CMPE 322/327 - Theory of Computation
Week 5: State Minimization & Myhill-Nerode Relations

Burak Ekici

March 21-25, 2022

Outline

1. A Quick Recap
2. State Minimization
3. Myhill-Nerode Relations

Definition

regular expressions are restricted patterns which use only

$$\boldsymbol{a} \in \Sigma \quad \boldsymbol{\varepsilon} \quad \boldsymbol{\varnothing} \quad \alpha + \beta \quad \alpha^* \quad \alpha\beta$$

Theorem

finite automata, patterns, and regular expressions are equivalent:

for all $A \subseteq \Sigma^*$ ➀ A is regular

$\iff$ ➁ $A = L(\alpha)$ for some pattern α

$\iff$ ➂ $A = L(\alpha)$ for some regular expression α

Proof.

➂ $\Longrightarrow$ ➁ trivial (every regular expression is a pattern)

➁ $\Longrightarrow$ ➀ induction on α

➀ $\Longrightarrow$ ➂

Theorem

regular sets are effectively closed under homomorphic image and preimage

Proof.

- DFA $M = (Q, \Gamma, \delta, s, F)$
- homomorphism $h \colon \Sigma^* \to \Gamma^*$
- $h^{-1}(L(M)) = L(M')$ for DFA $M' = (Q, \Sigma, \delta', s, F)$ with $\delta'(q, a) := \widehat{\delta}(q, h(a))$

Theorem

regular sets are effectively closed under homomorphic image and preimage

Proof.

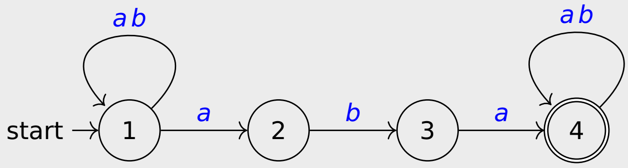
- regular expression α over Σ
- homomorphism $h\colon \Sigma^* \to \Gamma^*$
- $h(L(\alpha)) = L(\alpha')$ for regular expression α' defined inductively:

$$\begin{aligned} \mathbf{a}' &= h(\mathbf{a}) \quad \text{for } \mathbf{a} \in \Sigma & \qquad (\beta+\gamma)' &= \beta' + \gamma' \\ \boldsymbol{\varepsilon}' &= \boldsymbol{\varepsilon} & (\beta\gamma)' &= \beta'\gamma' \\ \boldsymbol{\varnothing}' &= \boldsymbol{\varnothing} & (\beta^*)' &= (\beta')^* \end{aligned}$$

Outline

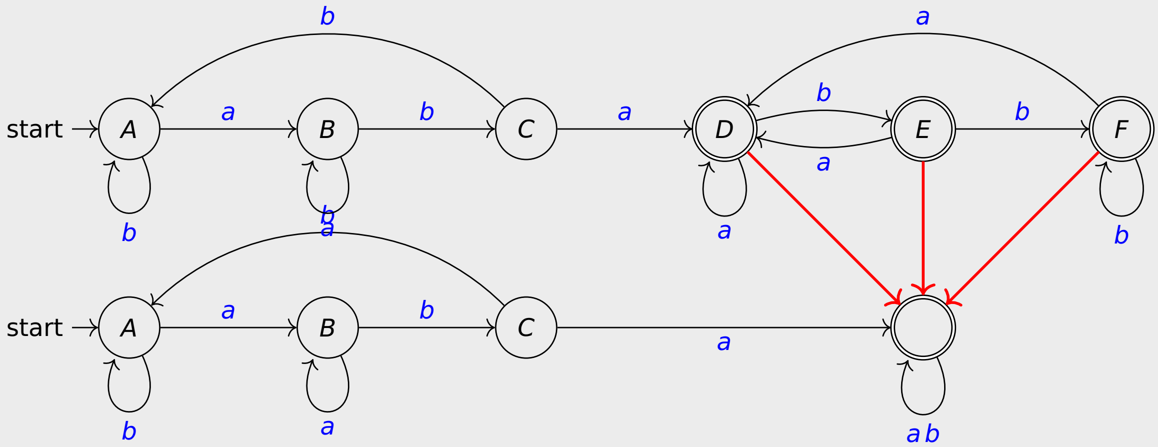
Example

NFA



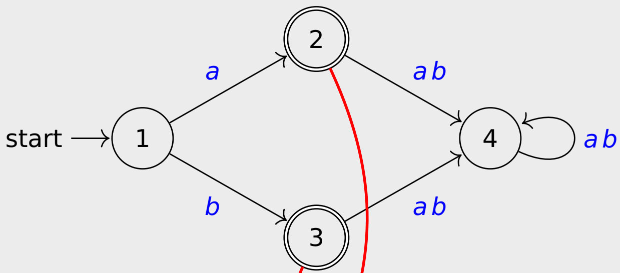
A = {1}   C = {1,3}   E = {1,3,4}
B = {1,2} D = {1,2,4} F = {1,4}

