Bol. Soc. Esp. Mat. Apl. n^o*23(2003), 91–100*

Matrices de Hadamard

T. Domínguez

Departamento de Análisis Matemático,
Facultad de Matemáticas, Universidad de Sevilla

tomasd@us.es

Resumen

Se definen las matrices de Hadamard y se indican algunos problemas referentes a su existencia, construcción y unicidad. Se mostrarán algunos ejemplos de aplicaciones de las matrices de Hadamard para resolver problemas de muy diferentes áreas de las matemáticas, concretamente: obtención de determinantes maximales, diseño de pesadas, detección de errores y corrección de códigos y finalmente problemas más modernos enmarcados en la Teoría Geométrica de los espacios de Banach.

Palabras clave: *Determinantes maximales, residuos cuadráticos, diseño de pesadas, estructura normal, corrección de códigos.*

Clasificación por materias AMS: *15A15, 11A07, 94B05, 46B20*

1 Introducción

El objeto de este artículo es hacer una recapitulación sobre ciertos resultados conocidos que muestran la interacción entre las diversas partes de las matemáticas. En concreto mostramos el interés que tiene un tipo especial de matrices, definidas por Hadamard en 1893 [4], para la resolución de problemas que surgen en áreas tan alejadas (aparentemente) como la teoría de códigos, diseños de pesadas o propiedades geométricas de los espacios de Banach. Al mismo tiempo y siguiendo la motivación que inspiró a Hadamard la definición de estas matrices, estudiamos el problema de buscar matrices con determinantes maximales. Por otra parte, la existencia de matrices de Hadamard de cualquier orden múltiplo de 4 es un problema aún abierto. Comentaremos este problema de existencia y mostraremos un método de construcción debido a Pailey, basado en el uso de residuos cuadráticos correspondientes a números primos.

Los resultados referidos a determinantes maximales pueden ser ampliados en [2]y [8] y los de teoría de códigos en [6].

Fecha de recepción: 20 de Mayo de 2002

2 Matrices de Hadamard: definición y ejemplos

Una matriz de Hadamard H de orden n es una matriz $n \times n$ formada por 1's y -1's tal que sus filas son ortogonales, esto es, $HH^t = nI$. Puesto que al multiplicar cualquier fila o columna por -1 en una matriz de Hadamard se obtiene otra matriz de Hadamard, podemos cambiar la primera fila y columna para que estén formadas sólo por 1's. Una matriz de este tipo se llama normalizada. Mostramos a continuación algunos ejemplos de matrices de Hadamard normalizadas:

$$H_1 = (1)\,, \qquad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

La primera cuestión que surge al considerar matrices de Hadamard es la siguiente: ¿existen matrices de Hadamard de cualquier orden? Veamos que si existe H_n y $n > 2$, entonces n tiene que ser múltiplo de 4. En efecto cambiando las columnas de orden podemos suponer que las tres primeras filas de H son como sigue (donde $-$ representa -1):

$$\begin{array}{cccc} 11\ldots1 & 11\ldots1 & 11\ldots1 & 11\ldots1 \\ 11\ldots1 & 11\ldots1 & --\ldots- & --\ldots- \\ \underbrace{11\ldots1}_{i} & \underbrace{--\ldots-}_{j} & \underbrace{11\ldots1}_{n/2-i} & \underbrace{--\ldots-}_{n/2-j} \end{array}$$

Como la segunda y la tercera fila son ortogonales, se tiene

$$i - j + n/2 - j - n/2 + i = 0,$$

$$2i - 2j = 0 \Longrightarrow i = j.$$

Así $n = 4i$ tiene que ser múltiplo de 4.

