Matrices cocíclicas de Hadamard sobre productos semidirectos.[1]

V. Álvarez, J.A. Armario, M.D. Frau y P. Real[2]

Resumen

La generación de matrices de Hadamard es un problema de primer orden debido en gran medida a sus importantes aplicaciones en diversas ramas de la Combinatoria (Teoría de Diseños, conjuntos diferencias, generación de secuencias semialeatorias, tablas perfectas binarias y códigos correctores de errores ...). En [6] se presenta un método para la generación de matrices de Hadamard donde la etapa principal consiste en el cálculo explícito de un sistema generador de los 2-cociclos $\psi: G \times G \to \mathbf{Z}_2$ desarrollado sobre un grupo finito G.

Aquí usando los resultados que hemos obtenido en [1] sobre la determinación explícita de 2-cociclos desarrollados sobre productos semidirectos de grupos, expondremos el método que se reseña en [6]. Comentaremos en detalle el caso los grupos diédricos D_{4t} y los principales problemas que surgen.

1 Introducción

Una matriz de Hadamard de orden n es una matriz cuadrada H con entradas $+1$ y -1, satisfaciendo que $HH^t = nI$; es decir, cuando tiene sus filas ortogonales dos a dos, (además, siempre es posible considerar, mediante ciertas transformaciones bajo las cuales el carácter de ser Hadamard permanece invariante, la primera fila y columna formadas sólo por $+1$). Es bien conocido que n debe ser 1, 2 o múltiplo de 4 para que exista dicha matriz, ninguna otra restricción es conocida para su existencia. Una importante clase de ejemplos de matrices de Hadamard lo constituyen las matrices de Sylvester:

$$H_0 = 1 \qquad H_{k+1} = \begin{pmatrix} H_k & H_k \\ H_k & -H_k \end{pmatrix}.$$

La centenaria conjetura de Hadamard afirma que una matriz de Hadamard existe para cualquier orden n múltiplo de 4. Muchas clases de matrices de Hadamard han sido encontradas (Sylvester, Paley ...) y por tanto muchas dimensiones ya han sido cubiertas. Sin embargo, aún quedan muchos ordenes para los cuales no se sabe de la existencia de matrices de Hadamard para ellos, según la bibliografía que manejamos, el orden más pequeño es 428. Un buen artículo de carácter introductorio en matrices de Hadamard y sus aplicaciones puede ser [7], donde también aparecen distintos métodos clásicos para la construcción de matrices de Hadamard.

Recientemente Horadam y de Launey [6] han desarrollado una nueva aproximación en la generación de matrices de Hadamard, haciendo usos de útiles de la cohomología de grupos. La etapa esencial de este método

[1]Trabajo parcialmente subvencionado por los proyectos de investigación FQM-296 de la Junta de Andalucía y PB98-1621-C02-02 de la DGES.

[2]Dpto. de Matemática Aplicada 1. Universidad de Sevilla.
E-mails: {valvarez,armario,mdfrau,real}@us.es

requiere de la determinación explícita de un sistema generador de los 2-cociclos sobre un grupo finito G. Hemos de hacer notar que esta cuestión no ha sido tradicionalmente tratada por los especialistas en cohomología, al menos, hasta esta última década [2, 4, 5, 1]. En lo que sigue, expondremos el método desarrollado por Horadam y de Launey en el caso de trabajar con grupos diédricos.

2 Cociclos y matrices cocíclicas

Sea G un grupo finito de orden v. Un 2-cociclo (nomalizado, binario) es una función $\psi: G \times G \to < -1 > \cong \mathbf{Z}_2$ satisfaciendo

$$\psi(g,h)\psi(gh,k) = \psi(g,hk)\psi(h,k),\ \forall g,\ h,\ k \in G$$

y $\psi(1,1) = 1$. Un cociclo es un coborde $\delta\alpha$ cuando se deriva de una función de conjuntos $\alpha: G \to \mathbf{Z}_2$ con $\alpha(1) = 1$ como $\delta\alpha(a,b) = \alpha(a)^{-1}\alpha(b)^{-1}\alpha(ab)$. El conjunto de cociclos constituye un grupo abeliano $Z^2(G)$ bajo la ley de grupos trivial, y los cobordes $B^2(G)$ forman un subgrupo suyo. Dos cobordes ψ y ψ' se dicen cohomólogos si existe un coborde $\delta\alpha$ tal que $\phi' = \phi \cdot \delta\alpha$, esto define una relación de equivalencia en $Z^2(G)$ y la clase de cohomología de ψ se denota por $[\psi]$. El grupo cociente $Z^2(G)/B^2(G)$ de clases de cohomología es un grupo abeliano denotado por $H^2(G)$, el cual es conocido como segundo grupo de cohomología de G con coeficientes en $\mathbf{Z}_2$.