DFA

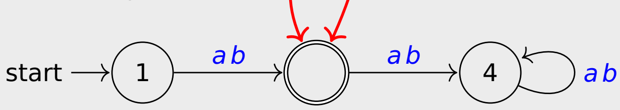


Example

DFA

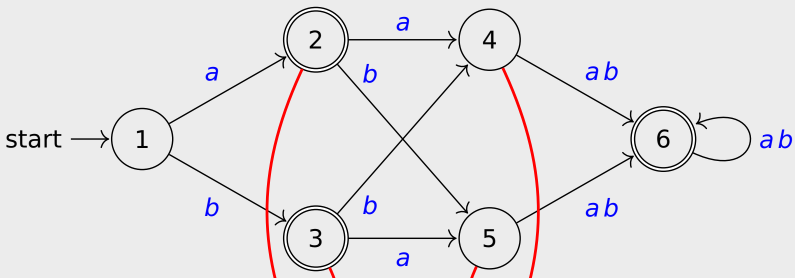


not minimal: states 2 and 3 can be collapsed

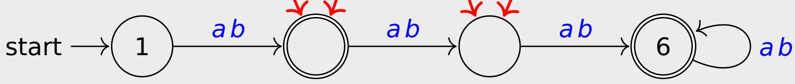


Example

DFA



not minimal: states 2 and 3 and states 4 and 5 can be collapsed



Definitions

DFA $M = (Q, \Sigma, \delta, s, F)$

- state p is inaccessible if $\widehat{\delta}(s, x) \neq p$ for all $x \in \Sigma^*$
- states p and q are distinguishable if

$$\exists x \in \Sigma^*, (\widehat{\delta}(p, x) \in F \wedge \widehat{\delta}(q, x) \notin F) \vee (\widehat{\delta}(p, x) \notin F \wedge \widehat{\delta}(q, x) \in F)$$

Minimization Algorithm

DFA $M = (Q, \Sigma, \delta, s, F)$

1. remove inaccessible states
2. for every two different states, determine whether they are distinguishable (marking)
3. collapse indistinguishable states

Marking Algorithm

given DFA $M = (Q, \Sigma, \delta, s, F)$ without inaccessible states

1. tabulate all unordered pairs $\{p, q\}$ with $p, q \in Q$, initially unmarked
2. mark $\{p, q\}$ if $p \in F$ and $q \notin F$ or vice versa
3. repeat until no change:

$$\text{mark } \{p, q\} \text{ if } \{\delta(p, a), \delta(q, a)\} \text{ is marked for some } a \in \Sigma$$

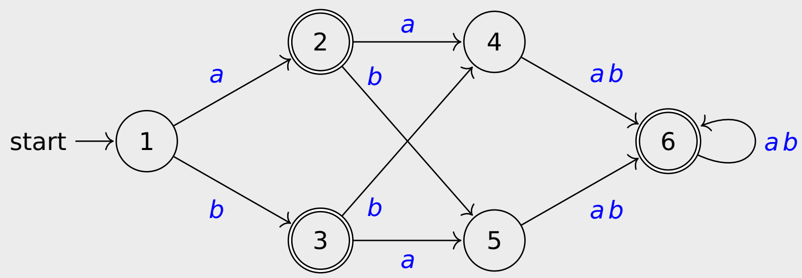
Notation

$p \approx q \quad \Longleftrightarrow \quad$ states p and q are indistinguishable

Lemma

$p \approx q \quad \Longleftrightarrow \quad \{p, q\}$ is unmarked

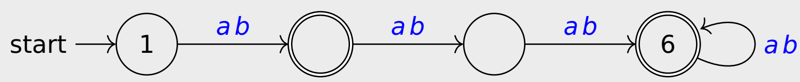
Example



1					
✓	2				
✓		3			
✓	✓	✓	4		
✓	✓	✓		5	
✓	✓	✓	✓	✓	6

1. final/non-final states are distinguishable
2. $\{2, 6\} \xrightarrow{a} \{4, 6\} \quad \{3, 6\} \xrightarrow{a} \{5, 6\}$
3. $\{1, 4\} \xrightarrow{a} \{2, 6\} \quad \{1, 5\} \xrightarrow{a} \{2, 6\}$

collapse states 2 and 3 and states 4 and 5:



Definition

states p and q of DFA $M = (Q, \Sigma, \delta, s, F)$ are indistinguishable ($p \approx q$) if

$$\forall x \in \Sigma^*, \widehat{\delta}(p, x) \in F \iff \widehat{\delta}(q, x) \in F$$

Lemma

$\approx$ is equivalence relation on Q

1. $\forall p \in Q \quad p \approx p$ (reflexivity)
2. $\forall p, q \in Q \quad p \approx q \implies q \approx p$ (symmetry)
3. $\forall p, q, r \in Q \quad p \approx q \wedge q \approx r \implies p \approx r$ (transitivity)

Notation

$[p]_\approx := \{q \in Q \mid p \approx q\}$ denotes equivalence class of p

Definition (Collapsing Indistinguishable States)

DFA $M/\approx$ is defined as $(Q', \Sigma, \delta', s', F')$ with

- $Q' := \{[p]_\approx \mid p \in Q\}$
- $\delta'([p]_\approx, a) := [\delta(p, a)]_\approx$ well defined: $p \approx q \implies \delta(p, a) \approx \delta(q, a)$
- $s' := [s]_\approx$
- $F' := \{[p]_\approx \mid p \in F\}$

Lemma

1. $\widehat{\delta'}([p]_\approx, x) = [\widehat{\delta}(p, x)]_\approx$ for all $x \in \Sigma^*$
2. $p \in F \iff [p]_\approx \in F'$

for all $p \in Q$

Theorem

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

Proof.

$$
\begin{aligned}
x \in L(M/\approx) &\iff \widehat{\delta'}([s]_\approx, x) \in F' \\
&\iff [\widehat{\delta}(s, x)]_\approx \in F' \\
&\iff \widehat{\delta}(s, x) \in F \\
&\iff x \in L(M)
\end{aligned}
$$

Question

is $M/\approx$ minimum-state DFA for $L(M)$?

Lemma

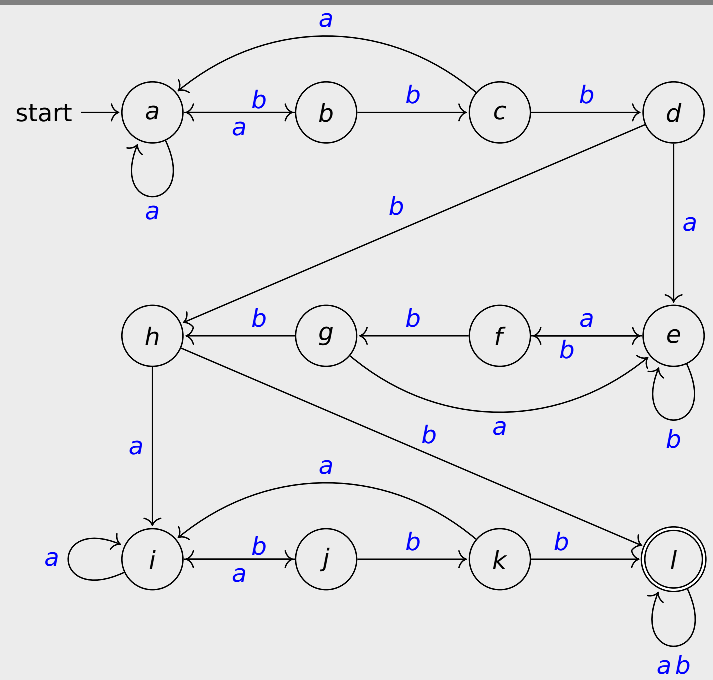
$M/\approx$ cannot be collapsed further

Proof.

$$
\begin{aligned}
[p]_\approx \approx [q]_\approx &\iff \forall x \in \Sigma^* \quad (\widehat{\delta'}([p]_\approx, x) \in F' \iff \widehat{\delta'}([q]_\approx, x) \in F') \\
&\iff \forall x \in \Sigma^* \quad ([\widehat{\delta}(p, x)]_\approx \in F' \iff [\widehat{\delta}(q, x)]_\approx \in F') \\
&\iff \forall x \in \Sigma^* \quad (\widehat{\delta}(p, x) \in F \iff \widehat{\delta}(q, x) \in F) \\
&\iff \forall x \in \Sigma^* \quad p \approx q \\
&\iff \forall x \in \Sigma^* \quad [p]_\approx = [q]_\approx
\end{aligned}
$$