Ahora la pregunta sería: ¿existen matrices de Hadamard de cualquier orden que sea múltiplo de 4? Si repasamos los ejemplos anteriores vemos que cada uno procede del anterior mediante la construcción

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}.$$

Así se obtienen matrices de orden $1, 2, 4, 8, \ldots, 2^n, \ldots$ que son llamadas matrices de Sylvester. ¿Qué sucede para otros órdenes, por ejemplo, 12? Veamos otro método de construcción, llamado de Payley. Para ello necesitamos considerar residuos cuadráticos.

3 Residuos cuadráticos. Construcción de Payley

Definición 1 *Sea p un número primo mayor que 2. Los números $1^2, 2^2, 3^2, \ldots, (p-1)^2$ módulo p son llamados residuos cuadráticos módulo p.*

Para encontrarlos basta considerar
$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$
En efecto
$$(p-a)^2 = p^2 - 2ap + a^2 \equiv a^2 \pmod p,$$
por lo cual $(p-a)^2$ y a^2 dan lugar al mismo residuo. Además son todos distintos. En efecto, si $i^2 \equiv j^2 \pmod p$, se tiene que p es divisor de $i^2 - j^2 = (i+j)(i-j)$. Como p es primo, tiene que dividir a $i-j$ o a $i+j$, lo cual es imposible si $i-j \neq 0$, pues $0 < i+j < p$. Por consiguiente hay $(p-1)/2$ residuos. Los restantes $(p-1)/2$ números $(\bmod\, p)$ son llamados no residuos. El cero no es considerado. Por ejemplo para $p = 7$ tenemos $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2$, con lo cual los residuos son $1, 2, 4$ y los no residuos $3, 5, 6$.

A partir de los residuos podemos definir la función χ de Legendre definida sobre los enteros por:
$$\begin{aligned}
\chi(i) &= 0, \quad \text{si } i \equiv 0 \pmod p,\\
\chi(i) &= 1, \quad \text{si } i \pmod p \text{ es residuo},\\
\chi(i) &= -1, \quad \text{si } i \pmod p \text{ es no residuo}.
\end{aligned}$$
Supongamos que p es un primo mayor que 2. Formamos la matriz de Jacobsthal $Q = (q_{ij})$ de orden p donde $q_{ij} = \chi(j-i)$. Por ejemplo, para $p = 7$ se obtiene
$$Q = \begin{pmatrix}
0 & 1 & 1 & - & 1 & - & - \\
- & 0 & 1 & 1 & - & 1 & - \\
- & - & 0 & 1 & 1 & - & 1 \\
1 & - & - & 0 & 1 & 1 & - \\
- & 1 & - & - & 0 & 1 & 1 \\
1 & - & 1 & - & - & 0 & 1 \\
1 & 1 & - & 1 & - & - & 0
\end{pmatrix}.$$
Si ponemos ahora
$$\begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1} & Q - I \end{pmatrix},$$
se puede probar que se obtiene una matriz de Hadamard de orden $p+1$. Todo esto es también cierto para cualquier potencia de p siendo p un número primo. Así podemos obtener matrices de orden $4, 8, 12, 20, 24, 28$. Este método de construcción fue dado por Pailey [7]. Por otros métodos de construcción (existen muchos diferentes) se han encontrado matrices de Hadamard de orden n si n es múltiplo de 4 hasta 264. No se conoce si existe una matriz de Hadamard de orden 268.

Otro problema interesante es el número de matrices de orden n que pueden ser construidas. Decimos que dos matrices son equivalentes si se puede pasar de una a otra por intercambio de filas o columnas, o multiplicando filas y columnas por -1. Se puede probar que sólo hay una clase de equivalencia para orden $1, 2, 4, 8, 12$. Sin embargo hay cinco clases de orden 16 y tres de orden 20. No se conoce el número de clases de equivalencia de orden 24.