Un 2-cociclo ψ se expresa de forma natural como una matriz cocíclica; esto es, una matriz M_ψ cuadrada de orden $|G|$ cuyas filas y columnas están indexadas por los elementos de G (bajo algún orden fijado) y cuya entrada en la posición (g,h) es $\psi(g,h)$.

Las matrices cocíclicas que son de Hadamard se llaman matrices cocíclicas de Hadamard. El siguiente ejemplo nos confirma que no es extraño encontrar matrices cocíclicas de Hadamard.

Ejemplo 1 *La aplicación* $f: \mathbf{Z}_2^k \times \mathbf{Z}_2^k \to \mathbf{Z}_2$ *definida por*

$$f[a,b] = (-1)^{a\cdot b}$$

donde $a \cdot b$ *denota el producto escalar en* $\mathbf{Z}_2^k$ *es un 2-cociclo. Además, la matriz cociclica* M_f *asociada a* f *vía la ordenación de los elementos de* $\mathbf{Z}_2^k$ *correspondiente a la expresión binaria de* $\{0,1,\ldots,2^k-1\}$ *son las matrices de Sylvester. Por tanto, éstas constituyen ejemplos de matrices cocíclicas de Hadamard.*

En [6] se conjetura que en toda dimensión múltiplo de 4 existe una matriz cocíclica de Hadamard. Además, se establece el siguiente lema, que caracteriza cuándo una matriz cocíclica es de Hadamard o no, proporcionando un ventajoso método para la comprobación de dicha propiedad.

Lema 2 *[6] Una matriz cocíclica es de Hadamard si, y sólo si, la suma de los elementos de cualquier fila, salvo la primera (de entradas sólo +1), es nula.*

Luego el comprobar si una matriz cocíclica es o no de Hadamard requiere tan sólo de, a lo más, $(v-1)^2$ sumas binarias, lo que supone una complejidad computacionalmente aceptable, y considerablemente inferior al de comprobar que las filas de la matriz son ortogonales dos a dos.

3 Generación de matrices cocíclicas de Hadamard sobre D_{4t}

El método desarrollado por Horadam y de Launey para la generación de matrices de

Hadamard consiste en obtener un sistema generador de 2-cociclos; a partir de éste, generar todas las posibles matrices cocíclicas y con el test que nos proporciona el Lema 2 determinar cuáles son de Hadamard. En [6] tratan este problema en el caso de ser G abeliano, casos más generales de grupos son tratados en [2, 4]. En [1] dábamos un algoritmo para la obtención de un sistema completo de generadores de los 2-cociclos para productos semidirectos de grupos. Aquí ilustraremos el método de Horadam y de Launey para el caso de los grupos diédricos D_{4t}, usando los 2-cociclos que nos proporciona nuestro algoritmo.

Estos cociclos los expresaremos mediante las matrices coclícicas asociada; teniendo en cuenta que $Z^2(G) = B^2(G) \oplus H^2(G)$, y la distinta técnica que se usa en su cálculo, distinguiremos entre cobordes y no cobordes, y dentro de estos últimos entre simétricos y conmutadores (ver [6, 2]). Hemos obtenido que el número de cociclos generadores de $Z^2(D_{4t})$ es $4t$, de los cuales $4t-3$ son cobordes, 2 cociclos simetricos y 1 conmutador.

Las matrices correspondientes a los 2-cobordes son de la forma:

Posiciones de los -1 para el 2-coborde α_i :

- En la fila k, con $2 \leq k \leq 2t$:
  - Para $2 \leq i \leq k-1$ las posiciones son $(k,i),(k,2t+i-k+1)$.
  - Para $i = k$ las posiciones son $(k,j) \forall j \neq 1,k$.
  - Para $k+1 \leq i \leq 2t$ las posiciones son $(k,i),(k,i-k+1)$.
  - Para $2t+1 \leq i \leq 2t+k-1$ las posiones son $(k,i),(k,2t+i-k+1)$.
  - Para $2t+k \leq i \leq 4t-2$ las posiciones son $(k,i),(k,i-k+1)$.
- En la fila k, con $2t+1 \leq k \leq 4t$.
  - Para $2 \leq i \leq k-2t$ las posiciones son $(k,i),(k,k-i+1)$.
  - Para $k-2t+1 \leq i \leq 2t$ las posiciones son $(k,i),(k,2t-i+k+1)$.
  - Para $2t+1 \leq i \leq k-1$ las posiones son $(k,i),(k,k-i+1)$.
  - Para $i = k$ las posiciones son $(k,j) \forall j \neq 1,k$.
  - Para $k+1 \leq i \leq 4t-2$ las posiciones son $(k,i),(k,2t-i+k+1)$.

