Exercise 1.

(a). We first prove some lemmas about the rewinding states q_1, q_2 and q_3.

L1. For $\forall \alpha, \beta \in \Sigma^*, \forall n \in \mathbb{N}$, and $x \in \{a, Y\}$, $\alpha q_1 x^n \beta \vdash^*_{\mathcal{M}} \alpha x^n q_1 \beta$.

Proof. Let $\alpha, \beta \in \Sigma^*$ be arbitrary. We prove by induction on n.

Base case. $n = 0$, $x^n = \epsilon$. $\alpha q_1 \beta \vdash^*_{\mathcal{M}} \alpha q_1 \beta$ is trivially true.

Step case. Assume true for some $n > 0$, we prove for the case of $n + 1$.

$$\alpha q_1 x^{n+1} \beta \vdash_{\mathcal{M}} \alpha x q_1 x^n \beta \vdash^*_{\mathcal{M}} \alpha x x^n q_1 \beta$$

where the first step is by the transition function of TM $\mathcal{M}$ on $x \in \{a, Y\}$ and state q_1, and the second step applies IH by treating αx as the new α.

L2. For $\forall \alpha, \beta \in \Sigma^*, \forall n \in \mathbb{N}$, and $x \in \{b, Z\}$, $\alpha q_2 x^n \beta \vdash^*_{\mathcal{M}} \alpha x^n q_2 \beta$.

Proof. Similar to L1.

L3. For $\forall \alpha = \gamma a$ where $a \in \Sigma$ or $a = \epsilon$, $\gamma \in \Sigma^*$ and for $\forall \beta \in \Sigma^*$ and $\forall n \in \mathbb{N}$, and $x \in \{a, Y, b, Z\}$, $\alpha x^n q_3 x \beta \vdash^*_{\mathcal{M}} \gamma q_3 a x^{n+1} \beta$. If $\alpha = \epsilon$, then $\alpha x^n q_3 x \beta \vdash^*_{\mathcal{M}} q_3 B x^{n+1} \beta$.

Proof. Let $\alpha, \beta \in \Sigma^*$ be arbitrary. Induct on n.

Base case. $n = 0$. $\alpha x^n q_3 x \beta = \alpha q_3 x \beta \vdash_{\mathcal{M}} \gamma q_3 a x \beta = \gamma q_3 a x^{n+1} \beta$ by one step transition.

Step case. Assume true for some $n > 0$, we prove for the case of $n + 1$.

$$\alpha x^{n+1} q_3 x \beta \vdash_{\mathcal{M}} \alpha x^n q_3 x x \beta \vdash^*_{\mathcal{M}} \gamma q_3 a x^{n+1} x \beta$$

where the first step is by one step transition in q_3 and the second step applies IH by treating $x\beta$ as the new β.

Proof for (a) Let $i, j \in \mathbb{N}, j \geq 1$ be arbitrary.

$$\begin{aligned}
X^i q_0 a^j Y^i b^j Z^i c^j &\vdash_{\mathcal{M}} X^i X q_1 a^{j-1} Y^i b^j Z^i c^j && \text{(transition from } q_0 \text{ to } q_1) \\
&\vdash^*_{\mathcal{M}} X^{i+1} a^{j-1} q_1 Y^i b^j Z^i c^j && \text{(since } j-1 \in \mathbb{N}\text{, apply L1 by taking } x = a) \\
&\vdash^*_{\mathcal{M}} X^{i+1} a^{j-1} Y^i q_1 b^j Z^i c^j && \text{(since } i \in \mathbb{N}\text{, apply L1 by taking } x = Y) \\
&\vdash_{\mathcal{M}} X^{i+1} a^{j-1} Y^i Y q_2 b^{j-1} Z^i c^j && \text{(transition from } q_1 \text{ to } q_2) \\
&\vdash^*_{\mathcal{M}} X^{i+1} a^{j-1} Y^{i+1} b^{j-1} q_2 Z^i c^j && \text{(L2 by taking } x = b) \\
&\vdash^*_{\mathcal{M}} X^{i+1} a^{j-1} Y^{i+1} b^{j-1} Z^i q_2 c^j && \text{(L2 by taking } x = Z)
\end{aligned}$$

Here we consider four cases since the representation of IDs after the transition from q_2 to q_3 is different.