4 Determinantes maximales

El origen de las matrices de Hadamard se debe al siguiente problema: sea $A = (a_{ij})$ una matriz de orden n tal que $|a_{ij}| \leq 1$. ¿Cuál es el valor máximo posible de $\det(A)$? Puesto que $\det(\lambda A) = \lambda^n \det(A)$, la restricción impuesta $\|A\|_\infty \leq 1$ es sólo una condición de normalización. La primera fácil observación es la siguiente: si $M = \text{máx} \det(A)$ con A como antes, existe A formada por 1's y -1's tal que $\det(A) = M$. En efecto, sacando cualquier a_{ij} como factor común resulta

$$\det(A) = a_{ij}c + d,$$

donde d es independiente de a_{ij}. Si $|a_{ij}| \neq 1$, reemplazando a_{ij} por 1 si $c \geq 0$, o por -1 si $c < 0$, se obtiene A_0 con $\det(A_0) \geq \det(A)$. Por otra parte, Hadamard probó que para matrices A con $\|A\|_\infty \leq 1$ se tiene $\det(A) \leq n^{n/2}$. Nótese que si A es una matriz de Hadamard, se tiene

$$AA^t = nI \Rightarrow (\det(A))^2 = n^n,$$

por lo que el determinante es maximal. Además Hadamard probó que $\det(A) = n^{n/2}$ si y sólo si A es una matriz de Hadamard. Por lo tanto, si no existe matriz de Hadamard de orden n, el máximo anterior es estrictamente menor que $n^{n/2}$. De hecho, no se conoce una fórmula general en este caso. Los primeros valores son

1	2	3	4	5	6	7	8	9	...
1	2	4	16	48	160	576	4096	14336	...

5 Teoría de Códigos

Una aplicación interesante de las matrices de Hadamard se refiere a la Teoría de Códigos. Esta es una rama de las Matemáticas e Ingeniería surgida a mediados del siglo pasado. Aunque tiene su origen en problemas de Ingeniería, el tema se ha desarrollado usando métodos matemáticos cada vez más sofisticados.

Los códigos se inventaron para corregir errores en canales de comunicación debidos al ruido. Supongamos que se envía un mensaje digitalizado (esto es, formado por 0's y 1's). Normalmente al enviar un 0 se recibe un 0, pero en algún caso (digamos con probabilidad 1/100) por problemas de ruido el 0 se recibe como un 1. Es importante para el receptor advertir la existencia del error y corregirlo. ¿Cómo puede hacerse esto? Podemos "alargar"el mensaje introduciendo signos de control. El ejemplo más usual para nosotros es el NIF con su letra de control al final de los números del DNI. Si se produce un error al introducir estos números (salvo que haya dos errores que se compensen, lo cual es altamente improbable) la letra de control lo marca. Los códigos más sencillos son los lineales. Veamos un ejemplo. Suponemos que estamos mandando una "palabra"digital de tres letras $u_1u_2u_3$ donde $u_i = 0$ ó 1. Tomamos una matriz de dimensión $n \times 3$ formada por 0's y 1's. Por ejemplo, para $n = 3$, consideramos

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

Alargamos el código poniendo

$$(u_1 u_2 u_3) \to \begin{pmatrix} I_{3\times 3} \\ A \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix}$$

en base 2, donde $x_i = u_i$ para $i = 1, 2, 3$. Así se obtiene la siguiente correspondencia entre los códigos que queremos enviar y los códigos alargados con tres cifras de control

$$\begin{array}{ccc} 000 & \to & 000000, \\ 100 & \to & 100011, \\ 010 & \to & 010101, \\ 001 & \to & 001110, \\ 110 & \to & 110110, \\ 101 & \to & 101101, \\ 011 & \to & 011011, \\ 111 & \to & 111000. \end{array}$$

