CC1004 - Modelos de Computação
Teóricas 9-13

Ana Paula Tomás

Departamento de Ciência de Computadores
Faculdade de Ciências da Universidade do Porto

Março 2021

Revisão de noções sobre relações binárias

- Uma relação binária R definida num conjunto A é um subconjunto de $A \times A = \{(a, b) \mid a \in A, b \in A\}$.

  Notação: $(x, y) \in R$ pode-se escrever xRy, usando notação infixa.

- $R \subseteq A \times A$ pode gozar ou não das propriedades seguintes:

  reflexiva: $\forall a \in A \ \ (a, a) \in R$.

  simétrica: $\forall a, b \in A \ \ (a, b) \in R \Rightarrow (b, a) \in R$.

  transitiva: $\forall a, b, c \in A \ \ ((a, b) \in R \wedge (b, c) \in R) \Rightarrow (a, c) \in R$.

  antissimétrica: $\forall a, b \in A \ \ ((a, b) \in R \wedge (b, a) \in R) \Rightarrow a = b$.

- R é uma relação de equivalência sse R é reflexiva, simétrica e transitiva.

- Uma relação de equivalência determina uma **partição** do conjunto A em classes de equivalência, que se denota por A/R. A classe de equivalência de $b \in A$ é o conjunto dos elementos que são equivalentes a b segundo R, ou seja, é $\{a \mid (a, b) \in R\}$. Qualquer elemento pode representar a sua classe.

Revisão de noções sobre relações binárias

- Uma relação binária de A em B é um subconjunto de $A \times B = \{(a, b) \mid a \in A, b \in B\}$.
- Para relações binárias $R \subseteq A \times B$ e $S \subseteq B \times C$, a relação composta $S \circ R = RS = \{(a, c) \mid \exists b \in B \ (a, b) \in R \wedge (b, c) \in S\}$.

  A composição é associativa.

- Para $R \subseteq A \times A$, definimos:

  $R^0 = \mathcal{I} = \{(a, a) \mid a \in A\}$.

  $R^1 = R = R \circ R^0 = R^0 \circ R$

  $R^k = R \circ R^{k-1} = R^{k-1} \circ R$, para $k \geq 1$

- Para A finito, podemos representar $R \subseteq A \times A$ por um **grafo** $G = (V, E)$, com conjunto de **nós** $V = A$ e conjunto de **ramos** $E = R$. Para $k \geq 1$, tem-se $(x, y) \in R^k$ sse existe um **percurso** em G do nó x para o nó y com comprimento k, isto é, com k ramos.

Revisão de noções sobre relações binárias

Para $R \subseteq A \times A$, o *fecho de R para uma propriedade P* é a menor relação que contém R e goza da propriedade P.

- O fecho reflexivo de R é $R \cup \mathcal{I}$, com $\mathcal{I} = \{(a, a) \mid a \in A\}$ a *relação identidade*.
- O fecho simétrico de R é $R \cup R^{-1}$, sendo $R^{-1} = \{(b, a) \mid (a, b) \in R\}$ a *relação inversa* de R.
- O fecho transitivo de $R \subseteq A \times A$, denota-se por R^+. Prova-se que $R^+ = \bigcup_{k \geq 1} R^k$.

  $(x, y) \in R^+$ sse existe um percurso de x para y no grafo de R.
- O fecho transitivo e reflexivo de $R \subseteq A \times A$, denota-se por $R^\star$ e é $R^\star = R \cup \mathcal{I} = \bigcup_{k \geq 0} R^k$.

  $(x, y) \in R^\star$ sse $x = y$ ou existe um percurso de x para y no grafo de R.

Noção formal de linguagem aceite por AFD

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um autómato finito determinístico.

- Uma **configuração** é um par (s, x), em que s seria **o estado** em que o autómato pode estar e x a **palavra que está na fita**.
- A **mudança de configuração num passo** é definida formalmente por uma relação binária $\vdash_{\mathcal{A}}$ em $S \times \Sigma^\star$ assim:

$$(s, x) \vdash_{\mathcal{A}} (s', x') \quad sse \quad x = ax' \text{ e } s' = \delta(s, a), \text{ com } a \in \Sigma$$

quaisquer que sejam os estados $s, s' \in S$ e as palavras $x, x' \in \Sigma^\star$.

Por definição, a relação binária $\vdash_{\mathcal{A}}$ é um subconjunto de $(S \times \Sigma^\star) \times (S \times \Sigma^\star)$.

Quando só temos um autómato, podemos escrever simplesmente $\vdash$. .

- Como δ é uma função, dado (s, x), com $x \neq \varepsilon$, existe um e um só (s', x') tal que $(s, x) \vdash_{\mathcal{A}} (s', x')$. O autómato é **determinístico.**

$$\forall s \in S \ \ \forall x \in \Sigma^\star \ \ \forall a \in \Sigma \qquad (s, ax) \vdash_{\mathcal{A}} (\delta(s, a), x)$$

Noção formal de linguagem aceite por AFD

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um autómato finito determinístico.

- Uma **configuração** é um par (s, x), em que s seria **o estado** em que o autómato pode estar e x a **palavra que está na fita**.
- A **mudança de configuração num passo** é definida formalmente por uma relação binária $\vdash_{\mathcal{A}}$ em $S \times \Sigma^\star$ assim:

$$(s, x) \vdash_{\mathcal{A}} (s', x') \quad \textit{sse} \quad x = ax' \text{ e } s' = \delta(s, a), \text{ com } a \in \Sigma$$

quaisquer que sejam os estados $s, s' \in S$ e as palavras $x, x' \in \Sigma^\star$.

Por definição, a relação binária $\vdash_{\mathcal{A}}$ é um subconjunto de $(S \times \Sigma^\star) \times (S \times \Sigma^\star)$.

Quando só temos um autómato, podemos escrever simplesmente $\vdash$. .

- Como δ é uma função, dado (s, x), com $x \neq \varepsilon$, existe um e um só (s', x') tal que $(s, x) \vdash_{\mathcal{A}} (s', x')$. O autómato é **determinístico.**

$$\forall s \in S \ \ \forall x \in \Sigma^\star \ \ \forall a \in \Sigma \qquad (s, ax) \vdash_{\mathcal{A}} (\delta(s, a), x)$$

Noção formal de linguagem aceite por AFD

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um autómato finito determinístico.

- Uma **configuração** é um par (s, x), em que s seria **o estado** em que o autómato pode estar e x a **palavra que está na fita**.
- A **mudança de configuração num passo** é definida formalmente por uma relação binária $\vdash_{\mathcal{A}}$ em $S \times \Sigma^\star$ assim:

$$(s, x) \vdash_{\mathcal{A}} (s', x') \quad \textit{sse} \quad x = ax' \text{ e } s' = \delta(s, a), \text{ com } a \in \Sigma$$

quaisquer que sejam os estados $s, s' \in S$ e as palavras $x, x' \in \Sigma^\star$.

Por definição, a relação binária $\vdash_{\mathcal{A}}$ é um subconjunto de $(S \times \Sigma^\star) \times (S \times \Sigma^\star)$.

Quando só temos um autómato, podemos escrever simplesmente $\vdash$. .

- Como δ é uma função, dado (s, x), com $x \neq \varepsilon$, existe um e um só (s', x') tal que $(s, x) \vdash_{\mathcal{A}} (s', x')$. O autómato é **determinístico.**

$$\forall s \in S \;\; \forall x \in \Sigma^\star \;\; \forall a \in \Sigma \qquad (s, ax) \vdash_{\mathcal{A}} (\delta(s, a), x)$$

Noção formal de linguagem aceite por AFD

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um autómato finito determinístico.

- A **mudança de configuração em 2 passos**, $\vdash_{\mathcal{A}}^2$, é definida formalmente pela **composta** $\vdash_{\mathcal{A}} \vdash_{\mathcal{A}}$ assim

  $(s, x) \vdash_{\mathcal{A}}^2 (s'', x'')$ sse $\exists x' \in \Sigma^\star \exists s' \in S \;\; (s, x) \vdash_{\mathcal{A}} (s', x') \wedge (s', x') \vdash_{\mathcal{A}} (s'', x'')$

  quaisquer que sejam os estados $s, s' \in S$ e as palavras $x, x' \in \Sigma^\star$.

- A **mudança de configuração em k passos**, $\vdash_{\mathcal{A}}^k$, com $k \geq 2$, é definida formalmente pela **composta** $\vdash_{\mathcal{A}}^{k-1} \vdash_{\mathcal{A}}$, que é igual a $\vdash_{\mathcal{A}} \vdash_{\mathcal{A}}^{k-1}$.

- O **fecho transitivo e reflexivo** da relação $\vdash_{\mathcal{A}}$, denotado por $\vdash_{\mathcal{A}}^\star$, representa a relação de **mudança de configuração num número finito de passos, possivelmente zero**.

- A linguagem reconhecida pelo AFD $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ é

  $$\mathcal{L}(\mathcal{A}) = \{x \mid \text{ existe } f \in F \text{ tal que } (s_0, x) \vdash_{\mathcal{A}}^\star (f, \varepsilon)\}$$

Noção formal de linguagem aceite por AFD

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um autómato finito determinístico.

- A **mudança de configuração em 2 passos**, $\vdash_{\mathcal{A}}^2$, é definida formalmente pela **composta** $\vdash_{\mathcal{A}} \vdash_{\mathcal{A}}$ assim

  $$(s, x) \vdash_{\mathcal{A}}^2 (s'', x'') \text{ sse } \exists x' \in \Sigma^\star \exists s' \in S \;\; (s, x) \vdash_{\mathcal{A}} (s', x') \wedge (s', x') \vdash_{\mathcal{A}} (s'', x'')$$

  quaisquer que sejam os estados $s, s' \in S$ e as palavras $x, x' \in \Sigma^\star$.

- A **mudança de configuração em k passos**, $\vdash_{\mathcal{A}}^k$, com $k \geq 2$, é definida formalmente pela **composta** $\vdash_{\mathcal{A}}^{k-1} \vdash_{\mathcal{A}}$, que é igual a $\vdash_{\mathcal{A}} \vdash_{\mathcal{A}}^{k-1}$.

- O **fecho transitivo e reflexivo** da relação $\vdash_{\mathcal{A}}$, denotado por $\vdash_{\mathcal{A}}^\star$, representa a relação de **mudança de configuração num número finito de passos, possivelmente zero**.

- A linguagem reconhecida pelo AFD $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ é

  $$\mathcal{L}(\mathcal{A}) = \{x \mid \text{ existe } f \in F \text{ tal que } (s_0, x) \vdash_{\mathcal{A}}^\star (f, \varepsilon)\}$$

Noção formal de linguagem aceite por AFD

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um autómato finito determinístico.

- A **mudança de configuração em 2 passos**, $\vdash_{\mathcal{A}}^2$, é definida formalmente pela **composta** $\vdash_{\mathcal{A}} \vdash_{\mathcal{A}}$ assim

  $$(s, x) \vdash_{\mathcal{A}}^2 (s'', x'') \text{ sse } \exists x' \in \Sigma^\star \exists s' \in S \;\; (s, x) \vdash_{\mathcal{A}} (s', x') \wedge (s', x') \vdash_{\mathcal{A}} (s'', x'')$$

  quaisquer que sejam os estados $s, s' \in S$ e as palavras $x, x' \in \Sigma^\star$.

- A **mudança de configuração em k passos**, $\vdash_{\mathcal{A}}^k$, com $k \geq 2$, é definida formalmente pela **composta** $\vdash_{\mathcal{A}}^{k-1} \vdash_{\mathcal{A}}$, que é igual a $\vdash_{\mathcal{A}} \vdash_{\mathcal{A}}^{k-1}$.

- O **fecho transitivo e reflexivo** da relação $\vdash_{\mathcal{A}}$, denotado por $\vdash_{\mathcal{A}}^\star$, representa a relação de **mudança de configuração num número finito de passos, possivelmente zero**.

- A linguagem reconhecida pelo AFD $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ é

  $$\mathcal{L}(\mathcal{A}) = \{x \mid \text{ existe } f \in F \text{ tal que } (s_0, x) \vdash_{\mathcal{A}}^\star (f, \varepsilon)\}$$

Noção formal de linguagem aceite por AFD

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um autómato finito determinístico.

- A **mudança de configuração em 2 passos**, $\vdash_{\mathcal{A}}^2$, é definida formalmente pela **composta** $\vdash_{\mathcal{A}} \vdash_{\mathcal{A}}$ assim

  $(s, x) \vdash_{\mathcal{A}}^2 (s'', x'')$ sse $\exists x' \in \Sigma^\star \exists s' \in S \;\; (s, x) \vdash_{\mathcal{A}} (s', x') \wedge (s', x') \vdash_{\mathcal{A}} (s'', x'')$

  quaisquer que sejam os estados $s, s' \in S$ e as palavras $x, x' \in \Sigma^\star$.

- A **mudança de configuração em k passos**, $\vdash_{\mathcal{A}}^k$, com $k \geq 2$, é definida formalmente pela **composta** $\vdash_{\mathcal{A}}^{k-1} \vdash_{\mathcal{A}}$, que é igual a $\vdash_{\mathcal{A}} \vdash_{\mathcal{A}}^{k-1}$.

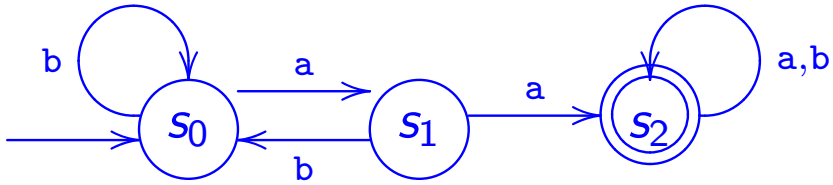
- O **fecho transitivo e reflexivo** da relação $\vdash_{\mathcal{A}}$, denotado por $\vdash_{\mathcal{A}}^\star$, representa a relação de **mudança de configuração num número finito de passos, possivelmente zero**.

- A linguagem reconhecida pelo AFD $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ é

$$\mathcal{L}(\mathcal{A}) = \{x \mid \text{ existe } f \in F \text{ tal que } (s_0, x) \vdash_{\mathcal{A}}^\star (f, \varepsilon)\}$$

Exemplo para AFD

Seja A o AFD de alfabeto $\Sigma = \{\mathtt{a}, \mathtt{b}\}$.



- $\mathtt{abaab} \in \mathcal{L}(A)$ pois
  $(s_0, \mathtt{abaab}) \vdash (s_1, \mathtt{baab}) \vdash (s_0, \mathtt{aab}) \vdash (s_1, \mathtt{ab}) \vdash (s_2, \mathtt{b}) \vdash (s_2, \varepsilon)$
- $\mathtt{ababa} \notin \mathcal{L}(A)$ pois
  $(s_0, \mathtt{ababa}) \vdash (s_1, \mathtt{baba}) \vdash (s_0, \mathtt{aba}) \vdash (s_1, \mathtt{ba}) \vdash (s_0, \mathtt{ba}) \vdash (s_0, \mathtt{a}) \vdash (s_1, \varepsilon)$

Por indução matemática sobre $|x|$ podemos mostrar:

- $\forall x \in \{\mathtt{ab}, \mathtt{b}\}^\star \;\; \forall y \in \Sigma^\star \;\; (s_0, xy) \vdash^\star (s_0, y)$
- $\forall x \in \Sigma^\star \;\; \forall y \in \Sigma^\star$ se $(s_0, xy) \vdash^\star (s_0, y)$ então $x \in \{\mathtt{ab}, \mathtt{b}\}^\star$

o que é interessante para concluir que $\mathcal{L}(A) = \mathcal{L}(\{\mathtt{ab}, \mathtt{b}\}^\star\{\mathtt{aa}\}\{\mathtt{a}, \mathtt{b}\}^\star)$ é o conjunto das **palavras que têm aa como subpalavra**.

Noção formal de linguagem aceite por AFND

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um autómato finito não determinístico.

- Definimos a relação $\vdash_{\mathcal{A}}$ em $2^S \times \Sigma^\star$ por

$$(E, x) \vdash_{\mathcal{A}} (E', x') \text{ sse } x = ax' \text{ e } E' = \bigcup_{s \in E} \delta(s, a)$$

- A linguagem reconhecida pelo AFND $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ é

$$\mathcal{L}(\mathcal{A}) = \{x \mid \text{ existe } E \in 2^S \text{ tal que } (\{s_0\}, x) \vdash^\star_{\mathcal{A}} (E, \varepsilon) \text{ e } E \cap F \neq \emptyset\}$$

sendo $\vdash^\star_{\mathcal{A}}$ o fecho reflexivo e transitivo de $\vdash_{\mathcal{A}}$.

Noção formal de linguagem aceite por AFND-ε

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um autómato finito não determinístico, com possivelmente transições por ε.

- Definimos a relação $\vdash_{\mathcal{A}}$ em $2^S \times \Sigma^\star$ por

$$(E, x) \vdash_{\mathcal{A}} (E', x') \text{ sse } x = ax' \text{ e } E' = Fecho_\varepsilon(\bigcup_{s \in Fecho_\varepsilon(E)} \delta(s, a))$$

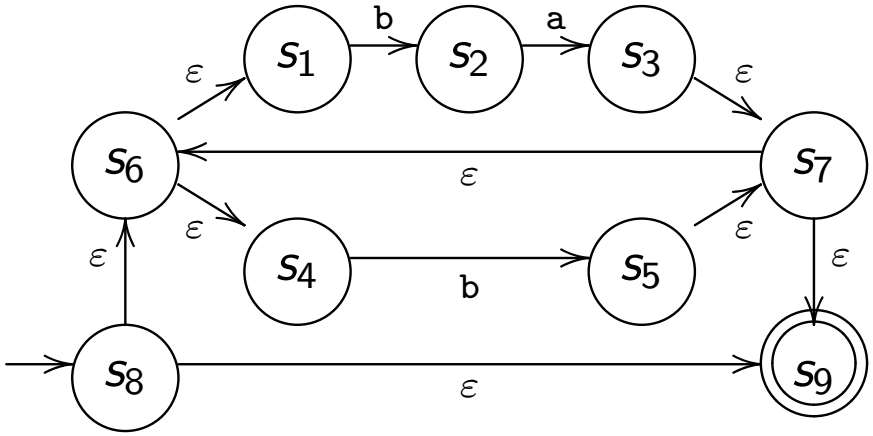
- A linguagem reconhecida pelo AFND-ε $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ é

$$\mathcal{L}(\mathcal{A}) = \{x \mid \text{ existe } E \in 2^S \text{ tal que } (Fecho_\varepsilon(s_0), x) \vdash_{\mathcal{A}}^\star (E, \varepsilon) \text{ e } E \cap F \neq \emptyset\}$$

sendo $\vdash_{\mathcal{A}}^\star$ o fecho reflexivo e transitivo de $\vdash_{\mathcal{A}}$.