- if $i = 0$ and $j = 1$.

$$\begin{aligned}
X^{i+1} a^{j-1} Y^{i+1} b^{j-1} Z^i q_2 c^j &= X Y q_2 c \\
&\vdash_{\mathcal{M}} X q_3 Y Z && \text{(transition from } q_2 \text{ to } q_3) \\
&\vdash^*_{\mathcal{M}} q_3 X Y Z && \text{(L3 by taking } x = Y) \\
&\vdash_{\mathcal{M}} X q_0 Y Z && \text{(transition from } q_3 \text{ to } q_0) \\
&= X^{i+1} q_0 a^{j-1} Y^{i+1} b^{j-1} Z^{i+1} c^{j-1}
\end{aligned}$$

- if $i = 0$ and $j > 1$.

$$\begin{aligned}
X^{i+1}a^{j-1}Y^{i+1}b^{j-1}Z^{i}q_2c^{j} &= Xa^{j-1}Yb^{j-1}q_2c^{j} \\
&\vdash_{\mathcal{M}} Xa^{j-1}Yb^{j-2}q_3bZc^{j-1} && \text{(transition from } q_2 \text{ to } q_3\text{)} \\
&\vdash^{*}_{\mathcal{M}} Xa^{j-1}q_3Yb^{j-1}Zc^{j-1} && \text{(L3 by taking x = b)} \\
&\vdash^{*}_{\mathcal{M}} Xa^{j-2}q_3aYb^{j-1}Zc^{j-1} && \text{(L3 by taking x = Y)} \\
&\vdash^{*}_{\mathcal{M}} q_3Xa^{j-1}Yb^{j-1}Zc^{j-1} && \text{(L3 by taking x = a)} \\
&\vdash_{\mathcal{M}} Xq_0a^{j-1}Yb^{j-1}Zc^{j-1} && \text{(transition from } q_3 \text{ to } q_0\text{)} \\
&= X^{i+1}q_0a^{j-1}Y^{i+1}b^{j-1}Z^{i+1}c^{j-1}
\end{aligned}$$

- if $i > 0$ and $j = 1$.

$$\begin{aligned}
X^{i+1}a^{j-1}Y^{i+1}b^{j-1}Z^{i}q_2c^{j} &= X^{i+1}Y^{i+1}Z^{i}q_2c \\
&\vdash_{\mathcal{M}} X^{i+1}Y^{i+1}Z^{i-1}q_3ZZ && \text{(transition from } q_2 \text{ to } q_3\text{)} \\
&\vdash^{*}_{\mathcal{M}} X^{i+1}Y^{i}q_3YZ^{i+1} && \text{(L3 by taking x = Z)} \\
&\vdash^{*}_{\mathcal{M}} X^{i}q_3XY^{i+1}Z^{i+1} && \text{(L3 by taking x = Y)} \\
&\vdash_{\mathcal{M}} X^{i+1}q_0Y^{i+1}Z^{i+1} && \text{(transition from } q_3 \text{ to } q_0\text{)} \\
&= X^{i+1}q_0a^{j-1}Y^{i+1}b^{j-1}Z^{i+1}c^{j-1}
\end{aligned}$$

- if $i > 0$ and $j > 1$.

$$\begin{aligned}
X^{i+1}a^{j-1}Y^{i+1}b^{j-1}Z^{i}q_2c^{j} &\vdash_{\mathcal{M}} X^{i+1}a^{j-1}Y^{i+1}b^{j-1}Z^{i-1}q_3ZZc^{j-1} && \text{(transition from } q_2 \text{ to } q_3\text{)} \\
&\vdash^{*}_{\mathcal{M}} X^{i+1}a^{j-1}Y^{i+1}b^{j-2}q_3bZ^{i+1}c^{j-1} && \text{(L3 by taking x = Z)} \\
&\vdash^{*}_{\mathcal{M}} X^{i+1}a^{j-1}Y^{i}q_3Yb^{j-1}Z^{i+1}c^{j-1} && \text{(L3 by taking x = b)} \\
&\vdash^{*}_{\mathcal{M}} X^{i+1}a^{j-2}q_3aY^{i+1}b^{j-1}Z^{i+1}c^{j-1} && \text{(L3 by taking x = Y)} \\
&\vdash^{*}_{\mathcal{M}} X^{i}q_3Xa^{j-1}Y^{i+1}b^{j-1}Z^{i+1}c^{j-1} && \text{(L3 by taking x = a)} \\
&\vdash_{\mathcal{M}} X^{i+1}q_0a^{j-1}Y^{i+1}b^{j-1}Z^{i+1}c^{j-1} && \text{(transition from } q_3 \text{ to } q_0\text{)}
\end{aligned}$$

