H = \delta_L$, we have
$(s_H, w) \vdash^*_{M_L} (f_H, e)$ for $f_H \in F_L$.
We can extend it as:
$(s_L, 0w) \vdash_{M_L} (s_H, w) \vdash^*_{M_L} (f_H, e)$ since $(s_L, 0, s_H) \in \delta_L$.
Then, we have the following case as well,
$(s_L, 0w1) \vdash^*_{M_L} (f_H, 1)$ (appending to the right)
$\vdash_{M_L} (f_L, e)$ since $(f_H, 1, f_L) \in \delta_L$ for all $f_H \in F_H$ and $f_L \in F_L$.

Thus we have
$(s_L, 0w1) \vdash^*_{M_L} (f_L, e)$ s.t. $f_L \in F_L$.
Consequently, $0w1 \in L$ and by definition $w \in H$.

II) $H \subseteq L(M_H)$: Assume that $w \in H$. Then, $0w1 \in L$.
So, $(s_L, 0w1) \vdash^*_{M_L} (f_L, e)$ for $f \in F_L$.
$(s_L, 0w1) \vdash_{M_L} (s_H, w1) \vdash^*_{M_L} (f_L, e)$ since $(s_L, 0, s_H) \in \delta_L$.
Also, $(s_L, 0w1) \vdash_{M_L} (s_H, w1) \vdash^*_{M_L} (q, 1) \vdash_{M_L} (f_L, e)$ for $\delta_L(q, 1) = f_L$ for $f_L \in F_L$, $q \in K_L$.
Since $(s_H, w1) \vdash^*_{M_L} (q, 1)$, we have $(s_H, w1) \vdash^*_{M_H} (q, 1)$,
and hence $(s_H, w) \vdash^*_{M_H} (q, e)$, where $q \in F_H$ is true since $(q, 1, f_L) \in \delta_L$ for $q \in K_L, f_L \in F_L$.

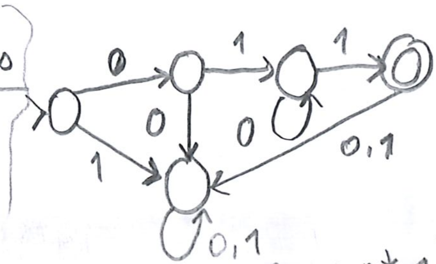
Therefore, $w \in L(M_H)$.

I) and II) proved $\Rightarrow L(M_H) = H$.

(Note that more through proof would be via mathematical induction on the length of w for all $w \in H$; but is not necessary in this case.)

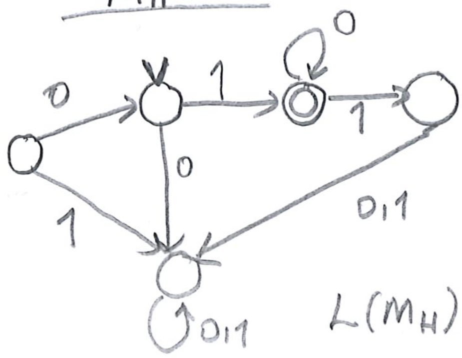
e.g. example constructions

M_L :

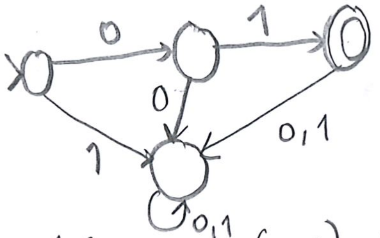


$L(M_L) = \mathcal{L}(010^*1)$.

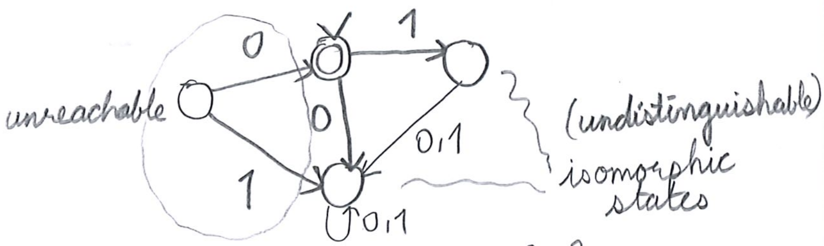
M_H :



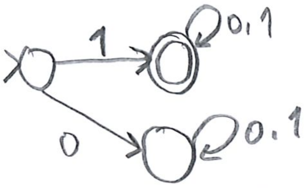
$L(M_H) = \mathcal{L}(10^*)$.