Exemplo para AFND-ε

Seja A o AFD de alfabeto $\Sigma = \{\mathtt{a}, \mathtt{b}\}$.



$Fecho_\varepsilon(s_8) = \{s_8, s_9, s_6, s_1, s_4\}$

- $\mathtt{babb} \in \mathcal{L}(A)$ pois

  $(\{s_8, s_9, s_6, s_1, s_4\}, \mathtt{babb}) \vdash (\{s_2, s_5, s_7, s_9, s_6, s_1, s_4\}, \mathtt{abb}) \vdash$
  $(\{s_3, s_7, s_9, s_6, s_1, s_4\}, \mathtt{bb}) \vdash (\{s_2, s_5, s_7, s_9, s_6, s_1, s_4\}, \mathtt{b}) \vdash$
  $(\{s_2, s_5, s_7, s_9, s_6, s_1, s_4\}, \varepsilon)$

- $\mathtt{aa} \notin \mathcal{L}(A)$ pois

  $(\{s_8, s_9, s_6, s_1, s_4\}, \mathtt{aa}) \vdash (\{\}, \mathtt{a}) \vdash (\{\}, \varepsilon)$

Sobre o método de conversão baseado em subconjuntos

Com as definições que acabámos de apresentar para $\mathcal{L}(A)$, a correção do AFD A' construído para um AFND ou AFND-ε A pelo método dos subconjuntos, isto é, a prova de que $x \in \mathcal{L}(A)$ sse $x \in \mathcal{L}(A')$, segue trivialmente.

Porquê?
Seja $A = (S, \Sigma, \delta, s_0, F)$ o AF de partida e $A' = (2^S, \Sigma, \delta', s_0', F')$ o AFD que construimos por aplicação do método.

Pelas definições de s_0' e de δ', podemos mostrar por indução sobre $|u|$ que, para todos $E, E' \in 2^S$ fechados por ε e todos $u, v \in \Sigma^\star$ se tem

$$(E, uv) \vdash_{A'}^\star (E', v) \text{ se e só se } (E, uv) \vdash_A^\star (E', v)$$

para concluir que

$$(Fecho_\varepsilon(s_0), x) \vdash_{A'}^\star (E', \varepsilon) \text{ se e só se } (Fecho_\varepsilon(s_0), x) \vdash_A^\star (E', \varepsilon), \text{ com } x \in \Sigma^\star$$

Não separamos a conversão para AFNDs pois corresponde à de AFNDs-ε. Num AFND, $Fecho_\varepsilon(s_0) = \{s_0\}$ e $Fecho_\varepsilon(E) = E$.

Qual é o AFD mínimo para uma linguagem regular L?

Para responder, vamos analisar duas questões:

- O que são palavras equivalentes para **um** AFD A dado? Ou seja, *indistinguíveis* para o AFD A?
- Que palavras **todos** os AFDs que aceitam uma linguagem L dada têm de distinguir para estar corretos?

Por exemplo: Seja L o conjunto das palavras que começam por 0. Esta linguagem é reconhecida pelos dois AFDs seguintes:

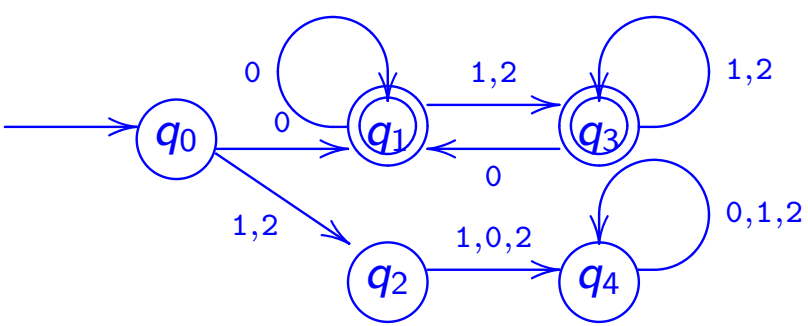
O AFD da esquerda tem mais estados. Distingue, por exemplo, 0 de 01, e o da direita não distingue! Mas, **todos os AFDs que aceitem L** têm de distinguir ε, 0 e 1. Terão **pelo menos 3 estados**. Caso contrário, não reconhecem L.

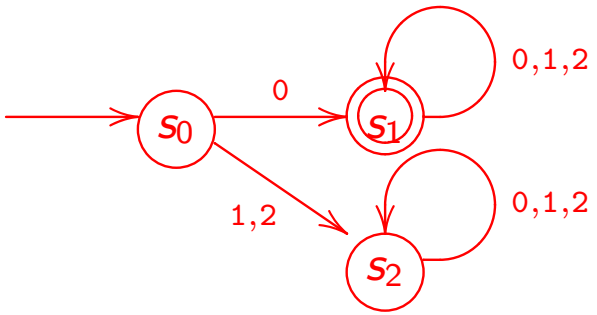
Qual é o AFD mínimo para uma linguagem regular L?

Para responder, vamos analisar duas questões:

- O que são palavras equivalentes para **um** AFD A dado? Ou seja, *indistinguíveis* para o AFD A?
- Que palavras **todos** os AFDs que aceitam uma linguagem L dada têm de distinguir para estar corretos?

Por exemplo: Seja L o conjunto das palavras que começam por 0. Esta linguagem é reconhecida pelos dois AFDs seguintes:





O AFD da esquerda tem mais estados. Distingue, por exemplo, 0 de 01, e o da direita não distingue! Mas, **todos os AFDs que aceitem L** têm de distinguir ε, 0 e 1. Terão **pelo menos 3 estados**. Caso contrário, não reconhecem L.

Que palavras todos os AFDs para L distinguirão?

Seja $A = (S, \Sigma, \delta, s_0, F)$ um AFD. Recordar que δ é uma função de $S \times \Sigma$ em S. Vamos definir uma extensão $\hat{\delta}$ de δ a $S \times \Sigma^\star$ assim

$$\begin{aligned} \hat{\delta}(s, \varepsilon) &= s, && \text{para todo } s \in S \\ \hat{\delta}(s, ax) &= \hat{\delta}(\,\delta(s, a),\, x), && \text{para todo } s \in S,\ x \in \Sigma^\star \text{ e } a \in \Sigma. \end{aligned}$$

- $\hat{\delta}(s, x)$ indica o estado a que x leva o AFD A se for consumida a partir de s.
- Seria equivalente definir $\hat{\delta}$ recursivamente à custa de δ por:

$$\begin{aligned} \hat{\delta}(s, \varepsilon) &= s, && \text{para todo } s \in S \\ \hat{\delta}(s, xa) &= \delta(\,\hat{\delta}(s, x),\, a), && \text{para todo } s \in S,\ x \in \Sigma^\star \text{ e } a \in \Sigma. \end{aligned}$$

- **Proposição:** $\hat{\delta}(s, xz) = \hat{\delta}(\hat{\delta}(s, x), z)$**, para todo** $x, z \in \Sigma^\star$ **e** $s \in S$. Ou seja, depois de consumir xz a partir de s, o AFD A fica no mesmo estado que ficaria se consumisse z a partir do estado $\hat{\delta}(s, x)$.

Que palavras todos os AFDs para L distinguirão?

Seja $A = (S, \Sigma, \delta, s_0, F)$ um AFD. Recordar que δ é uma função de $S \times \Sigma$ em S. Vamos definir uma extensão $\hat{\delta}$ de δ a $S \times \Sigma^\star$ assim

$$\begin{array}{rcll} \hat{\delta}(s, \varepsilon) & = & s, & \text{para todo } s \in S \\ \hat{\delta}(s, ax) & = & \hat{\delta}(\,\delta(s, a),\, x), & \text{para todo } s \in S,\ x \in \Sigma^\star \text{ e } a \in \Sigma. \end{array}$$

- $\hat{\delta}(s, x)$ indica o estado a que x leva o AFD A se for consumida a partir de s.
- Seria equivalente definir $\hat{\delta}$ recursivamente à custa de δ por:

$$\begin{array}{rcll} \hat{\delta}(s, \varepsilon) & = & s, & \text{para todo } s \in S \\ \hat{\delta}(s, xa) & = & \delta(\,\hat{\delta}(s, x),\, a), & \text{para todo } s \in S,\ x \in \Sigma^\star \text{ e } a \in \Sigma. \end{array}$$

- **Proposição:** $\hat{\delta}(s, xz) = \hat{\delta}(\hat{\delta}(s, x), z)$**, para todo** $x, z \in \Sigma^\star$ **e** $s \in S$. Ou seja, depois de consumir xz a partir de s, o AFD A fica no mesmo estado que ficaria se consumisse z a partir do estado $\hat{\delta}(s, x)$.

Que palavras todos os AFDs para L distinguirão?

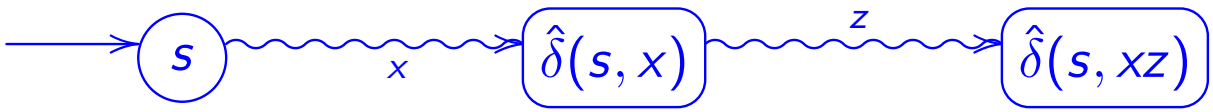
Seja $A = (S, \Sigma, \delta, s_0, F)$ um AFD. Recordar que δ é uma função de $S \times \Sigma$ em S. Vamos definir uma extensão $\hat{\delta}$ de δ a $S \times \Sigma^\star$ assim

$$\begin{aligned} \hat{\delta}(s, \varepsilon) &= s, && \text{para todo } s \in S \\ \hat{\delta}(s, ax) &= \hat{\delta}(\,\delta(s, a),\, x), && \text{para todo } s \in S,\ x \in \Sigma^\star \text{ e } a \in \Sigma. \end{aligned}$$

- $\hat{\delta}(s, x)$ indica o estado a que x leva o AFD A se for consumida a partir de s.
- Seria equivalente definir $\hat{\delta}$ recursivamente à custa de δ por:

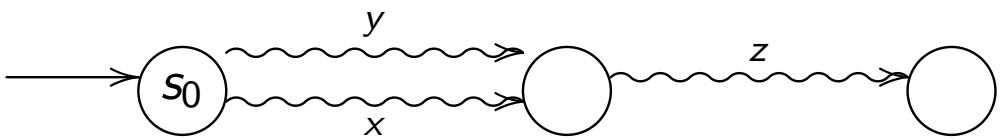
$$\begin{aligned} \hat{\delta}(s, \varepsilon) &= s, && \text{para todo } s \in S \\ \hat{\delta}(s, xa) &= \delta(\,\hat{\delta}(s, x),\, a), && \text{para todo } s \in S,\ x \in \Sigma^\star \text{ e } a \in \Sigma. \end{aligned}$$

- **Proposição:** $\hat{\delta}(s, xz) = \hat{\delta}(\hat{\delta}(s, x), z)$**, para todo** $x, z \in \Sigma^\star$ **e** $s \in S$. Ou seja, depois de consumir xz a partir de s, o AFD A fica no mesmo estado que ficaria se consumisse z a partir do estado $\hat{\delta}(s, x)$.



Que palavras todos os AFDs para L distinguirão?

Quaisquer que sejam $x, y \in \Sigma^\star$, se x e y levam o AFD de s_0 a um mesmo estado então xz e yz também levam o AFD de s_0 a um mesmo estado, para todo $z \in \Sigma^\star$.



Ou seja, em qualquer AFD $A = (S, \Sigma, \delta, s_0, F)$ tem-se

$$\text{se } \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \text{ então } \hat{\delta}(s_0, xz) = \hat{\delta}(s_0, yz), \text{ para todo } z \in \Sigma^\star.$$

Tal implica que, se $\hat{\delta}(s_0, x) = \hat{\delta}(s_0, y)$ então, para todo $z \in \Sigma^\star$, as palavras xz e yz serão *ou ambas aceites ou ambas rejeitadas* pelo autómato A. Isto é, sendo L a linguagem que o AFD A reconhece, tem-se:

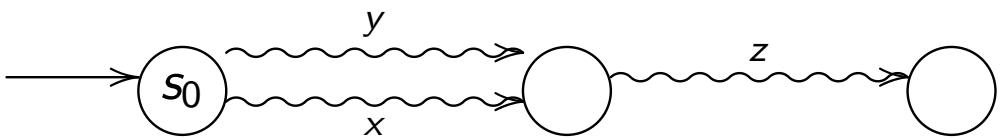
$$\textbf{se } \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \textbf{ então } xz \in L \Leftrightarrow yz \in L, \text{ para todo } z \in \Sigma^\star.$$

Qualquer AFD que reconheça L satisfaz tal propriedade. **O AFD mínimo para L satisfaz uma propriedade mais forte.** No AFD mínimo, tem-se

$$\hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \textbf{ se e só se } xz \in L \Leftrightarrow yz \in L, \text{ para todo } z \in \Sigma^\star.$$

Que palavras todos os AFDs para L distinguirão?

Quaisquer que sejam $x, y \in \Sigma^\star$, se x e y levam o AFD de s_0 a um mesmo estado então xz e yz também levam o AFD de s_0 a um mesmo estado, para todo $z \in \Sigma^\star$.



Ou seja, em qualquer AFD $A = (S, \Sigma, \delta, s_0, F)$ tem-se

$$\text{se } \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \text{ então } \hat{\delta}(s_0, xz) = \hat{\delta}(s_0, yz), \text{ para todo } z \in \Sigma^\star.$$

Tal implica que, se $\hat{\delta}(s_0, x) = \hat{\delta}(s_0, y)$ então, para todo $z \in \Sigma^\star$, as palavras xz e yz serão *ou ambas aceites ou ambas rejeitadas* pelo autómato A. Isto é, sendo L a linguagem que o AFD A reconhece, tem-se:

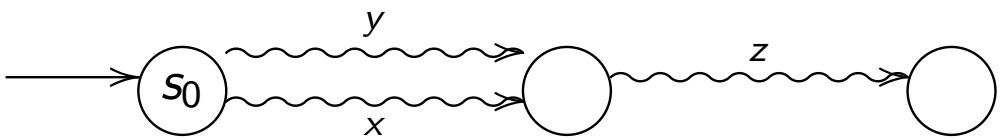
$$\textbf{se } \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \textbf{ então } xz \in L \Leftrightarrow yz \in L, \text{ para todo } z \in \Sigma^\star.$$

Qualquer AFD que reconheça L satisfaz tal propriedade. **O AFD mínimo para L satisfaz uma propriedade mais forte.** No AFD mínimo, tem-se

$$\hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \textbf{ se e só se } xz \in L \Leftrightarrow yz \in L, \text{ para todo } z \in \Sigma^\star.$$

Que palavras todos os AFDs para L distinguirão?

Quaisquer que sejam $x, y \in \Sigma^\star$, se x e y levam o AFD de s_0 a um mesmo estado então xz e yz também levam o AFD de s_0 a um mesmo estado, para todo $z \in \Sigma^\star$.



Ou seja, em qualquer AFD $A = (S, \Sigma, \delta, s_0, F)$ tem-se

$$\text{se } \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \text{ então } \hat{\delta}(s_0, xz) = \hat{\delta}(s_0, yz), \text{ para todo } z \in \Sigma^\star.$$

Tal implica que, se $\hat{\delta}(s_0, x) = \hat{\delta}(s_0, y)$ então, para todo $z \in \Sigma^\star$, as palavras xz e yz serão *ou ambas aceites ou ambas rejeitadas* pelo autómato A. Isto é, sendo L a linguagem que o AFD A reconhece, tem-se:

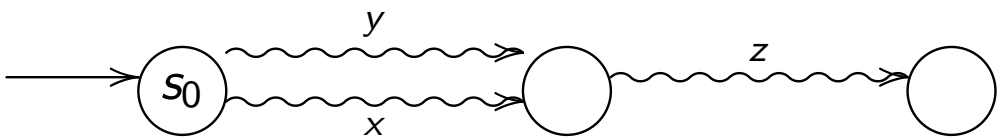
$$\textbf{se } \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \textbf{ então } xz \in L \Leftrightarrow yz \in L, \text{ para todo } z \in \Sigma^\star.$$

Qualquer AFD que reconheça L satisfaz tal propriedade. **O AFD mínimo para L satisfaz uma propriedade mais forte.** No AFD mínimo, tem-se

$$\hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \textbf{ se e só se } xz \in L \Leftrightarrow yz \in L, \text{ para todo } z \in \Sigma^\star.$$

Que palavras todos os AFDs para L distinguirão?

Quaisquer que sejam $x, y \in \Sigma^\star$, se x e y levam o AFD de s_0 a um mesmo estado então xz e yz também levam o AFD de s_0 a um mesmo estado, para todo $z \in \Sigma^\star$.



