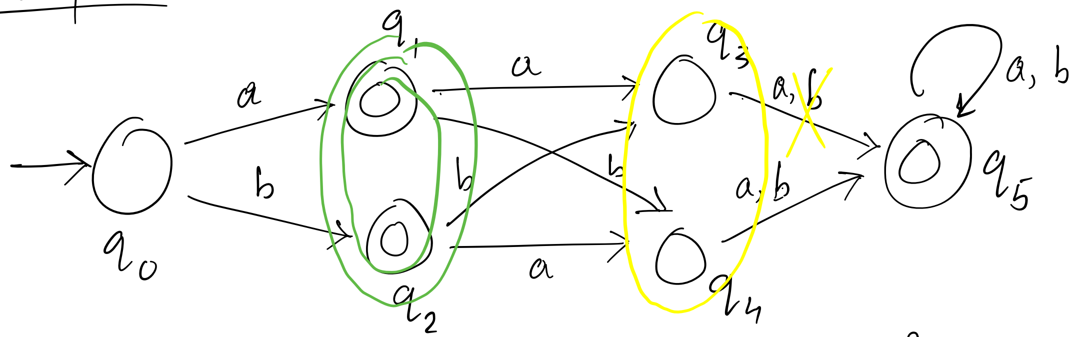
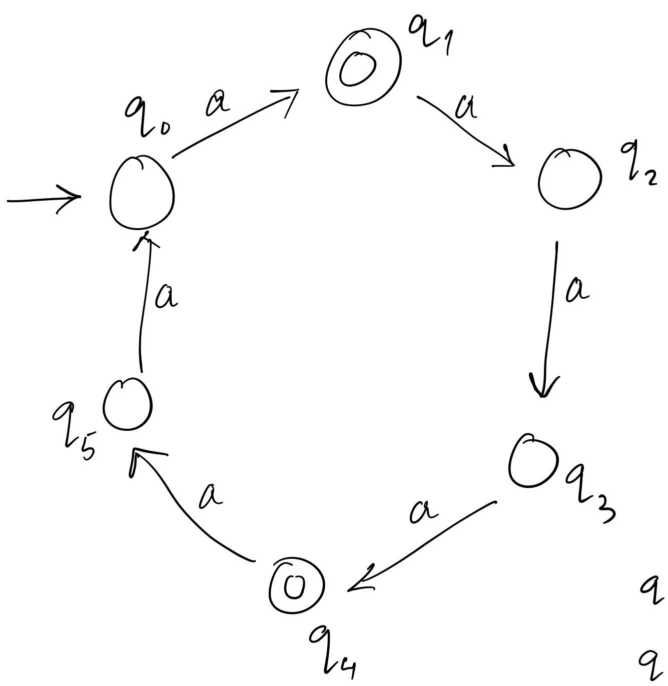
Example 1:



$L = \{ w \in \{a,b\}^* \mid |w| = 1 \text{ or } |w| \geq 3 \}$

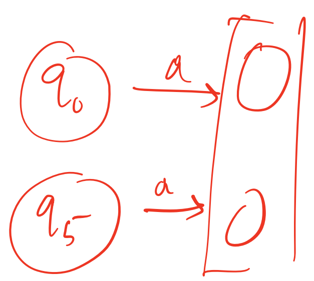
Example 2:

$L = \{ w \in \{a\}^* \mid |w| \equiv 1 \pmod 3 \}$



$q_0 \xrightarrow{a} q_1$

$q_5 \longrightarrow q_0$



	q_5	q_4	q_3	q_2	q_1
q_0	×	×		×	×
q_1	×		×	×	
q_2		×	×		
q_3	×	×			
q_4	×				
q_5					

Lesson learnt:

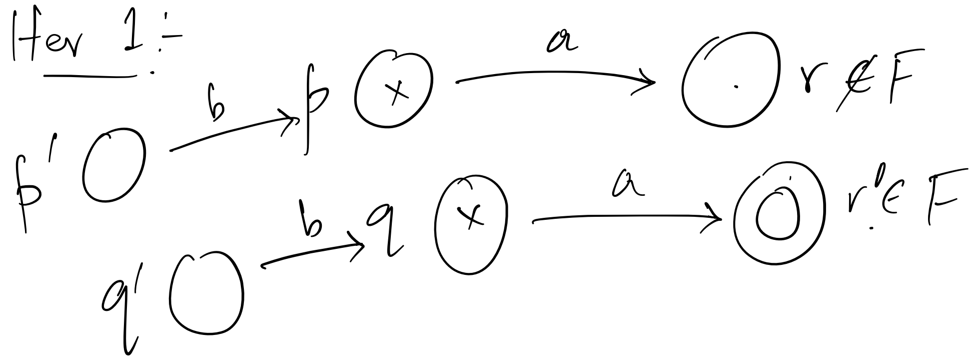
if $\underline{\exists} x \in \Sigma^*$, s.t. $\hat{\delta}(p, x) \in F$, $\hat{\delta}(q, x) \notin F$ (or vice versa)

Then p, q cannot be merged.