Hence, we have proven that for all $i, j \in \mathbb{N}$ with $j \geq 1$ that $X^iq_0a^jY^ib^jZ^ic^j \vdash^{*}_{\mathcal{M}} X^{i+1}q_0a^{j-1}Y^{i+1}b^{j-1}Z^{i+1}c^{j-1}$

(b). Similarly, we have a simple lemma for the rewinding state q_4.
L4. For $\forall \alpha, \beta \in \Sigma^*, \forall n \in \mathbb{N}$, and $x \in \{Y, Z\}$, $\alpha q_4 x^n \beta \vdash^{*}_{\mathcal{M}} \alpha x^n q_4 \beta$.
Proof. Similar to L1.
L5. For $\forall j \geq 1$, $j \in \mathbb{N}$, for $\forall i \in \mathbb{N}$, $X^iq_0a^jY^ib^jZ^ic^j \vdash^{*}_{\mathcal{M}} X^{i+j}q_0Y^{i+j}Z^{i+j}$
Proof. Let $i \in \mathbb{N}$ be arbitrary. We induct on j.
Base case. $j = 1$. $X^iq_0aY^ibZ^ic \vdash^{*}_{\mathcal{M}} X^{i+1}q_0Y^{i+1}Z^{i+1} = X^{i+j}q_0Y^{i+j}Z^{i+j}$ by applying the result of part (a).
Step case. Assume true for some $j > 1$, we prove for the case of $j + 1$.

$$\begin{aligned}
X^iq_0a^{j+1}Y^ib^{j+1}Z^ic^{j+1} &\vdash^{*}_{\mathcal{M}} X^{i+1}q_0a^{j}Y^{i+1}b^{j}Z^{i+1}c^{j} && \text{(result of part(a) since } i \in \mathbb{N} \text{ and } j+1 \geq 1\text{)} \\
&\vdash^{*}_{\mathcal{M}} X^{i+1+j}q_0Y^{i+1+j}Z^{i+1+j} && \text{(IH since } i \text{ is arbitrary in the IH)} \\
&= X^{i+j+1}q_0Y^{i+j+1}Z^{i+j+1}
\end{aligned}$$

Hence, we have proven L5 by induction.
Now for any $w \in L$, $w = a^k b^k c^k$ for some $k \geq 1$.

$$\begin{aligned}
q_0 a^k b^k c^k &= X^0 q_0 a^k Y^0 b^k Z^0 c^k \\
&\vdash^*_{\mathcal{M}} X^k q_0 Y^k Z^k && \text{(L5 by taking } i = 0,\ j = k) \\
&\vdash_{\mathcal{M}} X^k Y q_4 Y^{k-1} Z^k && \text{(transition from } q_0 \text{ to } q_4) \\
&\vdash^*_{\mathcal{M}} X^k Y^k q_4 Z^k && \text{(L4 by taking } x = Y) \\
&\vdash^*_{\mathcal{M}} X^k Y^k Z^k q_4 && \text{(L4 by taking } x = Z) \\
&\vdash_{\mathcal{M}} X^k Y^k Z^k B q_5 && \text{(transition from } q_4 \text{ to } q_5)
\end{aligned}$$

Since $q_0 a^k b^k c^k \vdash^*_{\mathcal{M}} X^k Y^k Z^k B q_5$ where q_5 is an accepting state, $a^k b^k c^k = w$ is accepted by $\mathcal{M}$. Hence all strings in L are accepted by $\mathcal{M}$.

(c). We prove by contraposition, i.e. for any string that is not in L, is not accepted by $\mathcal{M}$, in notation

$$w \notin L \Rightarrow q_0 w \nvdash^*_{\mathcal{M}} \alpha q_5 \beta$$

Strings that are not in L are of the form:

- The empty string ϵ.
  There is no transition from q_0 with the blank symbol, so $q_0 \epsilon \nvdash^*_{\mathcal{M}} \alpha q_5 \beta$ i.e. ϵ is not accepted by $\mathcal{M}$.

