Myhill-Nerode

Autómatas y Lenguajes Formales

24 de septiembre de 2022

Myhill-Nerode y las tortas

Para explicar el teorema de Myhill-Nerode tomaré prestada una idea de otro autor. Imagen que plasmó en unas notas en pdf[1], pero lo adaptaré a un caso más cercano (caballos de carreras se me hacen muy aburridos).

Supongamos que vamos a poner una tortería en una esquina de nuestra ciudad o población. Para distanciarnos de las clásicas fórmulas de *La Trevi*, *La Tyson*, *La Pachuqueña*, *La Suiza*, etcétera, vamos a generar nuestras propias combinaciones. En ese caso podemos tener el ingrediente x y lo mezclamos con el ingrediente z. Sí la combinación xz sabe bien la aceptamos en la lista de *especialidades* y le ponemos de nombre *La Myhill-Nerode*. Si la combinación yz no tiene ese sabor único, no puede entrar en la lista de *especialidades*, no puede estar en la misma clase que la sabrosa y ya probada combinación xz..

Si pensamos nuestra tortería como un autómata finito determinista cada una de estas listas de combinaciones sería un estado del autómata en el que puede caerse al concatenar la cadena/ingrediente z a la cadena/ingrediente x.

Imaginemos un conjunto de ingredientes S con k ingredientes que cumplen que cada par de ingredientes distintos $x, y \in S$ siempre están en listas distintas[1], $x \not\equiv_L y$. Para tener esta tortería necesitarías como vitrina todos los ventanales de la torre mayor, por la cantidad de listas distintas que solo contienen un tipo de torta.

Ya se van dando cuenta que no les conviene poner esa tortería, veamos como se escribiría esto como el teorema de Myhill-Nerode.

Teorema 1 ***Myhill-Nerode (version 1 de Regan)****: Sea $L \subseteq \Sigma^*$ cualquier lenguaje. Suponga hay un conjunto infinito S de cadenas tales que para todas $x, y \in S$ $(x \neq y)$, $x \not\equiv_L y$. Es decir, suponga:*

$$(\forall x \neq y \in S)(\exists z \in \Sigma^*) L(xz) \neq L(yz). \tag{1}$$

Entonces L no es un lenguaje regular.

Que es una forma *compacta* de escribir el teorema a diferencia de la versión de Kozen. Esta segunda versión es útil para ver cada detalle de lo que cubre el teorema. Veamos las relaciones de Myhill-Nerode.

[1] El subíndice L hace referencia a que la comparación es hecha respecto a la función $L(x) = 1$ si $x \in L(M)$ y $L(x) = 0$ si $x \notin L(M)$ para M algún autómata finito determinista.

Relaciones de Myhill-Nerode

Sea $R \subseteq \Sigma^*$ un conjunto regular, sea $M = (Q, \Sigma, \delta, s, F)$ un autómata finito determinista sin estados inaccesibles para R. Este autómata induce una relación de equivalencia $\equiv_M$ en Σ^* definida por:

$$x \equiv_M y \overset{def}{\iff} \hat{\delta}(s, x) = \hat{\delta}(s, y). \tag{2}$$

Ven que hay pequeñas diferencias con lo mencionado antes, como les dije en este caso vamos paso a paso, detalle a detalle, viendo las características. La relación de equivalencia en este caso (Kozen) es respecto al autómata finito determinista, no al lenguaje como en el caso anterior (Regan). Este salto entre DFA y lenguaje regular estoy seguro a estas alturas no los asusta, estamos diciendo lo mismo en ambos casos, sólo nos faltan detalles.

Esta relación de equivalencia además de ser reflexiva, simétrica y transitiva cumple:

1. Es una *congruencia por la derecha*: para cualesquiera $x, y \in \Sigma^*$ y $a \in \Sigma$,

   $$x \equiv_M y \Rightarrow xa \equiv_M ya.$$

   En la versión de Regan esta congruencia por la derecha estaba implícita aunque no muy bien especificada. Si recuerdan los ingredientes para las tortas se agregaban por la derecha, así si hay una equivalencia entre dos ingredientes esa equivalencia se mantiene al agregar un mismo ingrediente.

