Una aplicación de las matrices de Householder a la geometría

Josué Tonelli Cueto

(A lo largo de todo el escrito se usará la notación por columnas y los e_i representarán los vectores de la base canónica.)

En análisis numérico es habitual el uso de las llamadas matrices de Householder como primera aproximación del problema de descomposición QR, así resulta que esta matrices son de gran utilidad en geometría permitiendo dar pruebas elementales de muchos hechos profundos como son el embebimiento del espacio proyectivo en el grupo ortogonal, el teorema de Cartan-Dieudonné y la conexión de determinados grupos matriciales reales.

De este modo, el objetivo del presente escrito es mostrar cómo las matrices de Householder permiten realizar un enfoque elemental de estos hechos de un modo sencillo y directo. Por ello, se recurre al enfoque matricial,[1] en vez de a uno más abstracto.

1. Las matrices de Householder y su interpretación geométrica

El desarrolllo y demostración de las propiedades de la matrices de Householder son esenciales para las demostraciones que daremos a posteriori. Así, aquí, definiremos que es una matriz de Householder, además de dar finalmente una interpretación gemétrica de ellas.

Definición 1.1. *Dado un vector no nulo $u\in\mathbb{R}^n$, se denomina matriz de Householder asociada al vector u, $H(u)$, a la matriz dada por*

$$H(u)=\mathbb{I}_n-2\frac{u\cdot u^t}{u^t\cdot u}=\mathbb{I}_n-2\frac{u\cdot u^t}{|u|^2}$$

Ahora, probemos sus propiedades básicas,

Teorema 1.1. *Sean $u,v\in\mathbb{R}^n$ vectores no nulos, se verifica que*

A) $H(u)$ es simétrica.

B) Si P es ortogonal, entonces $P\cdot H(u)\cdot P^t=H(P\cdot u)$.

C) $H(u)$ es ortogonal negativa.

D) Si $|u|=|v|$, entonces $H(u-v)\cdot u=v$.

E) Si u y v son ortogonales, entonces $H(u)\cdot v=v$.

Demostración. A) Simplemente hemos que fijarnos en que

$$u\cdot u^t$$

es simétrica, y recordar que la trasposición es un automorfismo del grupo de matrices con la suma.

B) Por un lado las propiedades de la trasposición,

$$P\cdot u\cdot u^t\cdot P^t=(P\cdot u)\cdot(P\cdot u)^t$$

Y por otro lado, la ortogonalidad de P, $|u|=|P\cdot u|$, nos dan la igualdad deseada.

C) Por un lado, se da que

$$H(u)\cdot H(u)^t=H(u)^2=\left(\mathbb{I}_n-2\frac{u\cdot u^t}{|u|^2}\right)^2=\mathbb{I}_n-4\frac{u\cdot u^t}{|u|^2}+4\frac{(u\cdot u^t)\cdot(u\cdot u^t)}{|u|^4}=$$
$$=\mathbb{I}_n-4\frac{u\cdot u^t}{|u|^2}+4\frac{u\cdot|u|^2\cdot u^t}{|u|^4}=\mathbb{I}_n-4\frac{u\cdot u^t}{|u|^2}+4\frac{u\cdot u^t}{|u|^2}=\mathbb{I}_n$$

nos da que $H(u)$ es una isometría.

Y por otro lado, por el teorema del reemplazamiento y el teorema de ortogonalización de Gram-Schmidt, sabemos que existe una matriz ortogonal P tal que

$$P\cdot u=e_0=(\delta_i^0)$$

Así, es fácil ver que

$$\det(H(e_0))=-1$$

[1] Que, sin embargo, no ocultará la geometría subyacente.

Y así, como
$$P\cdot H(u)\cdot P^{-1}=P\cdot H(u)\cdot P^{t}=H(P\cdot u)$$
Concluímos que
$$\det(H(u))=-1$$
i.e. $H(u)$ es una isometría negativa.

D) Basta probar que
$$H(u-v)u-u=v-u$$
Así, como tenemos $|u|=|v|$, se da
$$|u-v|^2=2\cdot(|u|^2-u^t\cdot v)=2\cdot(u-v)^t\cdot u)$$
De donde, inmediatamente
$$H(u-v)\cdot u-u=-2\frac{(u-v)\cdot(u-v)^t\cdot u}{|u-v|^2}=-2\frac{(u-v)\cdot(u-v)^t\cdot u}{2\cdot(u-v)^t\cdot u)}=v-u$$
Concluyendo la afirmación.