□

Example



	a	b	c	d	e	f	g	h	i	j	k
b	✓										
c	✓	✓									
d	✓	✓	✓								
e	✓	✓	✓	✓							
f	✓	✓	✓	✓	✓						
g	✓	✓	✓		✓	✓					
h	✓	✓	✓	✓	✓	✓	✓				
i	✓	✓	✓	✓	✓	✓	✓	✓			
j	✓	✓	✓	✓	✓	✓	✓	✓	✓		
k	✓	✓	✓	✓	✓	✓	✓		✓	✓	
l	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

states d, g and h, k can be merged

Outline

Definition

Myhill-Nerode relation $\equiv$ for $L \subseteq \Sigma^*$ is an equivalence relation that

- is right congruent: $\forall x, y \in \Sigma^* \quad x \equiv y \implies \forall a \in \Sigma \quad xa \equiv ya$
- refines L: $\forall x, y \in \Sigma^* \quad x \equiv y \implies$ either $x, y \in L$ or $x, y \notin L$
- is of finite index: $\equiv$ has finitely many equivalence classes

Definition

equivalence relation $\equiv_M$ on Σ^* for DFA $M = (Q, \Sigma, \delta, s, F)$ is defined as follows:

$$x \equiv_M y \iff \widehat{\delta}(s, x) = \widehat{\delta}(s, y)$$

Lemma

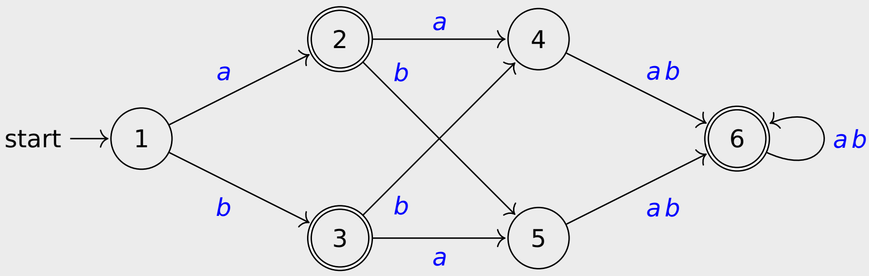
- $\equiv_M$ is right congruent: $\forall x, y \in \Sigma^* \quad x \equiv_M y \implies \forall a \in \Sigma \quad xa \equiv_M ya$
- $\equiv_M$ refines $L(M)$: $\forall x, y \in \Sigma^* \quad x \equiv_M y \implies$ either $x, y \in L(M)$ or $x, y \notin L(M)$
- $\equiv_M$ is of finite index: $\equiv_M$ has finitely many equivalence classes

Corollary

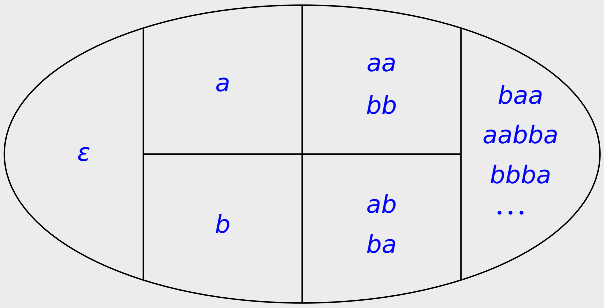
$\equiv_M$ is Myhill-Nerode relation for $L(M)$