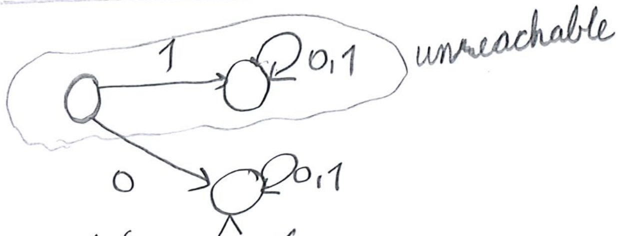
$L(M_L) = \mathcal{L}(01) = \{01\}$



$\mathcal{L}(M_H) = \mathcal{L}(e) = \{e\}$.



$L(M_L) = \mathcal{L}(1(0 \cup 1)^*)$



$L(M_H) = \emptyset$.

We must be able to construct a DFA M_H with $L(M_H) = H$ for any DFA M_L with $L(M_L) = L$.

Q. Why use DFA but not NFA in the proof of this question?

Q.9)

a.

sol^n (1): Assume that L is regular.

Then, pumping lemma for regular languages should apply:

Given pumping length $p \in \mathbb{N}^+$, {this is arbitrary, e.g. you cannot say $p=7$, etc}

$w = 0^p 1^{2^{(p+p!)}} \in L$ and $|w| = p + 2^{(p+p!)} \geq p$ for all p;

{select a string in L with length $\geq p$} and

for every decomposition of $w = xyz$ s.t. $|xy| \leq p$ and $y \neq e$,

i.e. $\begin{cases} x = 0^{p-q-r} \\ y = 0^q \\ z = 0^r 1^{2^{(p+p!)}} \end{cases}$ with $1 \leq q \leq p$ and $0 \leq r \leq p-q$

$xy^iz = 0^{p-q-r} 0^{q \cdot i} 0^r 1^{2^{(p+p!)}}$

$= 0^{p+(i-1)q} 1^{2^{(p+p!)}} \in L$ must be true for $i = 0, 1, 2, \cdots$

However, for every value of $q \in \{1, 2, \cdots, p\}$ we can find integer i that makes m and n equal:

$$\begin{cases} q = 1 \Rightarrow i = p! + 1. \\ q = k,\ k \in \{2, 3, \cdots, p-1\} \Rightarrow i = \dfrac{p!}{k} + 1 & \text{is an integer since } p \geq k \text{ and thus } k \mid p!. \\ q = p \Rightarrow i = (p-1)! + 1. \end{cases}$$

and in all cases $xy^iz = 0^{p+p!} 1^{2^{(p+p!)}} \notin L$.

Consequently, our initial assumption that L is regular is incorrect, i.e. L is not regular.

$\underline{sol^{\underline{n}}}$ ② Assume that L is regular.

Define $L' = \mathcal{L}\left((e \cup 1 \cup 11 \cup 111 \cup 1111)\, 0^* 1^*\right) - L$
$= \{1^t 0^n 1^{2^n} : t < 5,\ t, n \in \mathbb{N}\}$.

<u>L' is also regular</u> because <u>regular languages are closed under complementation</u>.

Then, P/L for regular languages should apply to L'.
Given pumping length $n \in \mathbb{N}^+$,
Select $w = 0^n 1^{(2^n)} \in L'$ s.t. $|w| = n + 2^n \geq n$.
Decompose $w = xyz$ s.t. $|xy| \leq n$ and $y \neq e$, i.e.

$$\begin{cases} x = 0^{n-q-r} \\ y = 0^q \\ z = 0^r 1^{2^n} \end{cases}, \quad \begin{matrix} 1 \leq q \leq n \\ 0 \leq r \leq n-q \end{matrix}$$

and $xy^iz \in L'$ must hold for $i = 0, 1, 2, \dots$.