Vemos que los números de control pueden coincidir, pero lo hacen para palabras que se diferencian en los tres dígitos. De esta forma, si suponemos que sólo se produce un error (o dos), la secuencia de control lo advertirá. Pero también es importante que en caso de error el receptor sea capaz de regenerar la palabra enviada. En efecto, la distancia mínima entre dos palabras de este código (esto es, la distancia de Hamming = número de cifras diferentes entre dos palabras) es 3. De esta manera, si hay un error, sólo una de las palabras correctas es posible. Los dos problemas —detección de errores y reconstrucción de la palabra correcta— son la clave de esta teoría. Elegir la matriz (de comprobación de la paridad) más apropiada en este caso o diseñar otros tipos de códigos es un problema de gran interés y dificultad. Para la reconstrucción de palabras es importante que la distancia de Hamming d sea lo mayor posible. Es fácil ver que un código con distancia mínima d puede corregir hasta $[(d-1)/2]$ errores. En el ejemplo anterior se puede corregir un error, pero no hay garantía para corregir dos errores.

En general, un (n, M, d) código es un conjunto de M vectores de dimensión n tal que dos vectores cualesquiera difieren en, al menos, d coordenadas. Lógicamente interesa que n sea lo más pequeño posible y en cambio M y d sean lo más grande posible. La siguiente desigualdad establece la cota mejor posible:

Teorema 1 (Cota de Plotkin) *Para cualquier* (n, M, d) *código* $\mathcal{C}$ *para el cual* $n < 2d$*, se tiene*

$$M \leq 2\left[\frac{d}{2d-n}\right].$$

Demostración . Para M par (la demostración es similar para M impar) vamos a calcular $S = \sum_{u,v\in\mathcal{C}} d(u,v)$ de dos formas diferentes. En primer lugar, como hay $M(M-1)$ parejas y la distancia entre ellas es al menos d, se tiene $S \geq M(M-1)d$. Por otra parte, pongamos las M palabras como filas de una matriz $M \times n$. Supongamos que la columna i contiene x_i 0's y $M - x_i$ 1's. Entonces esta columna contribuye $2x_i(M - x_i)$ a la suma. Por tanto $S = \sum_{i=1}^{n} 2x_i(M - x_i)$. Por cálculo elemental se prueba que el máximo de esta función de n variables se alcanza para $x_i = M/2$, obteniéndose de esta forma $S \leq nM^2/2$. Tenemos entonces

$$M(M-1)d \leq nM^2/2,$$

lo que implica

$$M \leq \frac{2d}{2d-n} \Rightarrow \frac{M}{2} \leq \frac{d}{2d-n} \Rightarrow \frac{M}{2} \leq \left[\frac{d}{2d-n}\right] \Rightarrow M \leq 2\left[\frac{d}{2d-n}\right].$$

Por ejemplo, si queremos con longitud $n = 6$ obtener $d = 4$, el número máximo de palabras es $2[4/2] = 4$. □

A la vista de la cota de Plotkin sería importante conseguir códigos en los que se alcance esta cota. Así para un n y d fijados se obtendría un código con el número máximo de palabras posibles. Para conseguir este código las desigualdades que hemos manejado se tienen que convertir en igualdades. Por tanto, todas las palabras tienen que estar a distancia d y en cada columna debe haber el mismo número de 0's que de 1's. Una herramienta fundamental para conseguirlo son las matrices de Hadamard.

Teorema 2 (Levenshteim [5]) *Si* n *y* d *son pares y existen matrices de Hadamard de orden* $4[d/(2d-n)]$ *y* $4[d/(2d-n)] + 4$*, las cotas de Plotkin son alcanzadas.*

Hay resultados similares para n y/o d impares. La demostración se basa en utilizar adecuadamente matrices de Hadamard, pegando trozos de ellas apropiadamente.

Mostramos como ejemplo un (12,4,8) código. Consideramos la matriz de Hadamard de orden 8 con los -1's convertidos en 1's y los 1's en 0's, esto es,

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1\\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 1\\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0\\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 1\\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0\\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 0\\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1
\end{pmatrix}.$$

Quitamos la primera columna y posteriormente las filas que comienzan por 1. Volvemos a quitar la primera columna y pegamos la matriz resultante consigo misma, obteniéndose el código $(12,4,8)$

$$\begin{pmatrix} 0&0&0&0&0&0&0&0&0&0&0&0\\ 1&1&1&0&0&1&1&1&1&0&0&1\\ 1&0&1&1&1&0&1&0&1&1&1&0\\ 0&1&0&1&1&1&0&1&0&1&1&1 \end{pmatrix},$$

que puede corregir hasta tres errores.

