CMPE 322/327 - Theory of Computation

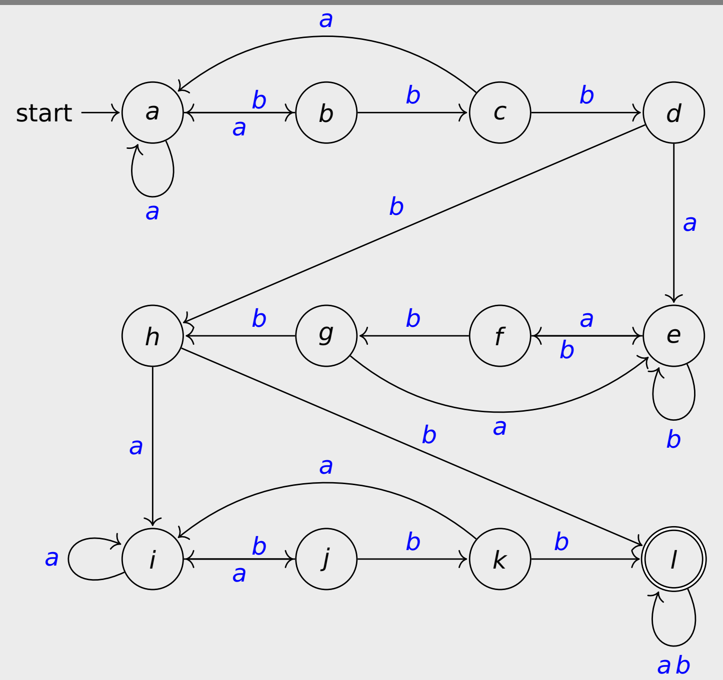
Week 6: Derivatives & Kleene Algebra & Equivalence of Regular Expressions

Burak Ekici

March 28 - April 1, 2022

Outline

Example (Marking Algorithm – Ordering)



	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

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

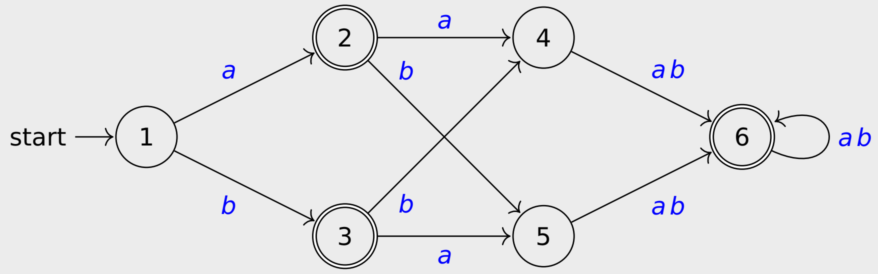
- $\equiv_M$ is right congruent: $\forall x, y \in \Sigma^* \quad x \equiv_M y \implies \forall a \in \Sigma \quad xa \equiv_M ya$
- $\equiv_M$ refines $L(M)$: $\forall x, y \in \Sigma^* \quad x \equiv_M y \implies$ either $x, y \in L(M)$ or $x, y \notin L(M)$
- $\equiv_M$ is of finite index: $\equiv_M$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

Definition

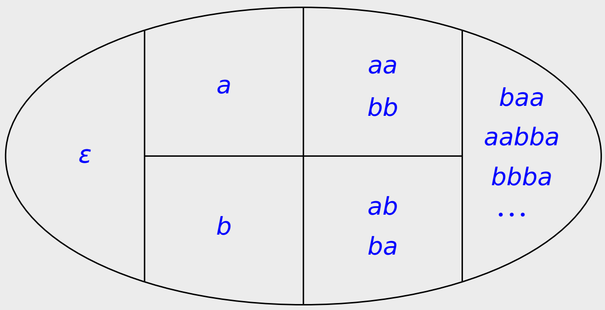
Myhill-Nerode relation for $L \subseteq \Sigma^*$ is right congruent equivalence relation of finite index on Σ^* that refines L

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 $x \in \Sigma^*$

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, $M/{\approx}\ \simeq\ M_{\equiv_L}$

Outline

$x \in \Sigma^*$ $\quad A \subseteq \Sigma^*$ $\quad a \in \Sigma$ $\quad$ regular expression α over Σ