   Si lo vemos en términos de autómatas finitos deterministas, siendo $x \equiv_M y$:

   $$\begin{aligned} \hat{\delta}(s, xa) &= \delta(\hat{\delta}(s, x), a) \\ &= \delta(\hat{\delta}(s, y), a) \text{ ya que supusimos } x \equiv_M y \\ &= \hat{\delta}(s, ya) \end{aligned}$$

2. Es un *refinamiento*[2] de R: para cualquier $x, y \in \Sigma*$,

   $$x \equiv_M y \Rightarrow (x \in R \iff y \in R). \tag{3}$$

   Ya que la relación de equivalencia nos dice que sí $x \equiv_M y$ entonces $\hat{\delta}(s, x) = \hat{\delta}(s, y)$. Sí hay equivalencia entre x y y deben llegar al mismo estado, sea de aceptación o rechazo, o todos los elementos están en R o no están. Entonces refina a R no porque lo haga más puro, si no porque nos da más detalles del conjunto, nos da el detalle *fino*.

3. Es de *índice finito*; es decir, tiene sólo finitamente muchas clases de equivalencia, pues hay exactamente una clase de equivalencia por estado del autómata finito determinista:

   $$\{x \in \Sigma^* | \hat{\delta}(s.x) = q\}$$

   (¿Recuerdan lo de la inmensa vitrina para todas las variedades de tortas? Es el caso contrario de lo que se nos dice aquí).

[2] El grado de refinación de la harina se da, no sé si en todos los países, por un número. El 000 refiere al más alto grado de refinación, también se usa en clave para la cocaína. Hay un gran libro de Roberto Saviano al respecto *Cero cero cero* en el que muy poco se basó la serie del mismo nombre de Amazon. El libro es un trabajo periodístico, la serie no es mala, pero muy cruda. Sólo como paréntesis informativo.

En este último punto vemos que hay algo de lo que nos dice la versión de Regan, pero al revés. Estos puntos nos dicen que debe cumplir el conjunto regular, la otra versión nos dice en qué caso no es regular (cuando no cumple esto).

Recomendaré le den una leída a esta parte en el Kozen, muestra que es equivalente definir un autómata finito determinista como lo hemos hecho tradicionalmente que definirlo a partir de las relaciones de Myhill-Nerode. No me detendré mucho en esto, pues además seguro lo explica mejor el libro mencionado. Vamos directo a como queda el teorema en la versión de Kozen, aún viendo unos detalles.

Teorema de Myhill-Nerode

Para continuar se debe remarcar que existe una relación más gruesa, o más tosca (no sé cuál sea la traducción correcta) de Myhill-Nerode ($\equiv_R$) para un conjunto R tal que cualquier otra relación de Myhill-Nerode es un refinamiento de esta en R.

Definición 1 *Se dice que una relación* $\equiv_1$ refina *otra relación* $\equiv_2$ *si* $\equiv_1 \subseteq \equiv_2$ *considerándolos conjuntos de pares ordenados. Es decir,* $\equiv_1$ refina *a* $\equiv_2$ *si para toda* x *y* y, $x \equiv_1 y$ *implica que* $x \equiv_2 y$.

Esta notación puede parecer extraña, elegimos nombrar al conjunto por lo que lo caracteriza, la relación. Si recuerdan sus clases de álgebra no les parecerá tan raro, los naturales pueden ser definidos por una relación característica, por ejemplo la suma (la suma de dos naturales es un natural y para construir todos los naturales hacemos uso de la suma). Si $\equiv_1$ *refina* a $\equiv_2$, etonces $\equiv_1$ es la relación más *fina* y $\equiv_2$ la más *gruesa* o más *tosca*.

Un ejemplo de una relación de equivalencia es $x \equiv y$ mód 6 que *refina* $x \equiv y$ mód 3, ya que todos los números módulo 6 son subconjunto de los módulo 3, incluso este hecho es utilizado para hacer más fácil la conversión de una base a otra[3].

Ahora sí regresamos un poco al tren de ideas seguido por Regan, definimos una relación de equivalencia como había mencionado para las tortas. Sea $R \subseteq \Sigma^*$ un conjunto sin importar si es regular o no. Definimos una relación de equivalencia $\equiv_R$ para Σ^* en términos de R como:

$$x \equiv_R y \underset{def}{\iff} \forall z \in \Sigma^* (xz \in R \iff yz \in R). \tag{4}$$

Dos cadenas son equivalentes bajo $\equiv_R$ si al agregarle la misma cadena por la derecha **ambas** cadenas resultantes están en R o no están en R, ¡pero ambas! En el caso de las tortas, dos ingredientes son equivalentes bajo la relación de

[3] ¿Han visto este juego de adivinación hecho por Martin Gardner? Se les presentan 6 cartas con números anotados en ellas, se les pide piensen en un número natural entre el 1 y el 60 y no se lo diga a quien realiza el truco. Una vez que lo tienen en mente se les pide indiquen en qué cartas se encuentra el número, puede bastar con ver el color o la parte trasera de las tarjetas para que el *adivinador* sepa cuál es el número en el que pensaron ¿saben cómo funcion esto? Tiene que ver con estas clases de equivalencia citadas. Para más referencia una página en portugués, no hallo la versión en español `https://problemasteoremas.wordpress.com/2008/12/31/enigma-adivinha-com-numeros-cartas-cores-e-base-2/`

equivalencia si al agregar el ingrediente z ambas terminan en la misma sección de *especialidades*, o ambas están fuera.

Antes de dar el teorema de Myhill-Nerode es necesario enunciar un lema.

Lema 1 *Sea $R \subseteq \Sigma^*$, regular o no. La relación $\equiv_R$ definida en 4 es un refinamiento congruente por la derecha de R y es la relación más tosca en Σ^*.*

Pareciera que algunos de estos puntos son muy directos de la definición de la relación, como sea no dejen de revisar la demostración de este lema en el Kozen, conociendo esta demostración se puede usar para demostrar el teorema de Myhill-Nerode en menos pasos (cosa muy bonita para un libro pero que quizá no lo más sencillo para el lector). De nuevo yo no lo hago aquí, mejor leerlo en la fuente original.

Ahora sí, el teorema de Myhill-Nerode quedaría:

Teorema 2 *(**Teorema de Myhill-Nerode, versión Kozen**) Sea $R \subseteq \Sigma^*$. Los siguientes enunciados son equivalentes:*

- *R es regular;*
- *existe una relación de Myhill-Nerode para R;*
- *la relación $\equiv_R$ es de índice finito.*

La demostración la pueden ver en el ya muy citado Kozen. Aquí en lo que me detendré es en qué nos quiere decir. Tal como antes vimos que es equivalente definir un automata finito determinista a través de puras relaciones de Myhill-Nerode a como lo hacíamos tradicionalmente, el teorema nos dice que es equivalente decir que un conjunto es regular, a decir que existe una relación de Myhill-Nerode para el mismo conjunto, a decir que una relación como la que se definió antes sobre ese mismo conjunto es de índice finito.

Para nuestro caso si no sabemos como construir el DFA que caracteriza al conjunto, entonces podemos buscar una relación de Myhill-Nerode sobre el conjunto, si tampoco podemos hacer eso entonces debemos mostrar que una relación como la que se definió (refinamiento congruente por la derecha) es de índice finito.

Si el conjunto no cumple alguno de los tres enunciados entonces no cumple ninguno. Es una forma de demostrar que ese conjunto no sería regular (que de los tres enunciados, a esta altura, es el que más nos interesa).

¿Cómo aplicamos este teorema para demostrar que un lenguaje no es regular? Hay dos opciones: ver que sólo se pueden construir relaciones que no son de Myhill-Nerode, o mostrar que una relación de afinación congruente por la derecha no es de índice finito.

Ejemplos

El ejemplo clásico es demostrar que el lenguaje (conjunto) L dado por:

$$L = \{a^n b^n | n \geq 0\}, \tag{5}$$

no es regular.

Ver si hay clases de equivalencia que no son de Myhill-Nerode se puede hacer complicado, pues no hemos visto muchos ejemplos de esas clases, pero contar clases lo podemos hacer más o menos, a ver si alcanzan las manos. Entonces contaremos clases de equivalencia que refinan y son congruentes por la derecha ($\equiv_R$).