- Any string that starts with b or c. i.e. $w = x\delta$ for $x \in \{b, c\}$, $\forall \delta \in \Sigma^*$.
  $q_0 x \delta \nvdash^*_{\mathcal{M}} \alpha q_5 \beta$ since there is no transition from q_0 to any other states with tape symbol b or c.

- $w = a^k c \delta$ for $\forall k \geq 1$, $\forall \delta \in \Sigma^*$.
  $q_0 a^k c \delta \vdash_{\mathcal{M}} X q_1 a^{k-1} c \delta \vdash^*_{\mathcal{M}} X a^{k-1} q_1 c \delta$ where the first step is the transition from q_0 to q_1 and the second is by **L1**. There is no transition from q_1 on symbol c to any other states, so $q_0 a^k c \delta \nvdash^*_{\mathcal{M}} \alpha q_5 \beta$. strings of the form $a^k c \delta$ are not accepted.

- $w = a^k$ for $\forall k \geq 1$.
  Similar to above, there is no transition from q_1 on the blank symbol to any other states, a^k is not accepted.

- $w = a^k b^j a \delta$ for $\forall k, j \geq 1$, $\forall \delta \in \Sigma^*$.
  $q_0 a^k b^j a \delta \vdash_{\mathcal{M}} X q_1 a^{k-1} b^j a \delta \vdash^*_{\mathcal{M}} X a^{k-1} q_1 b^j a \delta \vdash_{\mathcal{M}} X a^{k-1} Y q_2 b^{j-1} a \delta \vdash^*_{\mathcal{M}} X a^{k-1} Y b^{j-1} q_2 a \delta$ where the second last step is the transition from q_1 to q_2, and the last step is by **L2**. There is no transition from q_2 to other states with the symbol a, so $q_0 a^k b^j a \delta \nvdash^*_{\mathcal{M}} \alpha q_5 \beta$.

- $w = a^k b^j$ for $\forall k, j \geq 1$, $\forall \delta \in \Sigma^*$.
  Similar to above, there is no transition from q_2 on the blank symbol to any other states, so $q_0 a^k b^j \nvdash^*_{\mathcal{M}} \alpha q_5 \beta$.

- For the rest of proof, we need a lemma.
  L6. For $\forall n, i, j, k \in \mathbb{N}$ with $i, j, k \geq 1$, and for $\forall \gamma \in \{\epsilon, a\delta, b\delta\}$ with $\delta \in \Sigma^*$:

$$X^n q_0 a^i Y^n b^j Z^n c^k \gamma \vdash^*_{\mathcal{M}} X^{n+1} q_0 a^{i-1} Y^{n+1} b^{j-1} Z^{n+1} c^{k-1} \gamma$$

The rest of strings not in L are of the form

- $w = a^i b^j c^k \gamma$ for $\forall i, j, k \geq 1$, $i \neq j \vee j \neq k \vee i \neq k$, and $\gamma \in \{\epsilon, a\delta, b\delta\}$, $\delta \in \Sigma^*$
- $w = a^i b^j c^k \gamma$ for $i = j = k$ and $\gamma \in \{a\delta, b\delta\}$, $\delta \in \Sigma^*$

We consider these strings in three broad categories.