Definitions

- x-derivative of A: $\quad A_x := \{y \mid xy \in A\}$
- a-derivative of α is regular expression defined inductively as follows:

$$\alpha_a := \begin{cases} \varnothing & \text{if } \alpha = \varnothing \text{ or } \alpha = \varepsilon \text{ or } \alpha = b \text{ with } b \neq a \\ \varepsilon & \text{if } \alpha = a \\ \beta_a + \gamma_a & \text{if } \alpha = \beta + \gamma \\ \beta_a\gamma + \gamma_a & \text{if } \alpha = \beta\gamma \text{ and } \varepsilon \in L(\beta) \\ \beta_a\gamma & \text{if } \alpha = \beta\gamma \text{ and } \varepsilon \notin L(\beta) \\ \beta_a\beta^* & \text{if } \alpha = \beta^* \end{cases}$$

Lemma

$L(\alpha_a) = L(\alpha)_a$

Example

- $\alpha = (a+b)^*$

$$\begin{aligned} \alpha_a &= (a+b)_a(a+b)^* \\ &= (a_a+b_a)(a+b)^* \\ &= (\varepsilon+\varnothing)(a+b)^* \\ &\equiv (a+b)^* \end{aligned} \qquad \begin{aligned} \alpha_b &= (a+b)_b(a+b)^* \\ &= (a_b+b_b)(a+b)^* \\ &= (\varnothing+\varepsilon)(a+b)^* \\ &\equiv (a+b)^* \end{aligned}$$

- $\beta = (a^*b)^*a^*$

$$\begin{aligned} \beta_a &= ((a^*b)^*)_a a^* + (a^*)_a \\ &= (a^*b)_a(a^*b)^*a^* + a_a a^* \\ &= ((a^*)_a b + b_a)(a^*b)^*a^* + \varepsilon a^* \\ &= ((a_a)a^*b + \varnothing)(a^*b)^*a^* + \varepsilon a^* \\ &= (\varepsilon a^*b + \varnothing)(a^*b)^*a^* + \varepsilon a^* \\ &\equiv a^*b(a^*b)^*a^* + a^* \\ &\equiv (a^*b)^*a^* \end{aligned} \qquad \begin{aligned} \beta_b &= ((a^*b)^*)_b a^* + (a^*)_b \\ &= (a^*b)_b(a^*b)^*a^* + a_b a^* \\ &= ((a^*)_b b + b_b)(a^*b)^*a^* + \varnothing a^* \\ &= ((a_b)a^*b + \varepsilon)(a^*b)^*a^* + \varnothing a^* \\ &= (\varnothing a^*b + \varepsilon)(a^*b)^*a^* + \varnothing a^* \\ &\equiv (a^*b)^*a^* \end{aligned}$$

Notation

$\alpha{\downarrow}$ for $\varepsilon \in L(\alpha)$ $\qquad \alpha{\uparrow}$ for $\varepsilon \notin L(\alpha)$ $\qquad \varepsilon(\alpha) = \varnothing$ if $\alpha{\uparrow}$ $\qquad \varepsilon(\alpha) = \varepsilon$ if $\alpha{\downarrow}$

- $\varnothing{\uparrow}$
- $\varepsilon{\downarrow}$
- $a{\uparrow}$ for all $a \in \Sigma$
- $(\alpha+\beta){\downarrow} \iff \alpha{\downarrow}$ or $\beta{\downarrow}$
- $(\alpha\beta){\downarrow} \iff \alpha{\downarrow}$ and $\beta{\downarrow}$
- $a^*{\downarrow}$

Theorem

for every regular expression α over $\Sigma = \{a_1, \dots, a_n\}$ $\quad \alpha \equiv \varepsilon((\alpha)) + a_1\alpha_{a_1} + \cdots + a_n\alpha_{a_n}$

Outline

1. A Quick Recap
2. Derivatives
3. Kleene Algebra
4. Equivalence of Regular Expressions

Definition

Kleene Algebra consists of set K with distinguished elements $0, 1 \in K$ and operations $* : K \to K$ and $+, \times : K \times K \to K$ such that (A.1) – (A.13)

$$\begin{array}{rcl} a+(b+c) & = & (a+b)+c \\ a+b & = & b+a \\ a+a & = & a \\ a+0 & = & a \end{array} \qquad \begin{array}{rcl} a0 & = & 0 \\ 0a & = & 0 \\ 1a & = & a \\ a1 & = & a \end{array} \qquad \begin{array}{rcl} a(bc) & = & (ab)c \\ (a+b)c & = & ac+bc \\ a(b+c) & = & ab+ac \end{array} \qquad \begin{array}{rcl} 1+aa^* & = & a^* \\ 1+a^*a & = & a^* \\ ac \leqslant c & \Longrightarrow & a^*c \leqslant c \\ ca \leqslant c & \Longrightarrow & ca^* \leqslant c \end{array}$$