Iter 0: Mark all p, q s.t. $p \in F$, $q \notin F$.

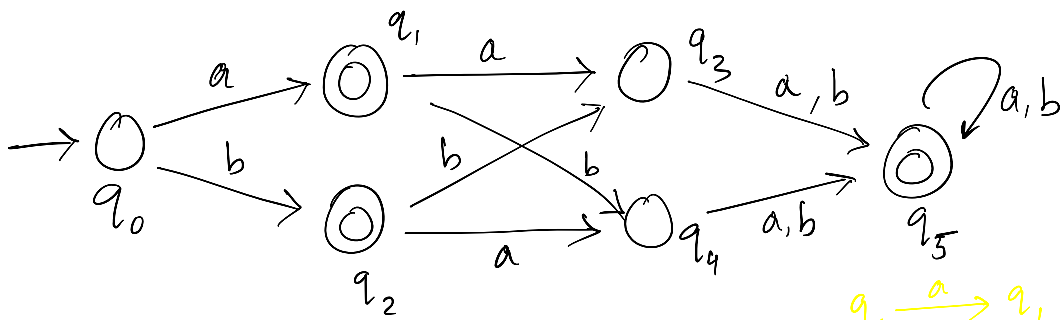
Intuitively, $x = \epsilon$ is the certificate.

Iter 1:-



- if $\exists x \in \Sigma^*$, $\hat{\delta}(p, x) \in F$, $\hat{\delta}(q, x) \notin F$ or vice-versa, then p, q cannot be merged.

- Can we merge the other pairs? YES. (needs a proof).



	q_5	q_4	q_3	q_2	q_1
q_0	×	×	×	×	×
q_1	×	×	×	O	
q_2	×	×	×		
q_3	×	O			
q_4	×				
q_5					

$q_0 \xrightarrow{a} q_1$ | $q_0 \xrightarrow{b} q_2$

$q_4 \xrightarrow{a} q_5$ | $q_4 \xrightarrow{b} q_5$

$q_0 \xrightarrow{a} q_1$

$q_4 \xrightarrow{a} q_5$

$x = aa.$

$\hat{\delta}(q_0, aa) = q_3$

$\hat{\delta}(q_4, aa) = q_5$

Equivalence Classes:

$p \approx q \overset{}{\underset{\text{def.}}{\Longleftrightarrow}} \forall x \in \Sigma^*, \ \hat{\delta}(p, x) \in F$ if and only if $\hat{\delta}(q, x) \in F$.

- Reflexive: $p \approx p$
- Symmetric, $p \approx q \Leftrightarrow q \approx p$
- Transitive: $p \approx q,\ q \approx r \Rightarrow p \approx r$.

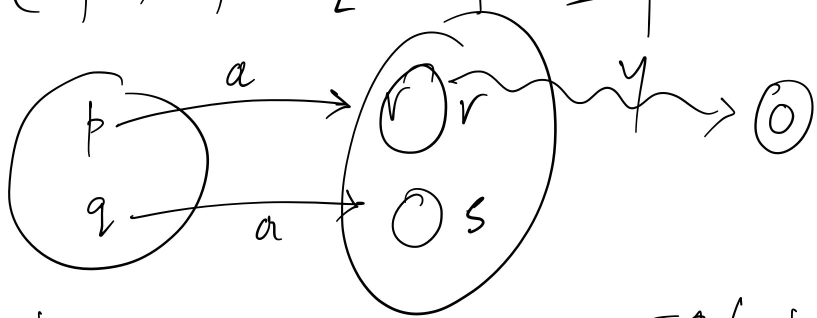
$[p] \stackrel{\text{def}}{=} \{q \mid q \approx p\}$ [Eq. class of p]

Quotient Automata:

$M/\!\approx \; = (Q', \Sigma, \delta', s', F')$

$\rightarrow Q' = \{ [p] \mid p \in Q \}$ | $s' = [s]$

$\rightarrow \delta'([p], a) = [\delta(p,a)]$ | $F' = \{ [q] \mid q \in F \}$

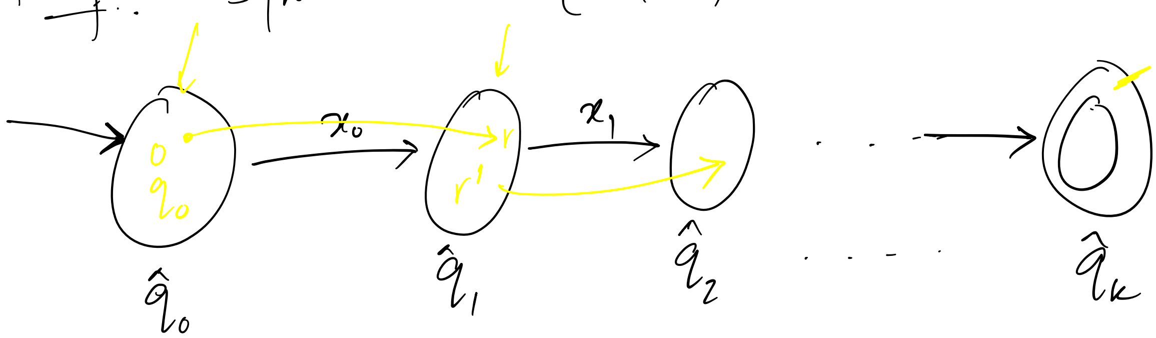


Proof: S'pose $p \approx q$, $a \in \Sigma$, $y \in \Sigma^*$ (arbitrary).

$$\begin{aligned}
\hat{\delta}(r, y) \in F &\iff \hat{\delta}(\delta(p,a), y) \in F \\
&\iff \hat{\delta}(p, ay) \in F \\
&\iff \hat{\delta}(q, ay) \in F \\
&\iff \hat{\delta}(\delta(q,a), y) \in F \\
&\iff \hat{\delta}(s, y) \in F
\end{aligned}$$

Thm: $L(M/\approx) = L(M)$

Proof: S'pose $x \in L(M/\approx)$ $\quad x = x_0 x_1 x_2 \cdots x_k$.



$[\delta(q_0, x_0)] = r.$

Punchline: The yellow transitions never go out of the equivalence classes.

Thm:- ~~L(M)~~ $M/\approx$ remains unaltered after applying merging again.

Thm:- Algorithm correctly computes $M/\approx$.

Proof: Claim:- After any iteration $k \geq 1$,

(p, q) are marked by algorithm

$$\iff \exists x, \text{ s.t. } |x| \leq k-1 \text{ and } \hat{\delta}(p, x) \in F, \ \hat{\delta}(q, x) \notin F$$

Proof by induction on k:

Base case ($k = 1$): True since $p \in F$, $q \notin F$ or vice versa.

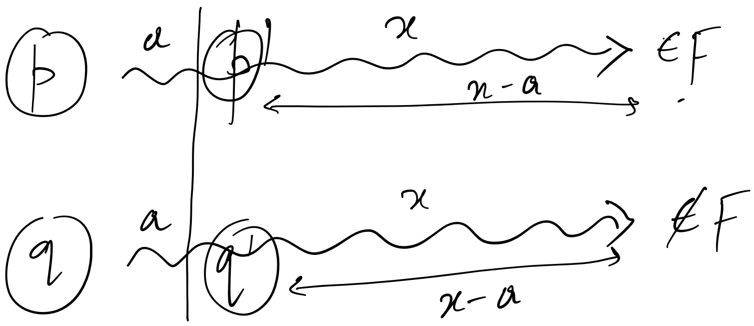
Suppose hypothesis holds for k. Let us look at iter. $k+1$.

$$\Rightarrow \quad p \xrightarrow{a} p' \underbrace{\xrightarrow{x}}_{\leq k-1} \in F$$

$$q \xrightarrow{a} q' \xrightarrow{x} \notin F$$

$\Rightarrow$ p, q are distinguishable by ax, where $|ax| \leq k$.

$\Leftarrow$



$|x| = k.$

$|x - a| = k-1$

Split x into $a \cdot \{x \setminus a\}$. S'pose
$\delta(p,a) = p'$, $\delta(q,a) = q'$.

$\Rightarrow$ p', q' are distinguishable by
$x - \{a\}$ which is of length $= k - 1$.

$\Rightarrow$ (p', q') are marked by induction hypothesis.