6 Diseño de pesada

Pesando varios objetos juntos, en lugar de hacerlo separadamente, es posible determinar los pesos con mayor exactitud. Las técnicas para hacer esto se llaman diseños de pesada y las mejores están basadas en las matrices de Hadamard. Estas técnicas se pueden aplicar a diferentes problemas de medidas, no sólo pesos, sino también longitudes, voltajes, resistencias, concentraciones químicas, frecuencias, etc. De hecho se puede aplicar a cualquier experimento en los que la medida de varios objetos es la suma de las medidas individuales.

Supongamos que queremos pesar cuatro objetos con una balanza de dos platillos, la cual comete un error ϵ cada vez que se usa. Podemos suponer que ϵ es una variable aleatoria con media cero (puesto que debe estar equilibrada) y varianza σ^2. Si pesamos los cuatro objetos separadamente y los valores obtenidos son y_1, y_2, y_3, y_4 con errores desconocidos $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$, los verdaderos valores serían $a = y_1 + \epsilon_1$, $b = y_2 + \epsilon_2$, $c = y_3 + \epsilon_3$, $d = y_4 + \epsilon_4$. Por otra parte supongamos que hacemos cuatro pesadas de la siguiente forma

$$\left\{ \begin{array}{rcl} a+b+c+d &=& y_1+\epsilon_1, \\ a-b+c-d &=& y_2+\epsilon_2, \\ a+b-c-d &=& y_3+\epsilon_3, \\ a-b-c+d &=& y_4+\epsilon_4, \end{array} \right.$$

lo cual significa que los objetos con signo $+$ son colocados a un lado de la balanza y los negativos al otro. Como la matriz de coeficientes es una matriz de Hadamard, es muy fácil resolver el sistema, obteniéndose

$$a = \frac{y_1+y_2+y_3+y_4}{4} + \frac{\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4}{4},$$

o sea, el error es ahora

$$\frac{\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4}{4}.$$

Al hacer una media de los cuatro errores, éste se reduce, lo cual en términos estadísticos se expresa en función de la varianza de la siguiente forma: la varianza de $c\epsilon$ es c^2 por la varianza de ϵ y la varianza de la suma de variables aleatorias independientes es la suma de las varianzas. Así la varianza de

$$\frac{\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4}{4}$$

es $\sigma^2/4$. Lo mismo sucede para las demás incógnitas. En general, para n objetos, usando una matriz de Hadamard de orden n reducimos la varianza de σ^2 a σ^2/n. Se puede demostrar que esta es la varianza más pequeña que se puede obtener con un diseño de pesada de este tipo (elección de signos para los objetos a pesar).

7 Geometría de los espacios de Banach

Sea X un espacio de Banach y A un subconjunto convexo acotado de X. Llamamos radio de Chebyshev de A al número

$$r(A) = \inf\{\sup_{y\in A} \|x - y\|\,;\, x \in A\}.$$

Nótese que de forma menos rigurosa podríamos decir que $r(A)$ es "el radio de la bola más pequeña con centro en un punto de A que contiene a A". La constante de Jüng del espacio se define como

$$N(X) = \inf\left\{\frac{\operatorname{diam} A}{r(A)}\right\},$$

donde el ínfimo se toma sobre todos los conjuntos convexos acotados no unitarios de X. Por ejemplo, para el plano euclídeo $N(X) = \operatorname{diam} T/r(T)$, donde T es un triángulo equilátero y su valor es $\sqrt{3}$.

