Mathematica Pannonica
25/2 (2014–2015), 115–123

COMPLEX HADAMARD MATRICES AND MULTIPLE FACTORIZATIONS OF FINITE ABELIAN GROUPS

Sándor **Szabó**

Institute of Mathematics and Informatics
University of Pécs
Ifjúság u. 6
7624 Pécs, HUNGARY

Received: May 17, 2017

MSC 2000: 20 K 01, Secondary 05 B 20, 52 C 22

Keywords: Hadamard matrices, multiple factorization of finite abelian groups, exact cover algorithm.

Abstract: Certain multiple factorizations of finite abelian groups can be used to construct complex Hadamard matrices.

1. Introduction

Let H be an n by n matrix whose entries are complex mth roots of unity. If $HH^* = nI$, then we say that H is a complex Hadamard matrix. Here I is the n by n identity matrix and H^* is the Hermite transpose of H. In the $m = 2$ particular case the entries of H are $+1$ or -1 and we get back the Hadamard matrices in the ordinary sense. Ordinary Hadamard matrices have important applications in combinatorics. For instance they can be used to construct error correcting codes and certain block designs.

The columns of a complex Hadamard matrix can be considered as

E-mail address: sszabo7@hotmail.com

a finite set of orthogonal functions defined on a finite set. Let G be a finite abelian group with elements $g_1, \ldots, g_n$ and let $\chi_1, \ldots, \chi_n$ be the characters of G. By the standard orthogonality relations the columns of the matrix

$$\begin{bmatrix} \chi_1(g_1) & \cdots & \chi_1(g_n) \\ \vdots & \ddots & \vdots \\ \chi_n(g_1) & \cdots & \chi_n(g_n) \end{bmatrix}$$

are orthogonal and the rows of the matrix are orthogonal. In other words the character table of a finite abelian group forms a set of orthogonal functions. In the Fourier analysis these orthogonal functions are called Vilenkin systems. The character table of a subgroup of G is clearly a Vilenkin system too. Restricting the characters of G to a subset of G in a typical case does not lead to an orthogonal system. As it turns out complex Hadamard matrices are related to certain multiple factorizations of finite abelian groups. Exploiting this connection we will be able to construct complex Hadamard matrices. We will see that there is a large collection of subsets of G such that restricting the characters of G to these subsets yield an orthogonal system of functions.

Let G be a finite abelian group and let $A_1, \ldots, A_n$ be subsets of G. If each element g of G can be expressed in the form

$$g = a_1 \cdots a_n, \quad a_1 \in A_1, \ldots, a_n \in A_n$$

in exactly k ways, then we say that the product $A_1 \cdots A_n$ is a k-fold factorization of G. We speak about multiple factorizations of G when we do not wish the refer to the value of k. If A is a subset of G and χ is a character of G, then the notation $\chi(A)$ stands for the complex number

$$\sum_{a \in A} \chi(a).$$

It is known (see for example [11]) that the product $A_1 \cdots A_n$ forms a multiple factorization of G if and only if $\chi(A_1 \cdots A_n) = \chi(A_1) \cdots \chi(A_n) = 0$ for each nonprincipal character χ of G.

2. Lemmas

Let the group G be the direct product of the cyclic groups $G_1, \ldots, G_n$ of orders $q_1, \ldots, q_n$. We assume that $q_i = u(i)v(i)$, $u(i), v(i) \geq 2$ for each

i, $1 \leq i \leq n$. In other words we assume that the order of the cyclic group G_i is composite. Let $x_1, \ldots, x_n$ be basis elements of the cyclic groups $G_1, \ldots, G_n$, respectively. We may say that the elements $x_1, \ldots, x_n$ are basis elements of the group G. Let ρ be a root of unity whose order is the least common multiple of $q_1, \ldots, q_n$. For each i, $1 \leq i \leq n$ there is a positive integer $w(i)$ such that the order of $\rho^{w(i)}$ is equal to q_i. Each character χ_i of G_i can be represented in the form $\chi(x_i) = \rho^{w(i)\nu(i)}$. Consequently each character χ of G can be represented in the form

$$\chi(x_1) = \rho^{w(1)\nu(1)}, \ldots, \chi(x_n) = \rho^{w(n)\nu(n)}, \tag{2.1}$$