(A.14) $b+ac \leqslant c \implies a^*b \leqslant c$ (A.15) $b+ca \leqslant c \implies ba^* \leqslant c$
(A.16) $(a+b)^* = (a^*b)^*a^*$ (A.17) $a(ba)^* = (ab)^*a$

for all $a, b, c \in K$

Notation

- ab for $a \times b$ a^* for $*(a)$ $a \leqslant b$ for $a+b=b$
- binding precedence: $* > \times > +$

Example

- regular sets over alphabet Σ form Kleene algebra
  - $\varnothing$ for 0
  - $\{\epsilon\}$ for 1
  - union for $+$
  - concatenation for $\times$
  - asterate for $*$
- binary relations over set A form Kleene algebra
  - empty relation $\varnothing$ for 0
  - identity relation $\{(a,a) \mid a \in A\}$ for 1
  - union for $+$
  - relational composition for $\times$
  - reflexive transitive closure for $*$

Theorem

for all regular expressions α and β

$$\alpha \equiv \beta \quad \iff \quad \alpha = \beta \text{ can be proven from Kleene algebra axioms}$$

Inference Rules

- equivalence

$$\frac{}{\alpha = \alpha} \qquad \frac{\alpha = \beta}{\beta = \alpha} \qquad \frac{\alpha = \beta \quad \beta = \gamma}{\alpha = \gamma}$$

- application

$$\frac{\sigma(\gamma) = \sigma(\delta)}{\sigma(\alpha) = \sigma(\beta)} \qquad \forall \text{ axioms } \gamma = \delta \implies \alpha = \beta \quad \forall \text{ substitutions } \sigma$$

- congruence

$$\frac{\alpha = \gamma \quad \beta = \delta}{\alpha + \beta = \gamma + \delta} \qquad \frac{\alpha = \gamma \quad \beta = \delta}{\alpha\beta = \gamma\delta} \qquad \frac{\alpha = \beta}{\alpha^* = \beta^*}$$

Example (page 11)

$$\begin{aligned}
\beta_a &= a^*b(a^*b)^*a^* + a^* \\
&= xx^*y + y \qquad x := (a^*b) \qquad y := (a^*) \\
&= (xx^* + \boldsymbol{\varepsilon})y \\
&= x^*y \\
&= (a^*b)^*a^* \\
&= (a+b)^*
\end{aligned}$$

Example (w4.pdf – page 19)

$$\begin{aligned}
\alpha &= (0+(1+\boldsymbol{\varepsilon})(1+\boldsymbol{\varepsilon})^*0)+(0+(1+\boldsymbol{\varepsilon})(1+\boldsymbol{\varepsilon})^*0)((0+\boldsymbol{\varepsilon})+1(1+\boldsymbol{\varepsilon})^*0)^*((0+\boldsymbol{\varepsilon})+1(1+\boldsymbol{\varepsilon})^*0) \\
&= x + xy^*y \qquad x := (0+(1+\boldsymbol{\varepsilon})(1+\boldsymbol{\varepsilon})^*0) \qquad y := ((0+\boldsymbol{\varepsilon})+1(1+\boldsymbol{\varepsilon})^*0) \\
&= x(\varepsilon + y^*y) \quad = \quad xy^*
\end{aligned}$$

$$\begin{aligned}
x &:= 0+(1+\boldsymbol{\varepsilon})(1+\boldsymbol{\varepsilon})^*0 \\
&= 0+(1+\boldsymbol{\varepsilon})1^*0 \\
&= 0+11^*0+1^*0 \\
&= (\boldsymbol{\varepsilon}+11^*+1^*)0 \\
&= (1^*+1^*)0 \\
&= 1^*0
\end{aligned}$$