- $\min(i, j, k) = i$ i.e. $q_0 a^i b^j c^k \gamma \vdash^*_{\mathcal{M}} X^i q_0 Y^i b^{j-i} Z^i c^{k-i} \gamma$ by repeatedly applying **L6**.
  * if $j > i, k \geq i$ and $\gamma \in \{\epsilon, a\delta, b\delta\}$.
    $X^i q_0 Y^i b^{j-i} Z^i c^{k-i} \gamma \vdash_{\mathcal{M}} X^i Y q_4 Y^{i-1} b^{j-i} Z^i c^{k-i} \gamma \vdash^*_{\mathcal{M}} X^i Y^i q_4 b^{j-i} Z^i c^{k-i} \gamma$ by **L4**. There is no transition out of q_4 on symbol b.
  * if $j = i, k > i$ and $\gamma \in \{\epsilon, a\delta, b\delta\}$.
    $X^i q_0 Y^i Z^i c^{k-i} \gamma \vdash^*_{\mathcal{M}} X^i Y^i Z^i q_4 c^{k-i} \gamma$ by **L4**. Still no transition out of q_4 on symbol c.
  * if $j = i, k = i$ and $\gamma \in \{a\delta, b\delta\}$.
    $X^i q_0 Y^i Z^i \gamma \vdash^*_{\mathcal{M}} X^i Y^i Z^i q_4 \gamma$ by **L4**. No transition out of q_4 on symbol a or b.
- $\min(i, j, k) = j$ i.e. $q_0 a^i b^j c^k \gamma \vdash^*_{\mathcal{M}} X^j q_0 a^{i-j} Y^j Z^j c^{k-j} \gamma$ by repeatedly applying **L6**.
  * We have covered the case when $i = j$, so the case left is $i > j, k \geq j$ and $\gamma \in \{\epsilon, a\delta, b\delta\}$.
    $X^j q_0 a^{i-j} Y^j Z^j c^{k-j} \gamma \vdash_{\mathcal{M}} X^j X q_1 a^{i-j-1} Y^j Z^j c^{k-j} \gamma \vdash^*_{\mathcal{M}} X^{j+1} a^{i-j-1} Y^j q_1 Z^j c^{k-j} \gamma$ by **L1**. There is no transition out of q_1 on symbol Z.
- $\min(i, j, k) = k$ i.e. $q_0 a^i b^j c^k \gamma \vdash^*_{\mathcal{M}} X^k q_0 a^{i-k} Y^k b^{j-k} Z^k \gamma$ by repeatedly applying **L6**.
  * We have covered cases when $i = k$ or $j = k$, so the case left is $i > k, j > k$ and $\gamma \in \{\epsilon, a\delta, b\delta\}$.
    $X^k q_0 a^{i-k} Y^k b^{j-k} Z^k \gamma \vdash_{\mathcal{M}} X^k X q_1 a^{i-k-1} Y^k b^{j-k} Z^k \gamma \vdash^*_{\mathcal{M}} X^{k+1} a^{i-k-1} Y^k q_1 b^{j-k} Z^k \gamma$
    $\vdash_{\mathcal{M}} X^{k+1} a^{i-k-1} Y^k Y q_2 b^{j-k-1} Z^k \gamma \vdash^*_{\mathcal{M}} X^{k+1} a^{i-k-1} Y^{k+1} b^{j-k-1} Z^k q_2 \gamma$. There is no transition out of q_2 on symbol a, b, B corresponding to $\gamma = a\delta, b\delta, \epsilon$.

Since for all cases, there is no transition to q_5, all such strings are not accepted by $\mathcal{M}$.

Hence, we have shown that all strings not in L are not accepted by $\mathcal{M}$. By contraposition, every string accepted by $\mathcal{M}$ is in L.
Proof of L6. Very similar to part (a).
Let $i, j, k \geq 1$, $n \geq 0$ be arbitrary.

$$
\begin{aligned}
X^n q_0 a^i Y^n b^j Z^n c^k \gamma &\vdash_{\mathcal{M}} X_n X q_1 a^{i-1} Y^n b^j Z^n c^k \gamma \\
&\vdash^*_{\mathcal{M}} X^{n+1} a^{i-1} Y^n q_1 b^j Z^n c^k \gamma && \text{(L1 by taking } x = a \text{ and } Y) \\
&\vdash_{\mathcal{M}} X^{n+1} a^{i-1} Y^n Y q_2 b^{j-1} Z^n c^k \gamma \\
&\vdash^*_{\mathcal{M}} X^{n+1} a^{i-1} Y^n Y b^{j-1} Z^n q_2 c^k \gamma && \text{(L2 by taking } x = b \text{ and } Z) \\
&\vdash_{\mathcal{M}} X^{n+1} a^{i-1} Y^{n+1} b^{j-1} Z^{n-1} q_3 Z Z c^{k-1} \gamma && \text{(* we don't look into cases for simplicity)} \\
&\vdash^*_{\mathcal{M}} X^n q_3 X a^{i-1} Y^{n+1} b^{j-1} Z^{n+1} c^{k-1} \gamma && \text{(L3 by taking } x = Z, b, Y, a) \\
&\vdash_{\mathcal{M}} X^{n+1} q_0 a^{i-1} Y^{n+1} b^{j-1} Z^{n+1} c^{k-1} \gamma
\end{aligned}
$$