E) Una consecuencia inmediata de que
$$u^t\cdot v=0$$
Y un mero cálculo.

□

Y finalmente veamos su significado geométrico,

Proposición 1.2. *Sea M el hiperplano dado por la ecuación implícita*
$$u\cdot x+p=0$$
Se verifica, que la reflexión respecto a este hiperplano en la dirección ortogonal está dada por
$$x\mapsto H(u)\cdot(x-p)+p$$

Demostración. Sea
$$G(x)=H(u)\cdot(x-p)+p$$
Es fácil ver que,

1. $G^2=id_{\mathbb{R}^n}$, por las propiedades A) y C) del teorema 1.1.

2. $G(x)=x$ syss $x\in M$, por la propiedad E) del teorema 1.1.

3. G es una isometría, por la propiedad C) del teorema 1.1.

De lo cual, G es la reflexión respecto del hiperplano M en la dirección ortogonal, como deseábamos mostrar. □

De esta manera, las matrices de Householder no son más que las aplicaciones lineales asociadas a las reflexiones respecto de hiperplanos de los espacios afines reales finitos.

2. El espacio proyectivo y un embebimiento topológico

En esta sección, mostraremos como la relación
$$u\mapsto H(u)$$
induce una aplicación continua, y a partir de ahí, analizando algunas de sus propiedades, mostraremos como el espacio proyectivo puede ser embebido en el espacio de matrices ortogonales, dándose así que el espacio proyectivo puede interpretarse como las reflexiones respecto a los hiperplanos que pasan por un punto en la dirección ortogonal.

Definición 2.1. *Se denomina función de Householder, a la aplicación*
$$H:\mathbb{R}^n-\{0\}\to O_n(\mathbb{R})$$
$$u\mapsto H(u)$$

De esta forma, veamos sus propiedades

Teorema 2.1. *Sea $H:(\mathbb{R}^n-\{0\},\tau_u)\to(O_n(\mathbb{R}),\tau_u)$ la función de Hosueholder, se verifica que*

a) H es continua.

b) $H(u) = H(v)$ *syss hay un* $\lambda \in \mathbb{R}^*$ *tal que* $u = \lambda v$.

Demostración. a) Un simple consecuencia de que el producto matricial de funciones continuas es continuo, y de que las funciones continuas sobre un $\mathbb{R}$-espacio vectorial topológico forman un $\mathbb{R}$-espacio vectorial.

b) Tenemos que si para un $\lambda \in \mathbb{R}^*$ se da $u = \lambda v$, entonces de forma trivial

$$H(u) = H(v)$$

Y por otro lado, si $H(u) = H(v)$, entonces

$$H(u) \cdot u = H(v) \cdot u$$

Y así,

$$u = \frac{u^t \cdot v}{v^t \cdot v} v$$

donde $\frac{u^t \cdot v}{v^t \cdot v} \in \mathbb{R}^*$ al ser u no nulo.

□

Ahora, el teorema del embebimiento

Teorema 2.2. *La aplicación*

$$\begin{aligned} \overline{H} : (P^{n-1}(\mathbb{R}), \tau_u) &\to (O_n(\mathbb{R}), \tau_u) \\ [u] &\mapsto H(u) \end{aligned}$$

es un embebimiento del espacio proyectivo real de dimensión $n-1$ *en el grupo de las matrices ortogonales reales de orden* n.

Demostración. Basta considerar

$$\begin{aligned} H : (\mathbb{S}^{n-1}, \tau_u) &\to (H(\mathbb{S}^{n-1}), \tau_u) \subset (O_n(\mathbb{R}), \tau_u) \\ u &\mapsto H(u) \end{aligned}$$

