Part XI. Properties of Regular Languages

Pumping Lemma for RLs

Gist: Pumping lemma demonstrates an infinite iteration of some substring in RLs.

- Let L be a RL. Then, there is $k \geq 1$ such that **if** $z \in L$ and $|z| \geq k$, **then** there exist u,v,w: $z = uvw$, **1)** $v \neq \varepsilon$ **2)** $|uv| \leq k$ **3)** for each $m \geq 0$, $uv^m w \in L$

Example: for RE $r = \boldsymbol{ab^*c}$, $L(r)$ is ***regular.***
There is $\boldsymbol{k} = 3$ such that **1)**, **2)** and **3)** holds.

Pumping Lemma for RLs

Gist: Pumping lemma demonstrates an infinite iteration of some substring in RLs.

• Let L be a RL. Then, there is $k \geq 1$ such that **if** $z \in L$ and $|z| \geq k$, **then** there exist u,v,w: $z = uvw$, **1)** $v \neq \varepsilon$ **2)** $|uv| \leq k$ **3)** for each $m \geq 0$, $uv^m w \in L$

Example: for RE $r = ab^*c$, $L(r)$ is ***regular.***
There is $k = 3$ such that **1)**, **2)** and **3)** holds.

• for $z = abc$: $z \in L(r)$ & $|z| \geq 3$:

$$\underset{u}{a}\,\underset{v}{b}\,\underset{w}{c}$$

$v \neq \varepsilon$, $|uv| = 2 \leq 3$

$uv^0w = ab^0c = ac \in L(r)$
$uv^1w = ab^1c = abc \in L(r)$
$uv^2w = ab^2c = abbc \in L(r)$
$\vdots$

Pumping Lemma for RLs

Gist: Pumping lemma demonstrates an infinite iteration of some substring in RLs.

• Let L be a RL. Then, there is $k \geq 1$ such that **if** $z \in L$ and $|z| \geq k$, **then** there exist u,v,w: $z = uvw$, **1)** $v \neq \varepsilon$ **2)** $|uv| \leq k$ **3)** for each $m \geq 0$, $uv^m w \in L$

Example: for RE $r = ab^*c$, $L(r)$ is ***regular.***
There is $k = 3$ such that **1)**, **2)** and **3)** holds.

• for $z = abc$: $z \in L(r)$ & $|z| \geq 3$: $uv^0w = ab^0c = ac \in L(r)$
$uv^1w = ab^1c = abc \in L(r)$
$uv^2w = ab^2c = abbc \in L(r)$
⋮

$u = a$, $v = b$, $w = c$

$v \neq \varepsilon$, $|uv| = 2 \leq 3$

• for $z = abbc$: $z \in L(r)$ & $|z| \geq 3$: $uv^0w = ab^0bc = abc \in L(r)$
$uv^1w = ab^1bc = abbc \in L(r)$
$uv^2w = ab^2bc = abbbc \in L(r)$
⋮

$u = a$, $v = b$, $w = bc$

$v \neq \varepsilon$, $|uv| = 2 \leq 3$

⋮

Pumping Lemma: Illustration

- L = any regular language:

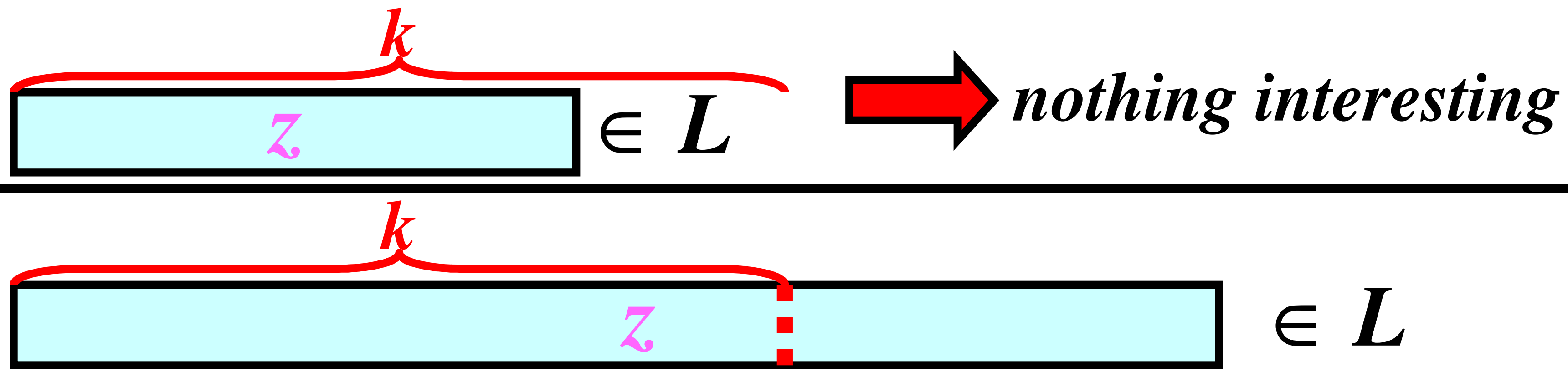
Pumping Lemma: Illustration

- L = any regular language:

$\overbrace{z}^{k} \in L$ $\Rightarrow$ ***nothing interesting***

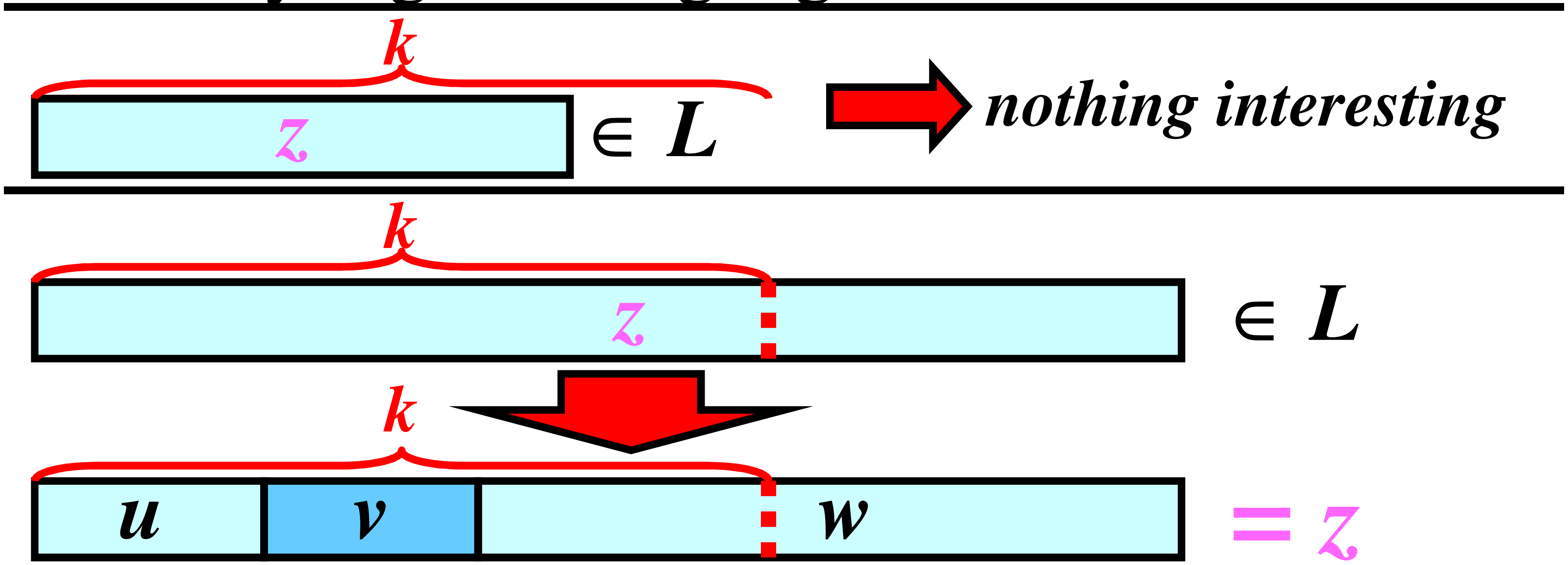
Pumping Lemma: Illustration

- L = any regular language:



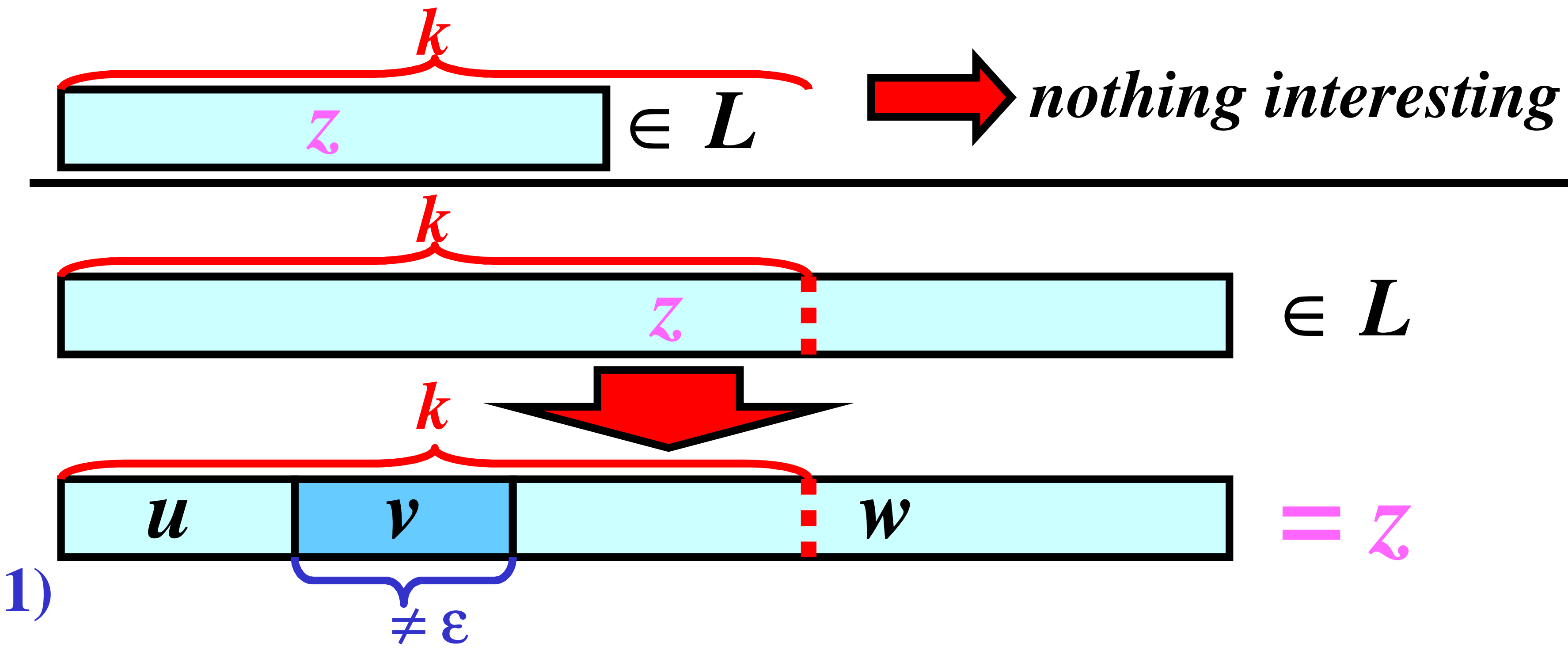
Pumping Lemma: Illustration

- L = any regular language:



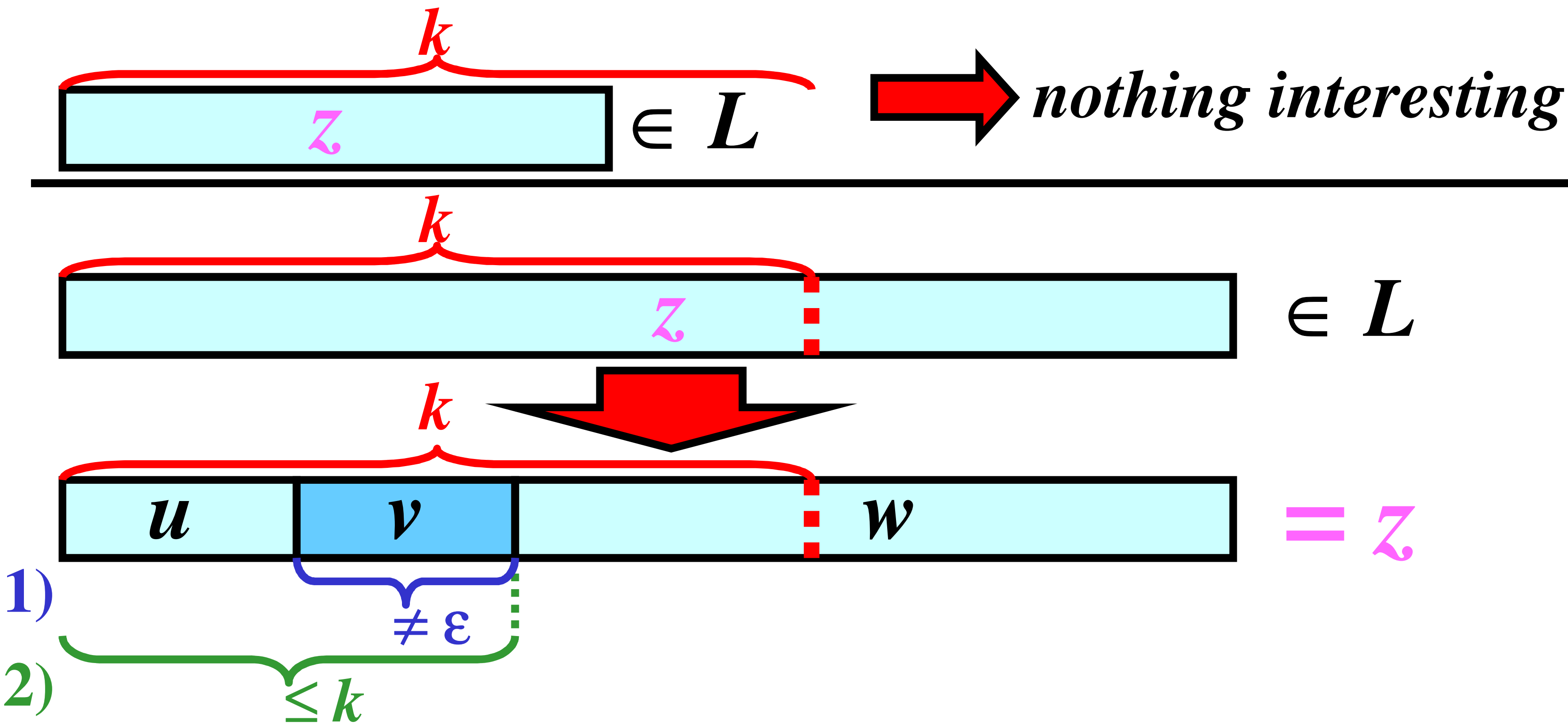
Pumping Lemma: Illustration

- L = any regular language:



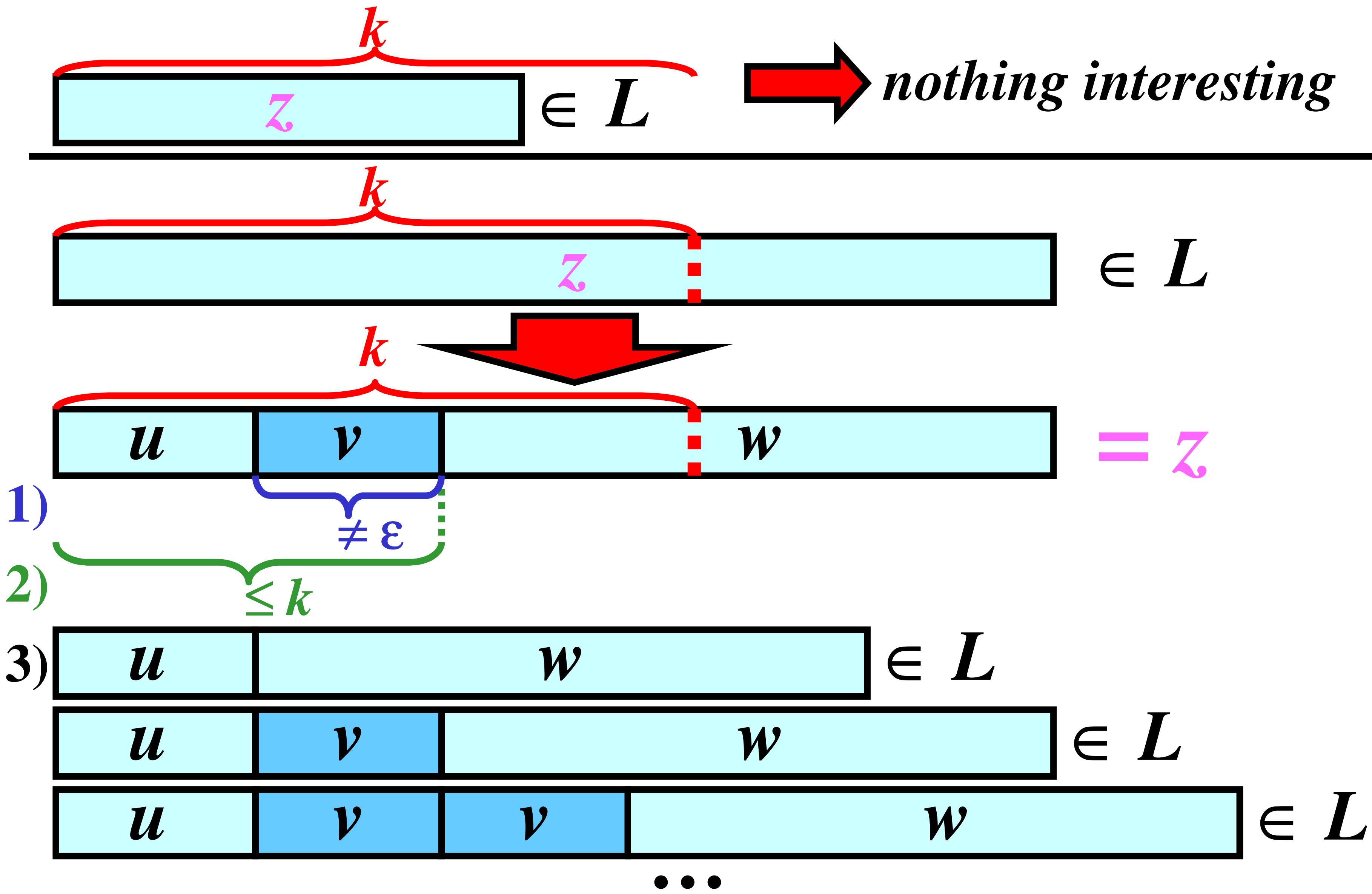
Pumping Lemma: Illustration

- L = any regular language:



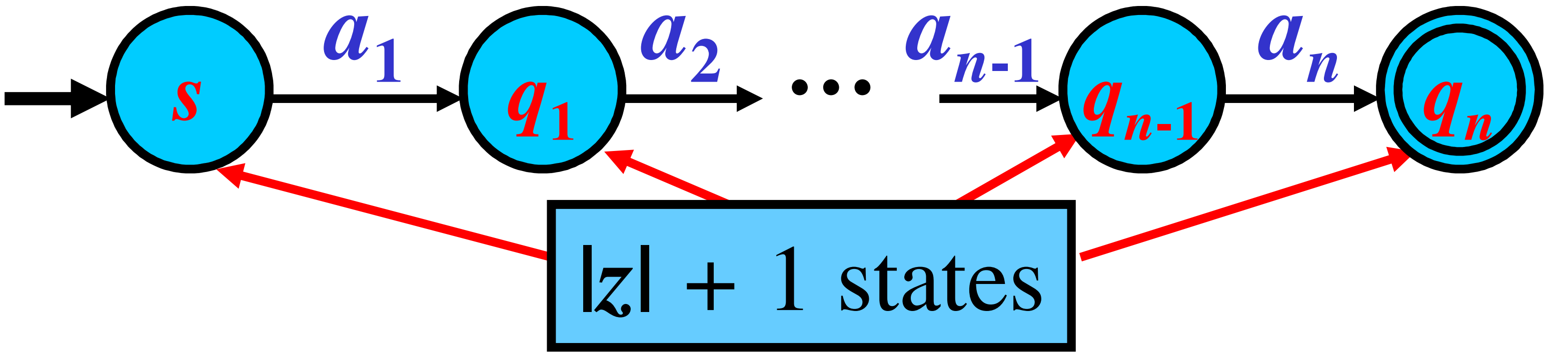
Pumping Lemma: Illustration

- L = any regular language:



Proof of Pumping Lemma 1/3

- Let L be a regular language. Then, there exists **DFA** $M = (Q, \Sigma, R, s, F)$, and $L = L(M)$.
- For $z \in L(M)$, M makes $|z|$ moves and M visits $|z| + 1$ states:
- for $z = a_1a_2 \ldots a_n$:



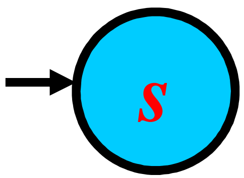
$$s\overbrace{a_1a_2\ldots a_n}^{|z|} \vdash q_1a_2\ldots a_n \vdash \ldots \vdash q_{n-1}a_n \vdash q_n$$

Proof of Pumping Lemma 2/3

- Let $\boldsymbol{k}$ = card(Q) (the number of states).

