Otra versión del lema del bombeo

Teorema

Sea $L = \{a^n b^n \mid n \geq 0\} = \{\epsilon, ab, aabb, aaabbb, \ldots\}$*. Entonces* B *no es un lenguaje regular.*

Dem. Por contradicción. Supongamos que B es regular. El teorema de Kleene asegura que existe M un AFD tal que $L = L(M)$. Pongamos

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

y sea k el número de elementos de Q. Consideremos $N >> k$ (N *mucho mayor* que k) y la palabra $w = a^N b^N$. Evidentemente $w \in L$ y w es aceptada por M. Consideremos los primeros estados que se emplean en la aceptación de w:

$$\begin{aligned} \delta(s, a) &= r_1 \in Q, \\ \delta(s, a^2) &= r_2 \in Q, \\ &\vdots \\ \delta(s, a^N) &= r_N \end{aligned}$$

$$\delta(s, a^N b) = r_{N+1}$$

$$\vdots$$

$$\delta(s, a^N b^N) = r_{2N} \in F.$$

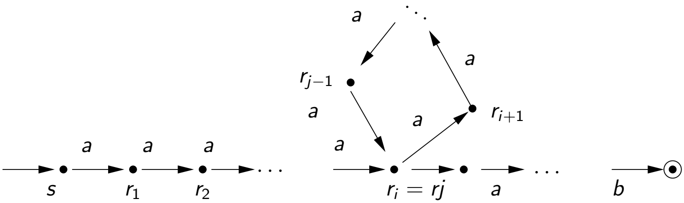
Tenemos que

$$\{r_1, r_2, \ldots, r_N\} \subseteq Q$$

luego como $N >> k$ y el principio de las casillas, se sigue que los estados r_i no pueden ser diferentes entre sí: se deben de repetir. Esto es: existen i, j tales que $1 \leq i < j \leq N$ y

$$r_i = r_j. \tag{1}$$

Esto indica que en el camino de las transiciones indicadas por $w = a^N b^N$, desde estado inicial, se forma un bucle:



por lo que el camino que usa el bucle es prescindible, i.e., $a^{N-(j-i)} b^N \in L$. En efecto:

$$\begin{aligned}
\delta(s, a^{N-(j-i)}) &= \delta(s, a^{N-j+i}) \\
&= \delta(s, a^i a^{N-j}) \\
&= \delta(\delta(s, a^i), a^{N-j}) \\
&= \delta(r_i, a^{N-j}) \\
&= \delta(r_j, a^{N-j}) \\
&= \delta(\delta(s, a^j), a^{N-j}) \\
&= \delta(s, a^j a^{N-j}) \\
&= \delta(s, a^N),
\end{aligned}$$

luego

$$\delta(s, a^{N-(j-i)} b^N) = \delta(\delta(s, a^{N-(j-i)}), b^N) = \delta(s, a^N b^N) \in F$$

por lo que $a^{N-(j-i)} b^N \in L(M) = L$: absurdo.
De hecho la prueba del teorema anterior se puede usar como un hecho general: *el lema del bombeo*. Veamos otra vez tal prueba en otro ejemplo.

Ejemplo

Sea $C = \{w \in \{a\}^* \mid |w| \text{ es una potencia de } 2\}$. *El lenguaje* C *también se puede escribir como*

$$\begin{aligned} C &= \{a^{2^n} \mid n \geq 0\} \\ &= \{a, a^2, a^4, a^8, a^{16}, \ldots\} \end{aligned}$$

Probar que C *no es un lenguaje regular.*

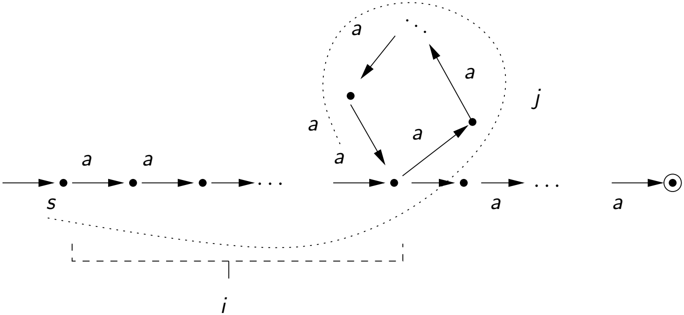
Dem.

Por contradicción. Supongamos que C es regular. Entonces existe M un DFA tal que $C = L(M)$. Sea Q el conjunto de estados de C y k el número de estados en Q. Consideremos $N >> k$ y la palabra $w = a^{2^N} \in C$. Los estados usados en la aceptación de w deben cumplir

$$\{\delta(s, a), \delta(s, a^2), \ldots, \delta(s, a^{2^N})\} \subseteq Q,$$

pero como en Q hay exactamente k estados y $2^N > k$, entonces, el principio del palomar asegura que deben de existir i, j tales que

$$\delta(s, a^i) = \delta(s, a^j), \quad 2^N \geq j > i$$



por lo que, en el camino hacia aceptación, el bucle puede ser despreciado, o bien utilizado varias veces. Si se usa dos veces se obtiene que $a^{2^N+(j-i)} \in L(M)$. En efecto: podemos poner $2^N = j + m$; luego

$$
\begin{aligned}
\delta(s, a^{2^N+(j-i)}) &= \delta(s, a^{j+m+(j-i)}) \\
&= \delta(\delta(s, a^j), a^{m+j-i}) \\
&= \delta(\delta(s, a^i), a^{m+j-i}) \\
&= \delta(s, a^{i+m+j-i}) \\
&= \delta(s, a^{j+m}) \\
&= \delta(s, a^{2^N}) \in F.
\end{aligned}
$$

esto es, $a^{2^N+(j-i)}$ es aceptada, por lo que $a^{2^N+(j-i)} \in C$. Pero $2^N + j - i$ NO es una potencia de 2, porque

$$2^N < 2^N + (j-i) < \underbrace{2^N + 2^N}_{=2^{N+1}}$$

lo que indica que el número $2^N + (j-i)$ está entre dos potencias consecutivas de 2, de donde $2^N + (j-i)$ no puede ser él mismo una potencia de 2. Por lo tanto $a^{2^N+(j-i)} \notin C$: contradicción.

Repitiendo el razonamiento de los dos ejemplos anteriores, se puede demostrar el siguiente teorema general.

Teorema (Lema del bombeo)

Sea A un lenguaje regular. La siguiente propiedad la cumple A:

(P) *Existe $k \geq 0$ tal que para cualesquiera x, y, z cadenas con*

$$xyz \in A \text{ y } |y| \geq k$$

existen cadenas u, v, w tales que

$$y = uvw \text{ con } v \neq \epsilon$$

y para todo $i \geq 0$ se cumple

$$xuv^i wy \in A$$