$$\begin{aligned}
y &:= (0+\boldsymbol{\varepsilon})+1(1+\boldsymbol{\varepsilon})^*0 \\
&= (0+\boldsymbol{\varepsilon})+11^*0 \\
&= \boldsymbol{\varepsilon}+(0+11^*0) \\
&= \boldsymbol{\varepsilon}+(\boldsymbol{\varepsilon}+11^*)0 \\
&= \boldsymbol{\varepsilon}+1^*0
\end{aligned}$$

$$\begin{aligned}
xy^* &:= (1^*0)(\boldsymbol{\varepsilon}+1^*0)^* \\
&= (1^*0)(1^*0)^* \\
&= (1^*0)^*(1^*0) \\
&= ((1^*0)^*1^*)0 \\
&= (1+0)^*0 \\
&= \color{red}{(0+1)^*0}
\end{aligned}$$

Outline

Theorem

equivalence problem for regular expression

instance: regular expressions α and β over alphabet Σ

question: $L(\alpha) = L(\beta)$

is decidable

Decision Procedure

1. convert α and β into equivalent finite automata N_α and N_β
2. determinize and minimize N_α and N_β into D_α and D_β
3. check whether D_α and D_β are identical (isomorphic):

yes $\implies$ $L(\alpha) = L(\beta)$ no $\implies$ $L(\alpha) \neq L(\beta)$

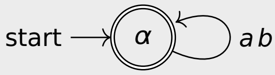
inefficient decision procedure

Alternative Approaches (employing derivatives)

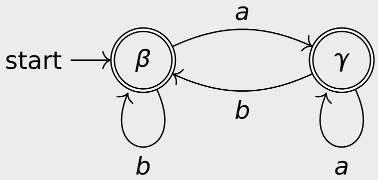
1. derivatives: build DFAs D_α and D_β then minimize and check whether $D_\alpha \simeq D_\beta$ (next slide)
2. derivatives + bisimulation: check whether $L(\alpha) = L(\beta)$ (slides $\#23 - \#26$)

Example

- $\alpha = (a+b)^*$, $\alpha_a \equiv \alpha$, $\alpha_b \equiv \alpha$, $\alpha{\downarrow}$



- $\beta = (a^* b)^* a^*$, $\beta_a \equiv a^* b (a^* b)^* a^* + a^* = \gamma$, $\beta_b \equiv \beta$, $\beta{\downarrow}$, $\gamma_a \equiv \gamma$, $\gamma_b \equiv \beta$, $\gamma{\downarrow}$



Lemma

every regular expression α can be transformed into equivalent DFA using derivatives
(and ‘easy’ Kleene algebra axioms for simplification)

Example

$\alpha = a^* \quad \alpha_a = \epsilon a^* \quad (\alpha_a)_a = \emptyset a^* + \epsilon a^* \quad ((\alpha_a)_a)_a = \emptyset a^* + \emptyset a^* + \epsilon a^* \quad (((\alpha_a)_a)_a)_a = \cdots$
$((\alpha_a)_a)_a = \emptyset a^* + \emptyset a^* + \epsilon a^* \ \equiv \ \emptyset a^* + \epsilon a^* = (\alpha_a)_a$ modulo ACI of $+$

Remark

- ‘easy’ Kleene algebra axioms: ACI of $+$

$$a + (b + c) = (a + b) + c \qquad a + b = b + a \qquad a + a = a$$

- using more Kleene algebra axioms might speed up computation of equivalent DFA

Lemma

every regular expression has finitely many derivatives modulo ACI of $+$

Notation

$A{\downarrow}$ denotes $\varepsilon \in A$

Definition

bisimulation is binary relation $\sim$ between languages over alphabet Σ such that if $A \sim B$ then

1. $A_a \sim B_a$ for all $a \in \Sigma$
2. $A{\downarrow} \iff B{\downarrow}$

Example (bisimulation of languages)

$L = \{aa, ba\}$ and $M = \{aa, bb\}$ over $\Sigma = \{a, b\}$

if $L \sim M$ then it must be that

1. $L_a \sim M_a = \{a\} \sim \{a\}$
2. $L_b \sim M_b = \{a\} \sim \{b\}$
3. $L{\downarrow} \iff M{\downarrow}$ ✓

if $L_b \sim M_b$ then it must be that

1. $(L_b)_a \sim (M_b)_a = \{\varepsilon\} \sim \varnothing$
2. $(L_b)_b \sim (M_b)_b = \varnothing \sim \{\varepsilon\}$ ✗
3. $L_b{\downarrow} \iff M_b{\downarrow}$ ✓

languages L_b and M_b are not bisimilar therefore L and M cannot be bisimilar

Remark

only equal languages are bisimilar (next slide)