De modo que cada matriz correspondiente a un 2-coborde tiene en cada fila y columna dos entradas -1 y el resto son $+1$, salvo en las líneas i-ésimas, que tiene dos $+1$ y el resto son -1.

Por otra parte, los 2-cociclos simétricos son:

- Bien de la forma

$$\begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & + & + \\ + & - & + & - \end{pmatrix}$$

  donde $+$ representa un bloque de orden $t \times t$ todo de 1 y $-$ representa un bloque de orden $t \times t$ todo de -1.

- Bien de la forma

$$\begin{pmatrix} + & + \\ + & - \end{pmatrix}$$

  siendo ahora $+$ un bloque de orden $2t \times 2t$ todo de 1 y $-$ un bloque de orden $2t \times 2t$ todo de -1.

Finalmente, el conjunto de generadores de la parte conmutadora para una base de matrices cocíclicas sobre $D_{2t \cdot 2}$ se reduce a $\left\{ \begin{pmatrix} A_t & A_t \\ B_t & B_t \end{pmatrix} \right\}$, donde A_t denota la correspondiente matriz reversa negacíclica y B_t

consiste en la matriz cuyas filas son las propias de A_t, pero dispuestas en orden inverso.

$$A_t = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & \cdots & 1 & -1 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & \cdots & -1 & -1 \\ 1 & -1 & \cdots & -1 & -1 \end{pmatrix},$$

$$B_t = \begin{pmatrix} 1 & -1 & \cdots & -1 & -1 \\ 1 & 1 & \cdots & -1 & -1 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & \cdots & 1 & -1 \\ 1 & 1 & \cdots & 1 & 1 \end{pmatrix}.$$

Debemos incidir en el hecho de que $Z^2(D_{4t})$ consiste en todas las posibles combinaciones lineales con coeficientes en $\mathbf{Z}_2$ de los $4t$ generadores obtenidos. Por tanto, $|Z^2(D_{4t})| = 2^{4t}$, y que sobre cada una de las matrices asociadas, en principio, habría que pasar el test (lema 2) de complejidad $O(t^2)$ para decidir si es Hadamard o no lo es. Para valores pequeños de t, ayudándonos de un programa escrito en MATHEMATICA se obtienen resultados satisfactorios. En la siguiente tabla indicamos el número n de matrices cocíclicas de Hadamard existentes en D_{4t}, para los primeros valores de t:

t	1	2	3	4	5
n	5	15	72	768	2380

Para valores pequeños de t y mayores a 5, ha de descartarse la búsqueda exhaustiva por el elevado coste computacional que supone, debido fundamentalmente al gran número de matrices cocíclicas que aparecen. En estos casos, se hace necesario el uso de técnicas más sofisticadas (ver [3]) que permitan focalizar, aún más, la búsqueda de matrices de Hadamard.

Referencias

[1] V. Álvarez, J.A. Armario, M.D. Frau y P. Real. *An algorithm for computing cocyclic matrices developed over some semidirect products.* Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, LNCS 2227, 287–296. Springer, (2001).

[2] D.L. Flannery. *Calculation of cocyclic matrices.* J. of Pure and Applied Algebra, **112**, 181–190, (1996).

[3] D.L. Flannery. *Cocyclic Hadamard Matrices and Hadamard Groups are equivalent* J. of Algebra, **192**, 749–779, (1997).

[4] D.L. Flannery and E.A. O'Brien. *Computing 2-cocycles for central extensions and relative difference sets.* Comm. Algebra, **28(4)**, 1939–1955, (2000).

[5] J. Grabmeier, L.A. Lambe. *Computing Resolutions Over Finite p-Groups.* Proceedings ALCOMA'99. Eds. A. Betten, A. Kohnert, R. Lave, A. Wassermann. *Springer Lecture Notes in Computational Science and Engineering*, Springer-Verlag, Heidelberg, (2000).

[6] W. de Launey and K.J. Horadam. *Generation of cocyclic Hadamard matrices.* Computational algebra and number theory (Sydney, 1992), volume **325** of *Math. Appl.*, 279–290. Kluwer Acad. Publ., Dordrecht, (1995).

[7] A. Hedayat y W.D. Wallis *Hadamard matrices and their applications.* The Annals of Statistics, Vol. 6, No. 6, 1184–1238, (1978).