For each $z \in L$ and $|z| \geq k$, M visits $k + 1$ or more states. As $k + 1 > \text{card}(Q)$, there exists a state $\boldsymbol{q}$ that M visits at least twice.

- For z exist u, v, w such that $z = \boldsymbol{uvw}$:

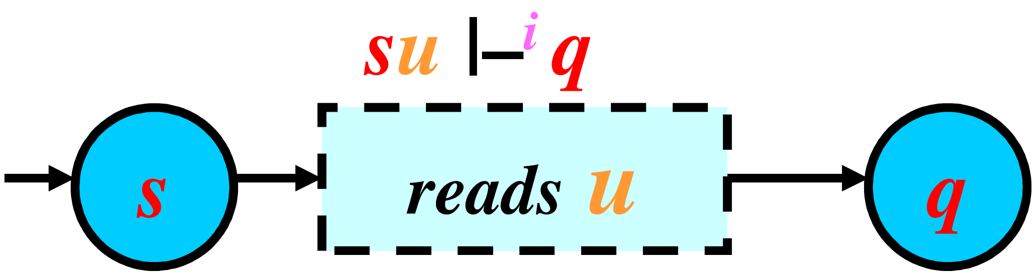


Proof of Pumping Lemma 2/3

- Let $\boldsymbol{k}$ = card(Q) (the number of states).

For each $z \in L$ and $|z| \geq k$, M visits $k + 1$ or more states. As $k + 1 >$ card(Q), there exists a state $\boldsymbol{q}$ that M visits at least twice.

- For z exist u, v, w such that $z = \boldsymbol{uvw}$:

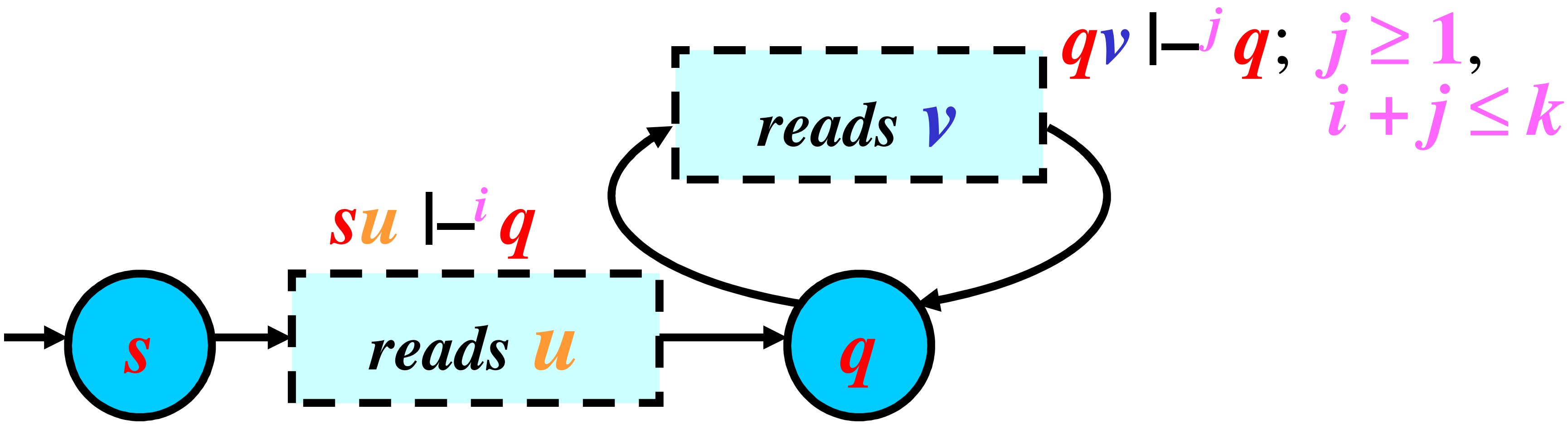


Proof of Pumping Lemma 2/3

- Let $\boldsymbol{k}$ = card(Q) (the number of states).

For each $z \in L$ and $|z| \geq k$, M visits $k + 1$ or more states. As $k + 1 > \text{card}(Q)$, there exists a state $\boldsymbol{q}$ that M visits at least twice.

- For z exist u, v, w such that $z = \boldsymbol{uvw}$:

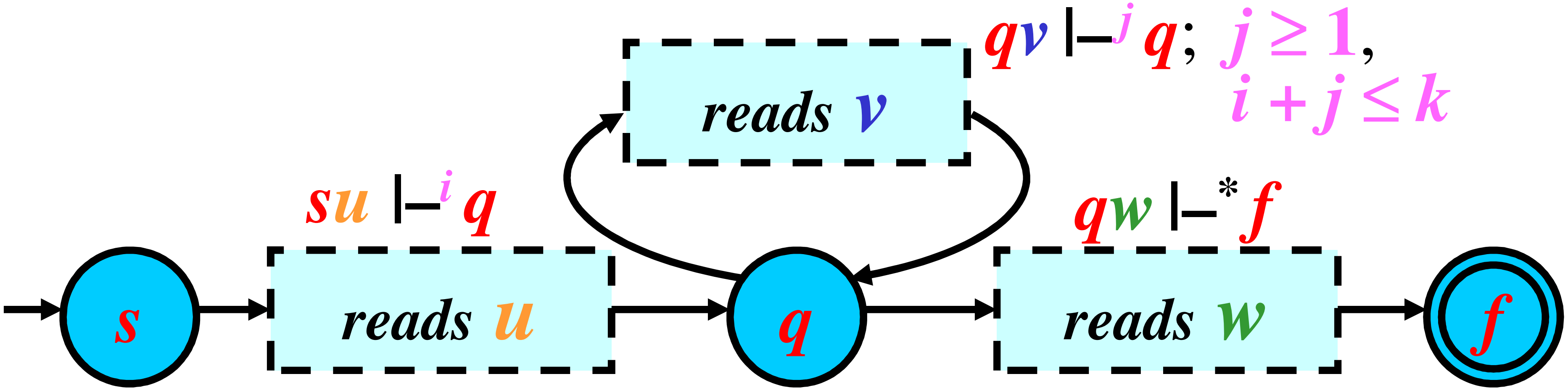


Proof of Pumping Lemma 2/3

- Let $\boldsymbol{k}$ = card(Q) (the number of states).

For each $z \in L$ and $|z| \geq k$, M visits $k + 1$ or more states. As $k + 1 > \text{card}(Q)$, there exists a state $\boldsymbol{q}$ that M visits at least twice.

- For z exist u, v, w such that $z = \boldsymbol{uvw}$:

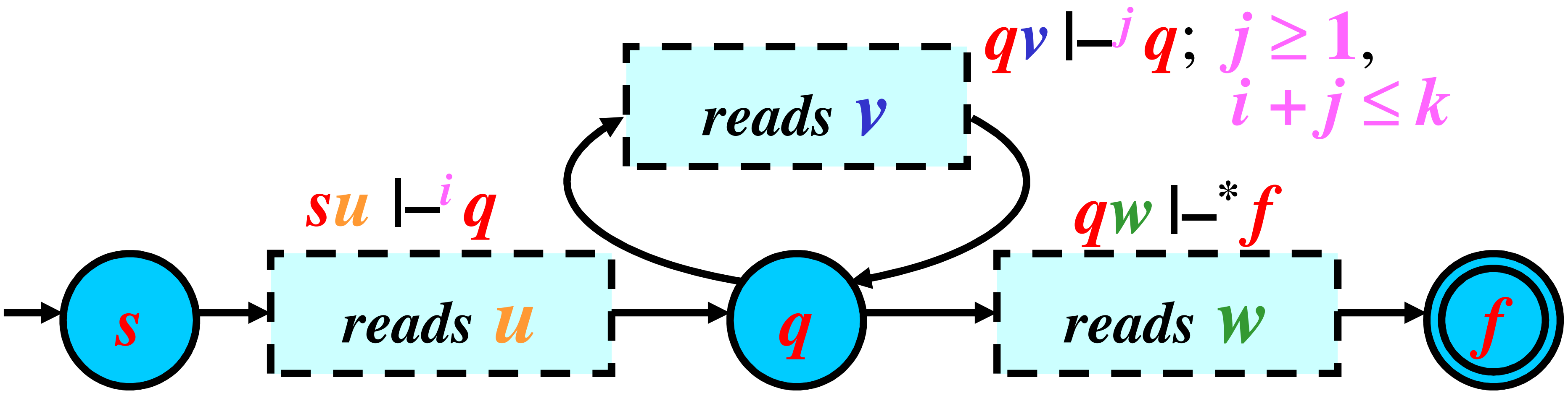


Proof of Pumping Lemma 2/3

- Let $\boldsymbol{k}$ = card(Q) (the number of states).

For each $z \in L$ and $|z| \geq k$, M visits $k + 1$ or more states. As $k + 1 >$ card(Q), there exists a state $\boldsymbol{q}$ that M visits at least twice.

- For z exist u, v, w such that $z = \boldsymbol{uvw}$:



Summary:

$$sz = suvw \vdash^i qvw \vdash^j qw \vdash^* f,\ f \in F$$

Proof of Pumping Lemma 3/3

- There exist moves:

1. $su \vdash^{i} q$; 2. $qv \vdash^{j} q$; 3. $qw \vdash^{*} f, f \in F$, so

Proof of Pumping Lemma 3/3

- There exist moves:

1. $su \vdash^{i} q$; 2. $qv \vdash^{j} q$; 3. $qw \vdash^{*} f, f \in F$, so

- for $m = 0$, $uv^{m}w = uv^{0}w = uw$,

suw

Proof of Pumping Lemma 3/3

- There exist moves:

1. $su \vdash^{i} q$; 2. $qv \vdash^{j} q$; 3. $qw \vdash^{*} f, f \in F$, so

- for $m = 0$, $uv^{m}w = uv^{0}w = uw$,

$$suw \overset{1.}{\vdash^{i}} qw$$

Proof of Pumping Lemma 3/3

- There exist moves:

1. $su \vdash^i q$; 2. $qv \vdash^j q$; 3. $qw \vdash^* f, f \in F$, so

- for $m = 0$, $uv^m w = uv^0 w = uw$,

$suw \overset{1.}{\vdash^i} qw \overset{3.}{\vdash^*} f,\ f \in F$

Proof of Pumping Lemma 3/3

- There exist moves:

1. $su \vdash^i q$; 2. $qv \vdash^j q$; 3. $qw \vdash^* f, f \in F$, so

- for $m = 0$, $uv^m w = uv^0 w = uw$,

$$suw \vdash^i qw \vdash^* f,\ f \in F$$

- for each $m > 0$,

$suv^m w$

Proof of Pumping Lemma 3/3

- There exist moves:

1. $su \vdash^{i} q$; 2. $qv \vdash^{j} q$; 3. $qw \vdash^{*} f, f \in F$, so

- for $m = 0$, $uv^{m}w = uv^{0}w = uw$,

$$suw \overset{1.}{\vdash^{i}} qw \overset{3.}{\vdash^{*}} f,\ f \in F$$

- for each $m > 0$,

$$suv^{m}w \overset{1.}{\vdash^{i}} qv^{m}w$$

Proof of Pumping Lemma 3/3

- There exist moves:

1. $su \vdash^{i} q$; 2. $qv \vdash^{j} q$; 3. $qw \vdash^{*} f, f \in F$, so

- for $m = 0$, $uv^{m}w = uv^{0}w = uw$,

$$su w \overset{1.}{\vdash^{i}} qw \overset{3.}{\vdash^{*}} f,\ f \in F$$

- for each $m > 0$,

$$suv^{m}w \overset{1.}{\vdash^{i}} qv^{m}w \overset{2.}{\vdash^{j}} qv^{m-1}w \overset{2.}{\vdash^{j}} \dots \overset{2.}{\vdash^{j}} qw$$

Proof of Pumping Lemma 3/3

- There exist moves:

1. $su \vdash^{i} q$; 2. $qv \vdash^{j} q$; 3. $qw \vdash^{*} f, f \in F$, so

- for $m = 0$, $uv^{m}w = uv^{0}w = uw$,

$$suw \overset{1.}{\vdash^{i}} qw \overset{3.}{\vdash^{*}} f,\ f \in F$$

- for each $m > 0$,

$$suv^{m}w \overset{1.}{\vdash^{i}} qv^{m}w \overset{2.}{\vdash^{j}} qv^{m-1}w \overset{2.}{\vdash^{j}} \ldots \overset{2.}{\vdash^{j}} qw \overset{3.}{\vdash^{*}} f,\ f \in F$$

Proof of Pumping Lemma 3/3

- There exist moves:

1. $su \vdash^{i} q$; 2. $qv \vdash^{j} q$; 3. $qw \vdash^{*} f, f \in F$, so

- for $m = 0$, $uv^m w = uv^0 w = uw$,

$$su w \overset{1.}{\vdash^{i}} qw \overset{3.}{\vdash^{*}} f,\ f \in F$$

- for each $m > 0$,

$$suv^m w \overset{1.}{\vdash^{i}} qv^m w \overset{2.}{\vdash^{j}} qv^{m\text{-}1} w \overset{2.}{\vdash^{j}} \dots \overset{2.}{\vdash^{j}} qw \overset{3.}{\vdash^{*}} f,\ f \in F$$

Summary:

1) $qv \vdash^{j} q$, $j \geq 1$; therefore, $|v| \geq \mathbf{1}$, so $v \neq \varepsilon$

2) $suv \vdash^{i} qv \vdash^{j} q$, $i + j \leq k$; therefore, $|uv| \leq k$

3) For each $m \geq 0$: $suv^m w \vdash^{*} f$, $f \in F$, therefore $uv^m w \in L$

QED

Pumping Lemma: Application I

- Based on the pumping lemma, we often make a proof by contradiction to demonstrate that a language is **not** regular

Pumping Lemma: Application I

- Based on the pumping lemma, we often make a proof by contradiction to demonstrate that a language is **not** regular

Assume that L is regular

Pumping Lemma: Application I

- Based on the pumping lemma, we often make a proof by contradiction to demonstrate that a language is **not** regular

Assume that L is regular

↓

Consider the PL constant $\boldsymbol{k}$ and select $z \in L$, whose length depends on $\boldsymbol{k}$ so $|z| \geq \boldsymbol{k}$ is surely true.

Pumping Lemma: Application I

- Based on the pumping lemma, we often make a proof by contradiction to demonstrate that a language is **not** regular

Assume that L is regular

↓

Consider the PL constant $\boldsymbol{k}$ and select $z \in L$, whose length depends on $\boldsymbol{k}$ so $|z| \geq \boldsymbol{k}$ is surely true.

↓

For all decompositions of z into $\boldsymbol{uvw}$, $v \neq \varepsilon$, $|uv| \leq k$, show:

$$\left.\begin{array}{l}\text{there exists } m \geq 0 \text{ such that } \boldsymbol{uv^m w} \notin \boldsymbol{L} \\ \text{from the pumping lemma, } \boldsymbol{uv^m w} \in \boldsymbol{L}\end{array}\right\} \textbf{contradiction}$$

Pumping Lemma: Application I

- Based on the pumping lemma, we often make a proof by contradiction to demonstrate that a language is **not** regular

Assume that L is regular

Consider the PL constant $\boldsymbol{k}$ and select $z \in L$, whose length depends on $\boldsymbol{k}$ so $|z| \geq \boldsymbol{k}$ is surely true.

For all decompositions of z into $\boldsymbol{uvw}$, $v \neq \varepsilon$, $|uv| \leq k$, show:

$$\left.\begin{array}{l}\text{there exists } m \geq 0 \text{ such that } \boldsymbol{uv^m w} \notin \boldsymbol{L} \\ \text{from the pumping lemma, } \boldsymbol{uv^m w} \in \boldsymbol{L}\end{array}\right\} \textbf{contradiction}$$

false assumption

Pumping Lemma: Application I

- Based on the pumping lemma, we often make a proof by contradiction to demonstrate that a language is **not** regular

Assume that L is regular

Consider the PL constant $\boldsymbol{k}$ and select $z \in L$, whose length depends on $\boldsymbol{k}$ so $|z| \geq \boldsymbol{k}$ is surely true.

For all decompositions of z into $\boldsymbol{uvw}$, $v \neq \varepsilon$, $|uv| \leq k$, show:

$$\left.\begin{array}{l}\text{there exists } m \geq 0 \text{ such that } \boldsymbol{uv^m w} \notin \boldsymbol{L} \\ \text{from the pumping lemma, } \boldsymbol{uv^m w} \in \boldsymbol{L}\end{array}\right\} \textbf{contradiction}$$

false assumption

Therefore,
***L* is not regular**

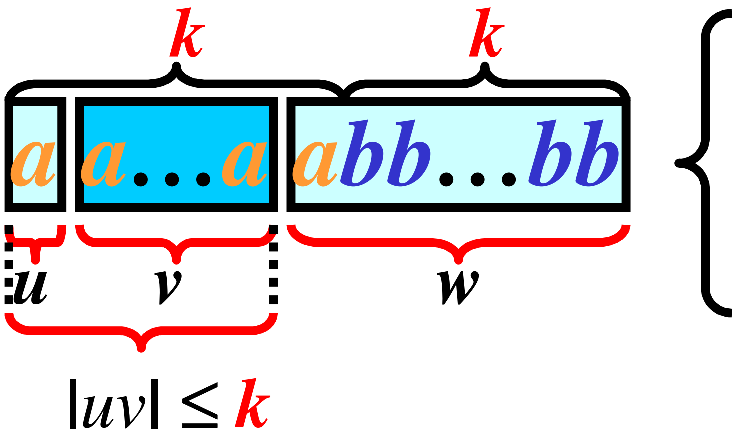
Pumping Lemma: Example

Prove that $L = \{a^n b^n : n \geq 0\}$ is not regular:

1) Assume that L is regular. Let $k \geq 1$ be the pumping lemma constant for L.