Aunque el coeficiente $N(\ell_2)$ fue calculado por Bynum en 1980, el valor de $N(\ell_p)$ y $N(L_p)$ fue un problema abierto durante diez años. En 1990 obtuvimos (véase [3]) el valor de estos coeficientes usando algunas desigualdades deducidas de teoría de la interpolación. La idea básica para encontrar este valor fue demostrar que bastaba considerar conjuntos que fueran la envolvente convexa de conjuntos finitos de puntos, todos equidistantes del centro de Chebyshev. Por otra parte, el Teorema de la Sección Esférica de Dvoretski nos dice que en cualquier espacio de Banach de dimensión infinita existen copias casi isométricas de un espacio euclídeo de cualquier dimensión finita. Este hecho, junto a las anteriores consideraciones, nos dice que el valor de $N(X)$ es mayor o igual que $\sqrt{2}$ para cualquier espacio Banach de dimensión infinita. Pero, ¿qué sucede para los espacios de dimensión finita? Por ejemplo para ℓ_p^n, esto es, $\mathbb{R}^n$ con la norma p.

Las técnicas usadas para calcular $N(\ell_p)$ pueden también ser aplicadas para obtener una cota superior de $N(\ell_p^n)$. El cálculo de $N(X)$ para espacios euclídeos (de dimensión finita) fue iniciado por Jüng en 1901, obteniendo $N(\ell_2^n)$. Recordando que sólo tenemos que considerar conjuntos finitos de X para calcular $N(X)$ y que en espacios n-dimensionales todo punto que está en la envolvente convexa de m puntos $x_1, \ldots, x_m$ está también en la envolvente convexa de un subconjunto formado por a lo más $n + 1$ puntos, podemos concluir que sólo debemos considerar conjuntos finitos de X formados por a lo más $n + 1$ puntos y que podemos suponer que estos puntos equidistan del centro de Chebyshev. Así el problema puede ser formulado equivalentemente de la siguiente forma: ¿cuál es el hiperpoliedro de $n + 1$ vértices inscribible en la esfera unidad, conteniendo 0 en su interior, con diámetro mínimo? Estudiemos con más detalle este problema.

Supongamos que $A = \{x_1, \ldots, x_N\}$, $N \leq n+1$, es un conjunto en ℓ_p^n. Por traslación podemos suponer que el origen es el centro de Chebyshev, el cual está en la envolvente convexa de A, y por homotecia que $\|x_i\| = 1$, $i = 1, \ldots, N$. Aplicando ciertas desigualdades de convexidad (ver [1], Lemma II.3.8) obtenemos

$$\left(1 - \frac{1}{N}\right)^{\alpha-2} \operatorname{diam} A^{\alpha} \ (1 - \sum_{j=1}^{N} t_j^2) \geq 2,$$

donde $\alpha = p$ si $2 \leq p < +\infty$, y $\alpha = \frac{p}{p-1}$ si $1 < p \leq 2$. Usando el Teorema de los multiplicadores de Lagrange es fácil comprobar que $1 - \sum_{j=1}^{N} t_j^2$, con la ligadura $\sum_{j=1}^{N} t_j = 1$, alcanza un máximo si $t_j = 1/N$, $j = 1, \ldots, N$. Por consiguiente, tenemos

$$\left(1 - \frac{1}{N}\right)^{\alpha-2} \left(1 - \frac{1}{N}\right) \operatorname{diam} A^{\alpha} \geq 2,$$

esto es,

$$\frac{\operatorname{diam} A}{r(A)} \geq 2^{1/\alpha} \left(\frac{n+1}{n}\right)^{1-\frac{1}{\alpha}}.$$