Exercise 2

(a). Denote $L = \{\langle M\rangle : \exists x \in \Sigma^*$ of length < 10 such that M halts in < 100 steps when run on $x\}$.
Language L is decidable. The idea is to construct a TM T that takes as input $\langle M\rangle$, and runs M on $\forall x \in \Sigma^*$ with $|x| < 10$ for at most 100 steps, and if M halts on any such x in less than 100 steps, T halts and accepts $\langle M\rangle$, otherwise T halts and rejects $\langle M\rangle$.
For details of the algorithm, we assume that the alphabet Σ of M is given or can be found out by T from the encoding $\langle M\rangle$. Then it is possible to enumerate and order all strings $x \in \Sigma^*$ by length, and by lexicographic order if they are of the same length, i.e. we have a mapping $\phi : \Sigma^* \mapsto \mathbb{N}$. Hence, there exists a $n \in \mathbb{N}$ such that for $\forall i \leq n, |\phi^{-1}(n)| < 10$ and $\forall i > n, |\phi^{-1}(n)| \geq 10$. T runs M on $\phi^{-1}(i)$ for $\forall i \leq n$ by the following procedure:

1. T initializes tape 2 with $\phi^{-1}(i)$ in its encoded form.

2. T initializes tape 3 with M's initial state in encoded form.

3. T initializes tape 4 as step count $= 1$.

4. To simulate a move of M on $\phi^{-1}(i)$, T reads tape 2 and tape 3 to identify M's current input symbol and state as 0^i and 0^j, and writes the pair onto tape 5 as a scratch tape. T then scans tape 1 i.e. $\langle M\rangle$ for a corresponding transition. If found, T updates $\phi^{-1}(i)$ on tape 2 and moves the head to the right or left symbol according to the transition function, and updates M's state on tape 3. T increases the count on tape 4 by 1.

5. T repeats step **4** on $\phi^{-1}(i)$ for at most 100 times.

- If M does not halt for a count < 100 i.e. tape 3 does not contain the accepting state or there is still transition found after running 100 steps, T restarts the procedure (from **1.**) for the next string $\phi^{-1}(i+1)$.
- If M halts on $\phi^{-1}(i)$ when count < 100, T halts and accepts $\langle M\rangle$.

6. If M does not halt on $\phi^{-1}(i)$ for $\forall i \leq n$, then T halts and rejects $\langle M\rangle$.

Since T halts on all its inputs and accepts precisely those $\langle M\rangle$ where there exists input of length < 10 on which M halts in < 100 steps, L is decided by T.

(b). Denote $L = \{\langle M\rangle : \exists x \in \Sigma^*$ of length ≥ 10 such that M halts in < 100 steps when run on $x\}$.
L is decidable. Since the number of steps that any M can run is bounded < 100, M can only inspect at most the first 99 symbols of all its inputs. Hence, we only need to consider a finite input space for each M, i.e. $\forall x \in \Sigma^*$ with $10 \leq |x| < 100$. The reason is that if M halts on any input of length ≥ 100, it would have halted for some prefix of length $10 \leq |x| < 100$, and that if M does not halt on any input x with $10 \leq |x| < 100$, it would also not halt for any input of length ≥ 100 since the prefixes are the same.
Similar to (a), we construct a TM T that takes as input $\langle M\rangle$, and runs M on $\forall x \in \Sigma^*$ with $10 \leq |x| < 100$ for at most 100 steps, and if M halts on any such x in less than 100 steps, T halts and accepts $\langle M\rangle$, otherwise T halts and rejects $\langle M\rangle$. We enumerate the input strings of M by the natural ordering ϕ as in part (a), and identify $n, m \in \mathbb{N}$ where for $\forall n \leq i \leq m$, $10 \leq |x_i| < 100$ and for $\forall i < n$, $|x_i| < 10$ and for $\forall i > m$, $|x_i| \geq 100$. We ask T to run M on x_i for $i = n..m$. The algorithm is the same as part (a).