Ou seja, em qualquer AFD $A = (S, \Sigma, \delta, s_0, F)$ tem-se

$$\text{se } \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \text{ então } \hat{\delta}(s_0, xz) = \hat{\delta}(s_0, yz), \text{ para todo } z \in \Sigma^\star.$$

Tal implica que, se $\hat{\delta}(s_0, x) = \hat{\delta}(s_0, y)$ então, para todo $z \in \Sigma^\star$, as palavras xz e yz serão *ou ambas aceites ou ambas rejeitadas* pelo autómato A. Isto é, sendo L a linguagem que o AFD A reconhece, tem-se:

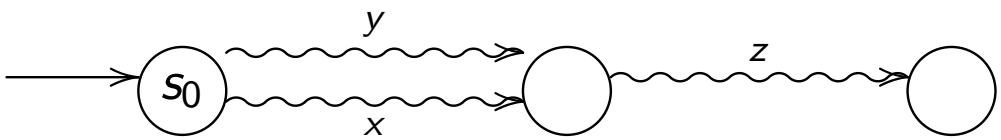
$$\textbf{se } \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \textbf{ então } xz \in L \Leftrightarrow yz \in L, \text{ para todo } z \in \Sigma^\star.$$

Qualquer AFD que reconheça L satisfaz tal propriedade. **O AFD mínimo para L satisfaz uma propriedade mais forte.** No AFD mínimo, tem-se

$$\hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \textbf{ se e só se } xz \in L \Leftrightarrow yz \in L, \text{ para todo } z \in \Sigma^\star.$$

Que palavras todos os AFDs para L distinguirão?

Quaisquer que sejam $x, y \in \Sigma^\star$, se x e y levam o AFD de s_0 a um mesmo estado então xz e yz também levam o AFD de s_0 a um mesmo estado, para todo $z \in \Sigma^\star$.



Ou seja, em qualquer AFD $A = (S, \Sigma, \delta, s_0, F)$ tem-se

$$\text{se } \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \text{ então } \hat{\delta}(s_0, xz) = \hat{\delta}(s_0, yz), \text{ para todo } z \in \Sigma^\star.$$

Tal implica que, se $\hat{\delta}(s_0, x) = \hat{\delta}(s_0, y)$ então, para todo $z \in \Sigma^\star$, as palavras xz e yz serão *ou ambas aceites ou ambas rejeitadas* pelo autómato A. Isto é, sendo L a linguagem que o AFD A reconhece, tem-se:

$$\textbf{se } \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \textbf{ então } xz \in L \Leftrightarrow yz \in L, \text{ para todo } z \in \Sigma^\star.$$

Qualquer AFD que reconheça L satisfaz tal propriedade. **O AFD mínimo para L satisfaz uma propriedade mais forte.** No AFD mínimo, tem-se

$$\hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \textbf{ se e só se } xz \in L \Leftrightarrow yz \in L, \text{ para todo } z \in \Sigma^\star.$$

Corolário do Teorema de Myhill-Nerode

A prova do teorema de Myhill-Nerode, que enunciamos mais à frente, indica-nos como obter o AFD mínimo para uma linguagem regular L.

O conjunto de estados do **AFD mínimo** que reconhece L corresponde ao conjunto das classes de equivalência da relação R_L definida em $\Sigma^\star$ por

$$R_L = \{(x, y) \mid x, y \in \Sigma^\star \text{ e } \forall z \in \Sigma^\star (xz \in L \Leftrightarrow yz \in L)\}$$

Corolário do Teorema de Myhill-Nerode (AFD mínimo para $L \subseteq \Sigma^\star$ regular):

Se L é uma linguagem regular, o conjunto $\Sigma^\star / R_L$ das classes de equivalência de R_L é finito. O **AFD mínimo** para L é $\mathcal{A} = (\Sigma^\star / R_L, \Sigma, \delta, [\varepsilon], F)$, com $F = \{[x] \mid x \in L\}$, e $\delta([x], a) = [xa]$, para todo $[x] \in \Sigma^\star / R_L$ e todo $a \in \Sigma$, sendo *único a menos da designação dos estados*.

Corolário do Teorema de Myhill-Nerode

A prova do teorema de Myhill-Nerode, que enunciamos mais à frente, indica-nos como obter o AFD mínimo para uma linguagem regular L.
O conjunto de estados do **AFD mínimo** que reconhece L corresponde ao conjunto das classes de equivalência da relação R_L definida em $\Sigma^\star$ por

$$R_L = \{(x, y) \mid x, y \in \Sigma^\star \text{ e } \forall z \in \Sigma^\star (xz \in L \Leftrightarrow yz \in L)\}$$

Corolário do Teorema de Myhill-Nerode (AFD mínimo para $L \subseteq \Sigma^\star$ regular):

Se L é uma linguagem regular, o conjunto $\Sigma^\star/R_L$ das classes de equivalência de R_L é finito. O **AFD mínimo** para L é $\mathcal{A} = (\Sigma^\star/R_L, \Sigma, \delta, [\varepsilon], F)$, com $F = \{[x] \mid x \in L\}$, e $\delta([x], a) = [xa]$, para todo $[x] \in \Sigma^\star/R_L$ e todo $a \in \Sigma$, sendo *único a menos da designação dos estados*.

Exemplo 1

AFD mínimo para $L = \{x \mid x$ começa por $0\}$, com $\Sigma = \{0, 1, 2\}$?

- Partimos do **estado inicial** $[\varepsilon]$. Vamos analisar as transições e ver se surjem novos estados, sabendo que δ é dada por

$$\delta([x], a) \stackrel{\text{def}}{=} [xa], \text{ para todo } a \in \Sigma \text{ e } x \in \Sigma^*.$$

  O conjunto de **estados finais** é $F = \{\, [x] \mid x \in L\}$.

- $xR_L y$ se e só se $\forall z \in \Sigma^*(xz \in L \Leftrightarrow yz \in L)$. $[x]$ denota a classe de equivalência de x para R_L.

Assim, temos:

- $[\varepsilon]$ é o estado inicial; $[\varepsilon] \notin F$ porque $\varepsilon \notin L$.
- $\delta([\varepsilon], 0) \stackrel{\text{def}}{=} [\varepsilon 0] = [0] \neq [\varepsilon]$, pois $(0, \varepsilon) \notin R_L$, porque $0 \in L$ e $\varepsilon \notin L$. Logo, $[0]$ é um **novo estado** e $[0] \in F$ pois $0 \in L$.

  Para ver que $(0, \varepsilon) \notin R_L$, tomamos $z = \varepsilon$ para ter $0z \in L$ e $\varepsilon z \notin L$.

Exemplo 1

AFD mínimo para $L = \{x \mid x$ começa por $0\}$, com $\Sigma = \{0, 1, 2\}$?

- Partimos do **estado inicial** $[\varepsilon]$. Vamos analisar as transições e ver se surjem novos estados, sabendo que δ é dada por

$$\delta([x], a) \stackrel{\text{def}}{=} [xa], \text{ para todo } a \in \Sigma \text{ e } x \in \Sigma^\star.$$

  O conjunto de **estados finais** é $F = \{\, [x] \mid x \in L\}$.

- xR_Ly se e só se $\forall z \in \Sigma^\star(xz \in L \Leftrightarrow yz \in L)$. $[x]$ denota a classe de equivalência de x para R_L.

Assim, temos:

- $[\varepsilon]$ é o estado inicial; $[\varepsilon] \notin F$ porque $\varepsilon \notin L$.
- $\delta([\varepsilon], 0) \stackrel{\text{def}}{=} [\varepsilon 0] = [0] \neq [\varepsilon]$, pois $(0, \varepsilon) \notin R_L$, porque $0 \in L$ e $\varepsilon \notin L$.
  Logo, $[0]$ é um **novo estado** e $[0] \in F$ pois $0 \in L$.

  Para ver que $(0, \varepsilon) \notin R_L$, tomamos $z = \varepsilon$ para ter $0z \in L$ e $\varepsilon z \notin L$.

Exemplo 1

AFD mínimo para $L = \{x \mid x$ começa por $0\}$, com $\Sigma = \{0, 1, 2\}$?

- Partimos do **estado inicial** $[\varepsilon]$. Vamos analisar as transições e ver se surjem novos estados, sabendo que δ é dada por

$$\delta([x], a) \stackrel{\text{def}}{=} [xa], \text{ para todo } a \in \Sigma \text{ e } x \in \Sigma^\star.$$

  O conjunto de **estados finais** é $F = \{\, [x] \mid x \in L\}$.

- xR_Ly se e só se $\forall z \in \Sigma^\star(xz \in L \Leftrightarrow yz \in L)$. $[x]$ denota a classe de equivalência de x para R_L.

Assim, temos:

- $[\varepsilon]$ é o estado inicial; $[\varepsilon] \notin F$ porque $\varepsilon \notin L$.
- $\delta([\varepsilon], 0) \stackrel{\text{def}}{=} [\varepsilon 0] = [0] \neq [\varepsilon]$, pois $(0, \varepsilon) \notin R_L$, porque $0 \in L$ e $\varepsilon \notin L$.
  Logo, $[0]$ é um **novo estado** e $[0] \in F$ pois $0 \in L$.

  Para ver que $(0, \varepsilon) \notin R_L$, tomamos $z = \varepsilon$ para ter $0z \in L$ e $\varepsilon z \notin L$.

Exemplo 1

AFD mínimo para $L = \{x \mid x$ começa por $0\}$, com $\Sigma = \{0, 1, 2\}$?

- Partimos do **estado inicial** $[\varepsilon]$. Vamos analisar as transições e ver se surjem novos estados, sabendo que δ é dada por

$$\delta([x], a) \stackrel{\text{def}}{=} [xa], \text{ para todo } a \in \Sigma \text{ e } x \in \Sigma^\star.$$

  O conjunto de **estados finais** é $F = \{\, [x] \mid x \in L\}$.

- xR_Ly se e só se $\forall z \in \Sigma^\star(xz \in L \Leftrightarrow yz \in L)$. $[x]$ denota a classe de equivalência de x para R_L.

Assim, temos:

- $[\varepsilon]$ é o estado inicial; $[\varepsilon] \notin F$ porque $\varepsilon \notin L$.
- $\delta([\varepsilon], 0) \stackrel{\text{def}}{=} [\varepsilon 0] = [0] \neq [\varepsilon]$, pois $(0, \varepsilon) \notin R_L$, porque $0 \in L$ e $\varepsilon \notin L$.
  Logo, $[0]$ é um **novo estado** e $[0] \in F$ pois $0 \in L$.

  Para ver que $(0, \varepsilon) \notin R_L$, tomamos $z = \varepsilon$ para ter $0z \in L$ e $\varepsilon z \notin L$.

Exemplo 1

AFD mínimo para $L = \{x \mid x$ começa por $0\}$, com $\Sigma = \{0, 1, 2\}$?

- Partimos do **estado inicial** $[\varepsilon]$. Vamos analisar as transições e ver se surjem novos estados, sabendo que δ é dada por

$$\delta([x], a) \stackrel{\text{def}}{=} [xa], \text{ para todo } a \in \Sigma \text{ e } x \in \Sigma^\star.$$

  O conjunto de **estados finais** é $F = \{\, [x] \mid x \in L\}$.

- xR_Ly se e só se $\forall z \in \Sigma^\star(xz \in L \Leftrightarrow yz \in L)$. $[x]$ denota a classe de equivalência de x para R_L.

Assim, temos:

- $[\varepsilon]$ é o estado inicial; $[\varepsilon] \notin F$ porque $\varepsilon \notin L$.
- $\delta([\varepsilon], 0) \stackrel{\text{def}}{=} [\varepsilon 0] = [0] \neq [\varepsilon]$, pois $(0, \varepsilon) \notin R_L$, porque $0 \in L$ e $\varepsilon \notin L$. Logo, $[0]$ é um **novo estado** e $[0] \in F$ pois $0 \in L$.

  Para ver que $(0, \varepsilon) \notin R_L$, tomamos $z = \varepsilon$ para ter $0z \in L$ e $\varepsilon z \notin L$.

Exemplo 1

AFD mínimo para $L = \{x \mid x$ começa por $0\}$, com $\Sigma = \{0, 1, 2\}$?

- Partimos do **estado inicial** $[\varepsilon]$. Vamos analisar as transições e ver se surjem novos estados, sabendo que δ é dada por

$$\delta([x], a) \stackrel{\text{def}}{=} [xa], \text{ para todo } a \in \Sigma \text{ e } x \in \Sigma^\star.$$

  O conjunto de **estados finais** é $F = \{\, [x] \mid x \in L\}$.

- xR_Ly se e só se $\forall z \in \Sigma^\star(xz \in L \Leftrightarrow yz \in L)$. $[x]$ denota a classe de equivalência de x para R_L.

Assim, temos:

- $[\varepsilon]$ é o estado inicial; $[\varepsilon] \notin F$ porque $\varepsilon \notin L$.
- $\delta([\varepsilon], 0) \stackrel{\text{def}}{=} [\varepsilon 0] = [0] \neq [\varepsilon]$, pois $(0, \varepsilon) \notin R_L$, porque $0 \in L$ e $\varepsilon \notin L$. Logo, $[0]$ é um **novo estado** e $[0] \in F$ pois $0 \in L$.

  Para ver que $(0, \varepsilon) \notin R_L$, tomamos $z = \varepsilon$ para ter $0z \in L$ e $\varepsilon z \notin L$.

Exemplo 1

AFD mínimo para $L = \{x \mid x$ começa por $0\}$, com $\Sigma = \{0, 1, 2\}$?

- Partimos do **estado inicial** $[\varepsilon]$. Vamos analisar as transições e ver se surjem novos estados, sabendo que δ é dada por

$$\delta([x], a) \stackrel{\text{def}}{=} [xa], \text{ para todo } a \in \Sigma \text{ e } x \in \Sigma^\star.$$

  O conjunto de **estados finais** é $F = \{\, [x] \mid x \in L\}$.

- xR_Ly se e só se $\forall z \in \Sigma^\star(xz \in L \Leftrightarrow yz \in L)$. $[x]$ denota a classe de equivalência de x para R_L.

Assim, temos:

- $[\varepsilon]$ é o estado inicial; $[\varepsilon] \notin F$ porque $\varepsilon \notin L$.
- $\delta([\varepsilon], 0) \stackrel{\text{def}}{=} [\varepsilon 0] = [0] \neq [\varepsilon]$, pois $(0, \varepsilon) \notin R_L$, porque $0 \in L$ e $\varepsilon \notin L$. Logo, $[0]$ é um **novo estado** e $[0] \in F$ pois $0 \in L$.

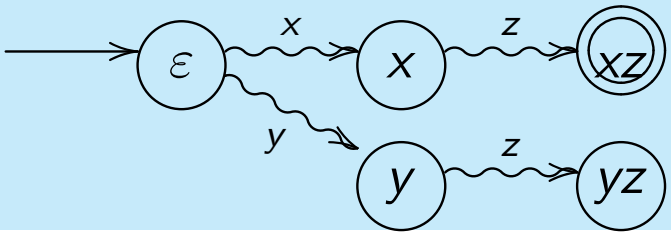
  Para ver que $(0, \varepsilon) \notin R_L$, tomamos $z = \varepsilon$ para ter $0z \in L$ e $\varepsilon z \notin L$.

Exemplo 1 (cont)

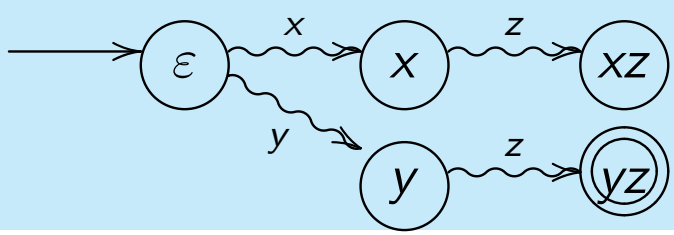
Recordar que $(x, y) \in R_L$ se e só se $\forall z \in \Sigma^\star(xz \in L \Leftrightarrow yz \in L)$ **quer dizer que**

$$(x, y) \notin R_L \text{ se e só se } \exists z \in \Sigma^\star(xz \in L \wedge yz \notin L) \vee (xz \notin L \wedge yz \in L)$$

o que significa que se $(x, y) \notin R_L$, existe alguma palavra z que obriga o AFD mínimo a distinguir $[x]$ de $[y]$, para poder ter $[xz] \neq [yz]$.



ou



- $\delta([\varepsilon], 1) \stackrel{\text{def}}{=} [\varepsilon 1] = [1]$. $[1]$ é um **novo estado** e $[1] \notin F$.

  Porquê?

  $[1] \neq [0]$ pois, como $1 \notin L$ e $0 \in L$, temos $(1, 0) \notin R_L$. Tomamos $z = \varepsilon$.

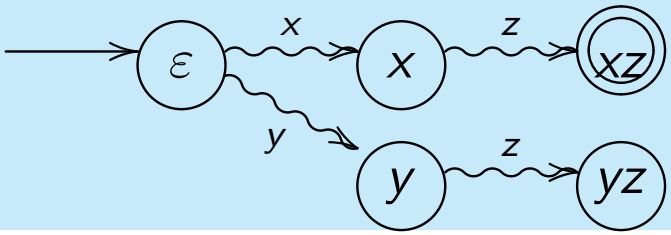
  $[1] \neq [\varepsilon]$ pois, embora $1 \notin L$ e $\varepsilon \notin L$, sabemos que $1z \notin L$, para todo $z \in \Sigma^\star$, o que não é verdade para ε. Para $z = 0$, temos $\varepsilon z = \varepsilon 0 = 0 \in L$ e $1z = 10 \notin L$.