Para $n = p = 2$ este es el valor exacto de $N(\ell_2^2) = \sqrt{3}$, puesto que es la razón entre el diámetro de un triángulo equilátero y el radio de la circunferencia circunscrita. Sucede igual para ℓ_2^n para todo n, pues en este caso

$$2^{1/\alpha} \left(\frac{n+1}{n}\right)^{1-\frac{1}{\alpha}} = \sqrt{\frac{2(n+1)}{n}}$$

es el diámetro del tetraedro (o hipertetraedro) inscrito en la hiperesfera unidad. ¿Qué sucede si $p \neq 2$? Desde luego la cota superior sólo puede ser alcanzada si todas las desigualdades se transforman en igualdades. Por tanto, todos los t_j tienen que ser iguales a $1/(n+1)$ y todas las distancias $\|x_j - x_k\|, j \neq k$, tienen que ser iguales a $\operatorname{diam} A$. Por tanto, el hiperpoliedro debe ser un hipertetraedro inscribible en la superficie esférica y cuyo centro geométrico sea el centro de la esfera. En el caso más simple, para $n = 2$, esto significa que la igualdad sólo puede ser alcanzada para un triángulo equilátero (en norma p) con vértices en la circunferencia unidad (otra vez debemos entender la circunferencia para la norma p) tal que el centro geométrico del triángulo es el origen de coordenadas. Por tanto la cuestión es ahora: ¿existe algún triángulo equilátero en ℓ_p^2 verificando esta condición? Si tal triángulo existe, ¿es $2^{2/\alpha-1}3^{1-1/\alpha}$ la longitud de su lado? Usando matrices de Hadamard veremos la respuesta en algunos casos especiales.

Supongamos que existe una matriz de Hadamard de orden $n+1$ y sea

$$\begin{pmatrix} 1 & v_1 \\ 1 & v_2 \\ \vdots & \vdots \\ 1 & v_{n+1} \end{pmatrix}$$

esta matriz, donde $v_1, \ldots, v_{n+1}$ son vectores en $\mathbb{R}^n$. Consideramos el conjunto $A = \{v_1, \ldots, v_{n+1}\}$ en ℓ_p^n para $p < 2$. Es claro que

$$\|v_i - v_j\| = 2\left(\frac{n+1}{2}\right)^{1/p}$$

si $i \neq j$, porque dos filas distintas de la matriz de Hadamard tienen $(n+1)/2$ 1's o -1's en la misma posición. Además $\|x_i\| = n^{1/p}$ para $i = 1, \ldots, n+1$. Entonces

$$\frac{\operatorname{diam} A}{r(A)} = 2^{1/q}\left(\frac{n+1}{n}\right)^{1/p},$$

que es el valor correspondiente a la cota superior. Por tanto en este caso

$$2^{1/q}\left(\frac{n+1}{n}\right)^{1/p}$$

es el valor exacto de $N(\ell_p^n)$. Es un problema abierto calcular $N(\ell_p^n)$ si $p > 2$ o si no existe matriz de Hadamard de orden $n+1$.

Referencias

[1] J. Ayerbe, T. Domínguez y G. López, *Measures of Noncompactness in Metric Fixed Point Theory*, Operator Theory Advances and Applications, Vol 99, Birkäuser, Berlin 1997.

[2] R. Bellman, *Introduction to Matrix Analysis*, McGraw Hill, New York 1970.

[3] T. Domínguez, *Normal structure coefficients in L_p-spaces*, Proc. Royal Soc. Edinburgh, 117A, pp. 299-303, 1991.

[4] J. Hadamard, *Résolution d'une question relative aux déterminants*, Bull. Sci. Math. 2, 240-248 (1893).

[5] V.I. Levenshtein, *The applications of Hadamard matrices to a problem in coding*, Problems of Cybernetic 5, 166-184 (1964).

[6] F.J. Macwilliams y N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam 1978.

[7] R.E.A.C. Pailey. *On orthogonal matrices*, J. Math. and Phys. 12, 311-320 (1933).

[8] J. Williamson, *Note on Hadamard's determinant Theorem*, Bull. Amer. Math. Soc. 53, 608-613 (1947).