where

$$0 \leq \nu(1) \leq q_1 - 1, \ldots, 0 \leq \nu(n) \leq q_n - 1.$$

For the sake of clarity we single out two special cases. When $q_1 = \cdots = q_n = q$, then G is a homocyclic abelian group. In this case the least common multiple of $q_1, \ldots, q_n$ is q and the $w(1), \ldots, w(n)$ numbers are all equal to one. When $q_1, \ldots, q_n$ are pair-wise relatively primes, then G is a cyclic group. Now the least common multiple of $q_1, \ldots, q_n$ is the product $q_1 \cdots q_n$ and $w(i) = (q_1 \cdots q_n)/q_i$ for each i, $1 \leq i \leq n$.

Set $C_i = \{e, x_i, x_i^2, \ldots, x_i^{u(i)-1}\}$. We may call C_i a cyclic subset of G. We should keep in mind that C_i is not necessarily a cyclic subgroup of G. Note that C_i is a subgroup of G if and only if $|x_i| = u(i)$. Suppose that $AC_1 \cdots C_n$ is a multiple factorization of G. Let $a_1, \ldots, a_\alpha$ be all the elements of A. Each a_i can be written uniquely in the form

$$a_i = x_1^{\lambda(i,1)} \cdots x_n^{\lambda(i,n)},$$

where

$$0 \leq \lambda(i,1) \leq q_1 - 1, \ldots, 0 \leq \lambda(i,n) \leq q_n - 1.$$

For the sake of brevity we introduce the notation

$$s(i) = [\lambda(i,1), \ldots, \lambda(i,n)].$$

Thus $s(i)$ is a vector with integer components. Pick a nonprincipal character χ of G defined by (2.1). Let $d = [\nu(1), \ldots, \nu(n)]$. Therefore d is a vector with integer components.

Lemma 2.1. Suppose that

$$\chi(C_1) \neq 0, \ldots, \chi(C_n) \neq 0. \tag{2.2}$$

Then

$$0 = \rho^{\langle d,s(1)\rangle} + \cdots + \rho^{\langle d,s(\alpha)\rangle}. \tag{2.3}$$

Here $\langle d, s(i)\rangle$ stands for

$$w(1)\nu(1)\lambda(i,1) + \cdots + w(n)\nu(n)\lambda(i,n).$$

The notation $\langle d, s(i)\rangle$ simply a short hand notation for the usual product of the vectors d and $s(i)$.

Proof. Let us watch the multiple factorization $AC_1 \cdots C_n = AB$ of G. As χ is a nonprincipal character of G, by the result we quoted, it follows that $0 = \chi(A)\chi(C_1)\cdots\chi(C_n)$. Using (2.2) we get that $\chi(A) = 0$. Therefore

$$\begin{aligned} 0 &= \chi(A) \\ &= \sum_{i=1}^{\alpha} \chi(a_i) \\ &= \sum_{i=1}^{\alpha} \rho^{w(1)\nu(1)\lambda(i,1)} \cdots \rho^{w(n)\nu(n)\lambda(i,n)} \\ &= \sum_{i=1}^{\alpha} \rho^{w(1)\nu(1)\lambda(i,1)+\cdots+w(n)\nu(n)\lambda(i,n)} \\ &= \sum_{i=1}^{\alpha} \rho^{\langle d,s(i)\rangle} \end{aligned}$$

as required. ◊

Using equation (2.3) we can construct complex Hadamard matrices. Let us start with a multiple factorization $AC_1 \cdots C_n = AB$ of G. Suppose that $|A| \leq |B|$. Choose a subset B_1 of B such that $|B_1| = |A|$. Let $b_1, \ldots, b_\alpha$ be all the elements of B_1 and write the element b_j in the form

$$b_j = x_1^{\mu(j,1)} \cdots x_n^{\mu(j,n)}.$$

Set

$$t(j) = [\mu(j,1), \ldots, \mu(j,n)].$$

Finally let $h_{i,j} = \rho^{\langle t(i),s(j)\rangle}$ and

$$H = \begin{bmatrix} h_{1,1} & \dots & h_{1,\alpha} \\ \vdots & \ddots & \vdots \\ h_{\alpha,1} & \dots & h_{\alpha,\alpha} \end{bmatrix}.$$

Lemma 2.2. The H defined above is a complex Hadamard matrix.

Proof. Multiplying the ith row of H by the jth column of H^* gives that

$$\sum_{k=1}^{\alpha} \rho^{\langle t(i),s(k)\rangle - \langle t(j),s(k)\rangle} = \sum_{k=1}^{\alpha} \rho^{\langle t(i)-t(j),s(k)\rangle}.$$

If $i = j$, then this sum is equal to α as required. It remains to show that it is zero if $i \neq j$. If (2.2) holds, then Lemma 2.1 is applicable with the $d = t(i) - t(j)$ choice. Note that $\chi(C_k) = 0$ if and only if $\chi(x_k) \neq 1$ and $\chi(x_k^{u(k)}) = 1$. We assume that $\chi(x_k^{u(k)}) = 1$ and we show that in this case $\chi(x_k) = 1$ holds. $\chi(x_k^{u(k)}) = 1$ means that $\rho^{u(k)w(k)[\mu(i,k)-\mu(j,k)]} = 1$. This in turns means

$$u(k)[\mu(i,k) - \mu(j,k)] \equiv 0 \pmod{u(k)v(k)}.$$

Hence

$$\mu(i,k) - \mu(j,k) \equiv 0 \pmod{v(k)}.$$

The kth component of $t(i)$ is running from 0 to $v(k) - 1$ and so it follows that $\mu(i,k) = \mu(j,k)$. Using this we get that $\chi(x_k) = 1$. This completes the proof. ◊

3. An example

In order to illustrate the procedure of constructing complex Hadamard matrices we work out a toy example. Let the group G be the direct product of three cyclic groups of order four. Let x_1, x_2, x_3 be a basis of G. Let $C_i = \{e, x_i\}$ and let $B = C_1C_2C_3$. Choosing A to be

$$\{e, x_1x_3^2, x_2^2x_3, x_2^2x_3^3, x_1^2x_2, x_1^3x_3^2, x_1^2x_2^3, x_1^2x_2^2x_3^2\}$$

the reader can verify that the product $AC_1C_2C_3$ is a multiple factorization of G. In fact it is a 1-fold factorization of G. The values of $s(i)$ and $t(j)$

Table 1: The values of $s(i), t(i)$

i	$s(i)$	$t(i)$
1	$(0,0,0)$	$(0,0,0)$
2	$(1,0,2)$	$(0,0,1)$
3	$(0,2,1)$	$(0,1,0)$
4	$(0,2,3)$	$(0,1,1)$
5	$(2,1,0)$	$(1,0,0)$
6	$(3,0,2)$	$(1,0,1)$
7	$(2,3,0)$	$(1,1,0)$
8	$(2,2,2)$	$(1,1,1)$

are listed in Table 1 Let ρ be a 4th primitive root of unity. Computing the scalar products $\langle s(i), t(i)\rangle$ we get the following 8 by 8 complex Hadamard matrix

$$H = \begin{bmatrix} \rho^0 & \rho^0 & \rho^0 & \rho^0 & \rho^0 & \rho^0 & \rho^0 & \rho^0 \\ \rho^0 & \rho^2 & \rho^0 & \rho^2 & \rho^1 & \rho^3 & \rho^1 & \rho^3 \\ \rho^0 & \rho^1 & \rho^2 & \rho^3 & \rho^0 & \rho^3 & \rho^2 & \rho^3 \\ \rho^0 & \rho^3 & \rho^2 & \rho^1 & \rho^0 & \rho^1 & \rho^2 & \rho^1 \\ \rho^0 & \rho^0 & \rho^1 & \rho^1 & \rho^2 & \rho^3 & \rho^3 & \rho^3 \\ \rho^0 & \rho^2 & \rho^0 & \rho^2 & \rho^3 & \rho^1 & \rho^3 & \rho^1 \\ \rho^0 & \rho^0 & \rho^3 & \rho^3 & \rho^2 & \rho^1 & \rho^1 & \rho^1 \\ \rho^0 & \rho^2 & \rho^2 & \rho^0 & \rho^2 & \rho^2 & \rho^0 & \rho^2 \end{bmatrix}.$$

Plainly there is another way to arrive at H. First write up the 64 by 64 character table of G. Then restrict the characters of G to the set A. Finally cancel the rows of the character table that does not correspond to elements of A. In short we can get H by restricting the character table of G to the subset A. We claim that H is not a character table of any finite abelian group. In other words H is not a Vilenkin system. The rows of H form an orthogonal system. Suppose that the rows of H are the rows of the character table of an abelian group G_1 of order 8. G_1 must have an element of order two and so the character table of G_1 must contain two columns in which the entries are $+1$ or -1. But H does not have two such columns. The columns of H form an orthogonal system too. Suppose that the columns of H are the rows of the character table of an abelian group G_1 of order 8. The elements of the first row of H are the values of the characters of G_1 on the identity element e. The elements

of the last row of H are the values of the characters of G_1 on a second order element of G_1 and we can see that G_1 cannot have more elements of order two. Consequently G_1 is a cyclic group of order 8. But in H each complex number has multiplicative order at most four. Therefore H is not a Vilenkin system.

4. The multiple cover problem

In this section we describe how to find multiple factorizations with the help of a computer.

Given an integer k, a universal set U and subsets $A_1, \ldots, A_m$ of U. The problem is to decide if there are subsets $B_1, \ldots, B_s \subset \{A_1, \ldots, A_m\}$ such that each element of U appears in $B_1 \cup \cdots \cup B_s$ exactly k times. The sets $B_1, \ldots, B_s$ form a k-fold covering of U and so the problem can be called the k-fold covering problem or simply the multiple covering problem. The $k = 1$ special case is called the exact cover problem. It is known that the exact cover problem is NP complete. Thus one cannot expect a polynomial running time algorithm for the k-fold cover problem. D. E. Knuth [6] describes an algorithm for the exact cover problem and this can be adopted to handle the multiple cover problem too.

We organize the data of the k-fold covering problem into an m by $|U|$ incidence matrix M. We label the rows of M by the sets $A_1, \ldots, A_m$ and we label the columns of M by the elements of U. For a $u \in U$ if $u \in A_i$, then we put a bullet into cell in the row of A_i and the column of u. If $B_1, \ldots, B_s$ is a k-fold covering of U, then each column of M contains exactly k bullets in the rows of $B_1, \ldots, B_s$.

Let G be a finite abelian group and let A, B subsets of G. Note that the product AB is a k-fold factorization of G if and only if the sets aB, $a \in A$ form a k-fold covering of G. Multiple factorizations are particular instances of the multiple covering problem. We choose the universal set U to be G. The family of given subsets of U is chosen to be the subsets gB, $g \in G$. If A is a subset of G such that the sets aB, $a \in A$ form a k-fold cover of $U = G$, then the product AB is a k-fold factorization of G.

5. Theory of combinatorial designs

The main purpose of this note is to illustrate that the theory of factorization of finite abelian groups has an application in connection with constructing complex Hadamard matrices. However a reader working on the field of combinatorial designs might be interested in the material. The terminology and notations are not identical on the two fields and so it maybe demanding for design theorists. In this section is an attempt to make their life easier.

Let G be a finite abelian group. The notation $Z(G)$ stands for the group ring over G. The elements of $Z(G)$ are linear combinations of elements of G with integer coefficients. Let Δ be a (v, k, λ)-symmetric design admitting a regular group action by G. Under there circumstances the group contains a difference set D. In other words $D \subseteq G$ for which the equation

$$DD^{(-1)} = (k - \lambda)1_G + \lambda G$$

holds. Here the subset D of G is identified with the set of its elements to get an element of the group ring $Z(G)$. The subset $D^{(-1)}$ consists of the inverses of the elements of D. There are projects to extend correspondence between group ring identities and subsets of groups to matrices with entries from a set larger than $\{0, 1\}$. The interested reader can consult with [1], [5], [7].

By the complexity theory of algorithms the multiple cover problem, described in section 4, is an NP-hard problem. Thus discarding the algebraic structures we can construct k-fold factorization only in limited trivial sizes. This again reinforces the intuition that exploring the theory of Fourier analysis on finite abelian groups and design theory is the promising avenue.

References

[1] T. BETH, D. JUNGNICKEL, and H. LENZ: Design Theory, *Cambridge University Press, Cambridge*, 2nd Edition, 1999.

[2] J. A. DAVIS and J. JEDWAB: A unifying construction for difference sets, *J. