Hadamard matrices, strongly regular graphs, and Galois fields

Jorge Sarmiento
Assocciate Professor

Abstract

In this paper the author uses the concept of circulant matrices and the superposition principle to find, from the adjacency matrices of three regular graphs of order 8 and degree 2, the adjacency matrix, M, of a strongly regular graph G(8,6,4,6). M is then decomposed, by means of addition, subtraction, and the Kronecker product of matrices, to get the Hadamard matrix OH(2,4). Finally, the paper shows how the row vectors of this matrix can be found by using the elements of the finite field $GF(2^2)$, and the concept of the T-character.

Sinopsis

En este artículo el autor usa el concepto de matrices circulantes y el principio de superposición para hallar, a partir de las matrices de incidencia de tres gráficos regulares de orden 8 y grado 2, la matriz de incidencia, M, de un gráfico f-regular (fuertemente regular), G(8,6,4,6). Por medio de la suma, la resta y el producto directo de matrices, M se descompone para obtener la matriz de Hadamard OH(2,4). Finalmente, se muestra como los vectores de fila de esta matriz se pueden determinar a partir de los elementos del cuerpo finito $GF(2^2)$ y del carácter-T.

1. Introduction

The theory of strongly regular graphs was introduced by Bose in 1963[1] in connection with partial geometries and 2-class association schemes. One year later (1964) Higman[2] initiated the study of the rank 3 permutation groups using strongly regular graphs. Both, combinatorial and groupal aspects have been developed in recent years. Moreover, the interest in strongly regular graphs has been stimulated by the discovery of new simple groups.

A graph, G, is a pair (X,R), where X is a set and R a symmetric, antireflexive relation on X, called adjacency. The elements of X are called vertices, and the elements of R edges. If G has v elements, and each one is adjacent to k other elements, the graph is regular. If, in addition to this, there are non-negative integers, λ and μ, such that any two adjacent elements are mutually adjacent to λ other elements, and any two non-adjacent elements are mutually adjacent to μ other elements, the graph is strongly regular. The integers v, k, λ and μ are called the parameters of G; v is the order and k is the degree of G.

The adjacency matrix, $A=[h_{i,j}]$, of a graph is defined as follows: $a_{ii}=0$, and for j different from i, $a_{ij} = {}^{-}1$ or 1 whether the vertices are adjacent or not.

A Hadamard matrix, OH(2,r), is a square matrix of order r with elements $\{1,{}^{-}1\}$ whose row vectors are orthogonal, i.e., $HH^t=rI_r$, where H^t is the transpose of H, and I_r the unit matrix of order r. Hadamard matrices were first studied by Sylvester in 1867 and later by Scarpis in 1898. The

---

1 Bose, R.C., *Strongly Regular Graphs, Partial Geometries, and Partially Balanced Designs*, Pacific J. Math. 13 (1963), 389-419.

2 Higman, D.G., *Finite Permutation Groups of Rank 3*, Math. Z. 86 (1964) 145-156.

next major work was done in 1933 by Paley. In 1944 and 1947 Williamson obtained further results of considerable interest. Since the 1950s these matrices have been studied considerably, and many contributions have been made toward proving the Hadamard conjecture, which states that OH(2,4t) matrices exist for every positive integer t. Applications of Hadamard matrices occur in statistics, engineering and optics.

The most powerful theorems on the existence of OH(2,r) matrices are stated next [3]

(i) Given any natural number n, there exists an $OH(2, 2^s n)$ matrix for every $s \geq [2\log_2(n-3)]$.
(ii) Given any natural number n, and s as before, there exists a regular (i.e., constant row sum) symmetric $OH(2, 2^{2s} n^2)$ matrix with constant diagonal.

Certain groups of Hadamard matrices, which play an important role in the construction of codes, are associated with Galois fields (finite fields) through the T-character. This is defined for the generic element a of GF(q) by

$$e(a) = \exp[2\pi i T_a) / p] \tag{1}$$

where T_a is any integer whose residue class mod p is the trace, T(a), and $q=p^m$. The trace is a linear mapping from GF(q) onto GF(p) defined by

$$T(w) = \sum_{k=1}^{m-1} (w^p)^k \tag{2}$$

2. Definitions
For 1<i, j<8 let

---

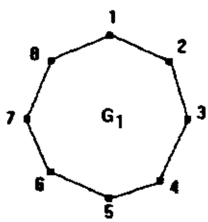
[3] Geramite, A.V. and Seberry, J., *Orthogonal Designs: Quadratic Forms and Hadamard Matrices* (Lec. Notes in pure and applied Math. 45, M. Dekker Inc 1979).

$$M_1 = [h_{ij}],\ h_{ii} = 0,\ h_{i\,i+1} = -1,\ h_{ij} = 1 \text{ for any other } j \tag{3}$$

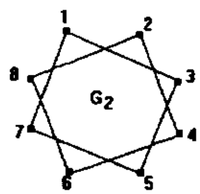
$$M_2 = [h_{ij}],\ h_{ii} = 0,\ h_{i\,i+2} = -1,\ h_{ij} = 1 \text{ for any other } j \tag{4}$$

$$M_3 = [h_{ij}],\ h_{ii} = 0,\ h_{i\,i+3} = -1,\ h_{ij} = 1 \text{ for any other } j \tag{5}$$

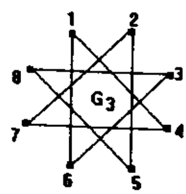
M_1, M_2, and M_3 are the adjacency matrices of regular graphs G_1, G_2, and G_3, of order v=8 and degree k=2 (fig. 1)



$$M_1 = \begin{bmatrix} 0 & -1 & 1 & 1 & 1 & 1 & 1 & -1 \\ -1 & 0 & -1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 0 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 0 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 0 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 0 & -1 \\ -1 & 1 & 1 & 1 & 1 & 1 & -1 & 0 \end{bmatrix}$$



$$M_2 = \begin{bmatrix} 0 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 0 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 0 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & 0 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 \end{bmatrix}$$

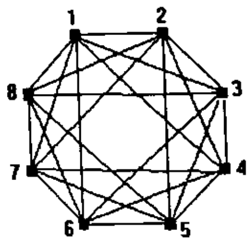


$$M_3 = \begin{bmatrix} 0 & 1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 0 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 0 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 0 & 1 \\ 1 & 1 & -1 & 1 & -1 & 1 & 1 & 0 \end{bmatrix}$$

Fig. 1 Regular graphs G_1, G_2, G_3 and their adjacency matrices M_1, M_2 and M_3

3. Superposition principle.

If we define the matrix operator $\cdot$ as, $M_u \cdot M_v = [a_{ij}] \cdot [b_{ij}] = [c_{ij}]$, where $c_{ij} = a_{ij} \cdot b_{ij} = a_{ij}$ if $a_{ij} = b_{ij}$ and $c_{ij} = -1$ otherwise, then the matrix $M = (M_1 \cdot M_2) \cdot M_3$ is the adjacency matrix of a strongly regular graph G with parameters v=8, k=6, λ=4, and μ=6 (fig. 2)



G(8,6,4,6)

$$M = \begin{bmatrix} 0 & -1 & -1 & -1 & 1 & -1 & -1 & -1 \\ -1 & 0 & -1 & -1 & -1 & 1 & -1 & -1 \\ -1 & -1 & 0 & -1 & -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 0 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 0 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 & -1 & 0 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 & -1 & 0 & -1 \\ -1 & -1 & -1 & 1 & -1 & -1 & -1 & 0 \end{bmatrix}$$

Fig. 2. Relationship between matrix M and the strongly regular graph G

4. Decomposition of M

The symmetric matrix M, can be expressed as the sum of two matrices,

$$M = \begin{bmatrix} 0 & -1 & -1 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ -1 & -1 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & -1 & -1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & -1 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & -1 & -1 & 1 & -1 \\ 0 & 0 & 0 & 0 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 \\ -1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 \\ -1 & -1 & 1 & -1 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (6)$$

which, using the Kronecker (direct) product can be written as shown in figure 4

$$M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & -1 & -1 & -1 \\ -1 & 0 & -1 & -1 \\ -1 & -1 & 0 & -1 \\ -1 & -1 & -1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix} \tag{7}$$

or

$$M = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \right) + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix} \tag{8}$$

In symbols

$$M = I_2 \otimes (I_4 - J_4) + P_1 \otimes H_1 \tag{9}$$

where I2 is the unit matrix of order 4, I_4 the unit matrix of order 16, J_4 the all one matrix of order 16, P_1 the permutation matrix of order 4 associated with 1 in the representation of A(4), the additive group of the finite field GF(4), and

$$H_1 = \begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix} \tag{10}$$

the OH(2,4) matrix.

6. Remarks.

(i) From H1, by means of M, we can get back the graph G(8,6,4,6).

(ii) Strongly regular graphs of order 2^{3m} exist, and their adjacency matrices can be obtained by means of the group of 2^m-1 $OH(2,2^{2m})$ matrices [4] (Delsarte, P. and Goethals, J.M., 1969)

7. Construction of the OH(2,4) matrix from the GF(4)

Let $GF(2^2)$ = {0,1,x,x+1}, where x is a root of the irreducible polynomial $x^2 = x+1$ over GF(2). Using definition (1), let

$$h_{xy}^{(a)} = e\ [a^{-1}(y-x)^{2+1}] \tag{11}$$

where x, y are elements of GF(4), and a=1. Thus, $h_{00}^{(1)} = e(0) = 1$. From definition (2), with m=1, and q=2 we have that T(1)=1, so

$$h_{01} = e\ (1) = e^{\pi i T_1} = \cos\ \pi T_1 = \cos\ \pi = -1 \tag{12}$$

[4] Delsarte, P. and Goethals, J.M., *Tri-weight Codes and Generalized Hadamard Matrices*, Infrm. Control, 15 (1969), 196-206.

$$h_{0x}^{(1)} = e\ (x^3) = e\ (x^2x) = e\ [(x+1)x] = (x^2+x)$$
$$= = e\ (x+1+x) = e\ (2x+1) = e\ (1) = -1 \tag{13}$$

$$h_{0X+1}^{(1)} = e\ (x+1)^3 = e\ [(x^2+1)\ (x+1)]$$
$$= e\ [(x+1+1)\ (x+1)]$$
$$= = e\ x\ (x+1) = e\ (1) = -1 \tag{14}$$

$$(h_{00})^{(1)}, h_{01}^{(1)}, h_{0x}^{(1)}, h_{0x+1}^{(1)}) = (1, -1, -1, -1) \tag{15}$$

Similarly we compute the remaining rows

$$h_{10}^{(1)} = e\ (-1) = e\ (1) = -1 \tag{16}$$

$$h_{11}^{(1)} = e\ (0) = 1 \tag{17}$$

$$h_{1x}^{(1)} = e\ [(x-1)^3] = e\ [(x+1)^3] = -1 \tag{18}$$

$$h_{1x+1}^{(1)} = e\ (x^3) = -1 \tag{19}$$

Thus the second row of H_1 is (-1,1,-1,-1)

$$h_{x0}^{(1)} = e\ (-x^3) = e\ (x^3) = -1 \tag{20}$$

$$h_{x1}^{(1)} = e\ [(1-x)^3] = e\ [(1+x)^3] = e\ [(x+1)^3] = -1 \tag{21}$$

$$h_{xx}^{(1)} = e\ (0) = 1 \tag{22}$$

$$h_{xx+1}^{(1)} = e\ (1) = -1 \tag{23}$$

The third row is (-1,-1,1,-1)

$$h_{x+10}^{(1)} = e\ [-(x+1)^3] = e\ [(x+1)^3] = -1 \tag{24}$$

$$h_{x+11}^{(1)} = e\ (-x^3) = -1 \tag{25}$$

$$h_{x+1x}^{(1)} = e\ (-1) = -1 \tag{26}$$

$$h_{x+1x+1}^{(1)} = e\ (0) = 1 \tag{27}$$

And (-1,-1,-1,1) is the forth row of H_1.