Exemplo 1 (cont)

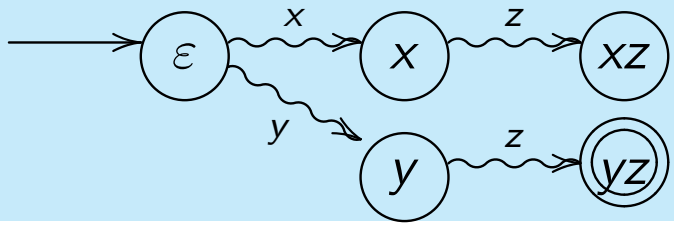
Recordar que $(x, y) \in R_L$ se e só se $\forall z \in \Sigma^\star(xz \in L \Leftrightarrow yz \in L)$ **quer dizer que**

$$(x, y) \notin R_L \text{ se e só se } \exists z \in \Sigma^\star(xz \in L \wedge yz \notin L) \vee (xz \notin L \wedge yz \in L)$$

o que significa que se $(x, y) \notin R_L$, existe alguma palavra z que obriga o AFD mínimo a distinguir $[x]$ de $[y]$, para poder ter $[xz] \neq [yz]$.



ou



- $\delta([\varepsilon], 1) \stackrel{\text{def}}{=} [\varepsilon 1] = [1]$. $[1]$ é um **novo estado** e $[1] \notin F$.

  Porquê?

  $[1] \neq [0]$ pois, como $1 \notin L$ e $0 \in L$, temos $(1, 0) \notin R_L$. Tomamos $z = \varepsilon$.

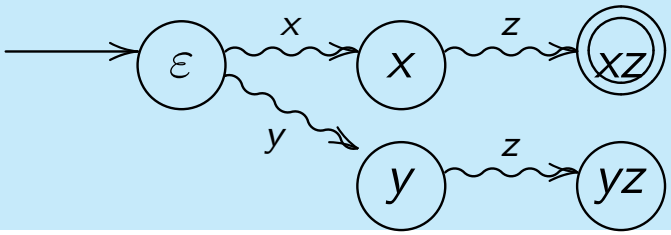
  $[1] \neq [\varepsilon]$ pois, embora $1 \notin L$ e $\varepsilon \notin L$, sabemos que $1z \notin L$, para todo $z \in \Sigma^\star$, o que não é verdade para ε. Para $z = 0$, temos $\varepsilon z = \varepsilon 0 = 0 \in L$ e $1z = 10 \notin L$.

Exemplo 1 (cont)

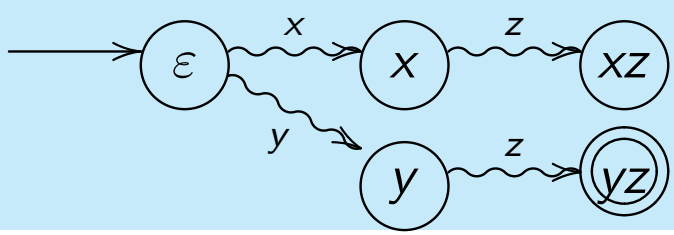
Recordar que $(x, y) \in R_L$ se e só se $\forall z \in \Sigma^\star(xz \in L \Leftrightarrow yz \in L)$ **quer dizer que**

$$(x, y) \notin R_L \text{ se e só se } \exists z \in \Sigma^\star(xz \in L \wedge yz \notin L) \vee (xz \notin L \wedge yz \in L)$$

o que significa que se $(x, y) \notin R_L$, existe alguma palavra z que obriga o AFD mínimo a distinguir $[x]$ de $[y]$, para poder ter $[xz] \neq [yz]$.



ou



- $\delta([\varepsilon], 1) \stackrel{\text{def}}{=} [\varepsilon 1] = [1]$. $[1]$ é um **novo estado** e $[1] \notin F$.

  Porquê?

  $[1] \neq [0]$ pois, como $1 \notin L$ e $0 \in L$, temos $(1, 0) \notin R_L$. Tomamos $z = \varepsilon$.

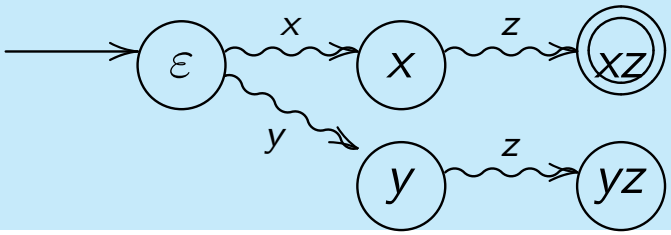
  $[1] \neq [\varepsilon]$ pois, embora $1 \notin L$ e $\varepsilon \notin L$, sabemos que $1z \notin L$, para todo $z \in \Sigma^\star$, o que não é verdade para ε. Para $z = 0$, temos $\varepsilon z = \varepsilon 0 = 0 \in L$ e $1z = 10 \notin L$.

Exemplo 1 (cont)

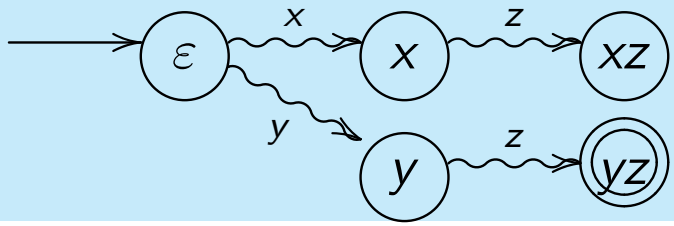
Recordar que $(x, y) \in R_L$ se e só se $\forall z \in \Sigma^\star(xz \in L \Leftrightarrow yz \in L)$ **quer dizer que**

$$(x, y) \notin R_L \text{ se e só se } \exists z \in \Sigma^\star(xz \in L \wedge yz \notin L) \vee (xz \notin L \wedge yz \in L)$$

o que significa que se $(x, y) \notin R_L$, existe alguma palavra z que obriga o AFD mínimo a distinguir $[x]$ de $[y]$, para poder ter $[xz] \neq [yz]$.



ou



- $\delta([\varepsilon], 1) \stackrel{\text{def}}{=} [\varepsilon 1] = [1]$. $[1]$ é um **novo estado** e $[1] \notin F$.

  Porquê?

  $[1] \neq [0]$ pois, como $1 \notin L$ e $0 \in L$, temos $(1, 0) \notin R_L$. Tomamos $z = \varepsilon$.

  $[1] \neq [\varepsilon]$ pois, embora $1 \notin L$ e $\varepsilon \notin L$, sabemos que $1z \notin L$, para todo $z \in \Sigma^\star$, o que não é verdade para ε. Para $z = 0$, temos $\varepsilon z = \varepsilon 0 = 0 \in L$ e $1z = 10 \notin L$.

Exemplo 1 (cont)

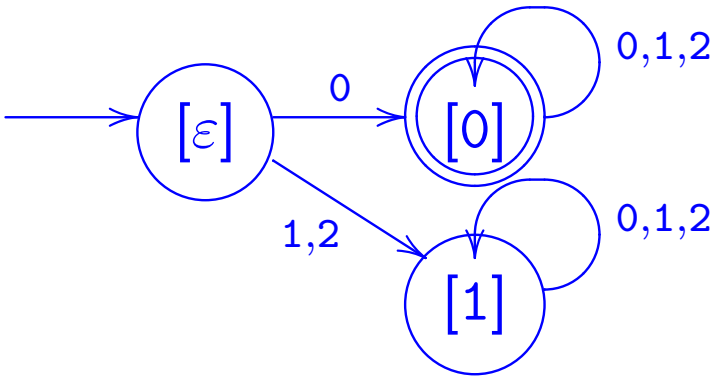
- $\delta([\varepsilon], 2) \stackrel{\text{def}}{=} [2] = [1]$, porque se tem $2z \notin L$, para todo $z \in \Sigma^\star$, à semelhança da palavra 1. Se começar por 1 ou 2, é rejeitada independentemente dos restantes símbolos.
- $\delta([0], 0) \stackrel{\text{def}}{=} [00] = [0]$, porque $00z \in L$, para todo $z \in \Sigma^\star$, à semelhança da palavra 0. Se começar por 0, é sempre aceite.
  $\delta([0], 1) \stackrel{\text{def}}{=} [01] = [0]$, porque $01z \in L$, para todo $z \in \Sigma^\star$.
  $\delta([0], 2) \stackrel{\text{def}}{=} [02] = [0]$, porque $02z \in L$, para todo $z \in \Sigma^\star$.
- $\delta([1], 0) = \delta([1], 1) = \delta([1], 2) = [1]$, porque $[10] = [11] = [12] = [1]$.
  Notar que $1z \notin L$, $10z \notin L$, $11z \notin L$, $12z \notin L$, para todo $z \in \Sigma^\star$.

Exemplo 1 (cont)

- $\delta([\varepsilon], 2) \stackrel{\text{def}}{=} [2] = [1]$, porque se tem $2z \notin L$, para todo $z \in \Sigma^\star$, à semelhança da palavra 1. Se começar por 1 ou 2, é rejeitada independentemente dos restantes símbolos.
- $\delta([0], 0) \stackrel{\text{def}}{=} [00] = [0]$, porque $00z \in L$, para todo $z \in \Sigma^\star$, à semelhança da palavra 0. Se começar por 0, é sempre aceite.
  $\delta([0], 1) \stackrel{\text{def}}{=} [01] = [0]$, porque $01z \in L$, para todo $z \in \Sigma^\star$.
  $\delta([0], 2) \stackrel{\text{def}}{=} [02] = [0]$, porque $02z \in L$, para todo $z \in \Sigma^\star$.
- $\delta([1], 0) = \delta([1], 1) = \delta([1], 2) = [1]$, porque $[10] = [11] = [12] = [1]$.
  Notar que $1z \notin L$, $10z \notin L$, $11z \notin L$, $12z \notin L$, para todo $z \in \Sigma^\star$.

Exemplo 1 (cont)

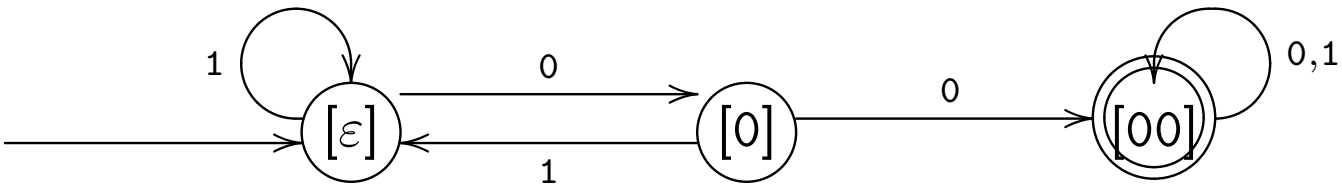
- $\delta([\varepsilon], 2) \stackrel{\text{def}}{=} [2] = [1]$, porque se tem $2z \notin L$, para todo $z \in \Sigma^\star$, à semelhança da palavra 1. Se começar por 1 ou 2, é rejeitada independentemente dos restantes símbolos.
- $\delta([0], 0) \stackrel{\text{def}}{=} [00] = [0]$, porque $00z \in L$, para todo $z \in \Sigma^\star$, à semelhança da palavra 0. Se começar por 0, é sempre aceite.
  $\delta([0], 1) \stackrel{\text{def}}{=} [01] = [0]$, porque $01z \in L$, para todo $z \in \Sigma^\star$.
  $\delta([0], 2) \stackrel{\text{def}}{=} [02] = [0]$, porque $02z \in L$, para todo $z \in \Sigma^\star$.
- $\delta([1], 0) = \delta([1], 1) = \delta([1], 2) = [1]$, porque $[10] = [11] = [12] = [1]$.
  Notar que $1z \notin L$, $10z \notin L$, $11z \notin L$, $12z \notin L$, para todo $z \in \Sigma^\star$.



Exemplo 2

Seja $L = \{x \mid x \text{ tem } 00 \text{ como subpalavra}\}$, com $\Sigma = \{0, 1\}$.

- Estado inicial: $[\varepsilon]$. Não é estado final porque $\varepsilon \notin L$.
- $\delta([\varepsilon], 0) \stackrel{\text{def}}{=} [0] \neq [\varepsilon]$, porque $\varepsilon 0 \notin L$ e $00 \in L$.
  $[0]$ é um novo estado e não é final pois $0 \notin L$.
- $\delta([\varepsilon], 1) \stackrel{\text{def}}{=} [1] = [\varepsilon]$, porque $1z \in L$ sse z tem 00 como subpalavra, i.e., $z \in L$ e, analogamente, $\varepsilon z \in L$ sse $z \in L$.
- $\delta([0], 1) \stackrel{\text{def}}{=} [01] = [\varepsilon]$, porque $01z \in L$ sse $z \in L$.
- $\delta([0], 0) \stackrel{\text{def}}{=} [00]$. É um estado novo e é final porque $00 \in L$. Com $z = \varepsilon$, podiamos ver que $(00, 0) \notin R_L$ e $(00, \varepsilon) \notin R_L$.
- $\delta([00], 0) = \delta([00], 1) = [00]$ porque $000z \in L$ sse $z \in \Sigma^\star$, à semelhança de $00z$ e de $001z$.



Teorema de Myhill-Nerode

Definições:

Diz-se que uma relação binária R definida em $\Sigma^\star$ é **invariante à direita para a concatenação** *se e só se* $\forall x, y \in \Sigma^\star \quad \forall z \in \Sigma^\star \quad (x\ R\ y \quad \Rightarrow \quad xz\ R\ yz)$.

Uma relação de equivalência é de **índice finito** *sse tem um número finito de classes.*

Enunciado do Teorema de Myhill-Nerode

As três afirmações seguintes, sobre uma linguagem L de $\Sigma^\star$, são equivalentes:

1. L é aceite por um autómato finito.
2. L é união de classes de equivalência de alguma relação de equivalência invariante à direita (para a concatenação) e de índice finito.
3. A relação de equivalência R_L é de índice finito.

A **caraterização do AFD mínimo para** L resulta da prova que iremos apresentar. Para a prova das três equivalências, basta mostrar que ① $\Rightarrow$ ② $\Rightarrow$ ③ $\Rightarrow$ ①.

Prova do Teorema de Myhill-Nerode

(1) $\Rightarrow$ (2)

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um AFD que aceita L. Seja $R_{\mathcal{A}}$ a relação definida em $\Sigma^\star$ por

$$\forall x, y \in \Sigma^\star \quad (x \; R_{\mathcal{A}} \; y \quad sse \quad \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \;)$$

ou seja, $xR_{\mathcal{A}}y$ sse x e y levam $\mathcal{A}$ do estado inicial ao mesmo estado.

- $R_{\mathcal{A}}$ é de equivalência.
- $R_{\mathcal{A}}$ é invariante à direita pois
  $\forall z \in \Sigma^\star \;\; x \; R_{\mathcal{A}} \; y \Rightarrow \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \Rightarrow \hat{\delta}(s_0, xz) = \hat{\delta}(s_0, yz) \Rightarrow xz \; R_{\mathcal{A}} \; yz$.
- $R_{\mathcal{A}}$ é de índice finito. O número de classes de $R_{\mathcal{A}}$ não excede o número de estados de $\mathcal{A}$, sendo $|S|$ se todos os estados de $\mathcal{A}$ forem acessíveis de s_0.
- L é união de classes de $R_{\mathcal{A}}$. Cada estado final de $\mathcal{A}$ que seja acessível de s_0 identifica-se com uma classe de $R_{\mathcal{A}}$ à qual só pertencem palavras reconhecidas pelo autómato (isto é, palavras de L). $\square$

Prova do Teorema de Myhill-Nerode

(2) $\Rightarrow$ (3)

Vamos provar que **se** L é reunião de classes de equivalência de alguma relação R de equivalência, invariante à direita e de índice finito, **então** cada classe $\mathcal{C}$ de R está contida em alguma classe de R_L. Tal permite concluir R_L é de índice finito, pois R é de índice finito e o número de classes de R_L não excede o número de classes de R.

Sejam $x, y \in \mathcal{C}$. Como R é invariante à direita e xRy então, qualquer que seja $z \in \Sigma^\star$, tem-se $xz\ R\ yz$. Ou seja, xz e yz estão na mesma classe de R.

Como L é união de classes de R, então $xz \in L$ sse $yz \in L$, pois cada classe de R tem ou palavras de L ou palavras de $\Sigma^\star \setminus L$.

Como z é qualquer e $xz \in L \Leftrightarrow yz \in L$ então $x\ R_L\ y$.

Logo, $x\ R\ y \Rightarrow x\ R_L\ y$ quaisquer que sejam $x, y \in \Sigma^\star$, ou seja, qualquer classe de R está contida em alguma das classes de R_L. $\square$

Prova do Teorema de Myhill-Nerode

(3) $\Rightarrow$ (1)

Dizer que R_L é de índice finito significa que $\Sigma^\star/R_L$ é finito. Defina-se o AFD

$$\mathcal{A} = (\Sigma^\star/R_L, \Sigma, [\epsilon], F, \delta)$$

em que o conjunto de estados $\Sigma^\star/R_L$ é o conjunto das classes de R_L, o estado inicial $[\epsilon]$ é a classe da palavra vazia, $F = \{[x] \mid x \in L\}$, e a função δ é dada por

$$\delta([x], a) \stackrel{\text{def}}{=} [xa], \quad \text{quaisquer que sejam } x \in \Sigma^\star \text{ e } a \in \Sigma,$$

onde $[x]$ denota a classe de equivalência de x. Pode concluir-se que $\mathcal{L}(\mathcal{A}) = L$, pois

$$\hat{\delta}([\epsilon], w) = [w],$$

para todo $w \in \Sigma^\star$, o que significa que w é aceite (i.e., $[w] \in F$) sse $w \in L$.