2) Let $z = a^k b^k$: $a^k b^k \in L$, $|z| = |a^k b^k| = 2k \geq k$

3) All decompositions of z into uvw, $v \neq \varepsilon$, $|uv| \leq k$:



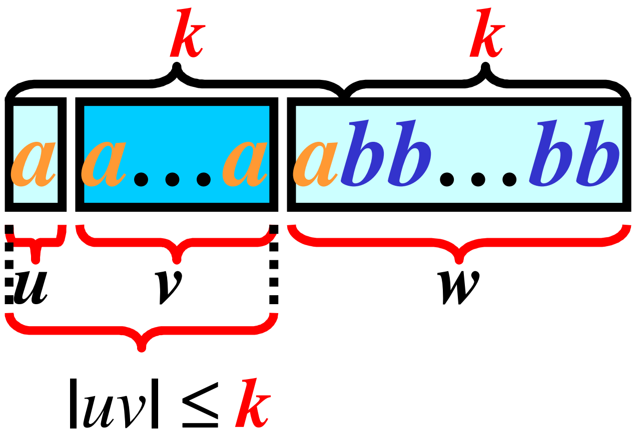
Pumping Lemma: Example

Prove that $L = \{a^n b^n : n \ge 0\}$ is not regular:

1) Assume that L is regular. Let $k \ge 1$ be the pumping lemma constant for L.

2) Let $z = a^k b^k$: $a^k b^k \in L$, $|z| = |a^k b^k| = 2k \ge k$

3) All decompositions of z into uvw, $v \ne \varepsilon$, $|uv| \le k$:



- pumping lemma: $uv^0w \in L$

Pumping Lemma: Example

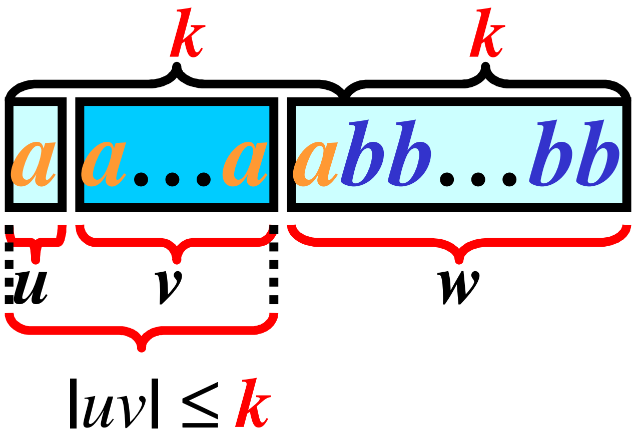
Prove that $L = \{a^n b^n : n \geq 0\}$ is not regular:

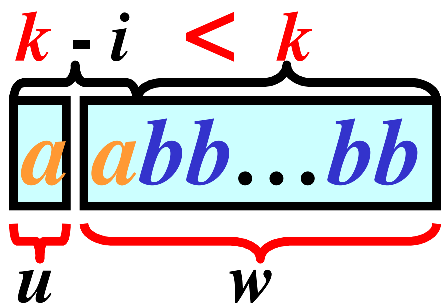
---

1) Assume that L is regular. Let $k \geq 1$ be the pumping lemma constant for L.

2) Let $z = a^k b^k$: $a^k b^k \in L$, $|z| = |a^k b^k| = 2k \geq k$

3) All decompositions of z into uvw, $v \neq \varepsilon$, $|uv| \leq k$:



- pumping lemma: $uv^0w \in L$
- $uv^0w = uw =$  $\notin L$

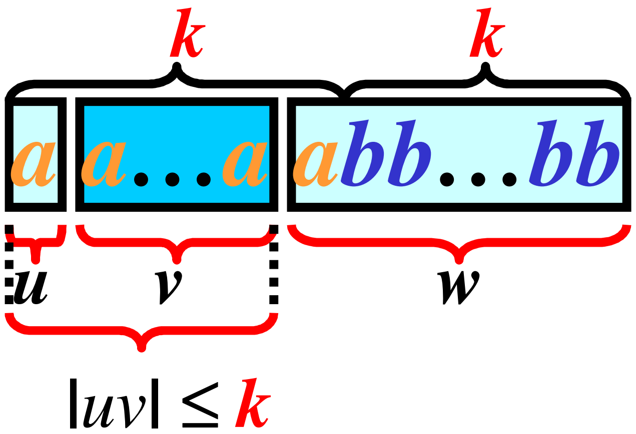
Pumping Lemma: Example

Prove that $L = \{a^n b^n : n \geq 0\}$ is not regular:

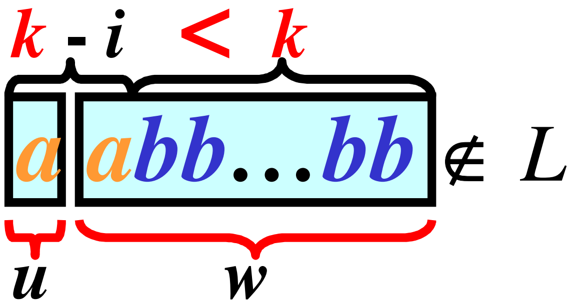
1) Assume that L is regular. Let $k \geq 1$ be the pumping lemma constant for L.

2) Let $z = a^k b^k$: $a^k b^k \in L$, $|z| = |a^k b^k| = 2k \geq k$

3) All decompositions of z into uvw, $v \neq \varepsilon$, $|uv| \leq k$:



- pumping lemma: $uv^0w \in L$
- $uv^0w = uw =$



Contradiction!

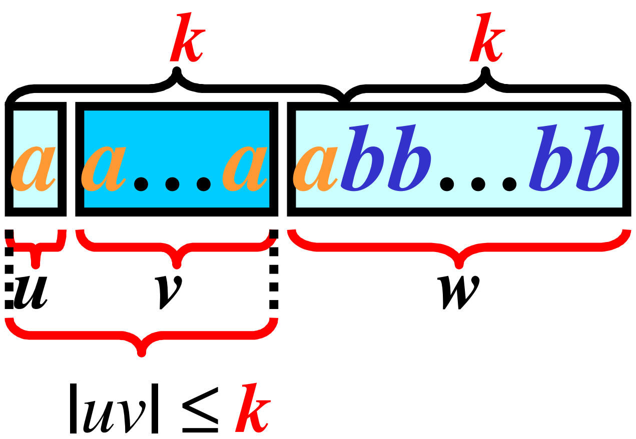
Pumping Lemma: Example

Prove that $L = \{a^n b^n : n \geq 0\}$ is not regular:

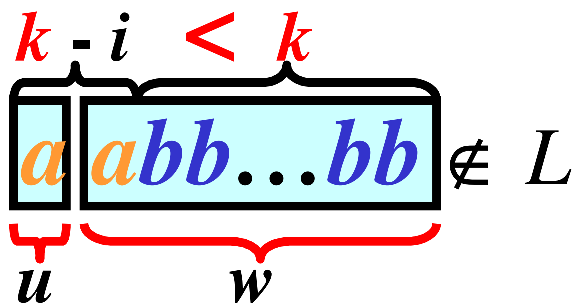
1) Assume that L is regular. Let $k \geq 1$ be the pumping lemma constant for L.

2) Let $z = a^k b^k$: $a^k b^k \in L$, $|z| = |a^k b^k| = 2k \geq k$

3) All decompositions of z into uvw, $v \neq \varepsilon$, $|uv| \leq k$:



- pumping lemma: $uv^0w \in L$
- $uv^0w = uw =$



Contradiction!

4) Therefore, L is not regular

Note on Use of Pumping Lemma

- **Pumping lemma:**

if *L* is regular **then** → exist $k \geq 1$ and ...

Main application of the pumping lemma:

- proof by contradiction that *L* is **not** regular.

Note on Use of Pumping Lemma

- **Pumping lemma:**

if $\boxed{L \text{ is regular}} \xrightarrow{\textbf{then}} \boxed{\text{exist } k \geq 1 \text{ and} \ldots}$

Main application of the pumping lemma:

- proof by contradiction that *L* is **not** regular.

- **However, the next implication is incorrect:**

~~**if** $\boxed{\text{exist } k \geq 1 \text{ and} \ldots} \xrightarrow{\textbf{then}} \boxed{L \text{ is regular}}$~~

- **We cannot use the pumping lemma to prove that *L* is regular.**

Pumping Lemma: Application II. 1/3

- We can use the pumping lemma to prove some other theorems.

Illustration:

- Let M be a DFA and k be the pumping lemma constant (k is the number of states in M). Then, $L(M)$ is infinite $\Leftrightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$

Proof:

1) there exists $z \in L(M)$, $k \leq |z| < 2k \Rightarrow L(M)$ is infinite:

Pumping Lemma: Application II. 1/3

- We can use the pumping lemma to prove some other theorems.

Illustration:

- Let M be a DFA and k be the pumping lemma constant (k is the number of states in M). Then, $L(M)$ is infinite $\Leftrightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$

Proof:

1) there exists $z \in L(M)$, $k \leq |z| < 2k \Rightarrow L(M)$ is infinite:

if $z \in L(M)$, $k \leq |z|$, then by PL:

$z = uvw$, $v \neq \varepsilon$, and for each $m \geq 0$: $uv^m w \in L(M)$

Pumping Lemma: Application II. 1/3

- We can use the pumping lemma to prove some other theorems.

Illustration:

- Let M be a DFA and k be the pumping lemma constant (k is the number of states in M). Then, $L(M)$ is infinite $\Leftrightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$

Proof:

1) there exists $z \in L(M)$, $k \leq |z| < 2k \Rightarrow L(M)$ is infinite:

if $z \in L(M)$, $k \leq |z|$, then by PL:

$z = uvw$, $\underbrace{v \neq \varepsilon}$, and for each $\underbrace{m \geq 0: uv^m w \in L(M)}$

$L(M)$ is infinite

Pumping Lemma: Application II. 2/3

2) $L(M)$ is infinite $\Rightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$**:**

- We prove by contradiction, that

$L(M)$ is infinite **a)** $\rightarrow$ there exists $z \in L(M)$, $|z| \geq k$

b) $\downarrow$

there exists $z \in L(M)$, $k \leq |z| < 2k$

---

a) Prove by contradiction that

- $\boldsymbol{L(M)}$ **is infinite** $\boldsymbol{\Rightarrow}$ **there exists** $\boldsymbol{z \in L(M), |z| \geq k}$

Pumping Lemma: Application II. 2/3

2) $L(M)$ is infinite $\Rightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$**:**

- We prove by contradiction, that

$L(M)$ is infinite $\xrightarrow{\text{a)}}$ there exists $z \in L(M)$, $|z| \geq k$

$\downarrow$ **b)**

there exists $z \in L(M)$, $k \leq |z| < 2k$

---

a) Prove by contradiction that

- **$L(M)$ is infinite $\Rightarrow$ there exists $z \in L(M)$, $|z| \geq k$**

Assume that **$L(M)$ is infinite** and there exists no $z \in L(M)$, $|z| \geq k$

Pumping Lemma: Application II. 2/3

2) $L(M)$ is infinite $\Rightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$**:**

- We prove by contradiction, that

$L(M)$ is infinite $\xrightarrow{\text{a)}}$ there exists $z \in L(M)$, $|z| \geq k$

$\downarrow$ **b)**

there exists $z \in L(M)$, $k \leq |z| < 2k$

---

a) Prove by contradiction that

- **$L(M)$ is infinite $\Rightarrow$ there exists $z \in L(M)$, $|z| \geq k$**

Assume that **$L(M)$ is infinite** and there exists no $z \in L(M)$, $|z| \geq k$

$\downarrow$

for all $z \in L(M)$ holds $|z| < k$

Pumping Lemma: Application II. 2/3

2) $L(M)$ is infinite $\Rightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$**:**

- We prove by contradiction, that

$L(M)$ is infinite $\xrightarrow{\textbf{a)}}$ there exists $z \in L(M)$, $|z| \geq k$

$\downarrow$ **b)**

there exists $z \in L(M)$, $k \leq |z| < 2k$

---

a) Prove by contradiction that

- ***L*(*M*) is infinite $\Rightarrow$ there exists $z \in L(M)$, $|z| \geq k$**

Assume that ***L*(*M*) is infinite** and there exists no $z \in L(M)$, $|z| \geq k$

$\downarrow$

for all $z \in L(M)$ holds $|z| < k$

$\downarrow$

***L*(*M*) is finite**

Pumping Lemma: Application II. 2/3

2) $L(M)$ is infinite $\Rightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$**:**

- We prove by contradiction, that

$L(M)$ is infinite $\xrightarrow{\text{a)}}$ there exists $z \in L(M)$, $|z| \geq k$

b) $\downarrow$

there exists $z \in L(M)$, $k \leq |z| < 2k$

---

a) Prove by contradiction that

- ***L*(*M*) is infinite $\Rightarrow$ there exists $z \in L(M)$, $|z| \geq k$**

Assume that ***L*(*M*) is infinite** and there exists no $z \in L(M)$, $|z| \geq k$

$\downarrow$

for all $z \in L(M)$ holds $|z| < k$

$\downarrow$

***L*(*M*) is finite**

Contradiction !

Pumping Lemma: Application II. 3/3

b) Prove by contradiction

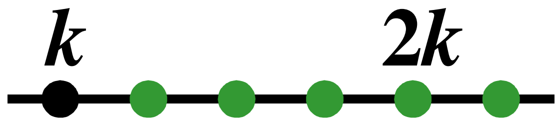
- **there exists** $z \in L(M)$**,** $|z| \geq k \Rightarrow$ **there exists** $z \in L(M)$**,** $k \leq |z| < 2k$

Pumping Lemma: Application II. 3/3

b) Prove by contradiction

- **there exists** $z \in L(M)$, $|z| \geq k \Rightarrow$
  there exists $z \in L(M)$, $k \leq |z| < 2k$

Assume that **there is** $z \in L(M)$, $|z| \geq k$

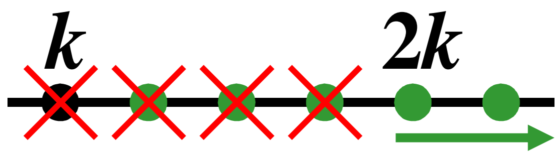


Pumping Lemma: Application II. 3/3

b) Prove by contradiction

- **there exists** $z \in L(M)$, $|z| \geq k \Rightarrow$
  there exists $z \in L(M)$, $k \leq |z| < 2k$

Assume that **there is** $z \in L(M)$, $|z| \geq k$
and **there is no** $z \in L(M)$, $k \leq |z| < 2k$

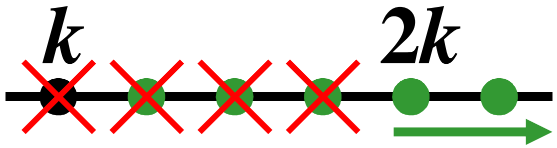


Pumping Lemma: Application II. 3/3

b) Prove by contradiction

- **there exists** $z \in L(M)$, $|z| \geq k \Rightarrow$
  there exists $z \in L(M)$, $k \leq |z| < 2k$

Assume that **there is** $z \in L(M)$, $|z| \geq k$
and **there is no** $z \in L(M)$, $k \leq |z| < 2k$



Let z_0 be **the shortest string** satisfying $z_0 \in L(M)$, $|z_0| \geq k$

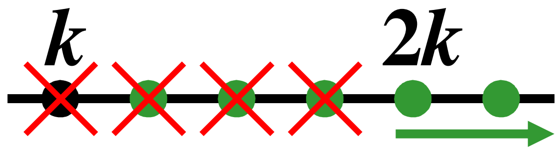
Because there exists no $z \in L(M)$, $k \leq |z| < 2k$, so $|z_0| \geq 2k$

Pumping Lemma: Application II. 3/3

b) Prove by contradiction

- **there exists $z \in L(M)$, $|z| \geq k \Rightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$**

Assume that **there is $z \in L(M)$, $|z| \geq k$**
and **there is no $z \in L(M)$, $k \leq |z| < 2k$**



Let z_0 be **the shortest string** satisfying $z_0 \in L(M)$, $|z_0| \geq k$

Because there exists no $z \in L(M)$, $k \leq |z| < 2k$, so $|z_0| \geq 2k$

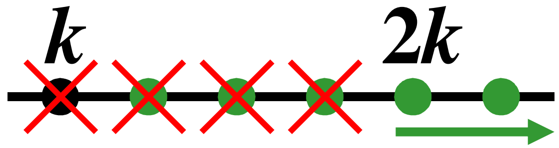
If $z_0 \in L(M)$ and $|z_0| \geq k$, the PL implies: $z_0 = uvw$,
$|uv| \leq k$, and for each $m \geq 0$, $uv^m w \in L(M)$

Pumping Lemma: Application II. 3/3

b) Prove by contradiction

- **there exists $z \in L(M)$, $|z| \geq k \Rightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$**

Assume that **there is $z \in L(M)$, $|z| \geq k$** and **there is no $z \in L(M)$, $k \leq |z| < 2k$**



Let z_0 be **the shortest string** satisfying $z_0 \in L(M)$, $|z_0| \geq k$

Because there exists no $z \in L(M)$, $k \leq |z| < 2k$, so $|z_0| \geq 2k$

If $z_0 \in L(M)$ and $|z_0| \geq k$, the PL implies: $z_0 = uvw$, $|uv| \leq k$, and for each $m \geq 0$, $uv^mw \in L(M)$

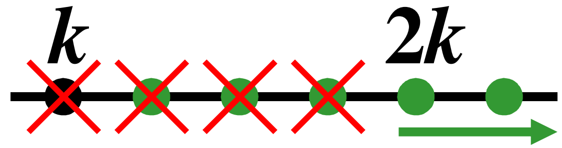
$$|uw| = \overbrace{|z_0|}^{\geq 2k} - \overbrace{|v|}^{\leq k} \geq k$$

Pumping Lemma: Application II. 3/3

b) Prove by contradiction

- **there exists** $z \in L(M)$, $|z| \geq k \Rightarrow$
  there exists $z \in L(M)$, $k \leq |z| < 2k$

Assume that **there is** $z \in L(M)$, $|z| \geq k$
and **there is no** $z \in L(M)$, $k \leq |z| < 2k$



Let z_0 be **the shortest string** satisfying $z_0 \in L(M)$, $|z_0| \geq k$

Because there exists no $z \in L(M)$, $k \leq |z| < 2k$, so $|z_0| \geq 2k$

If $z_0 \in L(M)$ and $|z_0| \geq k$, the PL implies: $z_0 = uvw$,
$|uv| \leq k$, and for each $m \geq 0$, $uv^m w \in L(M)$

$$|uw| = \overbrace{|z_0|}^{\geq 2k} - \overbrace{|v|}^{\leq k} \geq k$$

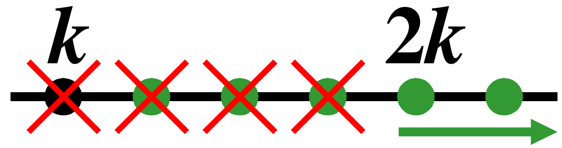
for $m = 0$: $uv^m w = uw \in L(M)$

Pumping Lemma: Application II. 3/3

b) Prove by contradiction

- **there exists** $z \in L(M)$, $|z| \geq k \Rightarrow$
  there exists $z \in L(M)$, $k \leq |z| < 2k$

Assume that **there is** $z \in L(M)$, $|z| \geq k$
and **there is no** $z \in L(M)$, $k \leq |z| < 2k$



Let z_0 be **the shortest string** satisfying $z_0 \in L(M)$, $|z_0| \geq k$

Because there exists no $z \in L(M)$, $k \leq |z| < 2k$, so $|z_0| \geq 2k$

If $z_0 \in L(M)$ and $|z_0| \geq k$, the PL implies: $z_0 = uvw$, $|uv| \leq k$, and for each $m \geq 0$, $uv^m w \in L(M)$

$$|uw| = \overbrace{|z_0|}^{\geq 2k} - \overbrace{|v|}^{\leq k} \geq k$$

for $m = 0$: $uv^m w = uw \in L(M)$

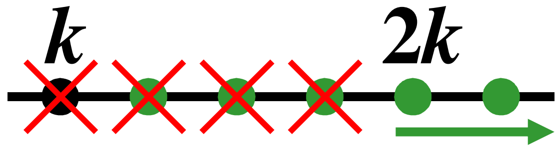
Summary: $uw \in L(M)$, $|uw| \geq k$ and $|uw| < |z_0|$!