Take $i = 0$, $xy^0z = 0^{n-q-r} 0^r 1^{2^n} = 0^{n-q} 1^{2^n}$

As $1 \leq q \leq n$, $0 \leq n-q \leq n-1 < n$,
consequently $xz \notin L'$.

Thus L' is not regular, neither is L.

$\underline{sol^{\underline{n}}}$ ③ Assume that L is regular. Then P/L for regular languages must apply to L. Given pumping length $n \in \mathbb{N}^+$, choose $w = 1^{2^n} \in L$ s.t. $|w| = 2^n \geq n$. Decompose $w = xyz$ with $|xy| \leq n$ and $y \neq e$, that is $x = 1^{n-q-r}$, $y = 1^q$, $z = 1^r 1^{2^n - n}$ under constraints $1 \leq q \leq n$ and $0 \leq r \leq n-q$. For all $i \in \mathbb{N}$, $xy^iz \in L$ must hold. Take $i = 2$, $xy^2z = 1^{q+2^n}$, because as $1 \leq q \leq n$, $2^n < 2^n + 1 \leq 2^n + q \leq 2^n + n < 2^{n+1}$, $n < 2^n$ for $n = 1, 2, 3, \dots$.

NOT-GRADED

b. Assume that L is regular. Then, according to the MyHill-Nerode theorem, L must be the union of some of the equivalence classes of a <u>right-invariant equivalence relation of finite index</u> (because a DFA with minimum number of states to recognize L must exist).

<u>Finiteness</u> of eq. rel$^{\underline{n}}$ suggests that

$$1^3 0^k \approx_L 1^3 0^p \quad s.t. \ k, p \in \mathbb{N} \text{ and } p > k.$$

Then, there exists $t \in \mathbb{N}^+$, $t = p - k$.

Via <u>right-invariance</u>,

$$1^3 0^k 1^{2^p} \approx_L 1^3 0^p 1^{2^p} \quad \text{must hold,}$$

but

$$\left.\begin{array}{l} 1^3 0^k 1^{2^p} \in L \text{ as } k \neq p \\ 1^3 0^p 1^{2^p} \notin L \end{array}\right\} \text{ and there are infinitely many } (k,p) \text{ pairs,}$$

and therefore $\approx_L$ has infinitely many equivalence classes, implying that L is not regular.

Q.10)

a. $L_1 = \{ w \in \{a,b\}^* : w = ttaat^{2k}t^{k+2}, t \in \{a,b\}, k \in \mathbb{N} \}$ is regular since $L_1 = \mathcal{L}((a\cup b)(a \cup b)aa((a\cup b)(a\cup b)(a\cup b))^*(a\cup b)(a\cup b))$.

b. $L_2 = \{ w \in \{a,b\}^* : w = t^{2k+1}aat^k, t \in \{a,b\}, k \in \mathbb{N} \}$ is not regular.

Assume that L_2 is regular. Then, $\approx_{L_2}$ has finitely many equivalence classes, meaning at least two distinct strings in Σ^* fall into the same equivalence class, e.g.

$$b^{2k+1} \approx_{L_2} b^{2p+1} \quad \text{for } p > k,\ p, k \in \mathbb{N}, \text{ i.e. } t = p - k \text{ and } t \in \mathbb{N}^+.$$

Via right-invariance of $\approx_{L_2}$, we get

$$b^{2k+1} b^{2t} aab^p \approx_{L_2} b^{2p+1} b^{2t} aab^p.$$

+1

NOT-GRADED

Then, $b^{2k+1} b^{2p-2k} aab^p \approx_{L_2} b^{2p+1} b^{2p-2k} aab^p$.

$$\underbrace{b^{2p+1}aab^p}_{\in L} \approx_{L_2} \underbrace{b^{4p-2k+1}aab^p}_{\notin L}$$

Yet, $\in L$, $\notin L$ since $4p-2k+1 > 2k+1$ as $4p > 4k$ and $p > k$.