Notar também que δ não depende da escolha do elemento da classe $[x]$ que usamos na definição, pois se $y \in [x]$ então yaR_Lxa. Logo, $[xa] = [ya]$. $\square$

Exemplo 2

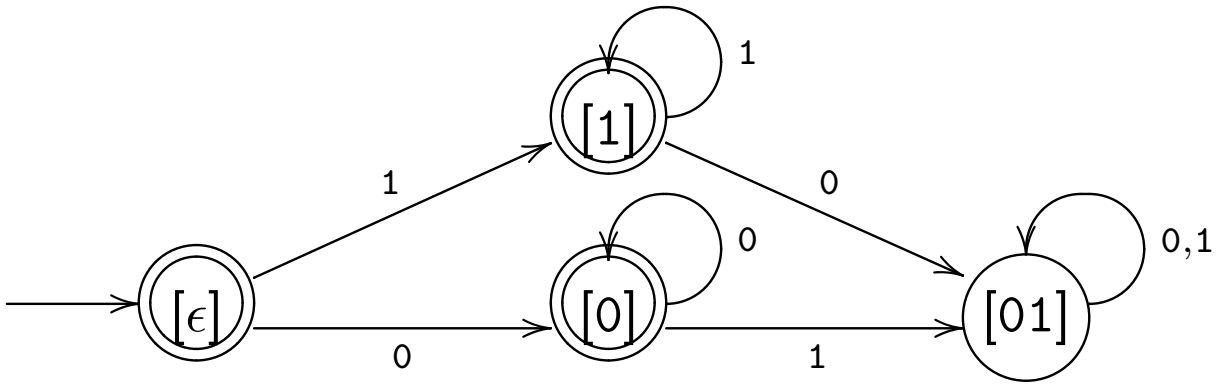
Seja $L = \mathcal{L}(0^\star + 1^\star)$ isto é, $L = \{x \in \{0,1\}^\star \mid x \text{ não tem 0's ou não tem 1's}\}$.
O conjunto das classes de equivalência de R_L é

$$\frac{\Sigma^\star}{R_L} = \{[\varepsilon], [1], [0], [01]\}$$

sendo

$$\begin{array}{lcl} [\varepsilon] & = & \{\epsilon\} \\ [1] & = & \{1^k \mid k \geq 1\} \\ [0] & = & \{0^k \mid k \geq 1\} \\ [01] & = & \{x \in \{0,1\}^\star \mid x \text{ tem 0's e tem 1's}\} \end{array}$$

Notar que $L = [\varepsilon] \cup [0] \cup [1]$. O **AFD mínimo para** L é:



Exemplo 3

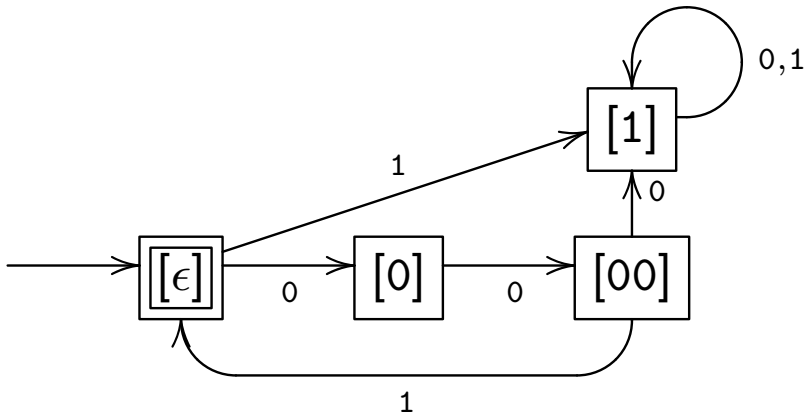
Seja $L = \mathcal{L}(\ (001)^\star\ )$. Por aplicação do corolário do Teorema de Myhill-Nerode, vamos determinar o AFD mínimo para L.

$\delta([\varepsilon], 0) = [0] \neq [\varepsilon]$ pois $(0, \varepsilon) \notin R_L$ já que $0\underline{01} \in L$ e $\varepsilon\underline{01} \notin L$.
$\delta([\varepsilon], 1) = [1]$, e $[1] \neq [\varepsilon]$ pois $(1, \varepsilon) \notin R_L$ já que $1\underline{\varepsilon} \notin L$ e $\varepsilon\underline{\varepsilon} \in L$; também $[1] \neq [0]$.

$\delta([1], 1) = [11] = [1]$ porque $\forall z \in \Sigma^\star\ 1z \notin L$ e também $\forall z \in \Sigma^\star\ 11z \notin L$.
$\delta([1], 0) = [10] = [1]$ porque $\forall z \in \Sigma^\star\ 10z \notin L$.

$\delta([0], 1) = [01] = [1]$.
$\delta([0], 0) = [00]$ um novo estado porque $00 \notin [0]$, $00 \notin [\varepsilon]$ e $00 \notin [1]$.

$\delta([00], 1) = [001] = [\varepsilon]$, porque $001z \in L$ se e só se $z \in L$.
$\delta([00], 0) = [000] = [1]$, porque $\forall z \in \Sigma^\star\ 000z \notin L$.



Teorema de Myhill-Nerode: ainda sobre ② ⇒ ③

Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um AFD. Vimos que a relação $R_{\mathcal{A}}$ definida em $\Sigma^\star$ por

$$\forall x, y \in \Sigma^\star \quad (x \; R_{\mathcal{A}} \; y \;\; \textit{sse} \;\; \hat{\delta}(s_0, x) = \hat{\delta}(s_0, y) \;)$$

satisfaz as condições indicadas em ②. Da prova de ② ⇒ ③ , tem-se

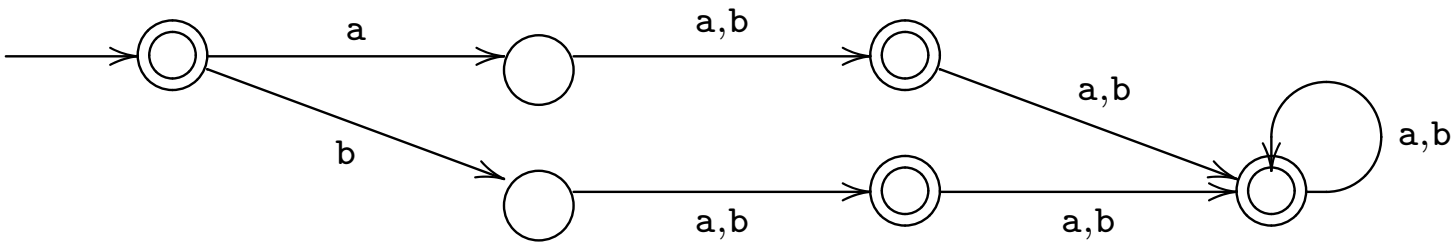
se $x \, R_{\mathcal{A}} \, y$ **então** $x \, R_L \, y$.

para $x, y \in \Sigma^\star$. Logo, se C_x é classe de x para $R_{\mathcal{A}}$ então $C_x \subseteq [x]$, sendo $[x]$ a classe para R_L. Logo,

$$\#(\Sigma^\star / R_L) \leq \#(\Sigma^\star / R_{\mathcal{A}}) \leq \#S$$

O número de estados de qualquer AFD que aceita L não é inferior ao número de estados do AFD que definimos como o AFD mínimo que aceita L.

Exemplo 4: $\{a, b\}^\star \setminus \{a, b\}$



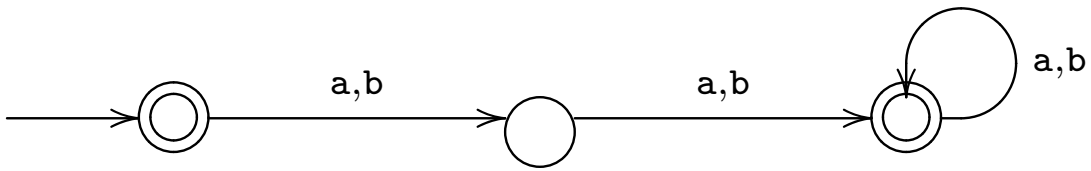
As classes de equivalência de $R_\mathcal{A}$ são

$$\begin{array}{llll} \mathcal{C}_\varepsilon & = & \{\varepsilon\}, & \mathcal{C}_a = \{a\}, \\ \mathcal{C}_b & = & \{b\}, & \mathcal{C}_{aa} = \{aa, ab\}, \\ \mathcal{C}_{ba} & = & \{ba, bb\} & \mathcal{C}_{aaa} = \{x \mid x \in \{a, b\}^\star,\ |x| \geq 3\} \end{array}$$

Para $L = \mathcal{L}(\mathcal{A})$, as classes de equivalência de R_L são $[\varepsilon] = \{\varepsilon\}$, $[a] = \{a, b\}$, e $[aa] = \{x \mid x \in \{a, b\}^\star,\ |x| \geq 2\}$.

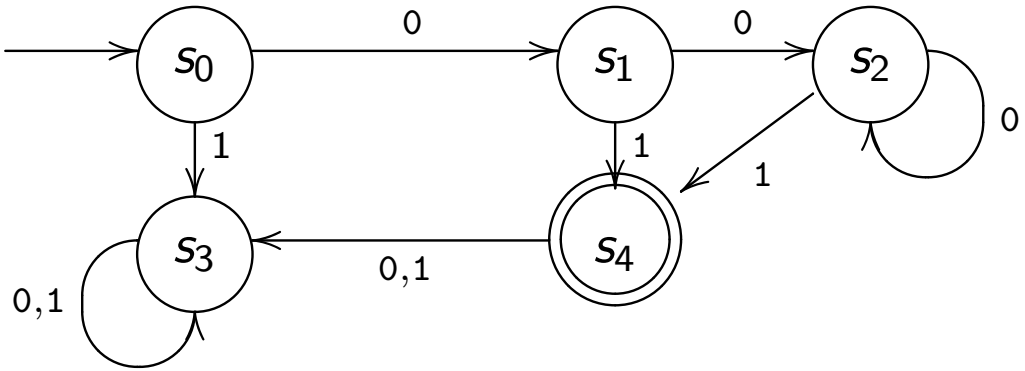
$$L = \mathcal{C}_\varepsilon \cup \mathcal{C}_{aa} \cup \mathcal{C}_{ba} \cup \mathcal{C}_{aaa} = [\varepsilon] \cup [aa]$$

e $[aa] = \mathcal{C}_{aa} \cup \mathcal{C}_{ba} \cup \mathcal{C}_{aaa}$, $[a] = \mathcal{C}_a \cup \mathcal{C}_b$ e $[\varepsilon] = \mathcal{C}_\varepsilon$. O AFD mínimo é:



Exemplo 5

O AFD seguinte reconhece $L = \mathcal{L}(00^\star 1)$.



As classes de equivalência de $R_{\mathcal{A}}$ são

$$\begin{aligned}
\mathcal{C}_\varepsilon &= \{\varepsilon\} = \{x \mid \hat{\delta}(s_0, x) = s_0\} \\
\mathcal{C}_0 &= \{0\} = \{x \mid \hat{\delta}(s_0, x) = s_1\} \\
\mathcal{C}_1 &= \mathcal{L}(1 + 0^\star 1(0+1)(0+1)^\star) = \{x \mid \hat{\delta}(s_0, x) = s_3\} \\
\mathcal{C}_{00} &= \{0^n \mid n \geq 2\} = \{x \mid \hat{\delta}(s_0, x) = s_2\} \\
\mathcal{C}_{001} &= L = \{x \mid \hat{\delta}(s_0, x) = s_4\}
\end{aligned}$$

As classes de equivalência de R_L: $[\varepsilon] = \{\varepsilon\}$, $[0] = \{0^n \mid n \in \mathbb{N}\}$, $= \mathcal{C}_0 \cup \mathcal{C}_{00}$, e $[001] = L$ e $[1] = \mathcal{C}_1$.

Existência de linguagens que não são regulares

Pelo teorema de Myhill-Nerode, L **é regular se e só se** R_L **é de índice finito.**

Exemplos de linguagens que não são regulares

$\{0^n 1^n \mid n \in \mathbb{N}\}$ de alfabeto $\{0, 1\}$

$\{0^n 1^n 2^n \mid n \in \mathbb{N}\}$ de alfabeto $\{0, 1, 2\}$

$\{0^n \mid n \text{ primo}\}$ de alfabeto $\{0\}$

$L = \{0^n 1^n \mid n \in \mathbb{N}\}$ não é regular

Prova (por redução ao absurdo):
Se $L = \{0^n 1^n \mid n \in \mathbb{N}\}$ fosse regular, existia um AFD $\mathcal{A}$ tal que $L = \mathcal{L}(\mathcal{A})$.
Seja s_0 o estado inicial de $\mathcal{A}$. Sejam $n_1, n_2 \in \mathbb{N}$ tais que $n_1 \neq n_2$. Como $\mathcal{A}$ é determinístico,

$$\text{se } \hat{\delta}(s_0, 0^{n_1}) = \hat{\delta}(s_0, 0^{n_2}) \text{ então } \hat{\delta}(s_0, 0^{n_1}1^{n_1}) = \hat{\delta}(s_0, 0^{n_2}1^{n_1})$$

o que é absurdo, pois $0^{n_1}1^{n_1} \in L$ mas $0^{n_2}1^{n_1} \notin L$.
Assim, $\forall n_1, n_2 \in \mathbb{N}\ \ \hat{\delta}(s_0, 0^{n_1}) = \hat{\delta}(s_0, 0^{n_2})$ se e só se $n_1 = n_2$. Logo, o conjunto de estados não é finito. Portanto $\mathcal{A}$ não existe. □

Prova (pelo Teorema de Myhill-Nerode):
Se $n_1 \neq n_2$, as palavras 0^{n_1} e 0^{n_2} estão em classes distintas de R_L pois $0^{n_1}1^{n_1} \in L$ mas $0^{n_2}1^{n_1} \notin L$. Logo, R_L não é de índice finito e, portanto, L não é regular. □

Minimização de AFDs

Dado um AFD $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$, podemos aplicar **o algoritmo de Moore** para:

- decidir se $\mathcal{A}$ é ou não o AFD mínimo que reconhece $\mathcal{L}(A)$;
- se não for mínimo, obter o AFD mínimo que reconhece $\mathcal{L}(A)$, se $\mathcal{A}$ não for mínimo.

O Algoritmo de Moore vai determinar a relação de equivalência em S definida por:

> $s \equiv s'$ *se e só se* **não** *existe uma palavra* $z \in \Sigma^\star$ *tal que se consumir* z *a partir de* s *chega a estado final e se consumir* z *a partir de* s' *não chega a estado final, ou vice-versa .*

Ou seja, $s \equiv s'$ sse as palavras que levam $\mathcal{A}$ de s_0 a s e as que levam de s_0 a s' são equivalentes segundo $R_{\mathcal{L}(A)}$.

Algoritmo de Moore

- Retirar de S os estados não acessíveis de s_0. Seja $S' = \{s_0, s_1, \ldots, s_m\}$ o conjunto dos restantes.
- Para representar $\equiv$, construir uma tabela com os pares (s_i, s_j), para $0 \leq i \leq j \leq m$. Os símbolos $\equiv$, `X` e `?` denotam $\equiv$, $\not\equiv$ e **decisão pendente**.
- Cada entrada (s_i, s_j) pode ter uma lista de pares pendentes, que aguardam a decisão sobre se $s_i \not\equiv s_j$
- Para preencher a tabela, assinalar com $\equiv$ todas as entradas (s_i, s_i), para todo i. Para todo (s_i, s_j), com $s_i \in F \wedge s_j \notin F$ ou $s_i \notin F \wedge s_j \in F$, assinalar $s_i \not\equiv s_j$, colocando `X` em (s_i, s_j).

Algoritmo de Moore (cont)

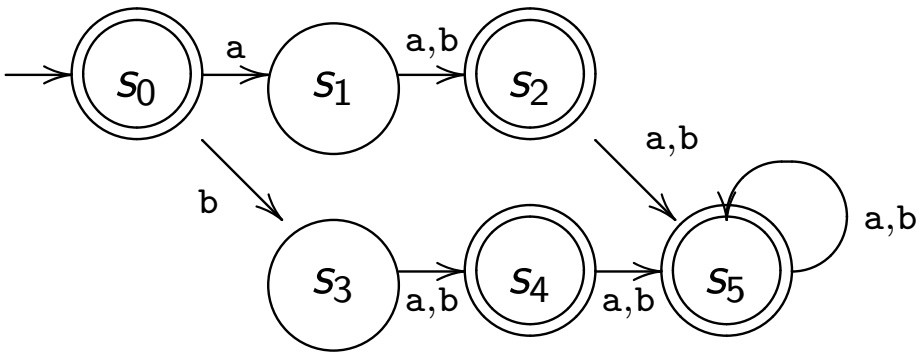
- Para $1 \leq j \leq m$ e $0 \leq i < j$, se (s_i, s_j) não contém `X`, averiguar se já é conhecido que $\delta(s_i, a) \not\equiv \delta(s_j, a)$, para algum $a \in \Sigma$ (para isso, ver se existe `X` na entrada do par $(\delta(s_i, a), \delta(s_j, a))$.
  - Se, para algum $a \in \Sigma$, já for conhecido que $\delta(s_i, a) \not\equiv \delta(s_j, a)$, registar $s_i \not\equiv s_j$, assinalando (s_i, s_j) com `X`, e propagar a informação a todos os pares que estiverem na lista de pendentes de (s_i, s_j). **Propagar** significa assinalar com `X` cada um dos pares nessa lista e, recursivamente, propagar aos pares que estiverem nas listas de pendentes desses.
  - Se já se sabe que $\delta(s_i, a) \equiv \delta(s_j, a)$, para todo $a \in \Sigma$, isto é, todos já estão marcados com $\equiv$ na tabela, então registar $s_i \equiv s_j$, assinalando a entrada (s_i, s_j) com $\equiv$.
  - Nas restantes situações, (s_i, s_j) *aguardará as decisões* para $(\delta(s_i, a), \delta(s_j, a))$, com $a \in \Sigma$: para todos os pares $(\delta(s_i, a), \delta(s_j, a))$ sem marcação $\equiv$, acrescentar (s_i, s_j) à **lista de pendentes** de $(\delta(s_i, a), \delta(s_j, a))$ e assinalar a entrada (s_i, s_j) com o símbolo ? (fica pendente).

Algoritmo de Moore (cont)

- Quando todos os pares estiverem analisados, substituir ? por $\equiv$ nas entradas que se mantiverem pendentes (cada entrada que não tem X, corresponde a um par de estados equivalentes).
- O conjunto de estados do AFD mínimo A' equivalente ao AFD A corresponde ao conjunto de classes de equivalência de $\equiv$ (restrita a $S' = \{s_0, s_1 \ldots, s_m\} \subseteq S$). Se $[s]$ denotar a classe do estado s, então a função de transição δ' é dada por $\delta'([s], a) = [\delta(s, a)]$, para todo $a \in \Sigma$. O estado inicial de A' é $[s_0]$ e o conjunto de estados finais é $F' = \{[s] \mid s \in F \cap S'\}$.

Aplicação do Algoritmo de Moore

Por aplicação do algoritmo de Moore, vamos averiguar se o AFD representado é mínimo.



	s_0	s_1	s_2	s_3	s_4	s_5
s_0	≡					
s_1	X	≡				
s_2		X	≡			
s_3	X		X	≡		
s_4		X		X	≡	
s_5		X		X		≡

A tabela inicial encontra-se acima à direita.

Aplicação do Algoritmo de Moore (cont)

Para os restantes pares, tem-se:

(s_0, s_2) : $s_0 \not\equiv s_2$ porque $\delta(s_0, \mathtt{a}) = s_1 \not\equiv s_5 = \delta(s_2, \mathtt{a})$.

(s_0, s_4) : $s_0 \not\equiv s_4$ porque $\delta(s_0, \mathtt{a}) = s_1 \not\equiv s_5 = \delta(s_4, \mathtt{a})$.

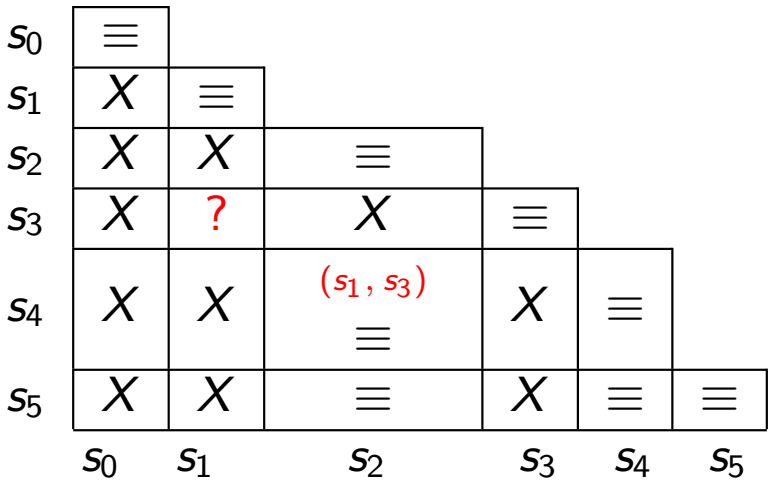
(s_0, s_5) : $s_0 \not\equiv s_5$ porque $\delta(s_0, \mathtt{a}) = s_1 \not\equiv s_5 = \delta(s_5, \mathtt{a})$.

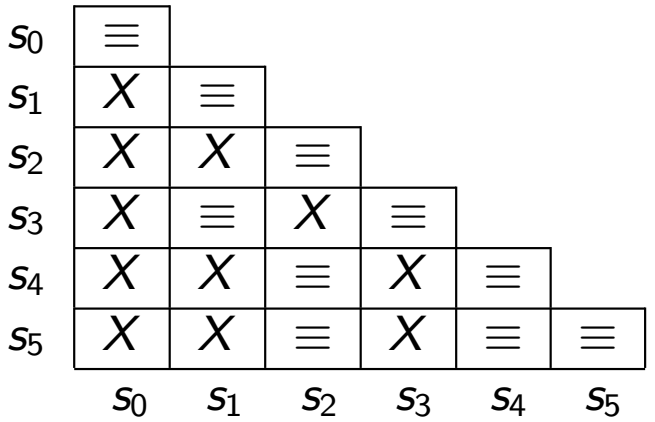
(s_1, s_3) : $\delta(s_1, \mathtt{a}) = s_2 = \delta(s_1, \mathtt{b})$ e $\delta(s_3, \mathtt{a}) = s_4 = \delta(s_3, \mathtt{b})$.
Fica pendente. Assinalar dependência em (s_2, s_4).

(s_2, s_4) : $s_2 \equiv s_4$ pois $\delta(s_2, \mathtt{a}) = \delta(s_4, \mathtt{a})$ e $\delta(s_2, \mathtt{b}) = \delta(s_4, \mathtt{b})$.

(s_2, s_5) : $s_2 \equiv s_5$ pois $\delta(s_2, \mathtt{a}) = \delta(s_5, \mathtt{a})$ e $\delta(s_2, \mathtt{b}) = \delta(s_5, \mathtt{b})$.

(s_4, s_5) : $s_4 \equiv s_5$ pois $\delta(s_4, \mathtt{a}) = \delta(s_5, \mathtt{a})$ e $\delta(s_4, \mathtt{b}) = \delta(s_5, \mathtt{b})$.





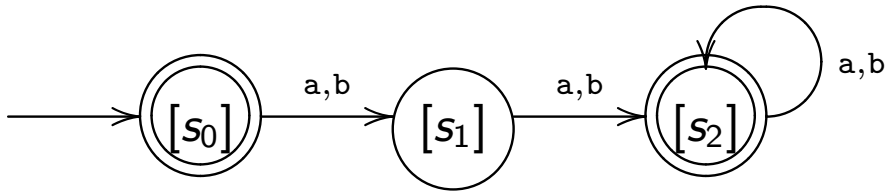
A tabela final (à direita) corresponde à (parte triangular inferior da) matriz da relação $\equiv$, se substituirmos $\equiv$ por 1 e `X` por 0.

Aplicação do Algoritmo de Moore (cont)

As classes de eqivalência de $\equiv$ são:

$$\{s_0\},\ \{s_1, s_3\},\ \{s_2, s_4, s_5\}.$$

O AFD mínimo equivalente ao AFD dado é:



Lema da Repetição para linguagens regulares

Lema da repetição

Qualquer que seja a linguagem de alfabeto Σ, **se** L é regular **então**

$$\exists_{n\in\mathbb{Z}^+}\forall_{x\in L}\ \ |x|\geq n\ \Rightarrow(\exists_{u,v,w}\ x=uvw\ \wedge\ v\neq\varepsilon\ \wedge\ |uv|\leq n\wedge\ (\forall_{i\geq 0}\ \ uv^iw\in L))$$

ou seja, existe uma constante $n\in\mathbb{N}\setminus\{0\}$ tal que, se $x\in L\wedge|x|\geq n$, podemos decompor x como $x=uvw$, com $|uv|\leq n$ e $|v|\geq 1$, e $\forall i\geq 0\ \ uv^iw\in L$. Mais ainda, n não excede o número de estados do menor autómato finito que aceita L.

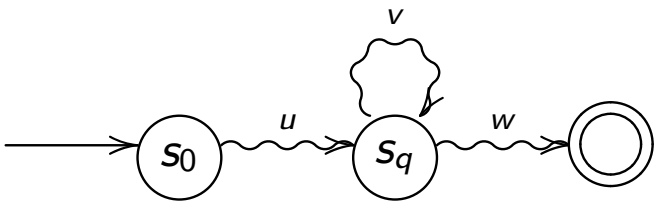
Observação:

- O Teorema de Myhill-Nerode dá uma condição necessária e suficiente para L ser regular. O lema da repetição dá apenas uma condição necessária. Existem linguagens que satisfazem a condição do lema e não são regulares. Por exemplo, $L=\{0^m1^k01^k\mid m\geq 1,k\geq 0\}\cup\{1^q0^r1^s\ \mid q,r,s\geq 0\}$.
- As **linguagens finitas** satisfazem trivialmente a condição, para $n=1+\max_{x\in L}|x|$.

Lema da Repetição ("Pumping Lemma")

Prova do lema da repetição:

- Seja L uma linguagem regular. Seja $\mathcal{A} = (S, \Sigma, \delta, s_0, F)$ um AF com menor número de estados que aceita L. Sem perda de generalidade, **assumimos que $\mathcal{A}$ é um AFND** e tomamos $n = |S|$.
- Seja $x \in L$, tal que $|x| \geq n$. Para processar x, o AFND efetua $|x|$ transições, que envolvem $|x| + 1$ estados. Repete estados pois $|x| + 1 > n$.
- Seja s_q o **primeiro estado que se repete** nessa análise e u o prefixo de x processado até chegar a s_q. Seja v a subpalavra processada desde que sai de s_q até regressar pela primeira vez a s_q. Seja w o resto da palavra.



- Tem-se $x = uvw$ com $|v| \geq 1$, pois v corresponde ao ciclo, e $|uv| \leq n$ pois, caso contrário, no processamento de uv existia um outro ciclo, o que contrariava as condições sobre s_q, u, e v.
- Como $\mathcal{A}$ aceita $x = uvw$, aceita uw, $uvvw$, $uvvvw$, $uvvvvw$, $uvvvvw$, ...
  Ou seja, $\mathcal{A}$ aceita $uv^i w$, para todo $i \geq 0$.

Aplicação do lema da repetição

Prova de que $\{0^k 1^k \mid k \geq 0\}$ não é regular, pelo lema da repetição:

- Se L fosse regular, satisfazia a condição do lema da repetição.
- Seja $n \in \mathbb{N}$ qualquer. Se *escolhemos* $x = 0^n 1^n$, temos $x \in L$ e $|x| = 2n \geq n$. Vamos ver que quaisquer que sejam $u, v, w \in \Sigma^\star$ tais que $x = uvw$, $|uv| \leq n$ e $v \neq \varepsilon$, tem-se $\exists i \in \mathbb{N}\ \ uv^i w \notin L$.
- Como $|uv| \leq n$ e $x = uvw$ podemos afirmar que $uv = 0^p$ para algum $p \leq n$, e como $|v| \geq 1$ temos $p \neq 0$.
- Se tomarmos $i = 0$ a palavra $uv^i w = uw$ não pertence a L porque tem n 1's mas apenas $n - |v|$ 0's.

  Logo, L não é regular. □

Aplicação do lema da repetição

Prova de que $\{0^k 1^k \mid k \geq 0\}$ não é regular, pelo lema da repetição:

- Se L fosse regular, satisfazia a condição do lema da repetição.
- Seja $n \in \mathbb{N}$ qualquer. Se *escolhemos* $x = 0^n 1^n$, temos $x \in L$ e $|x| = 2n \geq n$. Vamos ver que quaisquer que sejam $u, v, w \in \Sigma^\star$ tais que $x = uvw$, $|uv| \leq n$ e $v \neq \varepsilon$, tem-se $\exists i \in \mathbb{N}\ \ uv^i w \notin L$.
- Como $|uv| \leq n$ e $x = uvw$ podemos afirmar que $uv = 0^p$ para algum $p \leq n$, e como $|v| \geq 1$ temos $p \neq 0$.
- Se tomarmos $i = 0$ a palavra $uv^i w = uw$ não pertence a L porque tem n 1's mas apenas $n - |v|$ 0's.

  Logo, L não é regular. □

Aplicação do lema da repetição

Prova de que $\{0^k 1^k \mid k \geq 0\}$ não é regular, pelo lema da repetição:

- Se L fosse regular, satisfazia a condição do lema da repetição.
- Seja $n \in \mathbb{N}$ qualquer. Se *escolhemos* $x = 0^n 1^n$, temos $x \in L$ e $|x| = 2n \geq n$.
  Vamos ver que quaisquer que sejam $u, v, w \in \Sigma^\star$ tais que $x = uvw$, $|uv| \leq n$ e $v \neq \varepsilon$, tem-se $\exists i \in \mathbb{N}\ \ uv^i w \notin L$.
- Como $|uv| \leq n$ e $x = uvw$ podemos afirmar que $uv = 0^p$ para algum $p \leq n$, e como $|v| \geq 1$ temos $p \neq 0$.
- Se tomarmos $i = 0$ a palavra $uv^i w = uw$ não pertence a L porque tem n 1's mas apenas $n - |v|$ 0's.

  Logo, L não é regular. □

Aplicação do lema da repetição

Prova de que $\{0^k 1^k \mid k \geq 0\}$ não é regular, pelo lema da repetição:

- Se L fosse regular, satisfazia a condição do lema da repetição.
- Seja $n \in \mathbb{N}$ qualquer. Se *escolhemos* $x = 0^n 1^n$, temos $x \in L$ e $|x| = 2n \geq n$. Vamos ver que quaisquer que sejam $u, v, w \in \Sigma^\star$ tais que $x = uvw$, $|uv| \leq n$ e $v \neq \varepsilon$, tem-se $\exists i \in \mathbb{N} \;\; uv^i w \notin L$.
- Como $|uv| \leq n$ e $x = uvw$ podemos afirmar que $uv = 0^p$ para algum $p \leq n$, e como $|v| \geq 1$ temos $p \neq 0$.
- Se tomarmos $i = 0$ a palavra $uv^i w = uw$ não pertence a L porque tem n 1's mas apenas $n - |v|$ 0's.

  Logo, L não é regular. □

Aplicação do lema da repetição

Prova de que $\{0^k 1^k \mid k \geq 0\}$ não é regular, pelo lema da repetição:

- Se L fosse regular, satisfazia a condição do lema da repetição.
- Seja $n \in \mathbb{N}$ qualquer. Se *escolhemos* $x = 0^n 1^n$, temos $x \in L$ e $|x| = 2n \geq n$. Vamos ver que quaisquer que sejam $u, v, w \in \Sigma^\star$ tais que $x = uvw$, $|uv| \leq n$ e $v \neq \varepsilon$, tem-se $\exists i \in \mathbb{N}\ \ uv^i w \notin L$.
- Como $|uv| \leq n$ e $x = uvw$ podemos afirmar que $uv = 0^p$ para algum $p \leq n$, e como $|v| \geq 1$ temos $p \neq 0$.
- Se tomarmos $i = 0$ a palavra $uv^i w = uw$ não pertence a L porque tem n 1's mas apenas $n - |v|$ 0's.

  Logo, L não é regular. □

Aplicação do lema da repetição

Prova de que $\{0^k 1^k \mid k \geq 0\}$ não é regular, pelo lema da repetição:

- Se L fosse regular, satisfazia a condição do lema da repetição.
- Seja $n \in \mathbb{N}$ qualquer. Se *escolhemos* $x = 0^n 1^n$, temos $x \in L$ e $|x| = 2n \geq n$. Vamos ver que quaisquer que sejam $u, v, w \in \Sigma^\star$ tais que $x = uvw$, $|uv| \leq n$ e $v \neq \varepsilon$, tem-se $\exists i \in \mathbb{N} \;\; uv^i w \notin L$.
- Como $|uv| \leq n$ e $x = uvw$ podemos afirmar que $uv = 0^p$ para algum $p \leq n$, e como $|v| \geq 1$ temos $p \neq 0$.
- Se tomarmos $i = 0$ a palavra $uv^i w = uw$ não pertence a L porque tem n 1's mas apenas $n - |v|$ 0's.

Logo, L não é regular. □

Aplicação do lema da repetição

Prova de que $\{0^k 1^k \mid k \geq 0\}$ não é regular, pelo lema da repetição:

- Se L fosse regular, satisfazia a condição do lema da repetição.
- Seja $n \in \mathbb{N}$ qualquer. Se *escolhemos* $x = 0^n 1^n$, temos $x \in L$ e $|x| = 2n \geq n$. Vamos ver que quaisquer que sejam $u, v, w \in \Sigma^\star$ tais que $x = uvw$, $|uv| \leq n$ e $v \neq \varepsilon$, tem-se $\exists i \in \mathbb{N} \;\; uv^i w \notin L$.
- Como $|uv| \leq n$ e $x = uvw$ podemos afirmar que $uv = 0^p$ para algum $p \leq n$, e como $|v| \geq 1$ temos $p \neq 0$.
- Se tomarmos $i = 0$ a palavra $uv^i w = uw$ não pertence a L porque tem n 1's mas apenas $n - |v|$ 0's.

  Logo, L não é regular. □

Aplicação do lema da repetição

Prova, pelo lema da repetição, de que $L = \{0^p \mid p \text{ primo}\}$ não é regular:

- Seja $n \in \mathbb{N} \setminus \{0\}$ qualquer. Escolhemos $x = 0^M$ com $M > 2n$ e M primo. M existe porque **o conjunto de primos é infinito**.
- Tem-se $x \in L$ e $|x| = M > 2n > n$.
  Seja $x = uvw$, uma qualquer decomposição de x, tal que $|v| \geq 1$ e $|uv| \leq n$. Há que encontrar $i \geq 0$ tal que $uv^i w \notin L$, i.e., tal que $|uv^i w|$ não é primo.
- Mas, $|\, uv^i w \,| = |u| + i\,|v| + |w|$ e, como $|uv| \leq n$ implica $|v| \leq n$, conclui-se que $|uw| = M - |v| > n$. Então, se se escolher $i = |u| + |w|$ vem

$$|\, uv^i w \,| = |u| + i\,|v| + |w| = (|u| + |w|)(1 + |v|)$$

  com $1 + |v| \geq 2$ e $|u| + |w| \geq 2$. Logo, $(|u| + |w|)(1 + |v|)$ não é primo. Ou seja, para $i = |u| + |v|$, tem-se $uv^i w \notin L$.
- Mostrámos que, **dado n qualquer, existe** $x \in L$ tal que, para toda decomposição de x na forma uvw, com $v \neq \varepsilon$ e $|uv| \leq n$, existe i tal que $uv^i w \notin L$. Portanto, L não satisfaz a condição do Lema da Repetição e por isso não é regular. □

Aplicação do lema da repetição

Prova, pelo lema da repetição, de que $L = \{0^p \mid p \text{ primo}\}$ não é regular:

- Seja $n \in \mathbb{N} \setminus \{0\}$ qualquer. Escolhemos $x = 0^M$ com $M > 2n$ e M primo. M existe porque **o conjunto de primos é infinito**.
- Tem-se $x \in L$ e $|x| = M > 2n > n$.
  Seja $x = uvw$, uma qualquer decomposição de x, tal que $|v| \geq 1$ e $|uv| \leq n$. Há que encontrar $i \geq 0$ tal que $uv^i w \notin L$, i.e., tal que $|uv^i w|$ não é primo.
- Mas, $|\, uv^i w \,| = |u| + i\,|v| + |w|$ e, como $|uv| \leq n$ implica $|v| \leq n$, conclui-se que $|uw| = M - |v| > n$. Então, se se escolher $i = |u| + |w|$ vem

$$|\, uv^i w \,| = |u| + i\,|v| + |w| = (|u| + |w|)(1 + |v|)$$

  com $1 + |v| \geq 2$ e $|u| + |w| \geq 2$. Logo, $(|u| + |w|)(1 + |v|)$ não é primo. Ou seja, para $i = |u| + |v|$, tem-se $uv^i w \notin L$.
- Mostrámos que, **dado n qualquer, existe** $x \in L$ tal que, para toda decomposição de x na forma uvw, com $v \neq \varepsilon$ e $|uv| \leq n$, existe i tal que $uv^i w \notin L$. Portanto, L não satisfaz a condição do Lema da Repetição e por isso não é regular. □

Aplicação do lema da repetição

Prova, pelo lema da repetição, de que $L = \{0^p \mid p \text{ primo}\}$ não é regular:

- Seja $n \in \mathbb{N} \setminus \{0\}$ qualquer. Escolhemos $x = 0^M$ com $M > 2n$ e M primo.
  M existe porque **o conjunto de primos é infinito**.
- Tem-se $x \in L$ e $|x| = M > 2n > n$.
  Seja $x = uvw$, uma qualquer decomposição de x, tal que $|v| \geq 1$ e $|uv| \leq n$. Há que encontrar $i \geq 0$ tal que $uv^i w \notin L$, i.e., tal que $|uv^i w|$ não é primo.
- Mas, $|\, uv^i w \,| = |u| + i\,|v| + |w|$ e, como $|uv| \leq n$ implica $|v| \leq n$, conclui-se que $|uw| = M - |v| > n$. Então, se se escolher $i = |u| + |w|$ vem

$$|\, uv^i w \,| = |u| + i\,|v| + |w| = (|u| + |w|)(1 + |v|)$$

  com $1 + |v| \geq 2$ e $|u| + |w| \geq 2$. Logo, $(|u| + |w|)(1 + |v|)$ não é primo. Ou seja, para $i = |u| + |v|$, tem-se $uv^i w \notin L$.
- Mostrámos que, **dado n qualquer, existe** $x \in L$ tal que, para toda decomposição de x na forma uvw, com $v \neq \varepsilon$ e $|uv| \leq n$, existe i tal que $uv^i w \notin L$. Portanto, L não satisfaz a condição do Lema da Repetição e por isso não é regular. □

Aplicação do lema da repetição

Prova, pelo lema da repetição, de que $L = \{0^p \mid p \text{ primo}\}$ não é regular:

- Seja $n \in \mathbb{N} \setminus \{0\}$ qualquer. Escolhemos $x = 0^M$ com $M > 2n$ e M primo.
  M existe porque **o conjunto de primos é infinito**.
- Tem-se $x \in L$ e $|x| = M > 2n > n$.
  Seja $x = uvw$, uma qualquer decomposição de x, tal que $|v| \geq 1$ e $|uv| \leq n$. Há que encontrar $i \geq 0$ tal que $uv^i w \notin L$, i.e., tal que $|uv^i w|$ não é primo.
- Mas, $|\, uv^i w \,| = |u| + i\,|v| + |w|$ e, como $|uv| \leq n$ implica $|v| \leq n$, conclui-se que $|uw| = M - |v| > n$. Então, se se escolher $i = |u| + |w|$ vem

$$|\, uv^i w \,| = |u| + i\,|v| + |w| = (|u| + |w|)(1 + |v|)$$

  com $1 + |v| \geq 2$ e $|u| + |w| \geq 2$. Logo, $(|u| + |w|)(1 + |v|)$ não é primo. Ou seja, para $i = |u| + |v|$, tem-se $uv^i w \notin L$.
- Mostrámos que, **dado n qualquer, existe** $x \in L$ tal que, para toda decomposição de x na forma uvw, com $v \neq \varepsilon$ e $|uv| \leq n$, existe i tal que $uv^i w \notin L$. Portanto, L não satisfaz a condição do Lema da Repetição e por isso não é regular. □

Aplicação do lema da repetição

Prova, pelo lema da repetição, de que $L = \{0^p \mid p \text{ primo}\}$ não é regular:

- Seja $n \in \mathbb{N} \setminus \{0\}$ qualquer. Escolhemos $x = 0^M$ com $M > 2n$ e M primo.
  M existe porque **o conjunto de primos é infinito**.
- Tem-se $x \in L$ e $|x| = M > 2n > n$.
  Seja $x = uvw$, uma qualquer decomposição de x, tal que $|v| \geq 1$ e $|uv| \leq n$. Há que encontrar $i \geq 0$ tal que $uv^i w \notin L$, i.e., tal que $|uv^i w|$ não é primo.
- Mas, $| uv^i w | = |u| + i\,|v| + |w|$ e, como $|uv| \leq n$ implica $|v| \leq n$, conclui-se que $|uw| = M - |v| > n$. Então, se se escolher $i = |u| + |w|$ vem

$$| uv^i w | = |u| + i\,|v| + |w| = (|u| + |w|)(1 + |v|)$$

com $1 + |v| \geq 2$ e $|u| + |w| \geq 2$. Logo, $(|u| + |w|)(1 + |v|)$ não é primo. Ou seja, para $i = |u| + |v|$, tem-se $uv^i w \notin L$.

- Mostrámos que, **dado n qualquer, existe** $x \in L$ tal que, para toda decomposição de x na forma uvw, com $v \neq \varepsilon$ e $|uv| \leq n$, existe i tal que $uv^i w \notin L$. Portanto, L não satisfaz a condição do Lema da Repetição e por isso não é regular. □

Aplicação do lema da repetição

Prova, pelo lema da repetição, de que $L = \{0^p \mid p \text{ primo}\}$ não é regular:

- Seja $n \in \mathbb{N} \setminus \{0\}$ qualquer. Escolhemos $x = 0^M$ com $M > 2n$ e M primo.
  M existe porque **o conjunto de primos é infinito**.
- Tem-se $x \in L$ e $|x| = M > 2n > n$.
  Seja $x = uvw$, uma qualquer decomposição de x, tal que $|v| \geq 1$ e $|uv| \leq n$. Há que encontrar $i \geq 0$ tal que $uv^i w \notin L$, i.e., tal que $|uv^i w|$ não é primo.
- Mas, $| uv^i w | = |u| + i\,|v| + |w|$ e, como $|uv| \leq n$ implica $|v| \leq n$, conclui-se que $|uw| = M - |v| > n$. Então, se se escolher $i = |u| + |w|$ vem

$$| uv^i w | = |u| + i\,|v| + |w| = (|u| + |w|)(1 + |v|)$$

  com $1 + |v| \geq 2$ e $|u| + |w| \geq 2$. Logo, $(|u| + |w|)(1 + |v|)$ não é primo. Ou seja, para $i = |u| + |v|$, tem-se $uv^i w \notin L$.
- Mostrámos que, **dado n qualquer, existe** $x \in L$ tal que, para toda decomposição de x na forma uvw, com $v \neq \varepsilon$ e $|uv| \leq n$, existe i tal que $uv^i w \notin L$. Portanto, L não satisfaz a condição do Lema da Repetição e por isso não é regular. □

Aplicação do lema da repetição

Prova, pelo lema da repetição, de que $L = \{0^p \mid p \text{ primo}\}$ não é regular:

- Seja $n \in \mathbb{N} \setminus \{0\}$ qualquer. Escolhemos $x = 0^M$ com $M > 2n$ e M primo.
  M existe porque **o conjunto de primos é infinito**.
- Tem-se $x \in L$ e $|x| = M > 2n > n$.
  Seja $x = uvw$, uma qualquer decomposição de x, tal que $|v| \geq 1$ e $|uv| \leq n$. Há que encontrar $i \geq 0$ tal que $uv^i w \notin L$, i.e., tal que $|uv^i w|$ não é primo.
- Mas, $| uv^i w | = |u| + i\,|v| + |w|$ e, como $|uv| \leq n$ implica $|v| \leq n$, conclui-se que $|uw| = M - |v| > n$. Então, se se escolher $i = |u| + |w|$ vem

$$| uv^i w | = |u| + i\,|v| + |w| = (|u| + |w|)(1 + |v|)$$

  com $1 + |v| \geq 2$ e $|u| + |w| \geq 2$. Logo, $(|u| + |w|)(1 + |v|)$ não é primo. Ou seja, para $i = |u| + |v|$, tem-se $uv^i w \notin L$.
- Mostrámos que, **dado n qualquer, existe** $x \in L$ tal que, para toda decomposição de x na forma uvw, com $v \neq \varepsilon$ e $|uv| \leq n$, existe i tal que $uv^i w \notin L$. Portanto, L não satisfaz a condição do Lema da Repetição e por isso não é regular. □

Aplicação do lema da repetição

Prova, pelo lema da repetição, de que $L = \{0^p \mid p \text{ primo}\}$ não é regular:

- Seja $n \in \mathbb{N} \setminus \{0\}$ qualquer. Escolhemos $x = 0^M$ com $M > 2n$ e M primo.
  M existe porque **o conjunto de primos é infinito**.
- Tem-se $x \in L$ e $|x| = M > 2n > n$.
  Seja $x = uvw$, uma qualquer decomposição de x, tal que $|v| \geq 1$ e $|uv| \leq n$. Há que encontrar $i \geq 0$ tal que $uv^i w \notin L$, i.e., tal que $|uv^i w|$ não é primo.
- Mas, $| uv^i w | = |u| + i\,|v| + |w|$ e, como $|uv| \leq n$ implica $|v| \leq n$, conclui-se que $|uw| = M - |v| > n$. Então, se se escolher $i = |u| + |w|$ vem

$$| uv^i w | = |u| + i\,|v| + |w| = (|u| + |w|)(1 + |v|)$$

  com $1 + |v| \geq 2$ e $|u| + |w| \geq 2$. Logo, $(|u| + |w|)(1 + |v|)$ não é primo. Ou seja, para $i = |u| + |v|$, tem-se $uv^i w \notin L$.
- Mostrámos que, **dado n qualquer, existe** $x \in L$ tal que, para toda decomposição de x na forma uvw, com $v \neq \varepsilon$ e $|uv| \leq n$, existe i tal que $uv^i w \notin L$. Portanto, L não satisfaz a condição do Lema da Repetição e por isso não é regular. □

Aplicação do lema da repetição

Prova, pelo lema da repetição, de que $L = \{0^p \mid p \text{ primo}\}$ não é regular:

- Seja $n \in \mathbb{N} \setminus \{0\}$ qualquer. Escolhemos $x = 0^M$ com $M > 2n$ e M primo.
  M existe porque **o conjunto de primos é infinito**.
- Tem-se $x \in L$ e $|x| = M > 2n > n$.
  Seja $x = uvw$, uma qualquer decomposição de x, tal que $|v| \geq 1$ e $|uv| \leq n$. Há que encontrar $i \geq 0$ tal que $uv^iw \notin L$, i.e., tal que $|uv^iw|$ não é primo.
- Mas, $| uv^iw | = |u| + i\,|v| + |w|$ e, como $|uv| \leq n$ implica $|v| \leq n$, conclui-se que $|uw| = M - |v| > n$. Então, se se escolher $i = |u| + |w|$ vem

$$| uv^iw | = |u| + i\,|v| + |w| = (|u| + |w|)(1 + |v|)$$

  com $1 + |v| \geq 2$ e $|u| + |w| \geq 2$. Logo, $(|u| + |w|)(1 + |v|)$ não é primo. Ou seja, para $i = |u| + |v|$, tem-se $uv^iw \notin L$.
- Mostrámos que, **dado n qualquer, existe** $x \in L$ tal que, para toda decomposição de x na forma uvw, com $v \neq \varepsilon$ e $|uv| \leq n$, existe i tal que $uv^iw \notin L$. Portanto, L não satisfaz a condição do Lema da Repetição e por isso não é regular. □

Aplicação do lema da repetição

Prova de que $\{0^{k^2} \mid k \geq 0\}$ não é regular, pelo lema da repetição

Dado $n \in \mathbb{Z}^+$, tomamos $x = 0^{(n+1)^2}$. Tem-se $x \in L \wedge |x| > n$.

Vamos ver que, qualquer que seja a decomposição de x na forma uvw, com $|uv| \leq n$ e $v \neq \varepsilon$, existe um $i \in \mathbb{N}$ tal que a $uv^i w \notin L$, o que nos permite concluir que L não é regular. Se escrevermos $x = uvw$, temos

$$x = 0^{(n+1)^2} = 0^{|u|}0^{|v|}0^{(n+1)^2-|u|-|v|} = uvw$$

Se considerarmos a palavra $uv^i w$ e tomarmos $i = 0$, isto é, se retirarmos v, ficamos com palavra

$$0^{(n+1)^2-|v|}$$

a qual tem $(n+1)^2 - |v|$ zeros. Como $|uv| \leq n$ e $v \neq \varepsilon$, então $1 \leq |v| \leq n$. Podemos concluir que $(n+1)^2 - |v|$ não pode ser um quadrado perfeito, se $1 \leq |v| \leq n$, porque

$$n^2 < n^2 + n + 1 = (n+1)^2 - n \leq (n+1)^2 - |v| \leq (n+1)^2 - 1 < (n+1)^2.$$

Aplicação do lema da repetição

Prova de que $\{0^{k^2} \mid k \geq 0\}$ não é regular, pelo lema da repetição

Dado $n \in \mathbb{Z}^+$, tomamos $x = 0^{(n+1)^2}$. Tem-se $x \in L \wedge |x| > n$.
Vamos ver que, qualquer que seja a decomposição de x na forma uvw, com $|uv| \leq n$ e $v \neq \varepsilon$, existe um $i \in \mathbb{N}$ tal que a $uv^iw \notin L$, o que nos permite concluir que L não é regular. Se escrevermos $x = uvw$, temos

$$x = 0^{(n+1)^2} = 0^{|u|}0^{|v|}0^{(n+1)^2-|u|-|v|} = uvw$$

Se considerarmos a palavra uv^iw e tomarmos $i = 0$, isto é, se retirarmos v, ficamos com palavra

$$0^{(n+1)^2-|v|}$$

a qual tem $(n+1)^2 - |v|$ zeros. Como $|uv| \leq n$ e $v \neq \varepsilon$, então $1 \leq |v| \leq n$. Podemos concluir que $(n+1)^2 - |v|$ não pode ser um quadrado perfeito, se $1 \leq |v| \leq n$, porque

$$n^2 < n^2 + n + 1 = (n+1)^2 - n \leq (n+1)^2 - |v| \leq (n+1)^2 - 1 < (n+1)^2.$$

Aplicação do lema da repetição

Prova de que $\{0^{k^2} \mid k \geq 0\}$ não é regular, pelo lema da repetição

Dado $n \in \mathbb{Z}^+$, tomamos $x = 0^{(n+1)^2}$. Tem-se $x \in L \wedge |x| > n$.
Vamos ver que, qualquer que seja a decomposição de x na forma uvw, com $|uv| \leq n$ e $v \neq \varepsilon$, existe um $i \in \mathbb{N}$ tal que a $uv^iw \notin L$, o que nos permite concluir que L não é regular. Se escrevermos $x = uvw$, temos

$$x = 0^{(n+1)^2} = 0^{|u|}0^{|v|}0^{(n+1)^2-|u|-|v|} = uvw$$

Se considerarmos a palavra uv^iw e tomarmos $i = 0$, isto é, se retirarmos v, ficamos com palavra

$$0^{(n+1)^2-|v|}$$

a qual tem $(n+1)^2 - |v|$ zeros. Como $|uv| \leq n$ e $v \neq \varepsilon$, então $1 \leq |v| \leq n$. Podemos concluir que $(n+1)^2 - |v|$ não pode ser um quadrado perfeito, se $1 \leq |v| \leq n$, porque

$$n^2 < n^2 + n + 1 = (n+1)^2 - n \leq (n+1)^2 - |v| \leq (n+1)^2 - 1 < (n+1)^2.$$

Aplicação do lema da repetição

Prova de que $\{0^{k^2} \mid k \geq 0\}$ não é regular, pelo lema da repetição

Dado $n \in \mathbb{Z}^+$, tomamos $x = 0^{(n+1)^2}$. Tem-se $x \in L \wedge |x| > n$.
Vamos ver que, qualquer que seja a decomposição de x na forma uvw, com $|uv| \leq n$ e $v \neq \varepsilon$, existe um $i \in \mathbb{N}$ tal que a $uv^iw \notin L$, o que nos permite concluir que L não é regular. Se escrevermos $x = uvw$, temos

$$x = 0^{(n+1)^2} = 0^{|u|}0^{|v|}0^{(n+1)^2-|u|-|v|} = uvw$$

Se considerarmos a palavra uv^iw e tomarmos $i = 0$, isto é, se retirarmos v, ficamos com palavra

$$0^{(n+1)^2-|v|}$$

a qual tem $(n+1)^2 - |v|$ zeros. Como $|uv| \leq n$ e $v \neq \varepsilon$, então $1 \leq |v| \leq n$.
Podemos concluir que $(n+1)^2 - |v|$ não pode ser um quadrado perfeito, se $1 \leq |v| \leq n$, porque

$$n^2 < n^2 + n + 1 = (n+1)^2 - n \leq (n+1)^2 - |v| \leq (n+1)^2 - 1 < (n+1)^2.$$

Aplicação do Teorema de Myhill-Nerode

Prova de que $\{0^{k^2} \mid k \geq 0\}$ não é regular, pelo teorema de Myhill-Nerode

Vamos mostrar que

$$\forall p, q \in \mathbb{N} \quad q > p \Rightarrow (0^{p^2}, 0^{q^2}) \notin \mathcal{R}_L$$

o que permite concluir que $[0^{k^2}] = \{0^{k^2}\}$, qualquer que seja $k \geq 0$, pelo que o conjunto das classes de R_L não é finito e, consequentemente, L não é regular.