Pumping Lemma: Application II. 3/3

b) Prove by contradiction

- **there exists $z \in L(M)$, $|z| \geq k \Rightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$**

Assume that **there is $z \in L(M)$, $|z| \geq k$**
and **there is no $z \in L(M)$, $k \leq |z| < 2k$**



Let z_0 be **the shortest string** satisfying $z_0 \in L(M)$, $|z_0| \geq k$

Because there exists no $z \in L(M)$, $k \leq |z| < 2k$, so $|z_0| \geq 2k$

If $z_0 \in L(M)$ and $|z_0| \geq k$, the PL implies: $z_0 = uvw$,
$|uv| \leq k$, and for each $m \geq 0$, $uv^m w \in L(M)$

$$|uw| = \overbrace{|z_0|}^{\geq 2k} - \overbrace{|v|}^{\leq k} \geq k \qquad \text{for } m = 0\text{: } uv^m w = uw \in L(M)$$

Summary: $uw \in L(M)$, $|uw| \geq k$ and $|uw| < |z_0|$!

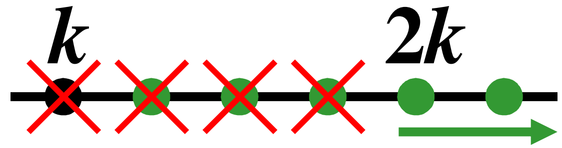
z_0 is not the shortest string satisfying $z_0 \in L(M)$, $|z_0| \geq k$

Pumping Lemma: Application II. 3/3

b) Prove by contradiction

- **there exists $z \in L(M)$, $|z| \geq k \Rightarrow$ there exists $z \in L(M)$, $k \leq |z| < 2k$**

Assume that **there is $z \in L(M)$, $|z| \geq k$** and **there is no $z \in L(M)$, $k \leq |z| < 2k$**



Let z_0 be **the shortest string** satisfying $z_0 \in L(M)$, $|z_0| \geq k$

Because there exists no $z \in L(M)$, $k \leq |z| < 2k$, so $|z_0| \geq 2k$

If $z_0 \in L(M)$ and $|z_0| \geq k$, the PL implies: $z_0 = uvw$, $|uv| \leq k$, and for each $m \geq 0$, $uv^m w \in L(M)$

$$|uw| = \underbrace{|z_0|}_{\geq 2k} - \underbrace{|v|}_{\leq k} \geq k \qquad \text{for } m = 0\text{: } uv^m w = uw \in L(M)$$

Summary: $uw \in L(M)$, $|uw| \geq k$ and $|uw| < |z_0|$!

z_0 is not the shortest string satisfying $z_0 \in L(M)$, $|z_0| \geq k$

Contradiction !

Closure properties 1/2

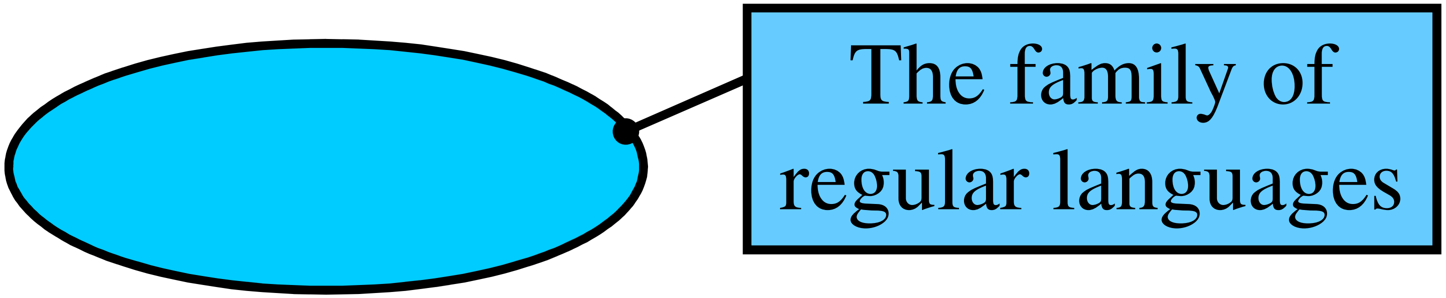
Definition: The family of regular languages is closed under an operation ***o*** if the language resulting from the application of ***o*** to any regular languages is also regular.

Closure properties 1/2

Definition: The family of regular languages is closed under an operation ***o*** if the language resulting from the application of ***o*** to any regular languages is also regular.

Illustration:

- The family of regular languages is closed under ***union***.
  It means:

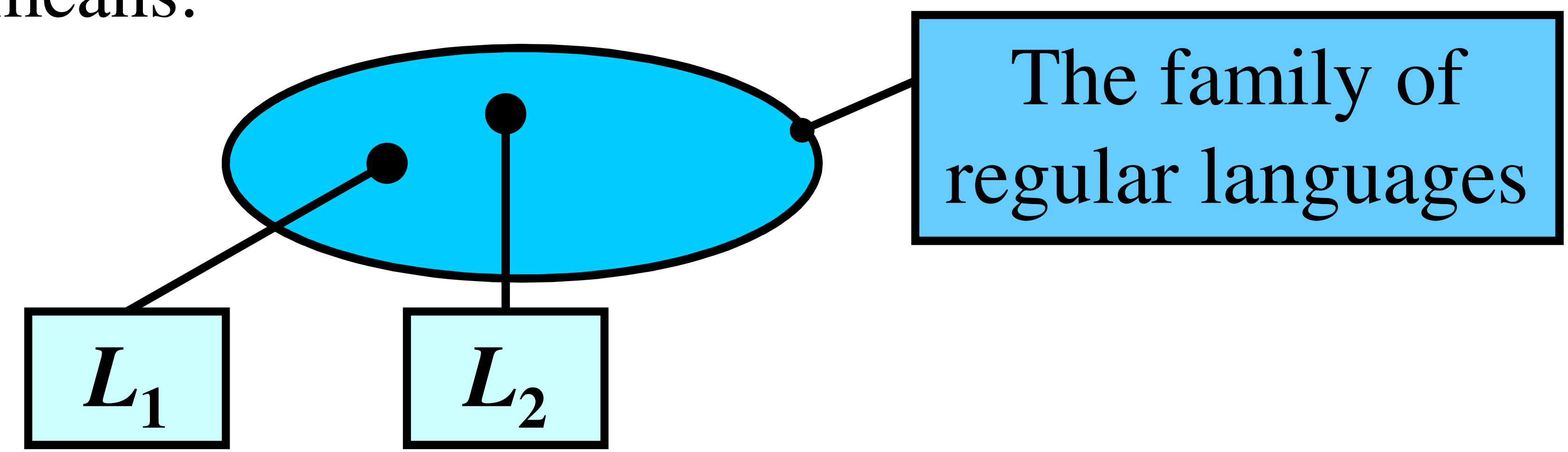


Closure properties 1/2

Definition: The family of regular languages is closed under an operation ***o*** if the language resulting from the application of ***o*** to any regular languages is also regular.

Illustration:

- The family of regular languages is closed under ***union***. It means:

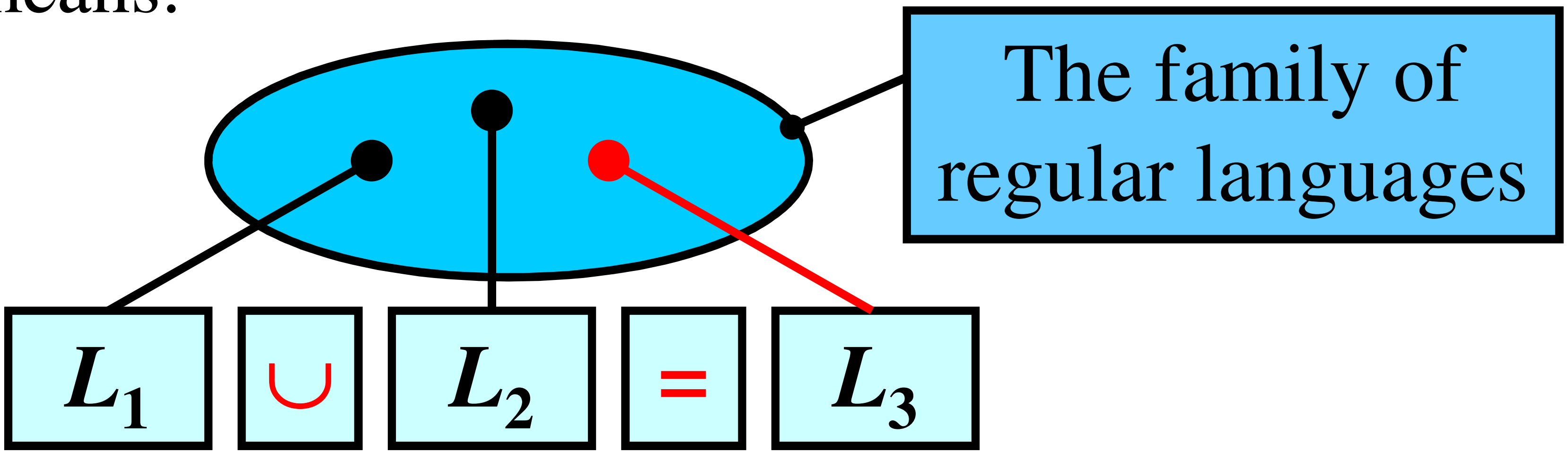


Closure properties 1/2

Definition: The family of regular languages is closed under an operation ***o*** if the language resulting from the application of ***o*** to any regular languages is also regular.

Illustration:

- The family of regular languages is closed under ***union***.
  It means:



Closure properties 2/2

Theorem: The family of regular languages is closed under **union**, **concatenation**, **iteration**.

Proof:

- Let $\boldsymbol{L_1}$, $\boldsymbol{L_2}$ be two **regular languages**
- Then, there exist two REs r_1, r_2: $L(r_1) = \boldsymbol{L_1}$, $L(r_2) = \boldsymbol{L_2}$;
- By the definition of regular expressions:
  - $r_1.r_2$ is a RE denoting $\boldsymbol{L_1 L_2}$
  - $r_1 + r_2$ is a RE denoting $\boldsymbol{L_1} \cup \boldsymbol{L_2}$
  - r_1^* is a RE denoting $\boldsymbol{L_1}^*$
- Every RE denotes regular language, so $\boldsymbol{L_1 L_2}$, $\boldsymbol{L_1} \cup \boldsymbol{L_2}$, $\boldsymbol{L_1}^*$ are a **regular languages**

Algorithm: FA for Complement

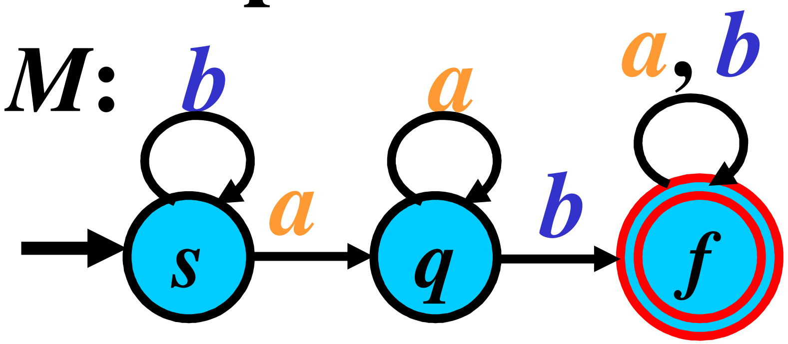
- **Input:** Complete FA: $M = (Q, \Sigma, R, s, F)$
- **Output:** Complete FA: $M' = (Q, \Sigma, R, s, F')$,

$$L(M') = \overline{L(M)}$$

- **Method:**
- $F' := Q - F$

Example:

***M*:**



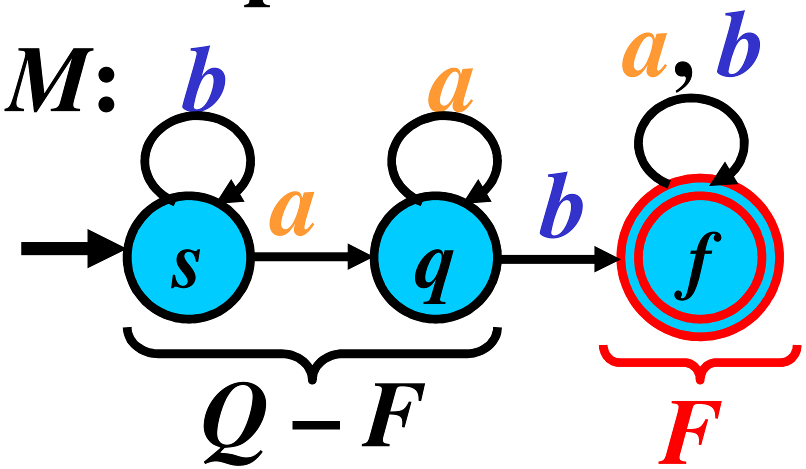
Algorithm: FA for Complement

- **Input:** Complete FA: $M = (Q, \Sigma, R, s, F)$
- **Output:** Complete FA: $M' = (Q, \Sigma, R, s, F')$,

$$L(M') = \overline{L(M)}$$

- **Method:**
- $F' := Q - F$

Example:



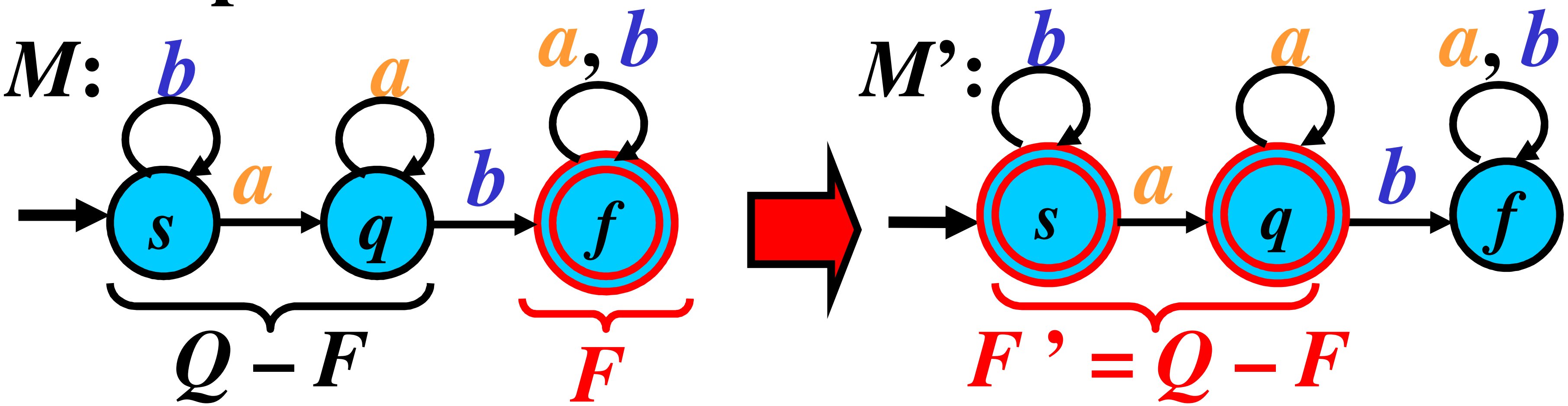
Algorithm: FA for Complement

- **Input:** Complete FA: $M = (Q, \Sigma, R, s, F)$
- **Output:** Complete FA: $M' = (Q, \Sigma, R, s, F')$,

$$L(M') = \overline{L(M)}$$

- **Method:**
- $F' := Q - F$

Example:



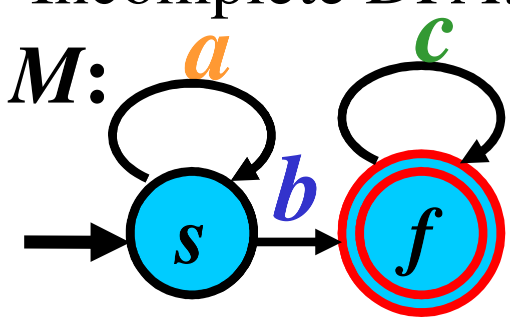
$L(M) = \{x$: ab is a *substring* of $x\}$; $L(M') = \{x$: ab is no *substring* of $x\}$

FA for Complement: Problem

- Previous algorithm requires a **complete** FA
- If *M* is incomplete FA, then *M* must be converted to a complete FA before we use the previous algorithm

Example:

Incomplete DFA:



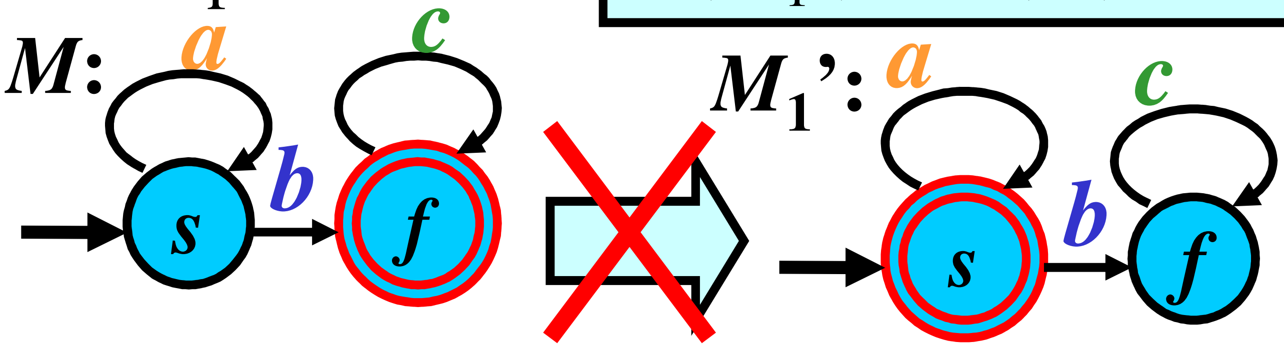
FA for Complement: Problem

- Previous algorithm requires a **complete** FA
- If M is incomplete FA, then M must be converted to a complete FA before we use the previous algorithm