(c). Denote $L = \{\langle M \rangle : \exists x \in \Sigma^*$ of length < 10 such that M halts in ≥ 100 steps when run on $x\}$.
L is undecidable. We reduce the halting problem to problem L. The idea is that for every pair of TM M and string w, we construct a TM M' that runs as follows:

1. ignores its own input / erases x on the tape
2. write w onto tape
3. runs M on w
   - if M accepts w, M' runs 100 steps to the right of its input tape and halts
   - if M halts on w in a non final state, then M' runs to the right of its input tape forever.
   - if M does not halt on w, M' because of simulateing M, also does not halt.

By construction, M accepts $w \Leftrightarrow \langle M' \rangle \in L$.

- $\Rightarrow$. M accepts $w \Rightarrow M'$ accepts and halts on all inputs in ≥ 100 steps $\Rightarrow \exists x$ with $|x| < 10$ such that M' accepts and halts in ≥ 100 steps $\Rightarrow \langle M' \rangle \in L$.
- $\Leftarrow$. Show contraposition. M does not accept w because M halts in a non final state or because M does not halt on $w \Rightarrow M'$ runs forever on all its inputs and never halts $\Rightarrow$ there is no input of length < 10 such that M' halts on it in ≥ 100 steps $\Rightarrow \langle M' \rangle \notin L$

Now note that we can construct a TM M_1 that takes $\langle M, w \rangle$ as input and outputs corresponding $\langle M' \rangle$ as we just concatenate the transition functions of several TMs that does the step 1,2,3. If L is decidable, then there exists a TM M_2 that always halts and that accepts $\langle M' \rangle$ iff $\langle M' \rangle \in L$. We can construct a TM M_3 that first runs M_1 on $\langle M, w \rangle$, and when M_1 halts with $\langle M' \rangle$ written on the tape, runs M_2 on $\langle M' \rangle$. Then M_3 accepts/rejects $\langle M, w \rangle$ iff $\langle M' \rangle \in / \notin L$ iff M accepts/rejects w. L_u is recursive, a contradiction. Hence L is undecidable.

(d). Denote $L = \{\langle M \rangle : \exists x \in \Sigma^*$ of length ≥ 10 such that M halts in ≥ 100 steps when run on $x\}$.
L is undecidable, and the reduction algorithm is essentially the same as part (c). We map each instance of the halting problem $\langle M, w \rangle$ to an instance of problem L $\langle M' \rangle$ where M' ignores its own input, runs M on w, and if M accepts w, M' runs 100 steps to the right of its input tape and halts; and if M halts on w in a non final state, M' runs to the right of its tape forever.
M accepts $w \Leftrightarrow \langle M' \rangle \in L$.

- $\Rightarrow$. M accepts $w \Rightarrow M'$ accepts and halts on all inputs in ≥ 100 steps $\Rightarrow \exists x$ with $|x| \geq 10$ such that M' accepts and halts in ≥ 100 steps $\Rightarrow \langle M' \rangle \in L$.
- $\Leftarrow$. Show contraposition. M does not accept w because M halts in a non final state or because M does not halt on $w \Rightarrow M'$ runs forever on all its inputs and never halts $\Rightarrow$ there is no input of length ≥ 10 such that M' halts on it in ≥ 100 steps $\Rightarrow \langle M' \rangle \notin L$

There exists a TM M_1 that takes $\langle M, w \rangle$ as input and outputs corresponding $\langle M' \rangle$. If L is decidable, then there exists a TM M_2 that always halts and that accepts $\langle M' \rangle$ iff $\langle M' \rangle \in L$. Then we can construct a TM M_3 that first runs M_1 on $\langle M, w \rangle$, and when M_1 halts with $\langle M' \rangle$ written on the tape, runs M_2 on $\langle M' \rangle$. Then M_3 accepts/rejects $\langle M, w \rangle$ iff $\langle M' \rangle \in / \notin L$ iff M accepts/rejects w. L_u is recursive, a contradiction. Hence L is undecidable.

Exercise 3.

(a). Denote $L = \{\langle M \rangle : \exists x \in \Sigma^* \text{ of length} < 10 \text{ such that } M \text{ halts in} \geq 100 \text{ steps when run on } x\}$.
We construct a TM T such that $L(T) = L$. Given $\langle M \rangle$ as the input of T, T follows the steps:

1. T initialises the step count $= 1$ on tape 2.

2. T lists initial IDs of all strings x of length < 10 on tape 3. The listing follows the order of increasing length, and follows lexicographic order if strings are of the same length. Separation of IDs can be indicated by a special tape symbol (#). Listing takes finitely many steps since the input space of interest for any given M is finite.