Se $p < q$ então $(0^{p^2}, 0^{q^2}) \notin \mathcal{R}_L$, porque existe $z \in \{0\}^\star$ tal que $0^{p^2} z \in L$ e $0^{q^2} z \notin L$. Basta tomar $z = 0^{2p+1}$. □

Aplicação do Teorema de Myhill-Nerode

Prova de que $\{0^{k^2} \mid k \geq 0\}$ não é regular, pelo teorema de Myhill-Nerode

Vamos mostrar que

$$\forall p, q \in \mathbb{N} \quad q > p \Rightarrow (0^{p^2}, 0^{q^2}) \notin \mathcal{R}_L$$

o que permite concluir que $[0^{k^2}] = \{0^{k^2}\}$, qualquer que seja $k \geq 0$, pelo que o conjunto das classes de R_L não é finito e, consequentemente, L não é regular.

Se $p < q$ então $(0^{p^2}, 0^{q^2}) \notin \mathcal{R}_L$, porque existe $z \in \{0\}^\star$ tal que $0^{p^2} z \in L$ e $0^{q^2} z \notin L$. Basta tomar $z = 0^{2p+1}$. □

Lema da repetição indica apenas condição necessária

A linguagem $L = \{0^k \mid k \in \mathbb{N}\} \cup \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, de alfabeto $\Sigma = \{0, 1\}$, **não é regular e satisfaz a condição do lema da repetição para** $n = 1$.

Prova

De facto, se $x \in L$ e $|x| \geq 1$ então x está num dos dois casos seguintes:

- $x = 00^k$, para algum $k \geq 0$, ou
- $x = 11^s 0^{q^2}$, para algum $s \geq 0$ e algum $q \geq 1$.

Vamos então escolher as decomposições de x como uvw, com $|uv| \leq n = 1$ e $v \neq \varepsilon$ tais que $\forall i \in \mathbb{N} \;\; uv^i w \in L$.

- Para $x = 00^k$, escolhemos $u = \varepsilon$, $v = 0$, e $w = 0^k$, e temos $uv^i w = 0^{k+i} \in L$.
- Para $x = 11^s 0^{q^2}$, escolhemos $u = \varepsilon$, $v = 1$, e $w = 1^s 0^{q^2}$, e vemos que, se $i \geq 1$ ou $s \geq 1$ então $uv^i w \in \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, e se $i = s = 0$ então $uv^i w \in \{0\}^\star$.

Portanto, L **satisfaz a condição do lema para** $n = 1$ porque

$$\forall x \in L \;\; |x| \geq n \Rightarrow \exists u, v, w \;\; (x = uvw \wedge v \neq \varepsilon \wedge |uv| \leq 1 \wedge (\forall i \in \mathbb{N} \;\; uv^i w \in L))$$

Mas, L **não é regular porque** R_L **é de índice infinito.** Se $p \neq q$, as palavras 10^{p^2} e 10^{q^2} não são equivalentes segundo R_L.

Lema da repetição indica apenas condição necessária

A linguagem $L = \{0^k \mid k \in \mathbb{N}\} \cup \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, de alfabeto $\Sigma = \{0, 1\}$, **não é regular e satisfaz a condição do lema da repetição para** $n = 1$.

Prova

De facto, se $x \in L$ e $|x| \geq 1$ então x está num dos dois casos seguintes:

- $x = 00^k$, para algum $k \geq 0$, ou
- $x = 11^s 0^{q^2}$, para algum $s \geq 0$ e algum $q \geq 1$.

Vamos então escolher as decomposições de x como uvw, com $|uv| \leq n = 1$ e $v \neq \varepsilon$ tais que $\forall i \in \mathbb{N} \;\; uv^i w \in L$.

- Para $x = 00^k$, escolhemos $u = \varepsilon$, $v = 0$, e $w = 0^k$, e temos $uv^i w = 0^{k+i} \in L$.
- Para $x = 11^s 0^{q^2}$, escolhemos $u = \varepsilon$, $v = 1$, e $w = 1^s 0^{q^2}$, e vemos que, se $i \geq 1$ ou $s \geq 1$ então $uv^i w \in \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, e se $i = s = 0$ então $uv^i w \in \{0\}^\star$.

Portanto, L **satisfaz a condição do lema para** $n = 1$ porque

$$\forall x \in L \;\; |x| \geq n \Rightarrow \exists u, v, w \;\; (x = uvw \wedge v \neq \varepsilon \wedge |uv| \leq 1 \wedge (\forall i \in \mathbb{N} \;\; uv^i w \in L))$$

Mas, L **não é regular porque** R_L **é de índice infinito.** Se $p \neq q$, as palavras 10^{p^2} e 10^{q^2} não são equivalentes segundo R_L.

Lema da repetição indica apenas condição necessária

A linguagem $L = \{0^k \mid k \in \mathbb{N}\} \cup \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, de alfabeto $\Sigma = \{0, 1\}$, **não é regular e satisfaz a condição do lema da repetição para** $n = 1$.

Prova

De facto, se $x \in L$ e $|x| \geq 1$ então x está num dos dois casos seguintes:

- $x = 00^k$, para algum $k \geq 0$, ou
- $x = 11^s 0^{q^2}$, para algum $s \geq 0$ e algum $q \geq 1$.

Vamos então escolher as decomposições de x como uvw, com $|uv| \leq n = 1$ e $v \neq \varepsilon$ tais que $\forall i \in \mathbb{N} \;\; uv^i w \in L$.

- Para $x = 00^k$, escolhemos $u = \varepsilon$, $v = 0$, e $w = 0^k$, e temos $uv^i w = 0^{k+i} \in L$.
- Para $x = 11^s 0^{q^2}$, escolhemos $u = \varepsilon$, $v = 1$, e $w = 1^s 0^{q^2}$, e vemos que, se $i \geq 1$ ou $s \geq 1$ então $uv^i w \in \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, e se $i = s = 0$ então $uv^i w \in \{0\}^\star$.

Portanto, L **satisfaz a condição do lema para** $n = 1$ porque

$$\forall x \in L \;\; |x| \geq n \Rightarrow \exists u, v, w \;\; (x = uvw \wedge v \neq \varepsilon \wedge |uv| \leq 1 \wedge (\forall i \in \mathbb{N} \;\; uv^i w \in L))$$

Mas, L **não é regular porque** R_L **é de índice infinito.** Se $p \neq q$, as palavras 10^{p^2} e 10^{q^2} não são equivalentes segundo R_L.

Lema da repetição indica apenas condição necessária

A linguagem $L = \{0^k \mid k \in \mathbb{N}\} \cup \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, de alfabeto $\Sigma = \{0, 1\}$, **não é regular e satisfaz a condição do lema da repetição para** $n = 1$.

Prova

De facto, se $x \in L$ e $|x| \geq 1$ então x está num dos dois casos seguintes:

- $x = 00^k$, para algum $k \geq 0$, ou
- $x = 11^s 0^{q^2}$, para algum $s \geq 0$ e algum $q \geq 1$.

Vamos então escolher as decomposições de x como uvw, com $|uv| \leq n = 1$ e $v \neq \varepsilon$ tais que $\forall i \in \mathbb{N} \;\; uv^i w \in L$.

- Para $x = 00^k$, escolhemos $u = \varepsilon$, $v = 0$, e $w = 0^k$, e temos $uv^i w = 0^{k+i} \in L$.
- Para $x = 11^s 0^{q^2}$, escolhemos $u = \varepsilon$, $v = 1$, e $w = 1^s 0^{q^2}$, e vemos que, se $i \geq 1$ ou $s \geq 1$ então $uv^i w \in \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, e se $i = s = 0$ então $uv^i w \in \{0\}^\star$.

Portanto, L **satisfaz a condição do lema para** $n = 1$ porque

$$\forall x \in L \;\; |x| \geq n \Rightarrow \exists u, v, w \;\; (x = uvw \wedge v \neq \varepsilon \wedge |uv| \leq 1 \wedge (\forall i \in \mathbb{N} \;\; uv^i w \in L))$$

Mas, L **não é regular porque** R_L **é de índice infinito.** Se $p \neq q$, as palavras 10^{p^2} e 10^{q^2} não são equivalentes segundo R_L.

Lema da repetição indica apenas condição necessária

A linguagem $L = \{0^k \mid k \in \mathbb{N}\} \cup \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, de alfabeto $\Sigma = \{0, 1\}$, **não é regular e satisfaz a condição do lema da repetição para** $n = 1$.

Prova

De facto, se $x \in L$ e $|x| \geq 1$ então x está num dos dois casos seguintes:

- $x = 00^k$, para algum $k \geq 0$, ou
- $x = 11^s 0^{q^2}$, para algum $s \geq 0$ e algum $q \geq 1$.

Vamos então escolher as decomposições de x como uvw, com $|uv| \leq n = 1$ e $v \neq \varepsilon$ tais que $\forall i \in \mathbb{N} \;\; uv^i w \in L$.

- Para $x = 00^k$, escolhemos $u = \varepsilon$, $v = 0$, e $w = 0^k$, e temos $uv^i w = 0^{k+i} \in L$.
- Para $x = 11^s 0^{q^2}$, escolhemos $u = \varepsilon$, $v = 1$, e $w = 1^s 0^{q^2}$, e vemos que, se $i \geq 1$ ou $s \geq 1$ então $uv^i w \in \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, e se $i = s = 0$ então $uv^i w \in \{0\}^\star$.

Portanto, L **satisfaz a condição do lema para** $n = 1$ porque

$$\forall x \in L \;\; |x| \geq n \Rightarrow \exists u, v, w \;\; (x = uvw \wedge v \neq \varepsilon \wedge |uv| \leq 1 \wedge (\forall i \in \mathbb{N} \;\; uv^i w \in L))$$

Mas, L **não é regular porque** R_L **é de índice infinito.** Se $p \neq q$, as palavras 10^{p^2} e 10^{q^2} não são equivalentes segundo R_L.

Lema da repetição indica apenas condição necessária

A linguagem $L = \{0^k \mid k \in \mathbb{N}\} \cup \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, de alfabeto $\Sigma = \{0, 1\}$, **não é regular e satisfaz a condição do lema da repetição para** $n = 1$.

Prova

De facto, se $x \in L$ e $|x| \geq 1$ então x está num dos dois casos seguintes:

- $x = 00^k$, para algum $k \geq 0$, ou
- $x = 11^s 0^{q^2}$, para algum $s \geq 0$ e algum $q \geq 1$.

Vamos então escolher as decomposições de x como uvw, com $|uv| \leq n = 1$ e $v \neq \varepsilon$ tais que $\forall i \in \mathbb{N} \;\; uv^i w \in L$.

- Para $x = 00^k$, escolhemos $u = \varepsilon$, $v = 0$, e $w = 0^k$, e temos $uv^i w = 0^{k+i} \in L$.
- Para $x = 11^s 0^{q^2}$, escolhemos $u = \varepsilon$, $v = 1$, e $w = 1^s 0^{q^2}$, e vemos que, se $i \geq 1$ ou $s \geq 1$ então $uv^i w \in \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, e se $i = s = 0$ então $uv^i w \in \{0\}^\star$.

Portanto, L **satisfaz a condição do lema para** $n = 1$ porque

$$\forall x \in L \;\; |x| \geq n \Rightarrow \exists u, v, w \;\; (x = uvw \wedge v \neq \varepsilon \wedge |uv| \leq 1 \wedge (\forall i \in \mathbb{N} \;\; uv^i w \in L))$$

Mas, L **não é regular porque** R_L **é de índice infinito.** Se $p \neq q$, as palavras 10^{p^2} e 10^{q^2} não são equivalentes segundo R_L.

Lema da repetição indica apenas condição necessária

A linguagem $L = \{0^k \mid k \in \mathbb{N}\} \cup \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, de alfabeto $\Sigma = \{0, 1\}$, **não é regular e satisfaz a condição do lema da repetição para** $n = 1$.

Prova

De facto, se $x \in L$ e $|x| \geq 1$ então x está num dos dois casos seguintes:

- $x = 00^k$, para algum $k \geq 0$, ou
- $x = 11^s 0^{q^2}$, para algum $s \geq 0$ e algum $q \geq 1$.

Vamos então escolher as decomposições de x como uvw, com $|uv| \leq n = 1$ e $v \neq \varepsilon$ tais que $\forall i \in \mathbb{N} \;\; uv^i w \in L$.

- Para $x = 00^k$, escolhemos $u = \varepsilon$, $v = 0$, e $w = 0^k$, e temos $uv^i w = 0^{k+i} \in L$.
- Para $x = 11^s 0^{q^2}$, escolhemos $u = \varepsilon$, $v = 1$, e $w = 1^s 0^{q^2}$, e vemos que, se $i \geq 1$ ou $s \geq 1$ então $uv^i w \in \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, e se $i = s = 0$ então $uv^i w \in \{0\}^\star$.

Portanto, L **satisfaz a condição do lema para** $n = 1$ porque

$$\forall x \in L \;\; |x| \geq n \Rightarrow \exists u, v, w \;\; (x = uvw \wedge v \neq \varepsilon \wedge |uv| \leq 1 \wedge (\forall i \in \mathbb{N} \;\; uv^i w \in L))$$

Mas, L **não é regular porque** R_L **é de índice infinito.** Se $p \neq q$, as palavras 10^{p^2} e 10^{q^2} não são equivalentes segundo R_L.

Lema da repetição indica apenas condição necessária

A linguagem $L = \{0^k \mid k \in \mathbb{N}\} \cup \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, de alfabeto $\Sigma = \{0, 1\}$, **não é regular e satisfaz a condição do lema da repetição para** $n = 1$.

Prova

De facto, se $x \in L$ e $|x| \geq 1$ então x está num dos dois casos seguintes:

- $x = 00^k$, para algum $k \geq 0$, ou
- $x = 11^s 0^{q^2}$, para algum $s \geq 0$ e algum $q \geq 1$.

Vamos então escolher as decomposições de x como uvw, com $|uv| \leq n = 1$ e $v \neq \varepsilon$ tais que $\forall i \in \mathbb{N} \;\; uv^i w \in L$.

- Para $x = 00^k$, escolhemos $u = \varepsilon$, $v = 0$, e $w = 0^k$, e temos $uv^i w = 0^{k+i} \in L$.
- Para $x = 11^s 0^{q^2}$, escolhemos $u = \varepsilon$, $v = 1$, e $w = 1^s 0^{q^2}$, e vemos que, se $i \geq 1$ ou $s \geq 1$ então $uv^i w \in \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, e se $i = s = 0$ então $uv^i w \in \{0\}^\star$.

Portanto, L **satisfaz a condição do lema para** $n = 1$ porque

$$\forall x \in L \;\; |x| \geq n \Rightarrow \exists u, v, w \;\; (x = uvw \wedge v \neq \varepsilon \wedge |uv| \leq 1 \wedge (\forall i \in \mathbb{N} \;\; uv^i w \in L))$$

Mas, L **não é regular porque** R_L **é de índice infinito.** Se $p \neq q$, as palavras 10^{p^2} e 10^{q^2} não são equivalentes segundo R_L.

Lema da repetição indica apenas condição necessária

A linguagem $L = \{0^k \mid k \in \mathbb{N}\} \cup \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, de alfabeto $\Sigma = \{0, 1\}$, **não é regular e satisfaz a condição do lema da repetição para** $n = 1$.

Prova

De facto, se $x \in L$ e $|x| \geq 1$ então x está num dos dois casos seguintes:

- $x = 00^k$, para algum $k \geq 0$, ou
- $x = 11^s 0^{q^2}$, para algum $s \geq 0$ e algum $q \geq 1$.

Vamos então escolher as decomposições de x como uvw, com $|uv| \leq n = 1$ e $v \neq \varepsilon$ tais que $\forall i \in \mathbb{N} \;\; uv^i w \in L$.

- Para $x = 00^k$, escolhemos $u = \varepsilon$, $v = 0$, e $w = 0^k$, e temos $uv^i w = 0^{k+i} \in L$.
- Para $x = 11^s 0^{q^2}$, escolhemos $u = \varepsilon$, $v = 1$, e $w = 1^s 0^{q^2}$, e vemos que, se $i \geq 1$ ou $s \geq 1$ então $uv^i w \in \{1^r 0^{p^2} \mid r, p \in \mathbb{N} \setminus \{0\}\}$, e se $i = s = 0$ então $uv^i w \in \{0\}^\star$.

Portanto, L **satisfaz a condição do lema para** $n = 1$ porque

$$\forall x \in L \;\; |x| \geq n \Rightarrow \exists u, v, w \;\; (x = uvw \wedge v \neq \varepsilon \wedge |uv| \leq 1 \wedge (\forall i \in \mathbb{N} \;\; uv^i w \in L))$$

Mas, L **não é regular porque** R_L **é de índice infinito.** Se $p \neq q$, as palavras 10^{p^2} e 10^{q^2} não são equivalentes segundo R_L.