Example:

Incomplete DFA:

$L(M_1') \neq \overline{L(M)}$**!** - $c \notin L(M)$, $c \notin L(M_1')$



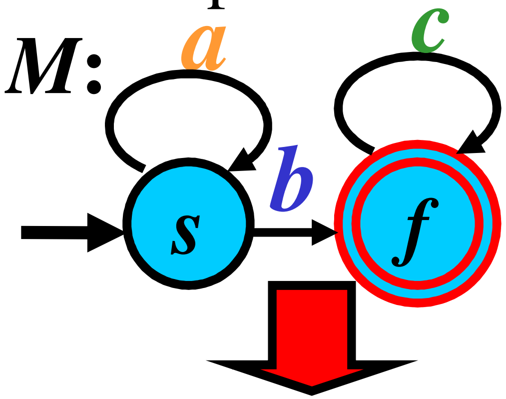
FA for Complement: Problem

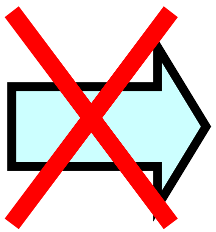
- Previous algorithm requires a **complete** FA
- If M is incomplete FA, then M must be converted to a complete FA before we use the previous algorithm

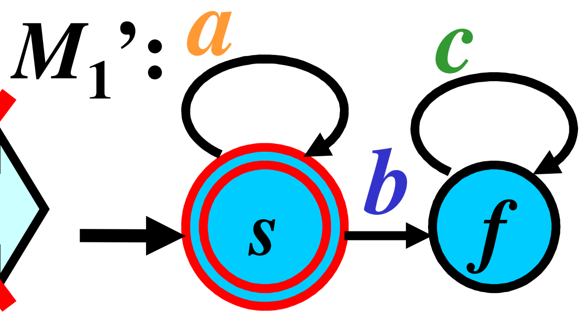
Example:

Incomplete DFA:

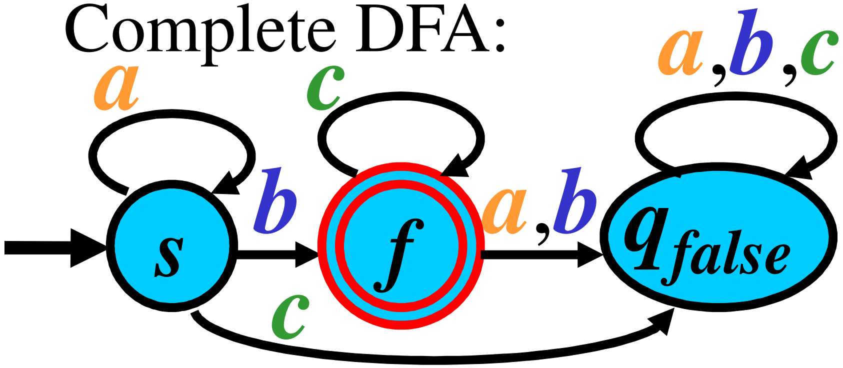
$L(M_1') \neq \overline{L(M)}$**!** - $c \notin L(M)$, $c \notin L(M_1')$







Complete DFA:



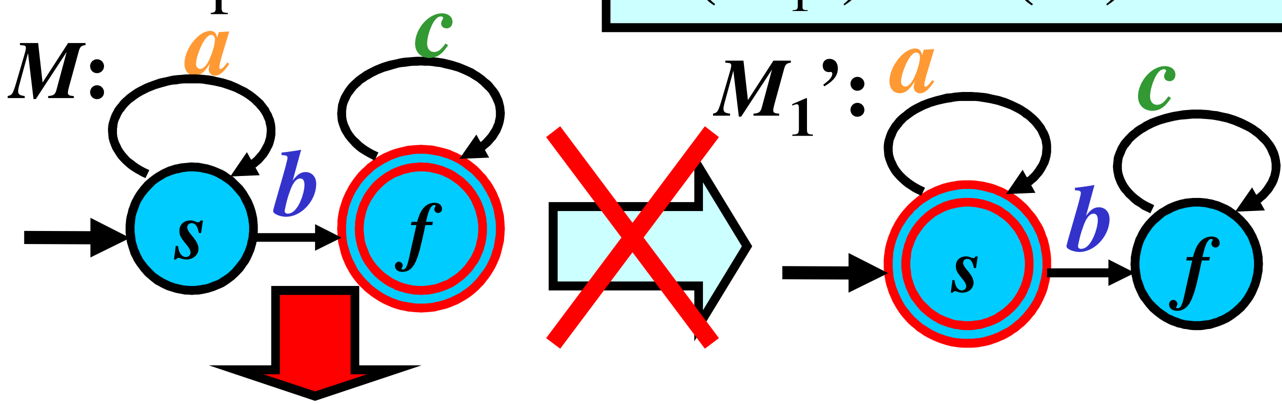
FA for Complement: Problem

- Previous algorithm requires a **complete** FA
- If M is incomplete FA, then M must be converted to a complete FA before we use the previous algorithm

Example:

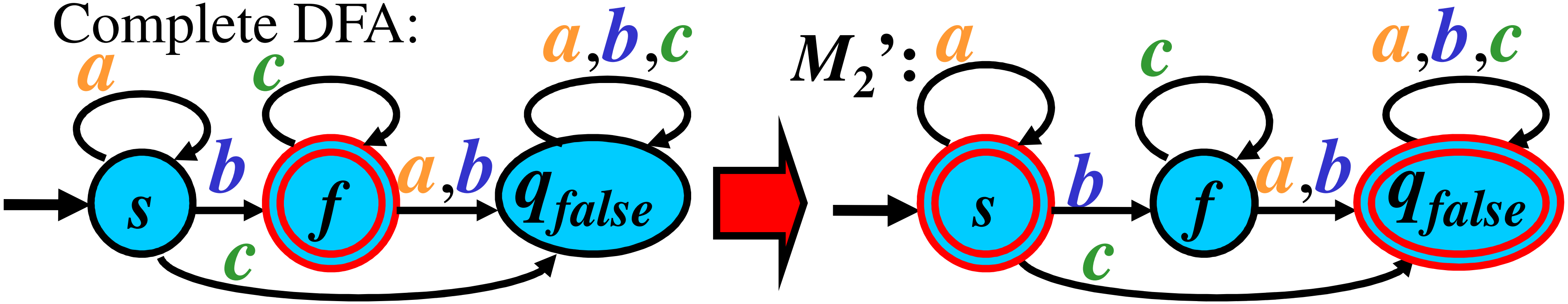
Incomplete DFA:

$L(M_1') \neq \overline{L(M)}$**!** - $c \notin L(M)$, $c \notin L(M_1')$



$L(M_2') = \overline{L(M)}$

Complete DFA:



Closure properties: Complement

Theorem: The family of regular languages is closed under **complement**.

Proof:

- Let L be a **regular language**
- Then, there exists a complete DFA M: $L(M) = L$
- We can construct a complete DFA M': $L(M') = \overline{L}$ by using the previous algorithm
- Every FA defines a regular language, so $\overline{L}$ is a **regular language**

Closure properties: Intersection

Theorem: The family of regular languages is closed under **intersection**.

Proof:

- Let L_1, L_2 be two **regular languages**
- $\overline{L_1}$, $\overline{L_2}$ are **regular languages**

(the family of regular languages is closed under complement)

- $\overline{L_1} \cup \overline{L_2}$ is a **regular language**

(the family of regular languages is closed under union)

- $\overline{\overline{L_1} \cup \overline{L_2}}$ is a **regular language**

(the family of regular languages is closed under complement)

- $L_1 \cap L_2 = \overline{\overline{L_1} \cup \overline{L_2}}$ is a **regular language** (DeMorgan's law)

Boolean Algebra of Languages

Definition: Let a family of languages be closed under union, intersection, and complement. Then, this family represents a ***Boolean algebra of languages***.

Theorem: The family of regular languages is a Boolean algebra of languages.

Proof:

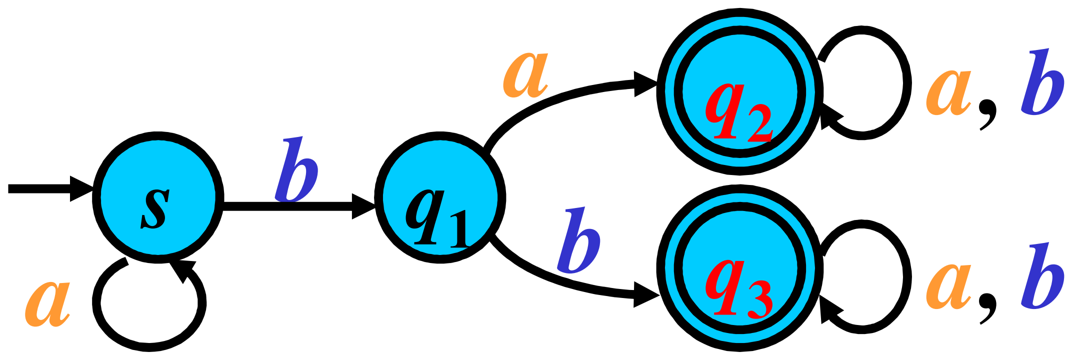
• The family of regular languages is closed under union, intersection, and complement.

Minimization: Distinguishable States

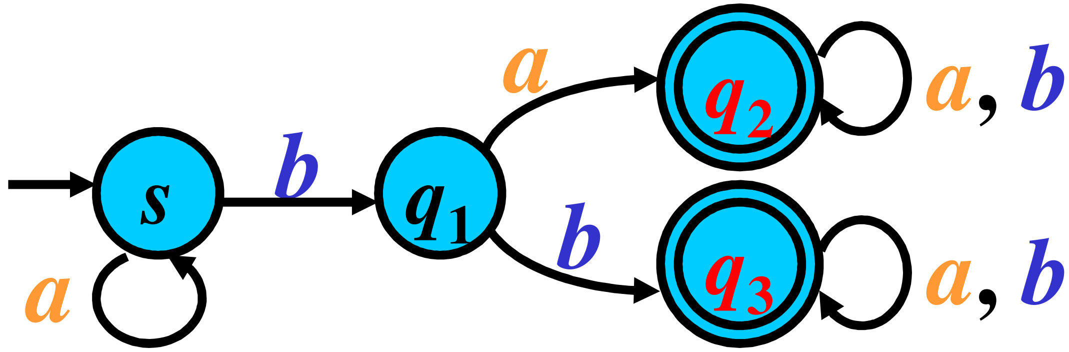
Gist: **String *w distinguishes* states *p* and *q* if WSFA reaches a final state from precisely one of configurations *pw* and *qw*.**

Definition: Let $M = (Q, \Sigma, R, s, F)$ be a WSFA, and let $p, q \in Q$, $p \neq q$. States p and q are *distinguishable* if there exists $w \in \Sigma^*$ such that: $pw \vdash^* p'$ and $qw \vdash^* q'$, where $p', q' \in Q$ and $((p' \in F$ and $q' \notin F)$ or $(p' \notin F$ and $q' \in F))$; otherwise, states p and q are *indistinguishable*

Distinguishable States: Example



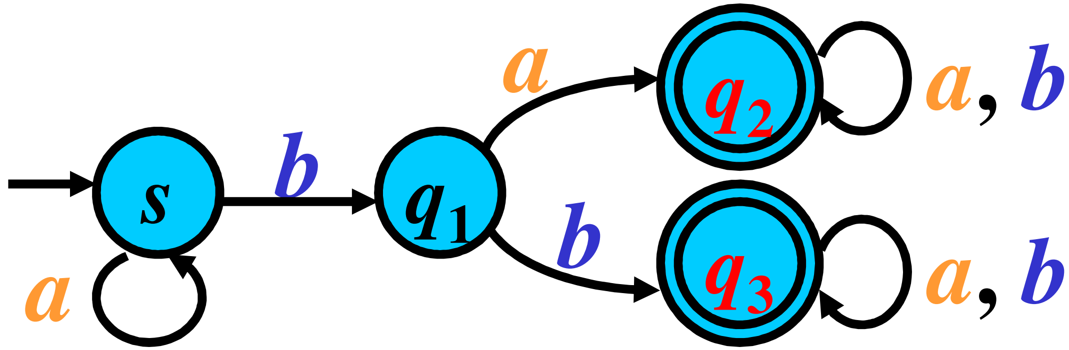
Distinguishable States: Example



- s and q_1 are **distinguishable**, because for $w = a$:

$$sa \vdash s \quad , s \quad \notin F$$
$$q_1 a \vdash q_2 , q_2 \in F$$

Distinguishable States: Example



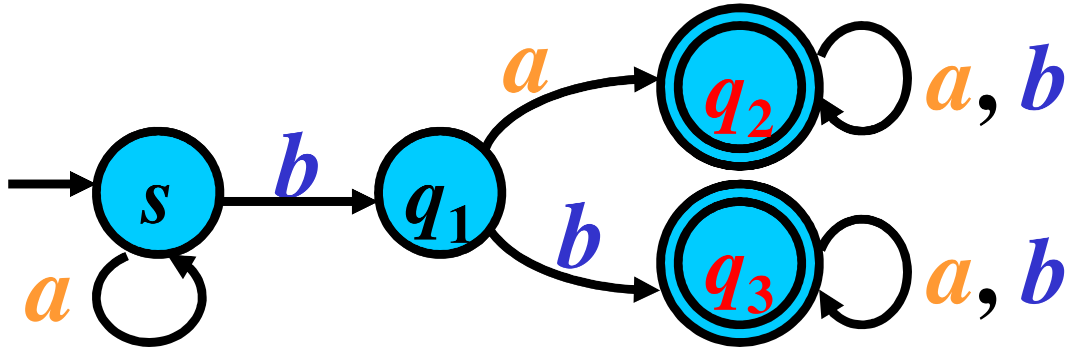
- s and q_1 are **distinguishable**, because for $w = a$:

$$sa \vdash s \ , s \notin F$$
$$q_1 a \vdash q_2 \, , q_2 \in F$$

- q_2 and q_3 are **indistinguishable**, because for each $w \in \Sigma^*$:

$$q_2 w \vdash^* q_2, q_2 \in F$$
$$q_3 w \vdash^* q_3, q_3 \in F$$

Distinguishable States: Example



- s and q_1 are **distinguishable**, because for $w = a$:

$$sa \vdash s \ , s \notin F$$
$$q_1a \vdash q_2 \, , q_2 \in F$$

- q_2 and q_3 are **indistinguishable**, because for each $w \in \Sigma^*$:

$$q_2w \vdash^* q_2, q_2 \in F$$
$$q_3w \vdash^* q_3, q_3 \in F$$

- Other pairs of states are trivially **distinguishable** for $w = \varepsilon$.

Minimum-State FA

Definition: Let M be a <u>**WSFA**</u>. Then, M is ***minimum-state FA*** if M contains only distinguishable states.

Theorem: For every WSFA M, there is an equivalent minimum-state FA M_m

Proof: Use the next algorithm.

Algorithm: WSFA to Min-State FA

- **Input:** WSFA $M = (Q, \Sigma, R, s, F)$
- **Output:** Minimum-State FA $M_m = (Q_m, \Sigma, R_m, s_m, F_m)$

- **Method:**
- $Q_m = \{\{p: p \in F\}, \{q: q \in Q - F\}\};$
- **repeat**

  if there exist $X \in Q_m,\ d \in \Sigma,\ X_1, X_2 \subset X$ such that

  $X = X_1 \cup X_2, X_1 \cap X_2 = \emptyset$ **and**

  $\{q_1: p_1 \in X_1, p_1d \rightarrow q_1 \in R\} \subseteq Q_1, Q_1 \in Q_m,$

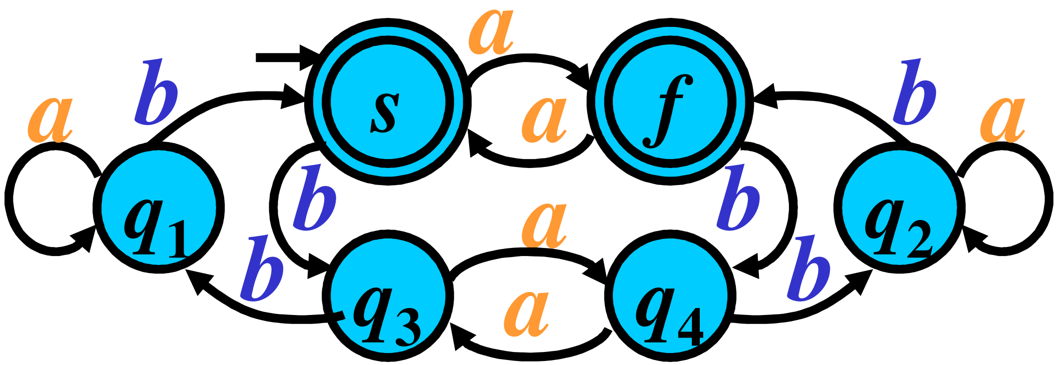
  $\{q_2: p_2 \in X_2, p_2d \rightarrow q_2 \in R\} \cap Q_1 = \emptyset$

  then divide X into X_1 and X_2 in Q_m

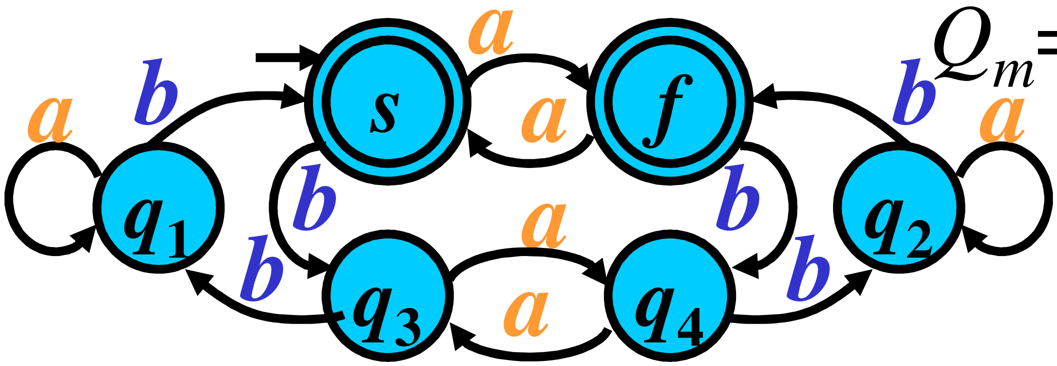
until no division is possible;

- $R_m = \{ Xa \rightarrow Y: X, Y \in Q_m, pa \rightarrow q \in R, p \in X, q \in Y, a \in \Sigma\};$
- $s_m = X$ with $s \in X$; $F_m := \{X: X \in Q_m, X \cap F \neq \emptyset\}.$

