El teorema de Myhill-Nerode

Horst H. von Brand
vonbrand@inf.utfsm.cl

Departamento de Informática
Universidad Técnica Federico Santa María

Contenido

Regularidad

La situación es incómoda: tenemos cómo demostrar que un lenguaje es regular, sabemos que hay lenguajes no regulares (tenemos alguna herramientas para demostrarlo), pero no tenemos nada que los caracterice.

Relaciones invariantes derechas

Definición

Sea R una relación sobre $\mathscr{A}$, donde $\mathscr{A}$ está equipado con una operación $\odot\colon \mathscr{A} \times \mathscr{A} \to \mathscr{A}$. Decimos que R es *invariante derecha* (respecto de $\odot$) si $a\,R\,b$ implica que $a \odot c\,R\,b \odot c$ para todo $c \in \mathscr{A}$.

Relaciones invariantes derechas

Esto suena árido y extraño, pero no es más que la propiedad que usamos sin pensar dos veces al simplificar por ejemplo:

$$a - c < b - c$$
$$a < b$$

(las relaciones de orden en $\mathbb{R}$ son invariantes derechas respecto de suma).
Claramente podemos definir invariante izquierda de forma similar.
Pero eso no es de interés ahora.

Particiones

Una *partición* de un conjunto lo divide en subconjuntos que son disjuntos entre sí.

Sean las particiones $\Pi_a = \{\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_m\}$ y $\Pi_b = \{\mathscr{B}_1, \mathscr{B}_2, \ldots, \mathscr{B}_n\}$ de un conjunto. Decimos que Π_b es un *refinamiento* de Π_a si todo $\mathscr{B}_i$ es un subconjunto de algún $\mathscr{A}_j$. La partición Π_b subdivide a Π_a.

Índice de una relación de equivalencia

Recordamos que una relación R sobre $\mathscr{A}$ es una *relación de equivalencia* si es:

Reflexiva: Para todo $a \in \mathscr{A}$ es $a\,R\,a$.

Transitiva: Para todo $a, b, c \in \mathscr{A}$, si $a\,R\,b$ y $b\,R\,c$ entonces $a\,R\,c$.

Simétrica: Si $a\,R\,b$ entonces $b\,R\,a$.

Índice de una relación de equivalencia

Una relación de equivalencia R sobre $\mathscr{A}$ *particiona* $\mathscr{A}$ en *clases de equivalencia*:

$$[a] = \{x \in \mathscr{A} : a\, R\, x\}$$

Lo de *partición* es que las clases de equivalencia o son iguales o son disjuntas ($[a] = [b]$ si $a\, R\, b$ o $[a] \cap [b] = \varnothing$ si $a \not R\, b$) y que su unión es todo $\mathscr{A}$.

Definición

El *índice* de una relación de equivalencia es el número de sus clases de equivalencia.

Índice de una relación de equivalencia

Por ejemplo, tenemos la relación de equivalencia módulo 6. Las clases de equivalencia son:

$$[0]_6 = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$$
$$[1]_6 = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$$
$$[2]_6 = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$$
$$[3]_6 = \{\ldots, -9, -3, 3, 9, 15, \ldots\}$$
$$[4]_6 = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$$
$$[5]_6 = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$$

El índice de esta relación de equivalencia es 6.

Índice de una relación de equivalencia

Tenemos la relación de equivalencia módulo 3:

$$[0]_3 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$
$$[1]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10 \ldots\}$$
$$[2]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

El índice de esta relación de equivalencia es 3. Vemos que las clases de la primera son todos subconjuntos de las clases de la segunda, por ejemplo $[3]_3 = [0]_6 \cup [3]_6$. Las clases módulo 6 refinan las clases módulo 3.

El teorema de Myhill-Nerode

Teorema (Myhill-Nerode)

El lenguaje L es regular si y solo si es la unión de clases de equivalencia de una relación de equivalencia de índice finito invariante derecha respecto de la concatenación.

El teorema de Myhill-Nerode

Demostración

Es un si y solo si, demostramos implicancia en ambas direcciones. Si L es regular, hay un DFA $M = (Q, \Sigma, \delta, q_0, F)$ que lo acepta. A M podemos asociar la relación:

$$\alpha \, R_M \, \beta \iff \delta(q_0, \alpha) = \delta(q_0, \beta)$$

Obviamente es una equivalencia de índice finito (las clases corresponden a estados del DFA). Es invariante derecha ya que $\alpha \, R_M \, \beta$ es $\delta(q_0, \alpha) = \delta(q_0, \beta)$, en cuyo caso para todo $\sigma \in \Sigma^*$ tenemos $\delta(q_0, \alpha\sigma) = \delta(q_0, \beta\sigma)$, o sea $\alpha\sigma \, R_M \, \beta\sigma$. L es la unión de las clases que corresponden a estados finales de M.

El teorema de Myhill-Nerode

Demostración

Consideremos la relación R_L asociada al lenguaje definida por:

$$\alpha \, R_L \, \beta \iff (\forall \sigma \in \Sigma^*, \alpha\sigma \in L \iff \beta\sigma \in L)$$

(se «completan igual» a una palabra en L, no se distinguen).

El teorema de Myhill-Nerode

Demostración

La relación R_L es de equivalencia:

Reflexiva: $\alpha \, R_L \, \alpha$ es obvio.

Simétrica: Si $\alpha \, R_L \, \beta$ es obvio que $\beta \, R_L \, \alpha$.

Transitiva: Si $\alpha \, R_L \, \beta$ y $\beta \, R_L \, \gamma$, para todo $\sigma \in \Sigma^*$
$\alpha\sigma \in L \iff \beta\sigma \in L$ y $\beta\sigma \in L \iff \gamma\sigma \in L$, con lo que
$\alpha\sigma \in L \iff \gamma\sigma \in L$; concluimos $\alpha \, R_L \, \gamma$.

El teorema de Myhill-Nerode

Demostración

Además, R_L es invariante derecha:

$$\begin{aligned}
\alpha\, R_L\, \beta &\iff (\forall \sigma \in \Sigma^*, \alpha\sigma \in L \iff \beta\sigma \in L) \\
&\iff (\forall \sigma_1, \sigma_2 \in \Sigma^*, \alpha\sigma_1\sigma_2 \in L \iff \beta\sigma_1\sigma_2 \in L) \\
&\iff (\forall \sigma_1, \sigma_2 \in \Sigma^*, (\alpha\sigma_1)\sigma_2 \in L \iff (\beta\sigma_1)\sigma_2 \in L) \\
&\iff (\forall \sigma_1 \in \Sigma^*, \alpha\sigma_1\, R_L\, \beta\sigma_1)
\end{aligned}$$

Está claro que si $\alpha \in L$ y $\alpha\, R_L\, \beta$ entonces $\beta \in L$ (complete con ε), con lo que:

$$L = \bigcup_{\alpha \in L} [\alpha]$$

El teorema de Myhill-Nerode

Demostración

Si L es regular, hay un DFA $M = (Q, \Sigma, \delta, q_0, F)$ que lo acepta. Demostraremos que las clases de equivalencia de R_M refinan las de R_L, con lo que el índice de R_M (finito, por ser a lo más $|Q|$) es mayor o igual al de R_L, que también debe ser finito.
Sea $\alpha\, R_M\, \beta$, es decir, $\delta(q_0, \alpha) = \delta(q_0, \beta)$. Para cualquier $\sigma \in \Sigma^*$, $\delta(q_0, \alpha\sigma) = \delta(q_0, \beta\sigma)$, con lo que $\alpha\sigma \in L \iff \beta\sigma \in L$. Esto corresponde a $\alpha\, R_L\, \beta$, las clases de equivalencia de R_M están contenidas en las de R_L. □

Uso del teorema

El lenguaje $L = \{a^n b^n : n \geq 0\}$ no es regular.

Construiremos las clases de equivalencia para R_L, concluyendo que hay infinitas. Iremos construyendo las clases desde las palabras más simples de $\{a, b\}^*$.

Uso del teorema

$[\varepsilon]$: La palabra ε se completa a algo en L únicamente con palabras de la forma $a^k b^k$ con $k \geq 0$, nada más se completa con eso, $[\varepsilon] = \{\varepsilon\}$.

$[a]$: Se completa a algo en L solo con $a^k b^{k+1}$ con $k \geq 0$, $[a] = \{a\}$.

$[a^r], r \geq 0$: Resume los anteriores. Se completa a algo en L con $a^k b^{k+r}$ con $k \geq 0$, $[a^r] = \{a^r\}$.

Ya con esto tenemos una colección infinita de clases, el lenguaje no es regular.

Uso del teorema

Continuemos:

$[b]$: Nada completa a algo en L. Este es un conjunto complejo, incluye todas las palabras que no son de la forma $a^* b^*$, pero también palabras de la forma $a^r b^s$ con $s > r$.

$[a^r b^s], r \geq s$: Se completa a algo en L solo con b^{r-s}, $[a^r b^s] = \{a^{r-s+k} b^k : k \geq 0\}$, bastan las clases $[a^r b] = \{a^{r+s} b^s : s \geq 1\}$

Consecuencias del teorema de Myhill-Nerode

Si el lenguaje es regular, el número de clases de equivalencia de R_L es finito. Podemos construir un DFA que tenga las clases de R_L como estados, definiendo:

$$
\begin{aligned}
q_0 &= [\varepsilon] \\
\delta([\alpha], a) &= [\alpha a] && \text{todo } \alpha \in \Sigma^*, \text{ todo } a \in \Sigma \\
F &= \{[\alpha] : \alpha \in L\}
\end{aligned}
$$

Lo espinudo es demostrar que δ es una función, es decir, que si $\alpha \, R_L \, \beta$ entonces $\alpha a \, R_L \, \beta a$. Esto se ve de la definición de R_L.

Consecuencias del teorema de Myhill-Nerode

De la demostración tenemos que el número de clases de equivalencia de R_L es el mínimo posible. ¡El DFA de arriba es el menor posible para L!

El DFA mínimo

Sea un DFA M que reconoce L. La demostración del teorema dice que las clases de equivalencia de R_L son la unión de clases de equivalencia de R_M. O sea, los estados del DFA mínimo son grupos de estados del DFA dado.

Construir el DFA mínimo es determinar estados que no se distinguen en R_L. Una idea es partir con dos grupos de estados (los estados finales y no finales se distinguen al consumir ε), y dividirlos en la medida que veamos que se distinguen (con el mismo símbolo van a grupos diferentes).

Ejemplo de construcción de DFA mínimo

Consideremos el DFA siguiente:

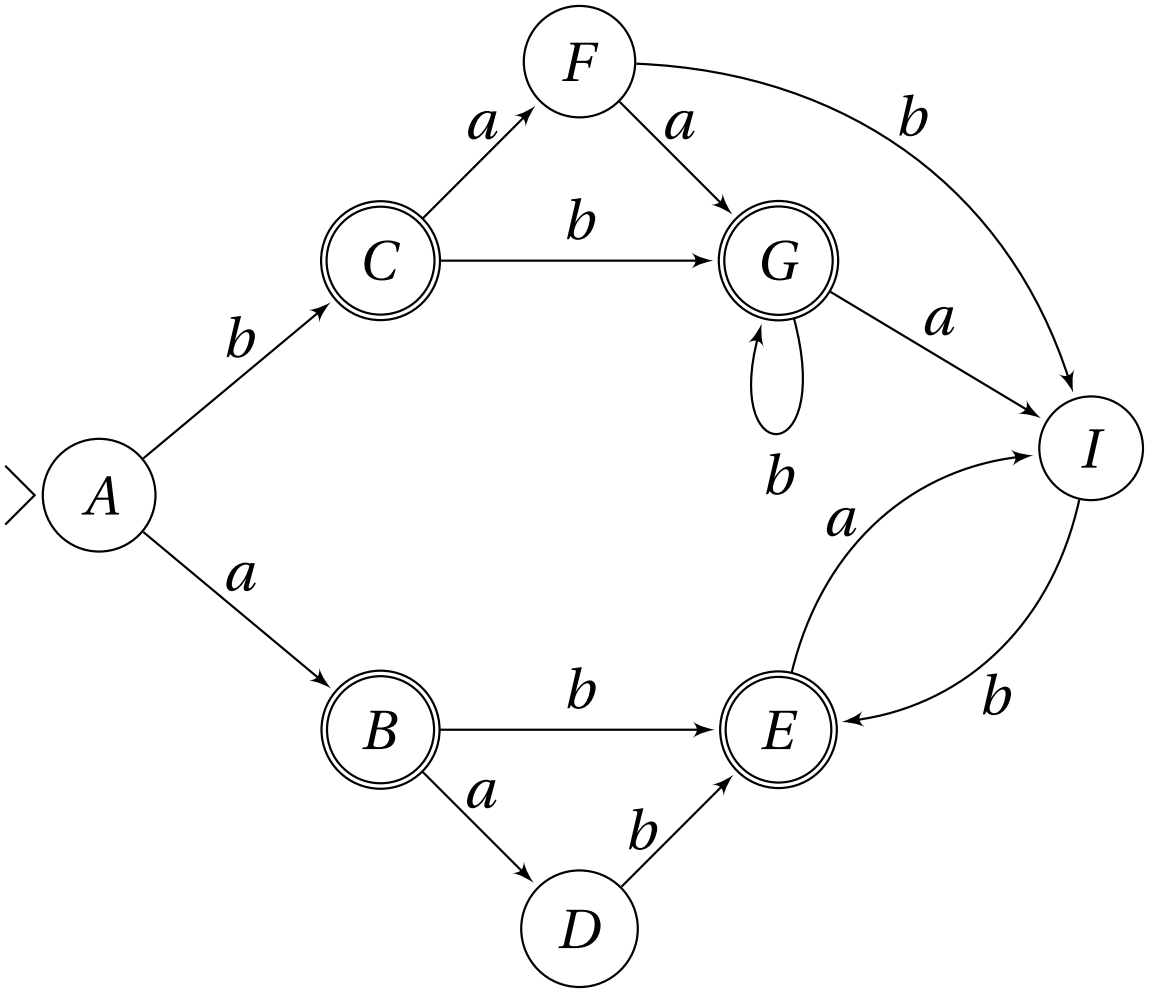
	a	b	Tipo
A	B	C	Inicial
B	D	E	Final
C	F	G	Final
D	H	E	
E	I	H	Final
F	G	I	
G	I	G	Final
H	H	H	(muerto)
I	H	E	

Ejemplo de construcción de DFA mínimo

Dividimos en dos grupos, estados no finales (0) y finales (1). Para cada estado indicamos a qué grupo pertenece el destino con cada símbolo. Si hay diferentes líneas en un grupo, se divide.

		a	b
0	A	$B(1)$	$C(1)$
	D	$H(0)$	$E(1)$
	F	$G(1)$	$I(0)$
	H	$H(0)$	$H(0)$
	I	$H(0)$	$E(1)$
1	B	$D(0)$	$E(1)$
	C	$F(0)$	$G(1)$
	E	$I(0)$	$H(0)$
	G	$I(0)$	$G(1)$

El DFA



Ejemplo de construcción de DFA mínimo

Se divide el grupo 0 en $\{\{A\},\{D,I\},\{F\},\{H\}\}$; el grupo 1 en $\{\{B,C,G\},\{E\}\}$.

		a	b
0	A	$B(4)$	$C(4)$
1	D	$H(3)$	$E(5)$
	I	$H(3)$	$E(5)$
2	F	$G(4)$	$I(1)$
3	H	$H(3)$	$H(3)$
4	B	$D(1)$	$E(5)$
	C	$F(2)$	$G(4)$
	G	$I(1)$	$G(4)$
5	E	$I(1)$	$H(3)$

Ejemplo de construcción de DFA mínimo

Se divide el grupo 4 en $\{\{B\},\{C\},\{G\}\}$. El grupo 1 imposible que se divida más.

		a	b
0	A	$B(4)$	$C(5)$
1	D	$H(3)$	$E(7)$
	I	$H(3)$	$E(7)$
2	F	$G(6)$	$I(1)$
3	H	$H(3)$	$H(3)$
4	B	$D(1)$	$E(7)$
5	C	$F(2)$	$G(6)$
6	G	$I(1)$	$G(6)$
7	E	$I(1)$	$H(3)$

Ejemplo de construcción de DFA mínimo

No hay más divisiones, terminamos. Estado inicial es el conjunto que contiene A (inicial del original), finales son conjuntos de estados finales del original (B, C, G, E).