3. T rewinds to the leftmost ID. For each ID, T uses tape 4 as a scratch tape to search for transitions based on the coding $\langle M \rangle$ on tape 1. If there is a possible transition, T updates the current ID on tape 3, and continues to the next ID on the right. If there is no transition found or the ID contains an accepting state (i.e.M halts on x) and if the current step count on tape 2 is < 100, T changes the left separator # to † as an indication that M has halted on this ID to avoid checking in the next cycle. T then continues running M on the next ID. After running one move of M on all IDs, T increments step count by 1, and rewinds to the leftmost ID and repeats step **3**.

4. If for any ID, T cannot find any transition on a non-final state or the ID contains an accepting state, and the current step count is ≥ 100, T halts and accepts $\langle M \rangle$.

cycle k	tape 2	tape 3
1	1	$\#ID_{0,1}\#ID_{1,1}\#ID_{2,1}..\#ID_{n,1}$
2	10	$\#ID_{0,2}\#ID_{1,2}\#ID_{2,2}..\#ID_{n,2}$
3	11	$\#ID_{0,3}\dagger ID_{1,3}\#ID_{2,3}..\#ID_{n,3}$

where $ID_{i,j}$ corresponds to the ID of $\phi^{-1}(i)$ after running M on it for $j = k$ steps. In the table, M halts on $\phi^{-1}(1)$ after 3 steps as indicated by the †.
By construction, T iterates running M on all strings of length < 10, and would accept only if M halts on any such string in ≥ 100 steps, so $L(T) = L$. L is recursively enumerable.

(b). Denote $L = \{\langle M \rangle : \exists x \in \Sigma^* \text{ of length} \geq 10 \text{ such that } M \text{ halts in} \geq 100 \text{ steps when run on } x\}$.
We construct a TM T such that $L(T) = L$. T still processes inputs of M following the natural numbering by ϕ, and we identify an $n \in \mathbb{N}$ such that $\forall i \geq n$, $|\phi^{-1}(i)| \geq 10$ and $\forall i < n, |\phi^{-1}(i)| < 10$. Given $\langle M \rangle$ as the input of T, T would conduct a breadth first search on the input space starting from $\phi^{-1}(n)$ by the following steps:

- T initializes cycle count $k = 1$ on tape 2. k is used to remember the number of strings T has processed so as to append the correct string onto tape 3. It is also used to compute the step count for each halted ID.

- T would use a tape 3 to record current IDs of M's inputs, where the inputs are appended following the natural ordering ϕ. In cycle k, T rewinds to the leftmost ID, and runs one move of M on each ID on the tape and then appends the initial ID of $\phi^{-1}(n + k - 1)$ onto tape 3. Here k is read from tape 2, and each ID is separated by a special tape symbol (#). After appending the ID of the new string, T increments the cycle count k by 1.

- To run a move of M on the i^{th} ID on tape 3 (where i can be tracked by counting the number of IDs T has processed duing a cycle), T uses tape 4 as a scratch tape to look for transitions from $\langle M \rangle$ on tape 1. If there is a transition, T updates the current ID on tape 3. If there is no transition on a non final state or if the ID contains a final state, then it means M has halted on the current string, and T checks M's step count on this string by computing $k - i$ on the scratch tape.
  - If the step count is < 100, T changes the left separator (#) of the ID to † as an indication of having halted so that it avoids checking for this ID in the next cycle. T then continues running M on the next ID on the right.
  - If the step count is ≥ 100, T halts and accepts $\langle M \rangle$.

cycle k	tape 2	tape 3
1	1	$\#ID_{1,0}$
2	10	$\#ID_{1,1}\#ID_{2,0}$
3	11	$\#ID_{1,2}\#ID_{2,1}\#ID_{3,0}$

where $ID_{i,j}$ corresponds to the ID of the input string $\phi^{-1}(n + i - 1)$ after running M on it for $j = k - i$ steps.

Since T searches for M's input space of interest in a breadth first manner, it would not miss any x of length ≥ 10 on which M might halt in ≥ 100 steps. And by construction, T accepts all $\langle M \rangle$ for which there exists x with $|x| \geq 10$ on which M halts in ≥ 100. Hence, $L(T) = L$ and L is recursively enumerable.