Minimization: Example 1/4

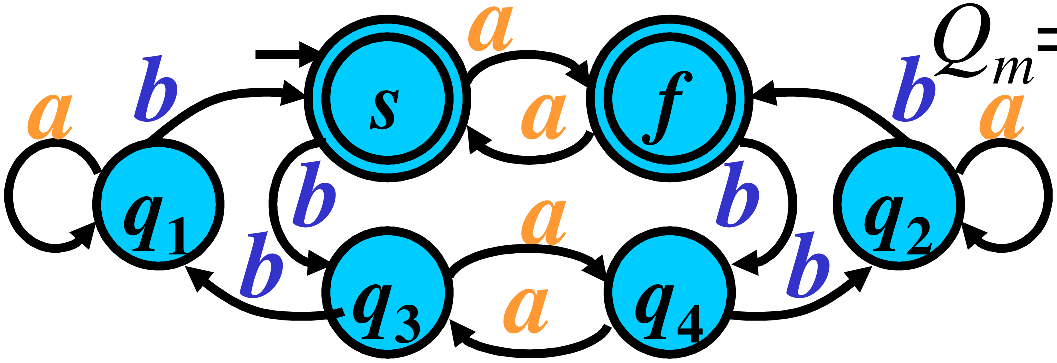


Minimization: Example 1/4



$$Q_m = \{\underbrace{\{s, f\}}_{\text{Final States}}, \underbrace{\{q_1, q_2, q_3, q_4\}}_{\text{Other States}}\}$$

Minimization: Example 1/4



$Q_m = \{\{s,f\},\ \{q_1,q_2,q_3,q_4\}\}$

Final States

Other States

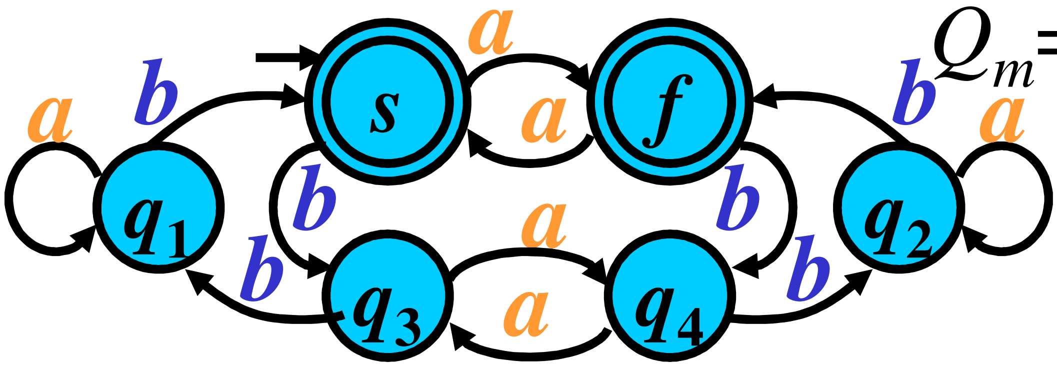
---

1) $X = \{s,f\}$:

$d = a$: $\quad sa \rightarrow f$

$\qquad\qquad fa \rightarrow s$

Minimization: Example 1/4



$Q_m = \{\underbrace{\{s, f\}}_{\text{Final States}}, \underbrace{\{q_1, q_2, q_3, q_4\}}_{\text{Other States}}\}$

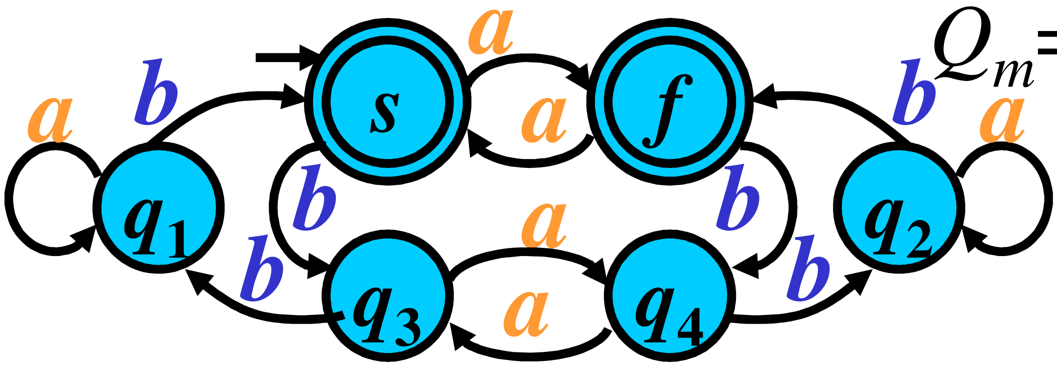
1) $X = \{s, f\}$:

From one set

$d = a$: $sa \rightarrow f$, $fa \rightarrow s$

$\boxed{\begin{matrix} f \\ s \end{matrix}}$

Minimization: Example 1/4



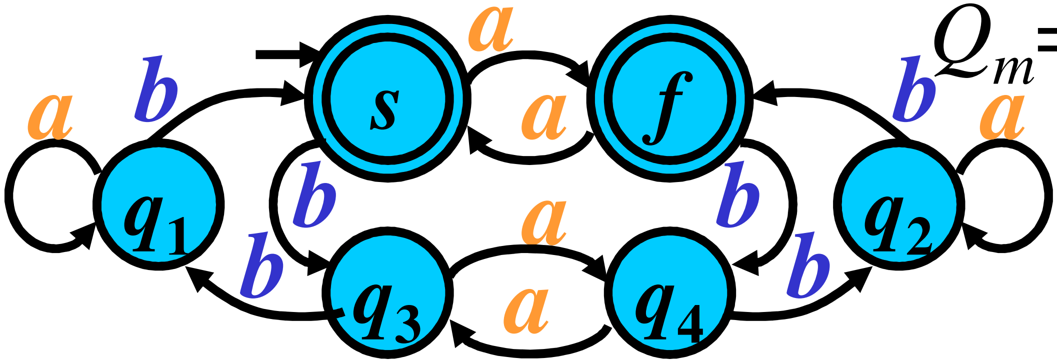
$Q_m = \{\underbrace{\{s, f\}}_{\text{Final States}}, \underbrace{\{q_1, q_2, q_3, q_4\}}_{\text{Other States}}\}$

1) $X = \{s, f\}$: **From one set**

$d = a$: $sa \to \boxed{f}$, $fa \to \boxed{s}$

$d = b$: $sb \to q_3$, $fb \to q_4$

Minimization: Example 1/4



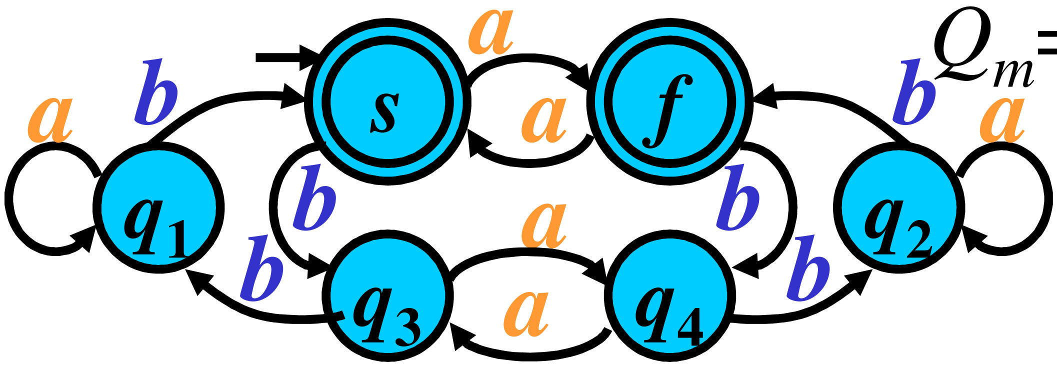
$Q_m = \{\underbrace{\{s,f\}}_{\text{Final States}}, \underbrace{\{q_1,q_2,q_3,q_4\}}_{\text{Other States}}\}$

1) $X = \{s,f\}$:

$d = a$: $sa \rightarrow f$, $fa \rightarrow s$ — From one set

$d = b$: $sb \rightarrow q_3$, $fb \rightarrow q_4$ — From one set

Minimization: Example 1/4



$Q_m = \{\{s,f\}, \{q_1,q_2,q_3,q_4\}\}$

$\underbrace{\{s,f\}}_{\text{Final States}}$, $\underbrace{\{q_1,q_2,q_3,q_4\}}_{\text{Other States}}$

1) $X = \{s,f\}$:

From one set

$d = a$: $sa \rightarrow f$, $fa \rightarrow s$

From one set

$d = b$: $sb \rightarrow q_3$, $fb \rightarrow q_4$

2) $X = \{q_1,q_2,q_3,q_4\}$:

$d = a$:

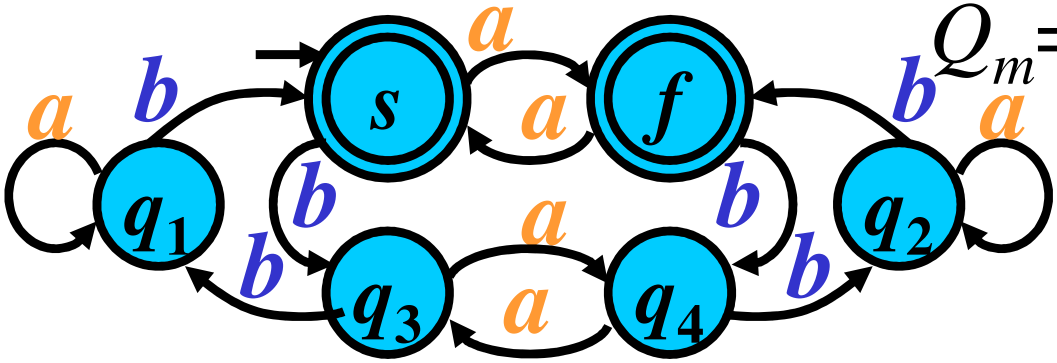
$q_1a \rightarrow q_1$

$q_2a \rightarrow q_2$

$q_3a \rightarrow q_4$

$q_4a \rightarrow q_3$

Minimization: Example 1/4



$$Q_m = \{\underbrace{\{s,f\}}_{\text{Final States}},\ \underbrace{\{q_1,q_2,q_3,q_4\}}_{\text{Other States}}\}$$

1) $X = \{s,f\}$:

From one set

$d = a$: $\quad sa \to f$, $\quad fa \to s$

From one set

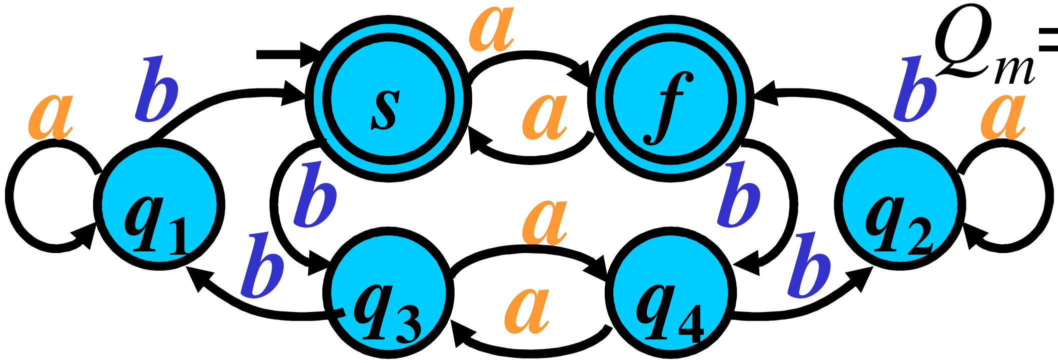
$d = b$: $\quad sb \to q_3$, $\quad fb \to q_4$

2) $X = \{q_1,q_2,q_3,q_4\}$:

From one set

$d = a$: $\quad q_1a \to q_1$, $\quad q_2a \to q_2$, $\quad q_3a \to q_4$, $\quad q_4a \to q_3$

Minimization: Example 1/4



$Q_m = \{\underbrace{\{s,f\}}_{\text{Final States}}, \underbrace{\{q_1,q_2,q_3,q_4\}}_{\text{Other States}}\}$

1) $X = \{s,f\}$:

From one set

$d = a$: $sa \rightarrow f$, $fa \rightarrow s$

From one set

$d = b$: $sb \rightarrow q_3$, $fb \rightarrow q_4$

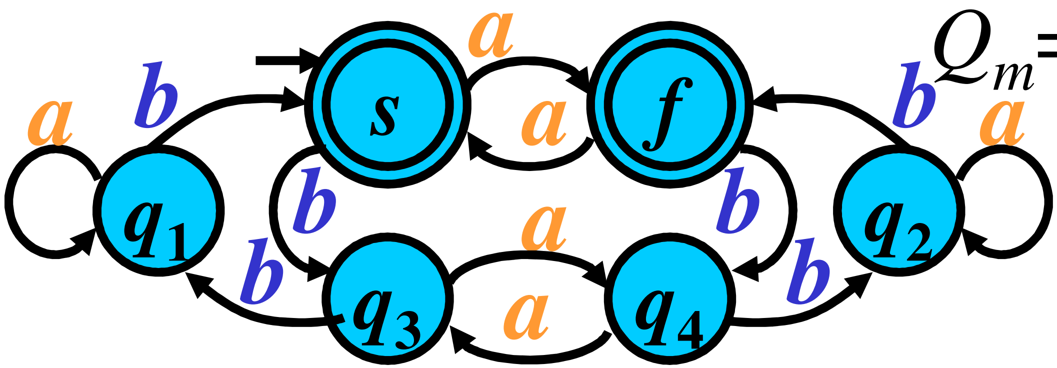
2) $X = \{q_1,q_2,q_3,q_4\}$:

From one set

$d = a$: $q_1a \rightarrow q_1$, $q_2a \rightarrow q_2$, $q_3a \rightarrow q_4$, $q_4a \rightarrow q_3$

$d = b$: $q_1b \rightarrow s$, $q_2b \rightarrow f$, $q_3b \rightarrow q_1$, $q_4b \rightarrow q_2$

Minimization: Example 1/4



$Q_m = \{\underbrace{\{s,f\}}_{\text{Final States}}, \underbrace{\{q_1,q_2,q_3,q_4\}}_{\text{Other States}}\}$

1) $X = \{s,f\}$:

From one set — $d = a$: $sa \rightarrow f$, $fa \rightarrow s$; $\boxed{f, s}$

From one set — $d = b$: $sb \rightarrow q_3$, $fb \rightarrow q_4$; $\boxed{q_3, q_4}$

2) $X = \{q_1,q_2,q_3,q_4\}$:

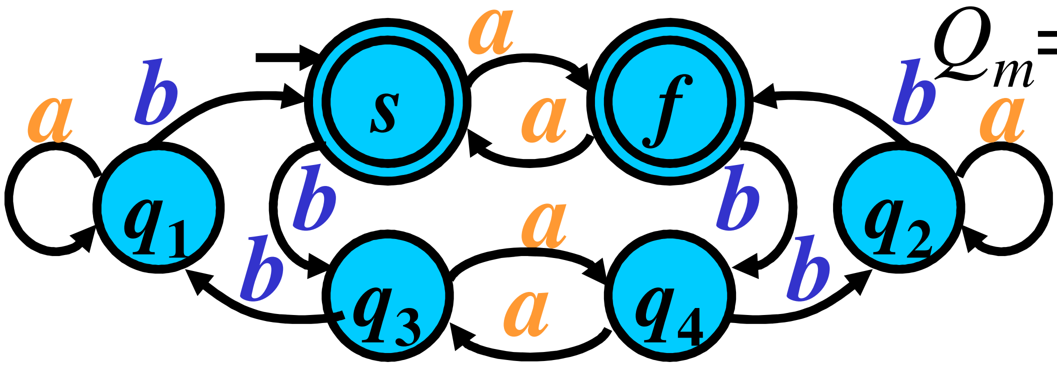
From one set — $d = a$: $q_1a \rightarrow q_1$, $q_2a \rightarrow q_2$, $q_3a \rightarrow q_4$, $q_4a \rightarrow q_3$; $\boxed{q_1, q_2, q_4, q_3}$

$d = b$: $q_1b \rightarrow s$, $q_2b \rightarrow f$; $\boxed{s, f} \subseteq Q_1 = \{s, f\}$

$q_3b \rightarrow q_1$

$q_4b \rightarrow q_2$

Minimization: Example 1/4



$Q_m = \{\underbrace{\{s,f\}}_{\text{Final States}}, \underbrace{\{q_1,q_2,q_3,q_4\}}_{\text{Other States}}\}$

---

1) $X = \{s,f\}$:

From one set $\qquad\qquad\qquad\qquad$ **From one set**

$d = a$: $\quad sa \to f$, $\quad fa \to s$ $\qquad\qquad$ $d = b$: $\quad sb \to q_3$, $\quad fb \to q_4$

---

2) $X = \{q_1,q_2,q_3,q_4\}$:

From one set

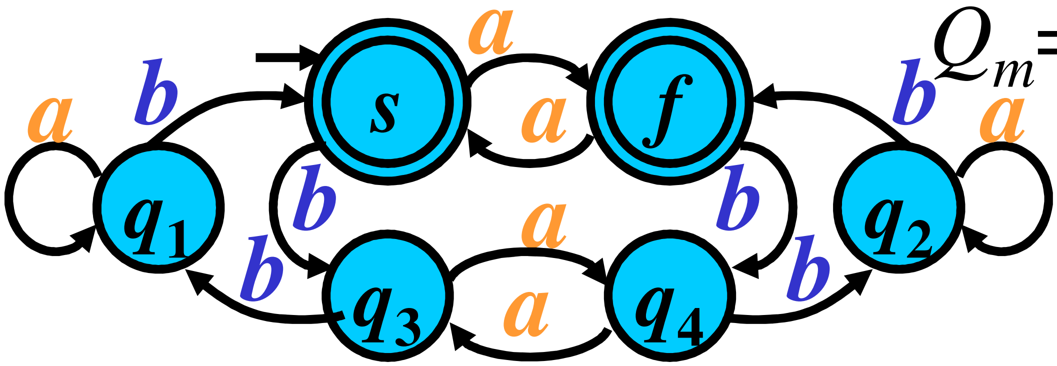
$d = a$: $\quad q_1a \to q_1$, $\quad q_2a \to q_2$, $\quad q_3a \to q_4$, $\quad q_4a \to q_3$

$d = b$: $\quad q_1b \to s$, $\quad q_2b \to f$, $\quad q_3b \to q_1$, $\quad q_4b \to q_2$

$\{s, f\} \subseteq Q_1 = \{s, f\}$

$\{q_1,q_2\} \cap Q_1 = \emptyset$

Minimization: Example 1/4



$$Q_m = \{\underbrace{\{s, f\}}_{\text{Final States}}, \underbrace{\{q_1, q_2, q_3, q_4\}}_{\text{Other States}}\}$$

1) $X = \{s, f\}$:

$d = a$: $\quad sa \rightarrow f, \quad fa \rightarrow s$ **From one set**

$d = b$: $\quad sb \rightarrow q_3, \quad fb \rightarrow q_4$ **From one set**

2) $X = \{q_1, q_2, q_3, q_4\}$:

$d = a$: $\quad q_1a \rightarrow q_1, \quad q_2a \rightarrow q_2, \quad q_3a \rightarrow q_4, \quad q_4a \rightarrow q_3$ **From one set**

$d = b$: $\quad q_1b \rightarrow s, \quad q_2b \rightarrow f$ $\quad \subseteq Q_1 = \{s, f\}$

$\quad q_3b \rightarrow q_1, \quad q_4b \rightarrow q_2$ $\quad \{q_1, q_2\} \cap Q_1 = \emptyset$

Division: $\{q_1, q_2, q_3, q_4\} \Rightarrow \underbrace{\{q_1, q_2\}}_{X_1}, \underbrace{\{q_3, q_4\}}_{X_2}$