Partamos de dos valores $k \neq m$, los elementos de la clase de equivalencia estarán dados por la cantidad de a's y b's, la potencia a la que se elevan en la notación. Siendo dos longitudes distintas k y m podemos ver que $a^k \not\equiv_R a^m$, no están en la misma clase de equivalencia, ya que $a^k b^k \in L$ pero no así $a^m b^k \notin L$. Esto implica que hay una clase de equivalencia para infinitos valores de la potencia k distintos. En el símil de la tortería, por cada ingrediente de la torta hay un cartel de tipo de combinación. Esto ya no es de índice finito pues hay infinitas clases y por el teorema de Myhill-Nerode L no es regular.

Para darle más peso podemos dar una expresión para la cantidad de clases de equivalencia. Podemos ver que el conjunto de expresiones a las que sí se les puede agregar b^k y están dentro del conjunto son:

$$H_k = \{a^{n+k}b^n | 1 \leq n\},\ k > 0,$$

si se le agrega por la derecha (concatena) b^k tenemos $a^{n+k}b^n b^k = a^{n+k}b^{n+k}$ y está en L. El conjunto que contiene a todas las clases de equivalencia, una por cada k:

$$G_k = \{a^k\},\ k \geq 0,$$

por cada potencia (longitud) hay una clase de equivalencia. Para los casos en los que sí se puede concatenar la cadena mencionada y se queda dentro del conjunto L esta dada por[4]:

$$\bigcup_{k \geq 0} G_k \cap H_k,$$

es la unión de todas las intersecciones del conjunto de clases de equivalencia con el conjunto que incluye todas las cadenas a las que se les puede agregar una b^k y siguen estando en L.

Lo que buscamos es el inverso de esto, entonces el conjunto que no cumple esta dado por la diferencia:

$$E = \Sigma^* - \bigcup_{k \geq 0} G_k \cap H_k,$$

y este conjunto es infinito ■.

Vemos otro ejemplo, uno que ya se hizo en las notas del lema del bombeo pero ahora hagámoslo por Myhill-Nerode:

Muestra que $L = \{a^p | p$ es primo$\}$ no es regular.

Empezamos suponiendo que L es regular y llegar a una contradicción. Si L s regular entonces existe una relación de equivalencia entre dos cadenas distintas

[4]Aquí hago una corrección al Kozen, probablemente yo soy quien no entiende bien, pero me parece que lo que buscamos es la intersección de las clases de equivalencia con el conjunto al que sí se le puede agregar la cadena b^k, $G_k \cap H_k$, pero no la unión, pues eso sería todas las clases de equivalencia

del lenguaje, $\alpha \in L$ y $\beta \in L$, es decir $\alpha = a^n$ y $\beta = a^m$ con n y m dos números primos distintos

$$\alpha \equiv_L \beta.$$

También podemos suponer que $n < m$, sabemos que son distintos, en caso de que sea el contrario sólo es cuestión de intercambiar nombres.

Si es una relación de Myhill-Nerode debe ser congruente por la derecha, sea $\gamma = a^{m-n}$. ya que sabemos que $n < m$ podemos elegir esta cadena a concatenar de forma conveniente, para que al concatenar α con γ obtener β. Pero en general la concatenación de k veces esta cadena debe seguir cumpliendo la congruencia por la derecha. Para tener el caso más general la cadena γ puede concatenarse cualquier cantidad de veces y seguir cumpliendo la relación de Myhill-Nerode (recuerden que seguimos suponiendo la regularidad), $\alpha \equiv_l \alpha\gamma^k$.

Veamos los casos:

- Cuando $k = 0$ tenemos la muestra de la reflexividad de la relación de equivalencia, $\alpha \equiv_L \alpha\gamma^0 = \alpha$.
- Cuando $k = 1$, tenemos nuestra suposición de que el lenguaje es regular y la relación de equivalencia se cumple para dos cadenas distintas, $\alpha \equiv_L \alpha\gamma^1 = a^n a^{m-n} = a^m = \beta$, ambos son cadenas con longitud igual a un número primo. Todo va pintado bien hasta aquí.
- Para naturales más grandes suponemos cierto $\alpha\gamma^{k+1}$ y vemos que pasa con[5] $k+2$. Vamos a ver si se sigue manteniendo la relación de equivalencia $\alpha \equiv_L \alpha\gamma^{k+2}$.
  - $\alpha\gamma^{k+2} = \alpha\gamma\gamma^{k+1} = \beta\gamma^{k+1}$
  - Si la relación se cumple es congruente por la derecha y debe cumplirse que $\alpha\gamma^{k+1} \equiv_L \beta\gamma^{k+1}$, parece que las cosas aún van cuadrando. Pero aún podemos esperar algo que lo contradiga.
  - Sabemos que si se cumple nuestra hipótesis de indicción, $\alpha \equiv_L \alpha\gamma^{k+1}$, entonces por transitividad de la relación $\alpha\gamma^{k+1} \equiv_l \beta\gamma^{k+1}$, tenemos que $\alpha \equiv_L \beta\gamma^{k+1} = \alpha\gamma^{k+2}$.