There are infinitely-many (p, k) pairs, so $\approx_{L_2}$ has infinitely-many equivalence classes, and hence L_2 is not regular.

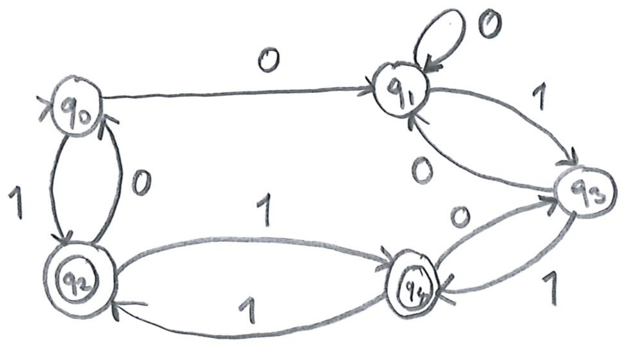
<u>exercise</u>: Use P/L for RL's to prove that L_2 is not regular.

I) Select $w = a^{2n+1}aaa^n$ for pumping length n, can you prove this way L_2 is not regular?

II) Select $w = a^{2n+1}aab^n$ for pumping length n, can you prove that L_2 is not regular?

Q.11)

M:



a. $\equiv_0 : \{q_0, q_1, q_3\}, \{q_2, q_4\}$ as $q_0, q_1, q_3 \in K-F$; $q_2, q_4 \in F$.

$\equiv_1 : \{q_0, q_3\}, \{q_1\}, \{q_2, q_4\}$ as
$\delta(q_0, 0) \in \{q_0, q_1, q_3\}$
$\delta(q_1, 0) \in \{q_0, q_1, q_3\}$
$\delta(q_3, 0) \in \{q_0, q_1, q_3\}$
but
$\delta(q_0, 1) \in \{q_2, q_4\}$
$\delta(q_1, 1) \in \{q_0, q_1, q_3\}$
$\delta(q_3, 1) \in \{q_2, q_4\}$

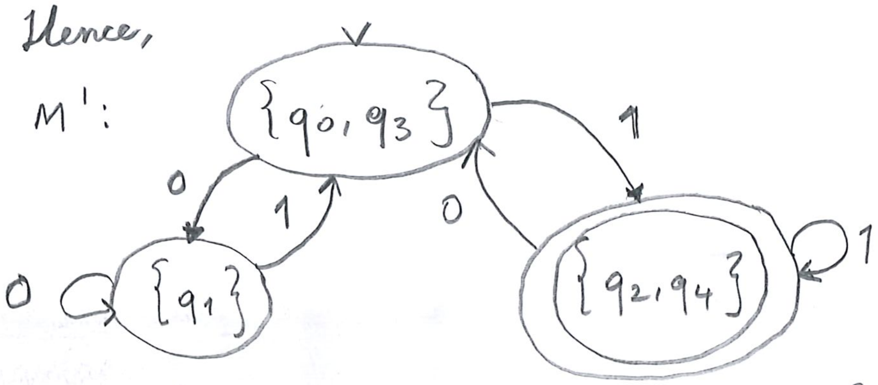
NOT-GRADED

$\equiv_2$: $\{q_0, q_3\}$, $\{q_1\}$, $\{q_2, q_4\}$

no more refinements are possible since $\equiv_1$ and $\equiv_2$ are equivalent.

Hence,

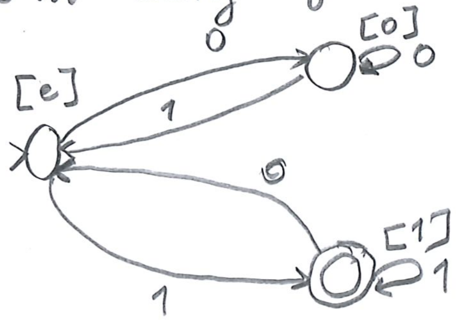
M':



;

$M' = (\{\{q_0, q_3\}, \{q_1\}, \{q_2, q_4\}\}, \{a, b\}, \delta',$
$\{q_0, q_3\}, \{\{q_2, q_4\}\})$ is a DFA with min number of states s.t. $L(M') = L(M)$.