Así, de forma inmediata que

$$H : (\mathbb{S}^{n-1}, \tau_u) \to (H(\mathbb{S}^{n-1}), \tau_u)$$

es una identificación, al ser H continua y por ello cerrada al ser el espacio de llegada T_2 y $(\mathbb{S}^{n-1}, \tau_u)$ compacto. Ahora, la relación inducida por H verifica que

$$x \sim y \text{ syss } H(x) = H(y) \text{ syss } x = y \text{ o } x = -y$$

Obtenemos por la caracterización de los espacios cocientes y la definición de espacio proyectivo que

$$(P^{n-1}(\mathbb{R}, \tau_u) \cong (\mathbb{S}^{n-1}/\sim, \tau_u) \cong (H(\mathbb{S}^{n-1}), \tau_u)$$

Por lo que la aplicación $\overline{H}$ es el embebmiento deseado. □

3. Teorema de Cartan-Dieudonné

El teorema de Cartan-Dieudonné es un teorema central a la hora de determinar la estructura de las ismotrías de los espacios euclídeos, dado que permite reducir teoremas de conservación por isometrías a teoremas de conservación por reflexiones respecto a hiperplanos.

De esta forma, probaremos el teorema de Cartan-Dieudonné, con un énfasis constructivo, en sus versiones vectorial y afín usando las matrices de Hosueholder. Así, la versión vectorial es

Teorema 3.1 (Teorema vectorial constructivo de Cartan-Dieoudonné)**.** *Si* $A \in O_n(\mathbb{R})$, *entonces* A *es producto de a lo sumo* n *reflexiones ortogonales respecto de hiperplanos vectoriales.*

Además, sea

$$A = (a_i)$$

Basta tomar la sucesión recurrente finita de matrices ortogonales

$$H_m = \begin{cases} H\left(a_m - \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_m\right) & \text{si } a_m - \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_m \neq 0 \\ \mathbb{I}_n & \text{en otro caso} \end{cases}$$

Para la cual

$$A = \prod_{i=0}^{n-1} H_{n-1-i}$$

Y así obtener la descomposición deseada.

Demostración. Sólo es necesario probar la segunda parte del enunciado, dado que por la proposición 1.2 las matrices de Householder son reflexiones respecto de hiperplanos vectoriales. De esta forma, lo que debemos de probar es que para cada k,

$$a_k = \prod_{i=0}^{n-1} H_{n-1-i} \cdot e_k$$

De este modo, el hecho fundamental es el siguiente:

Dado que A es ortogonal, $\{a_i\}$ constituye una base ortonormal de $\mathbb{R}^n$.

Así, dado un k cualquiera, hemos de probar que

$$a_k = \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_k$$

para cada $m \in \{k+1,...,n-1\}$.

Para ello, procedamos por inducción, así para $m = k+1$ tenemos que

$$a_k = \prod_{i=0}^{k} H_{k-i} \cdot e_k = H_k \cdot \left(\prod_{i=0}^{k-1} H_{k-i} \cdot e_k \right)$$

por definición de H_k y el punto D) del teorema 1.1, en virtud de que tanto a_k como $\prod_{i=0}^{k-1} H_{k-i} \cdot e_k$ son unitarios.

Ahora, supongamos que es cierto para un $m \in \{k+1, n-2\}$, así tenemos por hipótesis inductiva que

$$a_k = \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_k$$

Ahora, si H_m es la identidad, claramente

$$\prod_{i=0}^{m} H_{m-i} \cdot e_k = \prod_{i=1}^{m} H_{m-i} \cdot e_k = \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_k = a_k$$

Y la afirmación es cierta para $m+1$, sino

$$H_m = H\left(a_m - \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_m \right)$$

Y entonces,

$$\prod_{i=0}^{m} H_{m-i} \cdot e_k = H\left(a_m - \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_m \right) \cdot \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_k = H\left(a_m - \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_m \right) \cdot a_k = a_k$$

por la propiedad E) del teorema 1.1, dado que a_k es ortogonal a $a_m - \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_m$, en virtud de que

- a_k es ortogonal a a_m por ser $\{a_i\}$ una base ortonormal.
- $a_k = \prod_{i=0}^{m-1} H_{m-1-i} \cdot e_k$ es ortogonal a $\prod_{i=0}^{m-1} H_{m-1-i} \cdot e_m$, por serlo e_k a e_m y ser $\prod_{i=0}^{m-1} H_{m-1-i}$ ortogonal.