Minimization: Example 2/4

$Q_m = \{\{s, f\}, \{q_1, q_2\}, \{q_3, q_4\}\}$

Minimization: Example 2/4

$Q_m = \{\{s, f\}, \{q_1, q_2\}, \{q_3, q_4\}\}$

---

1) $X = \{s, f\}$**:**

$d = a$**:** $sa \to f$
$fa \to s$

Minimization: Example 2/4

$Q_m = \{\{s, f\}, \{q_1, q_2\}, \{q_3, q_4\}\}$

---

1) $X = \{s, f\}$:

From one set

$d = a$: $sa \rightarrow \boxed{f}$

$fa \rightarrow \boxed{s}$

Minimization: Example 2/4

$Q_m = \{\{s, f\}, \{q_1, q_2\}, \{q_3, q_4\}\}$

1) $X = \{s, f\}$:

From one set

$d = a$: $sa \rightarrow f$, $fa \rightarrow s$

$d = b$: $sb \rightarrow q_3$, $fb \rightarrow q_4$

Minimization: Example 2/4

$Q_m = \{\{s, f\}, \{q_1, q_2\}, \{q_3, q_4\}\}$

---

1) $X = \{s, f\}$:

From one set

$d = a$: $sa \rightarrow f$, $fa \rightarrow s$

From one set

$d = b$: $sb \rightarrow q_3$, $fb \rightarrow q_4$

Minimization: Example 2/4

$Q_m = \{\{s, f\}, \{q_1, q_2\}, \{q_3, q_4\}\}$

---

1) $X = \{s, f\}$:

From one set

$d = a$: $sa \rightarrow f$, $fa \rightarrow s$

From one set

$d = b$: $sb \rightarrow q_3$, $fb \rightarrow q_4$

---

2) $X = \{q_1, q_2\}$:

$d = a$: $q_1a \rightarrow q_1$, $q_2a \rightarrow q_2$

Minimization: Example 2/4

$Q_m = \{\{s, f\}, \{q_1, q_2\}, \{q_3, q_4\}\}$

1) $X = \{s, f\}$:

From one set

$d = a$: $sa \rightarrow f$, $fa \rightarrow s$

From one set

$d = b$: $sb \rightarrow q_3$, $fb \rightarrow q_4$

2) $X = \{q_1, q_2\}$:

From one set

$d = a$: $q_1a \rightarrow q_1$, $q_2a \rightarrow q_2$

Minimization: Example 2/4

$Q_m = \{\{s, f\}, \{q_1, q_2\}, \{q_3, q_4\}\}$

---

1) $X = \{s, f\}$:

From one set

$d = a$: $sa \rightarrow f$, $fa \rightarrow s$

From one set

$d = b$: $sb \rightarrow q_3$, $fb \rightarrow q_4$

---

2) $X = \{q_1, q_2\}$:

From one set

$d = a$: $q_1a \rightarrow q_1$, $q_2a \rightarrow q_2$

$d = b$: $q_1b \rightarrow s$, $q_2b \rightarrow f$

Minimization: Example 2/4

$Q_m = \{\{s,f\}, \{q_1,q_2\}, \{q_3,q_4\}\}$

1) $X = \{s,f\}$:

From one set

$d = a$: $sa \to f$, $fa \to s$

From one set

$d = b$: $sb \to q_3$, $fb \to q_4$

2) $X = \{q_1,q_2\}$:

From one set

$d = a$: $q_1a \to q_1$, $q_2a \to q_2$

From one set

$d = b$: $q_1b \to s$, $q_2b \to f$

Minimization: Example 2/4

$Q_m = \{\{s,f\}, \{q_1,q_2\}, \{q_3,q_4\}\}$

---

1) $X = \{s,f\}$**:**

From one set

$d = a$: $sa \to f$, $fa \to s$ $\quad \boxed{f,\ s}$

From one set

$d = b$: $sb \to q_3$, $fb \to q_4$ $\quad \boxed{q_3,\ q_4}$

---

2) $X = \{q_1,q_2\}$**:**

From one set

$d = a$: $q_1a \to q_1$, $q_2a \to q_2$ $\quad \boxed{q_1,\ q_2}$

From one set

$d = b$: $q_1b \to s$, $q_2b \to f$ $\quad \boxed{s,\ f}$

---

3) $X = \{q_3,q_4\}$**:**

$d = a$: $q_3a \to q_3$, $q_4a \to q_4$

Minimization: Example 2/4

$Q_m = \{\{s, f\}, \{q_1, q_2\}, \{q_3, q_4\}\}$

1) $X = \{s, f\}$**:**

$d = a$: $sa \rightarrow f$, $fa \rightarrow s$ — **From one set**

$d = b$: $sb \rightarrow q_3$, $fb \rightarrow q_4$ — **From one set**

2) $X = \{q_1, q_2\}$**:**

$d = a$: $q_1a \rightarrow q_1$, $q_2a \rightarrow q_2$ — **From one set**

$d = b$: $q_1b \rightarrow s$, $q_2b \rightarrow f$ — **From one set**

3) $X = \{q_3, q_4\}$**:**

$d = a$: $q_3a \rightarrow q_3$, $q_4a \rightarrow q_4$ — **From one set**

Minimization: Example 2/4

$Q_m = \{\{s,f\}, \{q_1,q_2\}, \{q_3,q_4\}\}$

1) $X = \{s,f\}$:

$d = a$: $sa \to f$, $fa \to s$ — **From one set**

$d = b$: $sb \to q_3$, $fb \to q_4$ — **From one set**

2) $X = \{q_1,q_2\}$:

$d = a$: $q_1a \to q_1$, $q_2a \to q_2$ — **From one set**

$d = b$: $q_1b \to s$, $q_2b \to f$ — **From one set**

3) $X = \{q_3,q_4\}$:

$d = a$: $q_3a \to q_3$, $q_4a \to q_4$ — **From one set**

$d = b$: $q_3b \to q_1$, $q_4b \to q_2$

Minimization: Example 2/4

$Q_m = \{\{s,f\}, \{q_1,q_2\}, \{q_3,q_4\}\}$

1) $X = \{s,f\}$:

From one set

$d = a$: $sa \rightarrow \boxed{f}$, $fa \rightarrow \boxed{s}$

From one set

$d = b$: $sb \rightarrow \boxed{q_3}$, $fb \rightarrow \boxed{q_4}$

2) $X = \{q_1,q_2\}$:

From one set

$d = a$: $q_1a \rightarrow \boxed{q_1}$, $q_2a \rightarrow \boxed{q_2}$

From one set

$d = b$: $q_1b \rightarrow \boxed{s}$, $q_2b \rightarrow \boxed{f}$

3) $X = \{q_3,q_4\}$:

From one set

$d = a$: $q_3a \rightarrow \boxed{q_3}$, $q_4a \rightarrow \boxed{q_4}$

From one set

$d = b$: $q_3b \rightarrow \boxed{q_1}$, $q_4b \rightarrow \boxed{q_2}$

No next divisions !!!

Minimization: Example 3/4

$Q_m = \{\{s, f\}, \{q_1, q_2\}, \{q_3, q_4\}\}$

$$\left.\begin{array}{l} sa \rightarrow f \in R; \\ fa \rightarrow s \in R; \end{array}\right\} \Longrightarrow \{s, f\}a \rightarrow \{s, f\} \in R_m$$

$$\left.\begin{array}{l} sb \rightarrow q_3 \in R; \\ fb \rightarrow q_4 \in R; \end{array}\right\} \Longrightarrow \{s, f\}b \rightarrow \{q_3, q_4\} \in R_m$$

$$\left.\begin{array}{l} q_1a \rightarrow q_1 \in R; \\ q_2a \rightarrow q_2 \in R; \end{array}\right\} \Longrightarrow \{q_1, q_2\}a \rightarrow \{q_1, q_2\} \in R_m$$

$$\left.\begin{array}{l} q_1b \rightarrow s \in R; \\ q_2b \rightarrow f \in R; \end{array}\right\} \Longrightarrow \{q_1, q_2\}b \rightarrow \{s, f\} \in R_m$$

$$\left.\begin{array}{l} q_3a \rightarrow q_3 \in R; \\ q_4a \rightarrow q_4 \in R; \end{array}\right\} \Longrightarrow \{q_3, q_4\}a \rightarrow \{q_3, q_4\} \in R_m$$

$$\left.\begin{array}{l} q_3b \rightarrow q_1 \in R; \\ q_4b \rightarrow q_2 \in R; \end{array}\right\} \Longrightarrow \{q_3, q_4\}b \rightarrow \{q_1, q_2\} \in R_m$$

Minimization: Example 4/4

$s \in \{s,f\} \Rightarrow s_m := \{s,f\}$

$\left.\begin{array}{l} s \in F: \\ f \in F: \end{array}\right\} \Rightarrow \{s,f\} \in F_m$

$M_m = (Q_m, \Sigma, R_m, s_m, F_m)$, where: $\Sigma = \{a, b\}$, $s_m = \{s,f\}$
$Q_m = \{\{s,f\}, \{q_1,q_2\}, \{q_3,q_4\}\}$, $F_m = \{\{s,f\}\}$
$R_m = \{\{s,f\}a \rightarrow \{s,f\}, \{s,f\}b \rightarrow \{q_3,q_4\}, \{q_1,q_2\}a \rightarrow \{q_1,q_2\},$
$\{q_1,q_2\}b \rightarrow \{s,f\}, \{q_3,q_4\}a \rightarrow \{q_3,q_4\}, \{q_3,q_4\}b \rightarrow \{q_1,q_2\}\}$

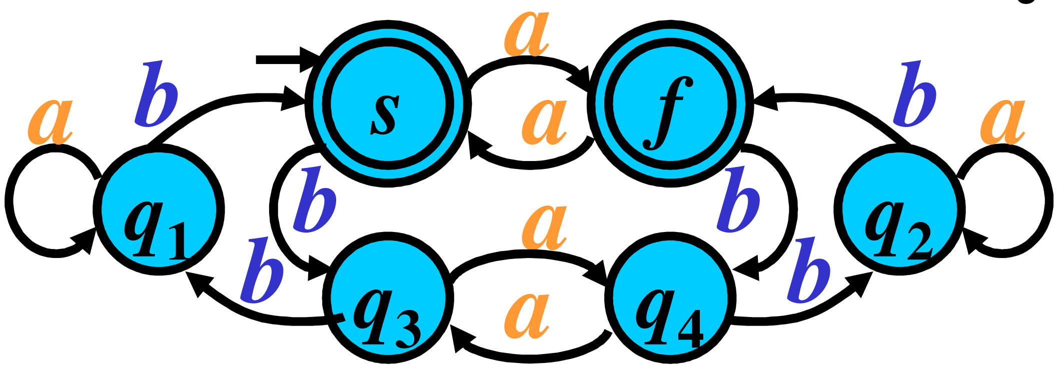
Minimization: Example 4/4

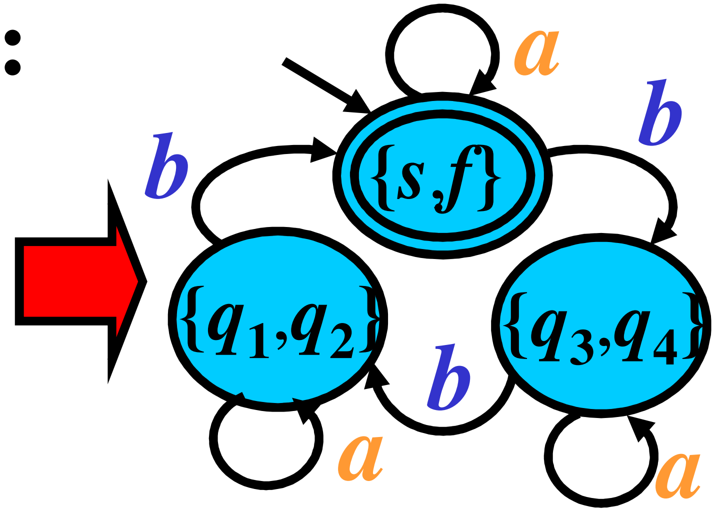
$s \in \{s,f\} \Rightarrow s_m := \{s,f\}$

$\left.\begin{array}{l} s \in F: \\ f \in F: \end{array}\right\} \Rightarrow \{s,f\} \in F_m$

$M_m = (Q_m, \Sigma, R_m, s_m, F_m)$, where: $\Sigma = \{a, b\}$, $s_m = \{s,f\}$
$Q_m = \{\{s,f\}, \{q_1,q_2\}, \{q_3,q_4\}\}$, $F_m = \{\{s,f\}\}$
$R_m = \{\{s,f\}a \rightarrow \{s,f\}, \{s,f\}b \rightarrow \{q_3,q_4\}, \{q_1,q_2\}a \rightarrow \{q_1,q_2\},$
$\{q_1,q_2\}b \rightarrow \{s,f\}, \{q_3,q_4\}a \rightarrow \{q_3,q_4\}, \{q_3,q_4\}b \rightarrow \{q_1,q_2\}\}$

Summary:





Variants of FA: Summary

	FA	ε-free FA	DFA	Complete FA	WSFA	Min-State FA
Number of rules of the form $p \rightarrow q$, where $p, q \in Q$	**0-*n***	**0**	**0**	**0**	**0**	**0**
Number of rules of the form $pa \rightarrow q$, for any $p \in Q$, $a \in \Sigma$	**0-*n***	**0-*n***	**0-1**	**1**	**1**	**1**
Number of inaccessible states	**0-*n***	**0-*n***	**0-*n***	**0-*n***	**0**	**0**
Number of nonterminating states	**0-*n***	**0-*n***	**0-*n***	**0-*n***	**0-1**	**0-1**
Number of this FAs for any regular language.	∞	∞	∞	∞	∞	**1**

Main Decidable Problems

1. Membership problem:

- **Instance:** FA M, $w \in \Sigma^*$; **Question:** $w \in L(M)$?

2. Emptiness problem:

- **Instance:** FA M; **Question:** $L(M) = \emptyset$?

3. Finiteness problem:

- **Instance:** FA M; **Question:** Is $L(M)$ finite?

4. Equivalence problem:

- **Instance:** FA M_1, M_2; **Question:** $L(M_1) = L(M_2)$?

Algorithm: Membership Problem

- **Input:** DFA $M = (Q, \Sigma, R, s, F)$; $w \in \Sigma^*$
- **Output:** **YES** if $w \in L(M)$

  NO if $w \notin L(M)$

- **Method:**
- **if** $sw \vdash^* f,\ f \in F$ **then** write ('**YES**')

  else write ('**NO**')

Summary:

The membership problem for FAs is decidable

Algorithm: Emptiness Problem

- **Input:** FA $M = (Q, \Sigma, R, s, F)$;
- **Output:** **YES** if $L(M) = \emptyset$
  NO if $L(M) \neq \emptyset$

- **Method:**
- **if** s is nonterminating **then** write ('**YES**')
  else write ('**NO**')

Summary:

The emptiness problem for FAs is decidable

Algorithm: Finiteness Problem

- **Input:** DFA $M = (Q, \Sigma, R, s, F)$;
- **Output:** **YES** if $L(M)$ is finite
  NO if $L(M)$ is infinite

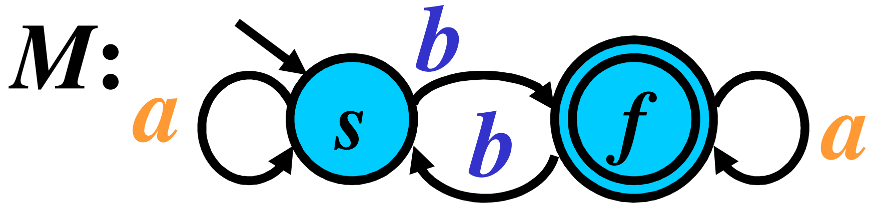
- **Method:**
- Let $k = \text{card}(Q)$
- **if** there exist $z \in L(M)$, $k \leq |z| < 2k$ **then** write ('**NO**')
  else write ('**YES**')

Note: This algorithm is based on
$L(M)$ is infinite $\Leftrightarrow$ there exists z: $z \in L(M)$, $k \leq |z| < 2k$

Summary:

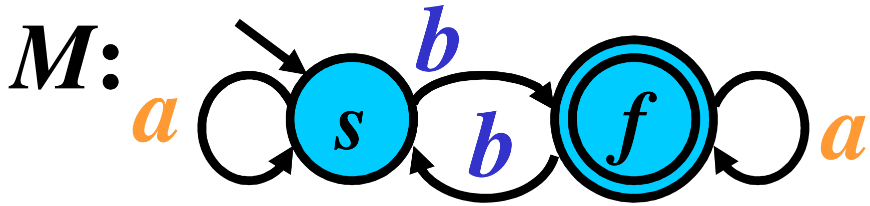
The finiteness problem for FAs is decidable

Decidable Problems: Example



Question: $ab \in L(M)$?

Decidable Problems: Example

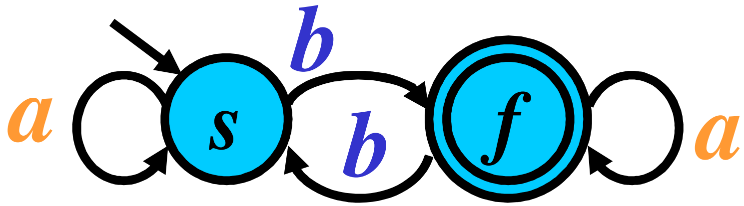


Question: $ab \in L(M)$?

$sab \vdash sb \vdash f, f \in F$

Decidable Problems: Example

M:



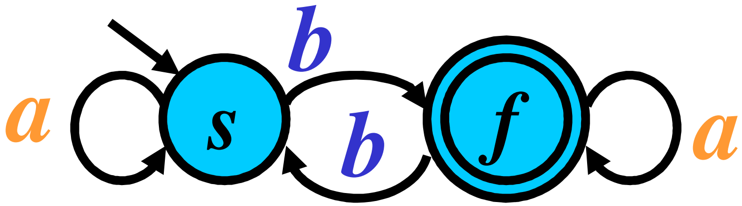
Question: $ab \in L(M)$?