Example

M

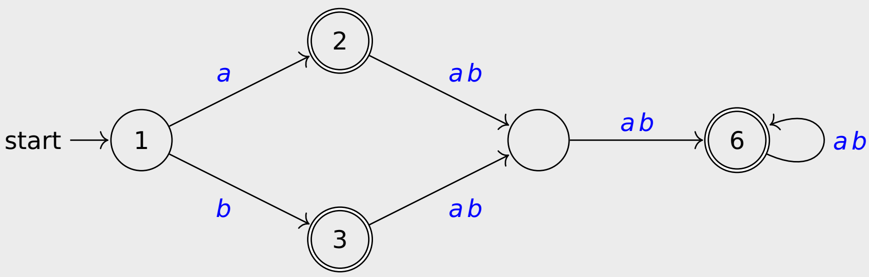


$\equiv_M$

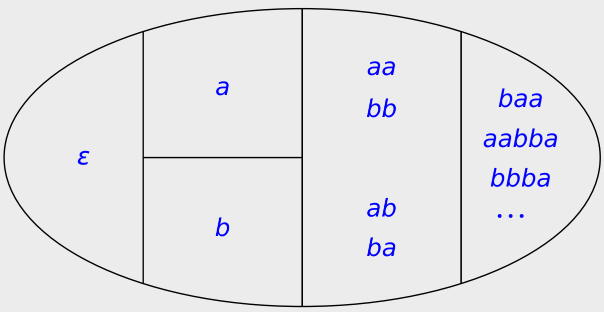


Example

M

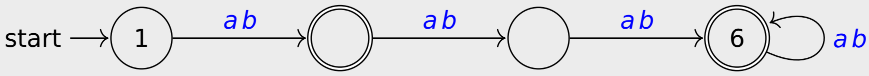


$\equiv_M$

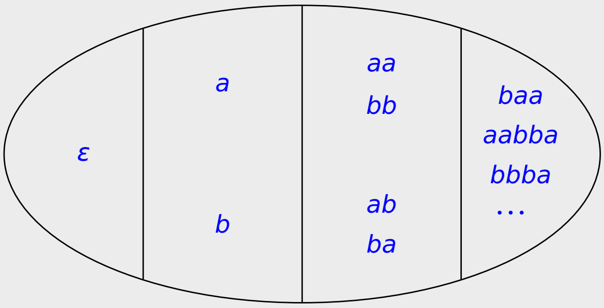


Example

M



$\equiv_M$



Definition

given Myhill-Nerode relation $\equiv$ for set $L \subseteq \Sigma^*$, DFA $M_{\equiv}$ is defined as $(Q, \Sigma, \delta, s, F)$ with

- $Q := \{ [x]_{\equiv} \mid x \in \Sigma^* \}$
- $\delta([x]_{\equiv}, a) := [xa]_{\equiv}$ well-defined: $x \equiv y \implies xa \equiv ya$
- $s := [\epsilon]_{\equiv}$
- $F := \{ [x]_{\equiv} \mid x \in L \}$

Lemma

1. $\widehat{\delta}([x]_{\equiv}, y) = [xy]_{\equiv}$ for all $y \in \Sigma^*$
2. $x \in L \iff [x]_{\equiv} \in F$

for all $x \in \Sigma^*$

Theorem

$L(M_\equiv) = L$

Proof.

$$
\begin{aligned}
x \in L(M_\equiv) &\iff \widehat{\delta}([\varepsilon]_\equiv, x) \in F \\
&\iff [x]_\equiv \in F \\
&\iff x \in L
\end{aligned}
$$