		a	b	Tipo
0	A	$B(4)$	$C(5)$	Inicial
1	D	$H(3)$	$E(7)$	
	I	$H(3)$	$E(7)$	
2	F	$G(6)$	$I(1)$	
3	H	$H(3)$	$H(3)$	(muerto)
4	B	$D(1)$	$E(7)$	Final
5	C	$F(2)$	$G(6)$	Final
6	G	$I(1)$	$G(6)$	Final
7	E	$I(1)$	$H(3)$	Final

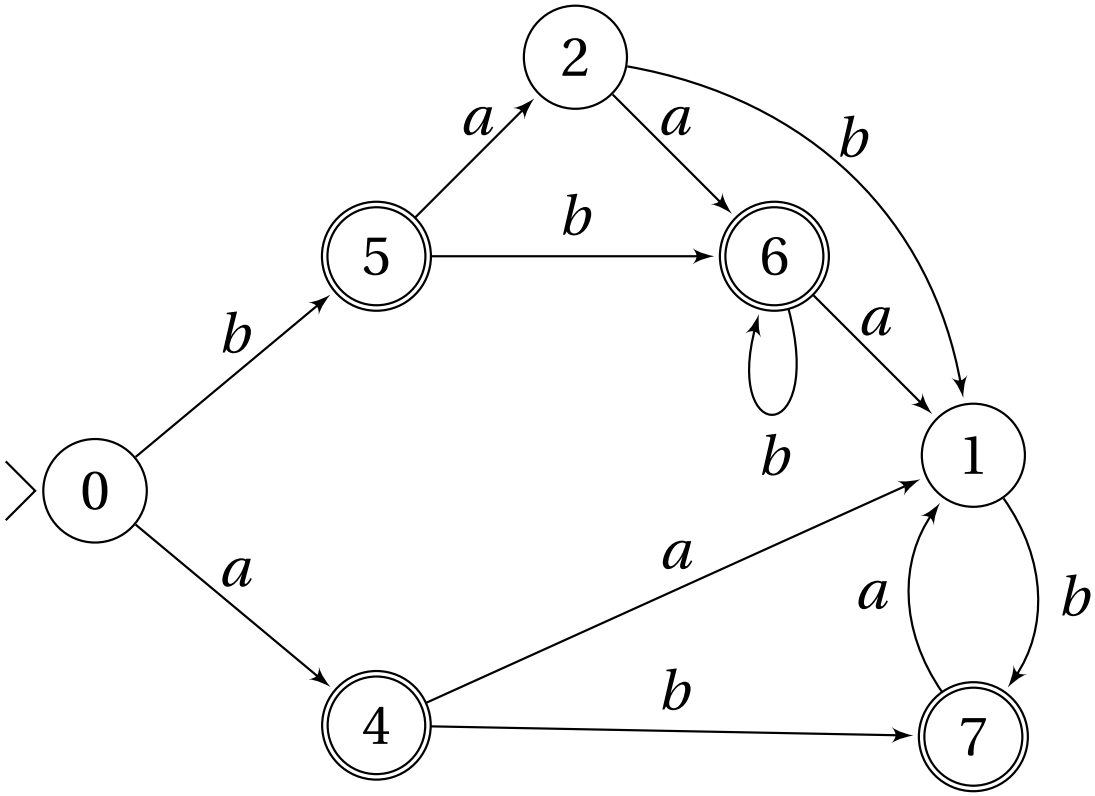
Ejemplo de construcción de DFA mínimo

Las letras (estados del DFA original) ya no son relevantes, retenemos solo una línea de cada grupo.

	a	b	Tipo
0	4	5	Inicial
1	3	7	
2	6	1	
3	3	3	(muerto)
4	1	7	Final
5	2	6	Final
6	1	6	Final
7	1	3	Final

No nos fue particularmente bien, solo disminuyó en un estado.

El DFA mínimo resultante



Resumen

- Obtuvimos una condición necesaria y suficiente para que un lenguaje sea regular. Es incómoda de usar, eso sí.
- Como consecuencia, obtenemos un algoritmo para hallar el DFA con el mínimo número de estados que reconoce el lenguaje.
- El apunte discute también el algoritmo de Brzozowski para construir el DFA mínimo, basado en ideas muy distintas.