Siendo también cierta la afirmación para $m+1$. Finalmente, por el principio de inducción concluimos nuestra afirmación y la del teorema. □

Observación 3.2. *El teorema de Cartan-Dieudonné uede servirnos para convertir $O_n(\mathbb{R})$ en un espacio métrico discreto, imponiendo que la distancia entre dos matrices sea dada por el número mínimo de reflexiones ortogonales respecto a hiperplanos vectoriales necesaria para pasar de una matriz a otra. En ese contexto, el teorema de Cartan-Dieudonné nos dice que esa métrica está bien definida y que su diámetro es n.*

Y la versión afín es

Teorema 3.3. *Si $G \in AO_n(\mathbb{R})$, entonces G es producto de a lo sumo $n+1$ reflexiones ortogonales respecto de hiperplanos.*

Además, sean

$$G = \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}$$

y

$$A = (a_i)$$

Basta tomar por un lado

$$M = \begin{cases} H(v) & si\ v \neq 0 \\ I_n & si\ v = 0 \end{cases}$$

y por otro lado, la sucesión recurrente finita de matrices ortogonales

$$H_m = \begin{cases} H\left(M^{-1}a_m - \prod_{i=0}^{m-1} H_{m-1-i}\cdot e_m\right) & \text{si } M^{-1}a_m - \prod_{i=0}^{m-1} H_{m-1-i}\cdot e_m \neq 0 \\ \mathbb{I}_n & \text{en otro caso} \end{cases}$$

Para las cuales

$$G = \begin{pmatrix} M & v \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} M^{-1}A & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} M & v \\ 0 & 1 \end{pmatrix} \cdot \prod_{i=0}^{n-1} \begin{pmatrix} H_{n-1-i} & 0 \\ 0 & 1 \end{pmatrix}$$

Y así obtener la descomposición deseada.

Demostración. Inmediato del teorema vectorial anterior. □

4. Teoremas de conexión en grupos de matrices

El teorema de Cartan-Dieoudonné anterior tiene implicaciones no triviales, siendo una de las más importantes la conexión por caminos de muchos de los grupos de matrices positivas reales, cuya importancia radica en que nos permiten afirmar que las transformaciones positivas son especiales al poder transformar continuamente el espacio del estado inicial en el final.

De este modo, probemos primero un pequeño lema sobre el número de reflexiones que intervienen en la descomposición Cartan-Dieudonné de una isometría positiva.

Lema 4.1. *Sea $A \in SO_n(\mathbb{R})$. Si*

$$A = \prod_{i=0}^{m} H_i$$

es una descomposición de Cartan-Dieudonné reducida, i.e. ninguna H_i es la identidad; entonces m es par.

Demostración. Como para cada i,

$$\det(H_i) = -1$$

Y $\det(A) = 1$, la afirmación es inmediata, dado que $(-1)^m = 1$ syss m es par. □

Observación 4.2. *Fijarse que de esta lema, puede obtenerse sin mucha dificultad que toda isometría positiva afín puede expresarse como composición de una traslación y $\lfloor \frac{n}{2} \rfloor$ rotaciones planas a lo sumo.*

Y ahora, entremos en los teoremas de conexión propiamente dichos.

Teorema 4.3. *El espacio topológico $(SO_n(\mathbb{R}), \tau_u)$ es conexo por caminos.*

Demostración. Sea $A \in SO_n(\mathbb{R})$, por el teorema constructivo de Cartan-Dieudonné y el lema 4, consideremos que

$$A = \prod_{i=0}^{m} H(u_i)H(v_i)$$

en su descomposición como producto de matrices de Householder, de modo que u_i y v_i no sean proporcionales. En caso de que lo fueran para algún j, se tendría

$$H(u_j)H(v_j) = H(u_j)H(u_j) = \mathbb{I}_n$$

Y se podría eliminar el factor del producto, en viertud de los teoremas 1.1 y 2.1. De esta forma, definamos la función

$$A : ([0,1], \tau_u) \to (SO_n(\mathbb{R}), \tau_u)$$

$$t \mapsto \prod_{i=0}^{m} H(u_i)H(t\cdot v_i + (1-t)\cdot u_i)$$

La cual dado que $t\cdot v_i + (1-t)\cdot u_i \neq 0$ para cada i y cada $t \in [0,1]$, está bien definida, y por el teorema 2.1 y el hecho de que el producto matricial de funciones continuas sea continuo es continua.