Theorem

1. regular expressions α and β are equivalent $\iff L(\alpha) \sim L(\beta)$ for some bisimulation $\sim$
2. $L(\alpha) = L(\beta) \iff L(\alpha) \sim L(\beta)$ for some bisimulation $\sim$

Proof. (second statement)

$\Longrightarrow$ identity relation on languages is bisimulation that satisfies $L(\alpha) = L(\beta)$

$\Longleftarrow$ suppose $x \in L(\alpha)$

we show $x \in L(\beta)$ by induction on x

- if $x = \varepsilon$ then $L(\alpha)\downarrow$
  $L(\beta)\downarrow$ because $L(\alpha) \sim L(\beta)$ and thus $x \in L(\beta)$
- $x = ay$ for some $a \in \Sigma$ with IH: $\forall a \in \Sigma, y \in L(\alpha)_a \longleftrightarrow y \in L(\beta)_a$
  given $x = ay$ then $y \in L(\alpha)_a$
  $y \in L(\beta)_a$ according to IH
  therefore $L(\alpha)_a = L(\beta)_a \quad \forall a \in \Sigma$
  and thus $L(\alpha) = L(\beta)$

Example

$\alpha = (a+b)^*$ and $\beta = (a^*b)^*a^*$ and $\gamma = a^*b(a^*b)^*a^* + a^*$

	a	b	
α	α	α	$\downarrow$

	a	b	
β	γ	β	$\downarrow$
γ	γ	β	$\downarrow$

if $L(\alpha) \sim L(\beta)$, it must be that

1. $L(\alpha)_a \sim L(\beta)_a = L(\alpha_a) \sim L(\beta_a) = L(\alpha) \sim L(\gamma)$ ✓
2. $L(\alpha)_b \sim L(\beta)_b = L(\alpha_b) \sim L(\beta_b) = L(\alpha) \sim L(\beta)$ ✓
3. $L(\alpha)\downarrow \iff L(\beta)\downarrow$ ✓

if $L(\alpha) \sim L(\gamma)$, it must be that

1. $L(\alpha)_a \sim L(\gamma)_a = L(\alpha_a) \sim L(\gamma_a) = L(\alpha) \sim L(\gamma)$ ✓
2. $L(\alpha)_b \sim L(\gamma)_b = L(\alpha_b) \sim L(\gamma_b) = L(\alpha) \sim L(\beta)$ ✓
3. $L(\alpha)\downarrow \iff L(\gamma)\downarrow$ ✓

hence $\{(L(\alpha), L(\beta)), (L(\alpha), L(\gamma))\}$ is bisimulation and thus $L(\alpha) = L(\beta) = L(\gamma)$

Example

$\alpha = ab^*(a+b)^*b$ and $\beta = aa^*(b^*a)^*b$

tables

	a	b	
α	α_1	$\varnothing$	$\uparrow$
α_1	α_2	α_3	$\uparrow$
α_2	α_2	α_4	$\uparrow$
α_3	α_2	α_3	$\downarrow$
α_4	α_2	α_4	$\downarrow$
$\varnothing$	$\varnothing$	$\varnothing$	$\uparrow$

	a	b	
β	β_1	$\varnothing$	$\uparrow$
β_1	β_2	β_3	$\uparrow$
β_2	β_2	β_3	$\uparrow$
β_3	β_4	β_5	$\downarrow$
β_4	β_4	β_3	$\uparrow$
β_5	β_4	β_5	$\uparrow$
$\varnothing$	$\varnothing$	$\varnothing$	$\uparrow$

- any bisimulation $\sim$ satisfying $L(\alpha) \sim L(\beta)$ requires $L(\alpha_3) \sim L(\beta_5)$
- $L(\alpha_3)\downarrow$ and $L(\beta_5)\uparrow$ ↯
- $L(\alpha) \neq L(\beta)$ $\big($witness: $abb \in L(\alpha) \setminus L(\beta)\big)$

Thanks! & Questions?