□

Corollary

if L admits Myhill-Nerode relation then L is regular

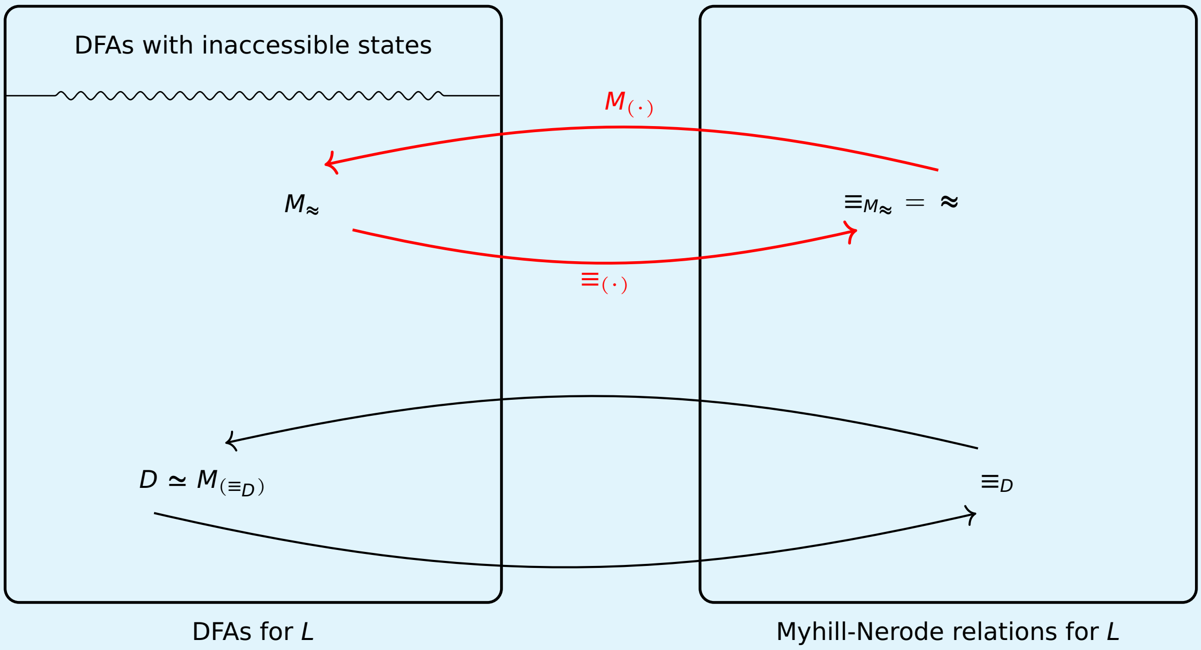
Theorem

two mappings (for $L \subseteq \Sigma^*$)

- $D \mapsto \equiv_D$ from DFAs for L to Myhill-Nerode relations for L
- $\approx \mapsto M_\approx$ from Myhill-Nerode relations for L to DFAs for L

are each others inverse (up to isomorphism of automata):

- $M_{(\equiv_D)} \simeq D$ $\forall$ DFA D without inaccessible states
- $\equiv_{(M_\approx)} = \approx$ $\forall$ Myhill-Nerode relation $\approx$



Definition

for any set $L \subseteq \Sigma^*$, equivalence relation $\equiv_L$ on Σ^* is defined as follows:

$$x \equiv_L y \iff \forall z \in \Sigma^*,\ (xz \in L \iff yz \in L)$$

Lemma

for any set $L \subseteq \Sigma^*$, $\equiv_L$ is coarsest right congruent refinement of L:

if $\sim$ is right congruent equivalence relation refining L then

$$\forall x, y \in \Sigma^*,\ x \sim y \implies x \equiv_L y$$

$\equiv_L$ has fewest equivalence classes

Theorem (Myhill-Nerode)

following statements are equivalent for any set $L \subseteq \Sigma^*$:

- L is regular
- L admits Myhill-Nerode relation
- $\equiv_L$ is of finite index

Corollary

for every regular set L, $M_{(\equiv_L)}$ is minimum-state DFA for L

Theorem

for every DFA M, $M/{\approx} \ \simeq \ M_{\equiv_L}$

Example

1. $A := \{a^n b^n \mid n \geq 0\}$ is not regular
   because $\equiv_A$ has infinitely many equivalence classes

$$i \neq j \implies a^i \not\equiv_A a^j \quad (a^i b^i \in A \text{ and } a^j b^i \notin A)$$

2. $B := \{a^{2^n} \mid n \geq 0\}$ is not regular
   because $\equiv_B$ has infinitely many equivalence classes

$$i < j \implies a^{2^i} \not\equiv_B a^{2^j} \quad (a^{2^i} a^{2^i} = a^{2^{i+1}} \in B \text{ and } a^{2^j} a^{2^i} \notin B)$$

3. $C := \{a^{n!} \mid n \geq 0\}$ is not regular
   because $\equiv_C$ has infinitely many equivalence classes

$$i < j \implies a^{i!} \not\equiv_C a^{j!} \quad (a^{i!} a^{i!i} = a^{(i+1)!} \in C \text{ and } a^{j!} a^{i!i} \notin C)$$

Example

4. $D := \{a^p \mid p \text{ is prime}\}$ is not regular
   because $\equiv_D$ has infinitely many equivalence classes

$$i < j \text{ and } i, j \text{ are primes} \implies a^i \not\equiv_D a^j$$

- suppose $a^i \equiv_D a^j$ and let $k = j - i$
- $a^i \equiv_D a^j = a^i a^k \equiv_D a^j a^k \equiv_D a^j a^k a^k = a^j a^{2k} \equiv_D \cdots \equiv_D a^j a^{jk} = a^{j(k+1)}$
- $a^j \in D$ and $a^{j(k+1)} \notin D$
- $\equiv_D$ does not refine D

A Quick Recap State Minimization Myhill-Nerode Relations

Thanks! & Questions?