De esta forma, $A : ([0,1], \tau_u) \to (SO_n(\mathbb{R}), \tau_u)$ es un camino de la matriz identidad a A, dado que

$$A(0) = \prod_{i=0}^{m} H(u_i)H(u_i) = \mathbb{I}_n$$

y

$$A(1)=\prod_{i=0}^{m} H(u_i)H(v_i)=A$$

Por lo que concluimos que $(SO_n(\mathbb{R}),\tau_u)$ es conexo por caminos, dado que hay un camino desde la matriz identidad a cualquier otra matriz de este espacio. □

Y a partir de aquí, se tiene toda una serie de colorarios acerca de la conexión.

Colorario 4.4. *El espacio topológico $(ASO_n(\mathbb{R}),\tau_u)$ es conexo por caminos.*

Demostración. Sea

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}$$

una matriz en este espacio. Basta considerar, el camino dado por

$$\begin{pmatrix} A(t) & v\cdot t \\ 0 & 1 \end{pmatrix}$$

donde $t\mapsto A(t)$ un camino desde la identidad hasta A en virtud de la conexión de $SO(\mathbb{R}^n)$. De aquí, se obtiene la conexión por caminos deseada. □

Colorario 4.5. *El espacio topológico $(O_n(\mathbb{R}),\tau_u)$ tiene exactamente dos componentes conexas (por caminos): $SO_n(\mathbb{R})$ y $SO_n^-(\mathbb{R})$.*

Demostración. La continuidad de la función determinante nos determina que por lo menos hay dos componentes conexas (por caminos), y que el espacio se haya dividido en unión disjunta de $SO_n(\mathbb{R})$ y $SO_n^-(\mathbb{R})$. Finalmente, el teorema anterior nos confirma que efectivamente estas son las dos componentes conexas (por caminos) del espacio. □

Colorario 4.6. *El espacio topológico $(AO_n(\mathbb{R}),\tau_u)$ tiene exactamente dos componentes conexas (por caminos): $ASO_n(\mathbb{R})$ y $ASO_n^-(\mathbb{R})$.*

Demostración. Igual que el anterior, la continuidad de la función determinante nos da que hay al menos dos y el colorario 4.4 nos confirma que las componentes del espacio son dos, y precisamente las deseadas. □

Colorario 4.7. *El espacio topológico $(GL_n(\mathbb{R}),\tau_u)$ tiene exactamente dos componentes conexas (por caminos): $GL_n^+(\mathbb{R})$ y $GL_n^-(\mathbb{R})$.*

Demostración. Por un lado, la continuidad de la función determinante nos da que hay a lo sumo dos componentes conexas, y que el espacio puede expresarse como unión disjunta de $GL_n^+(\mathbb{R})$ y $GL_n^-(\mathbb{R})$. Ahora, dada $A\in GL_n^+(\mathbb{R})$, se verifica por la descomposición QR que podemos escribirla como

$$A=Q\cdot R$$

siendo $Q\in SO_n(\mathbb{R})$ y R triangular superior con los elementos de la diagonal positivos. Así, por la conexión por caminos de $SO_n(\mathbb{R})$, tenemos un camino $t\in Q(t)$ de la identidad a Q, de modo que

$$t\mapsto Q(t)\cdot(t\cdot R+(1-t)\cdot\mathbb{I}_n)$$

es un camino de la identidad a A, y así $GL_n^+(\mathbb{R})$ es conexo por caminos.

Para la conexión de $GL_n^-(\mathbb{R})$, basta notar que la multiplicación por

$$\begin{pmatrix} -1 & \mathbb{O} \\ \mathbb{O} & \mathbb{I}_{n-1} \end{pmatrix}$$

induce un homeomorfismo entre $GL_n^+(\mathbb{R})$ y $GL_n^-(\mathbb{R})$. □

Colorario 4.8. *El espacio topológico $(AGL_n(\mathbb{R}),\tau_u)$ tiene exactamente dos componentes conexas (por caminos): $AGL_n^+(\mathbb{R})$ y $AGL_n^-(\mathbb{R})$.*

Demostración. Inmediato del colorario anterior, al considerar los caminos de la forma

$$\begin{pmatrix} A(t) & v\cdot t \\ 0 & 1 \end{pmatrix}$$

□