Rewrite M' using eq. class not$^{\underline{n}}$:



b. $[e], [0], [1]$ partition Σ^* as

$$\Sigma^* = [e] \cup [0] \cup [1].$$

To write $[e], [0], [1]$ as $L(\alpha)$ s.t. α is a regular expression, you may use the following algorithmic procedure in case it is not straightforward to see what they are:

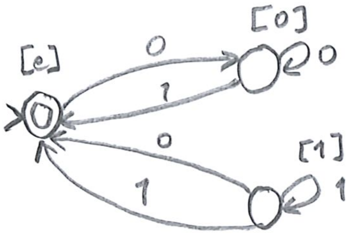
→ For each state q, create a GFA out of a DFA eq. to the original DFA except for q is made the only accepting state

→ Convert each GFA to RE's.

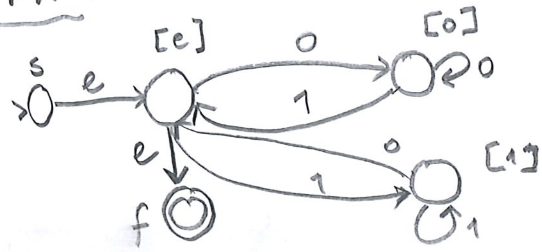
NOT-GRADED

(I) To compute [e]:

DFA:



GFA:

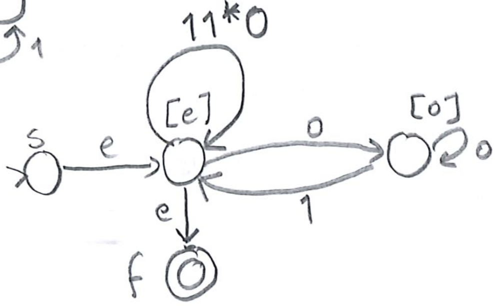


i. eliminate [1]

incoming: [e], [1]

outgoing: [e], [1]

path: [e], [1], [e]

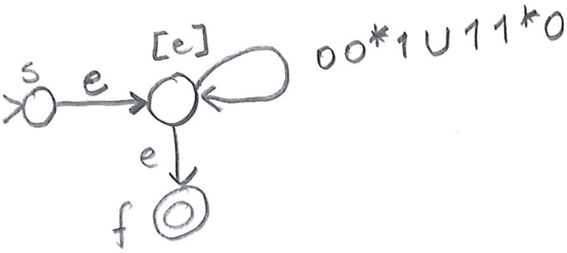


ii. eliminate [0]

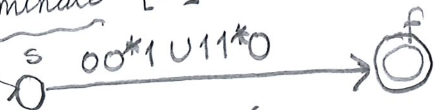
incoming: [e], [0]

outgoing: [e], [0]

path: [e], [0], [e]



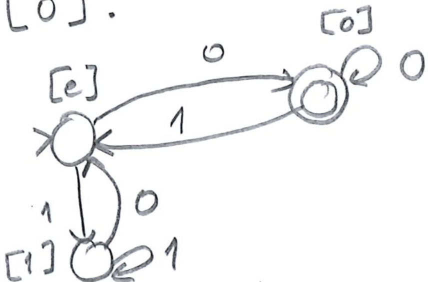
iii. eliminate [e]



Thus $[e] = \mathcal{L}(11^*0 \cup 00^*1)$.

(II) To compute [0]:

DFA:



GFA: write & compute

RE: $(11^*0)^*0(0 \cup (1(11^*0)^*0))^*$

$[0] = \mathcal{L}((11^*0)^*0(0 \cup (1(11^*0)^*0))^*)$.

(iii) $[1] = \mathcal{L}((00^*1)^*1(0(00^*1)^*1 \cup 1)^*)$.

Conclusion:

$$\begin{cases} L = [1] \\ \overline{L} = [e] \cup [0] \\ \Sigma^* = L \cup \overline{L} \end{cases}$$

NOT-GRADED