Pero si recuerdan una de las condiciones para que la relación sea de Myhill-Nerode es que sea un refinamiento, como se mencione en la ecuación**??**. SI tomamos $k = n$

$$\begin{aligned}\alpha\gamma^n &= a^n a^{n(m-n)} \\ &= a^{n+n(m-n)} \\ &= a^{n(1+m-n)}\end{aligned}$$

Y esto es una contradicción, $\alpha\gamma^n \notin L$ ya que esta cadena tiene una longitud de $n(1 + m - n)$, con[6] $(1 + m - n) > 1$, pero este valor por definición no es

[5] Sí, esto es inducción

[6] Si recuerdan tomamos que $m > n$, y si aparte le sumamos 1, seguro el valor es mayor que 1.

un primo, pues sus factores no son el mismo número y la unidad, entonces para cada k hay una clase de equivalencia distinta y son infinitas ■.

Ese ejemplo estuvo medio complicado, pero veamos otro ejemplo que se resolvió por lema del bombeo y resolvámoslo por Myhill-Nerode.

Demuestra que el lenguaje $\mathbf{A} = \{a^{2^n} | n \geq 0\}$ *no es regular.*

Pues ya saben el clásico proceder con Myhill-Nerode, supongamos que es regular y que por ello hay una relación de Myhill-Nerode que se cumple para dos cadenas distintas en el lenguaje, sean esas cadenas $\alpha, \beta \in A$ tales que $\alpha = a^{2^r}$ y $\beta = a^{2^s}$, son distintas ya que $r \neq s$. Suponemos que existe

$$\alpha \equiv_A \beta$$

Si es regular es equivalente a decir que se puede dar una relación de equivalencia para esas dos cadenas, de las finitas relaciones que podemos tener, y por ser de Myhill-Nerode, en particular, debe cumplirse la congruencia por la derecha. Tomemos la cadena $\gamma = a^{2^r}$. No es la norma tomar $\gamma = \alpha$, pero en este caso va a ser útil.

$$\begin{aligned} \alpha\gamma =& a^{2^r} a^{2^r} = a^{2^r+2^r} = a^{2(2^r)} = a^{2^{r+1}} \ (\alpha\gamma \in A) \\ \beta\gamma =& a^{2^s} a^{2^r} = a^{2^s+2^r} \end{aligned}$$

De la última parte no podemos decir que $\beta\gamma \in A$, no está claro, pero veamos los casos.

Si $s > r$	Si $s < r$
$2^s + 2^r = 2^{s-r+r} + 2^r$	$2^s + 2^r = 2^s + 2^{r-s+s}$
$2^s + 2^r = 2^{s-r}2^r + 2^r$	$2^s + 2^r = 2^s + 2^{r-s}2^s$
$2^s + 2^r = 2^r(2^{s-r} + 1)$	$2^s + 2^r = 2^s(1 + 2^{r-s})$

Notemos que en ambos casos la longitud de la cadena es un término del tipo $2^{algo}(1 + 2^{\text{otro algo}})$, veámos también que 2^w siempre es un número par, es un número 2^{w-1} multiplicado por 2, un número par a todo lo que da. Pero $(1 + 2^{algo})$ nunca es un número par, no puede ser representado como 2^w, de tal forma $a^{2^s} a^{2^r} \neq a^{2^w}$, no está en el lenguaje, por lo tanto hay infinitas clases de equivalencia pues para cada elección de r se requiere una clase de equivalencia distinta ■.

Referencias

[1] Regan, Kenneth, "Notes on the Myhill-Nerode Theorem" (PDF) (2010), consultadas en abril de 2022.

[2] Kozen, Dexter C. "Automata and Computability" Springer (1997)