$sab \vdash sb \vdash f, f \in F$

Answer: **YES** because $sab \vdash^* f, f \in F$

Decidable Problems: Example

***M*:**



Question: $ab \in L(M)$ **?**

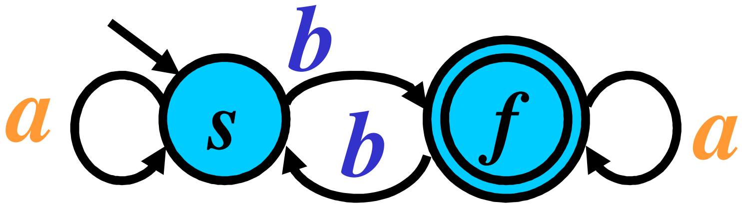
$sab \vdash sb \vdash f, f \in F$

Answer: YES because $sab \vdash^* f, f \in F$

Question: $L(M) = \varnothing$ **?**

Decidable Problems: Example

***M*:**



Question: $ab \in L(M)$ **?**

$sab \vdash sb \vdash f, f \in F$

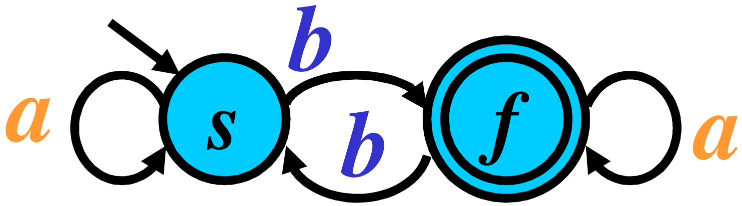
Answer: YES because $sab \vdash^* f, f \in F$

Question: $L(M) = \emptyset$ **?**

$Q_0 = \{f\}$

Decidable Problems: Example

M:



Question: $ab \in L(M)$ **?**

$sab \vdash sb \vdash f, f \in F$

Answer: YES because $sab \vdash^* f, f \in F$

Question: $L(M) = \emptyset$ **?**

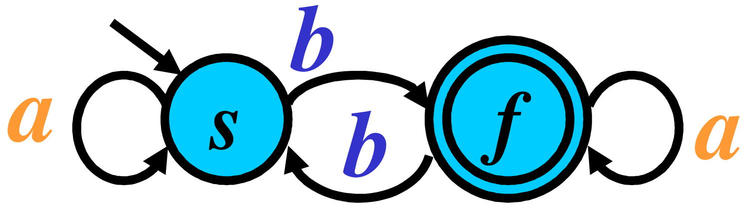
$Q_0 = \{f\}$

1. $qa' \rightarrow f$; $q \in Q$; $a' \in \Sigma$: $sb \rightarrow f, fa \rightarrow f$

$Q_1 = \{f\} \cup \{s, f\} = \{f, s\}$ … s is terminating

Decidable Problems: Example

***M*:**



Question: $ab \in L(M)$ **?**

$sab \vdash sb \vdash f, f \in F$

Answer: YES because $sab \vdash^* f, f \in F$

Question: $L(M) = \emptyset$ **?**

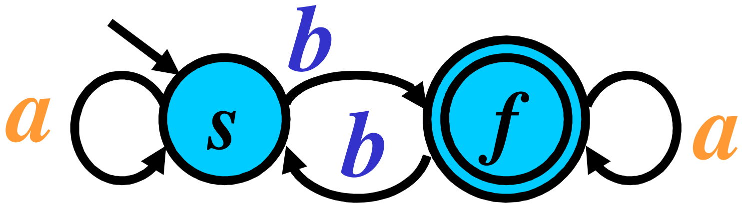
$Q_0 = \{f\}$

1. $qa' \rightarrow f$; $q \in Q$; $a' \in \Sigma$: $sb \rightarrow f, fa \rightarrow f$

$Q_1 = \{f\} \cup \{s, f\} = \{f, s\}$ … ***s*** is terminating

Answer: NO because ***s*** is terminating

Decidable Problems: Example

M: 

Question: $ab \in L(M)$?

$sab \vdash sb \vdash f, f \in F$

Answer: YES because $sab \vdash^* f, f \in F$

Question: $L(M) = \varnothing$?

$Q_0 = \{f\}$

1. $qa' \rightarrow f$; $q \in Q$; $a' \in \Sigma$: $sb \rightarrow f, fa \rightarrow f$

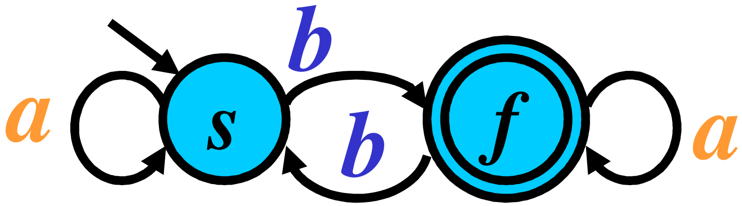
$Q_1 = \{f\} \cup \{s, f\} = \{f, s\}$ … s is terminating

Answer: NO because s is terminating

Question: Is $L(M)$ finite?

Decidable Problems: Example

***M*:**



Question: $ab \in L(M)$ **?**

$sab \vdash sb \vdash f, f \in F$

Answer: YES because $sab \vdash^{*} f, f \in F$

Question: $L(M) = \emptyset$ **?**

$Q_0 = \{f\}$

1. $qa' \rightarrow f$; $q \in Q$; $a' \in \Sigma$: $sb \rightarrow f, fa \rightarrow f$

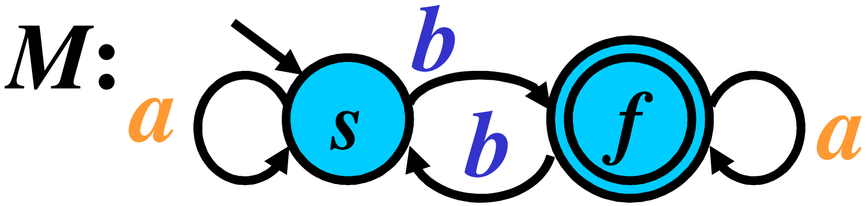
$Q_1 = \{f\} \cup \{s, f\} = \{f, s\}$ … s is terminating

Answer: NO because s is terminating

Question: Is $L(M)$ finite? $k = \text{card}(Q) = 2$

All strings $z \in \Sigma^*$: $2 \leq |z| < 4$: aa, bb, ab, ...

Decidable Problems: Example



Question: $ab \in L(M)$?

$sab \vdash sb \vdash f, f \in F$

Answer: YES because $sab \vdash^* f, f \in F$

Question: $L(M) = \varnothing$?

$Q_0 = \{f\}$

1. $qa' \rightarrow f$; $q \in Q$; $a' \in \Sigma$: $sb \rightarrow f, fa \rightarrow f$

$Q_1 = \{f\} \cup \{s, f\} = \{f, s\}$ **…** s is terminating

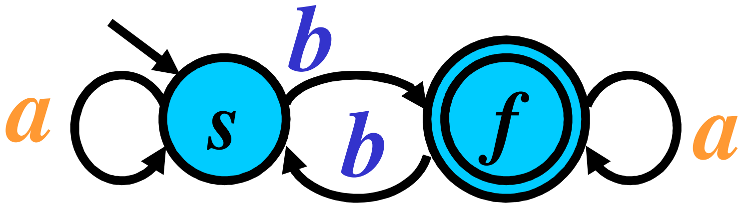
Answer: NO because s is terminating

Question: Is $L(M)$ finite? $k = \text{card}(Q) = 2$

All strings $z \in \Sigma^*$: $2 \leq |z| < 4$: aa, bb, $\boxed{ab \in L(M)}$, …

Decidable Problems: Example

***M*:**



Question: $ab \in L(M)$?

$sab \vdash sb \vdash f, f \in F$

Answer: YES because $sab \vdash^* f, f \in F$

Question: $L(M) = \emptyset$?

$Q_0 = \{f\}$

1. $qa' \rightarrow f$; $q \in Q$; $a' \in \Sigma$: $sb \rightarrow f, fa \rightarrow f$

$Q_1 = \{f\} \cup \{s, f\} = \{f, s\}$ **…** s is terminating

Answer: NO because s is terminating

Question: Is $L(M)$ finite? $k = \text{card}(Q) = 2$

All strings $z \in \Sigma^*$: $2 \leq |z| < 4$: aa, bb, $\boxed{ab \in L(M)}$, **…**

Answer: NO because there exist $z \in L(M)$, $k \leq |z| < 2k$

Algorithm: Equivalence Problem

- **Input:** Two minimum state FA, M_1 and M_2
- **Output:** **YES** if $L(M_1) = L(M_2)$

  NO if $L(M_1) \neq L(M_2)$

- **Method:**
- **if** M_1 coincides with M_2 except for the name of states

  then write ('**YES**')

  else write ('**NO**')

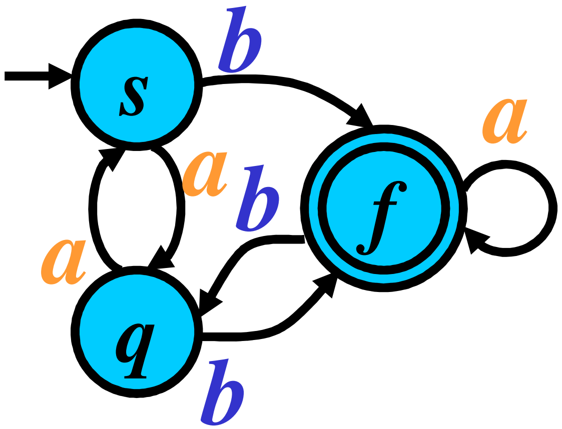
Summary:

The equivalence problem for FA is decidable

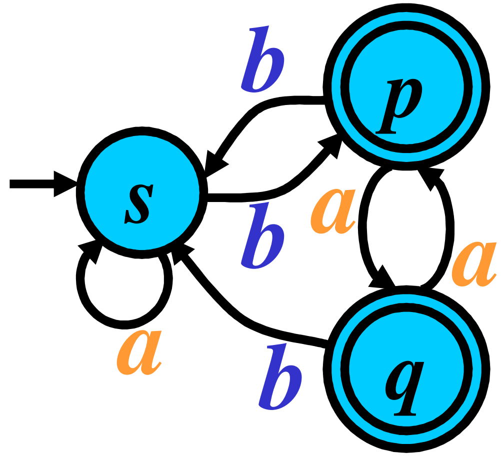
Equivalence Problem: Example

Question: $L(M_1) = L(M_2)$?

M_1:



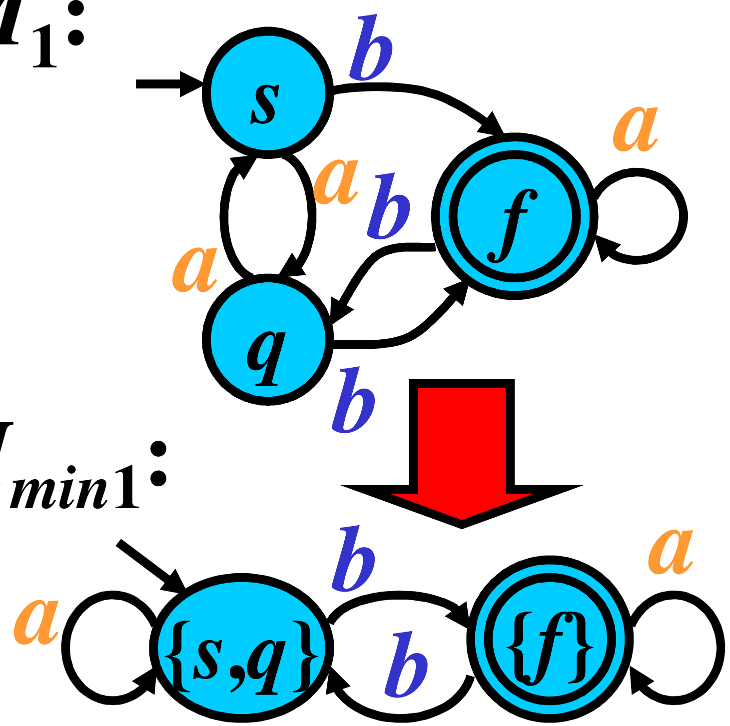
M_2:



Equivalence Problem: Example

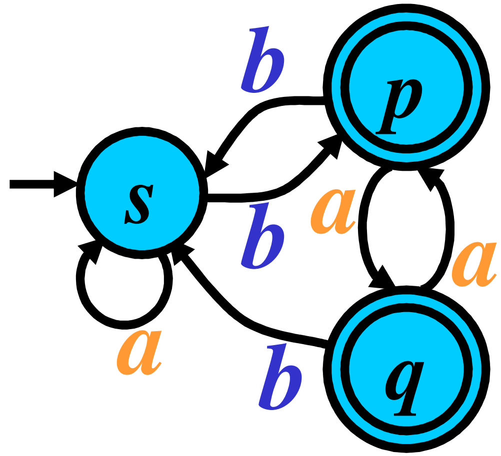
Question: $L(M_1) = L(M_2)$?

M_1:



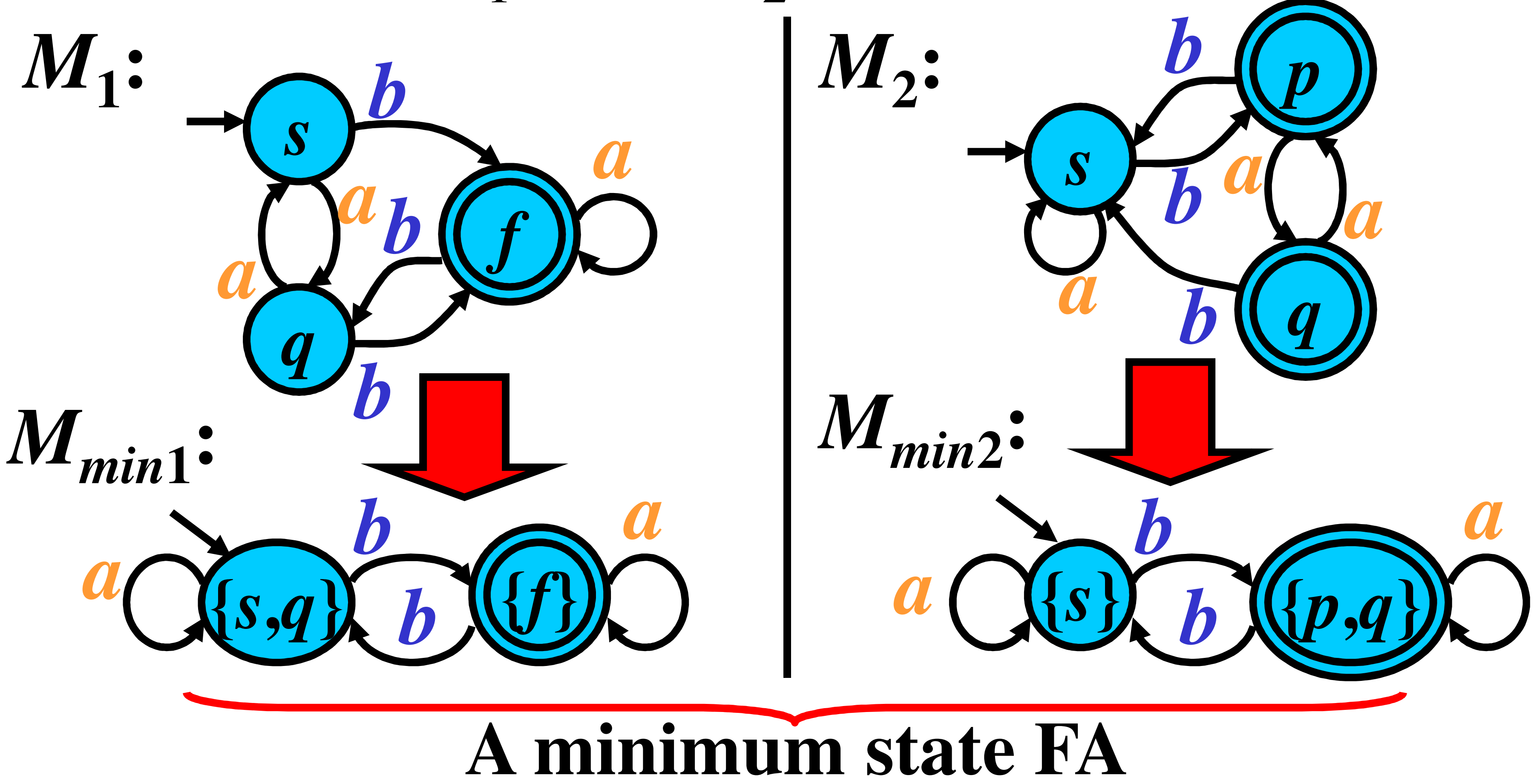
M_{min1}:

M_2:



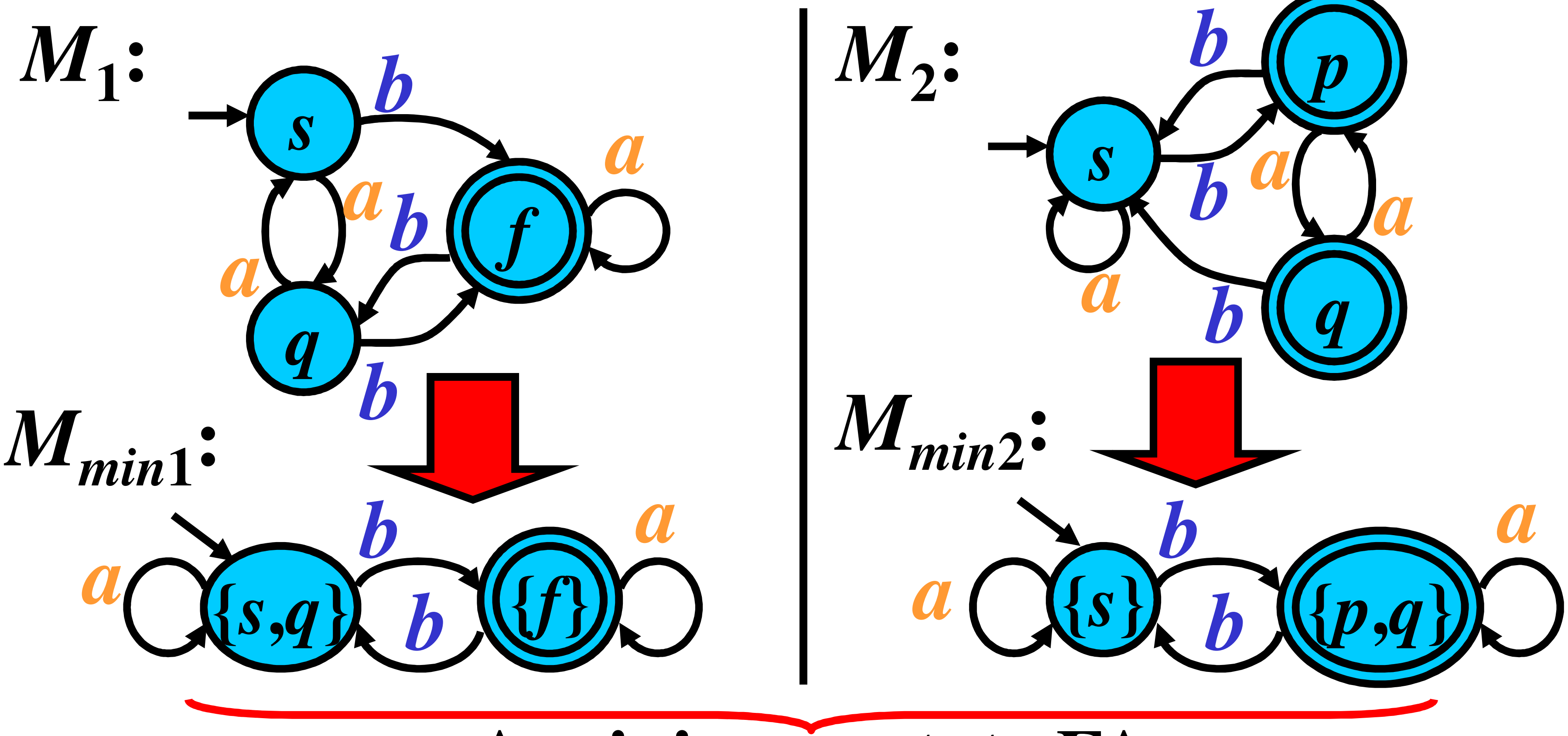
Equivalence Problem: Example

Question: $L(M_1) = L(M_2)$?



Equivalence Problem: Example

Question: $L(M_1) = L(M_2)$?



A minimum state FA

Answer: **YES** because M_{min1} coincides with M_{min2}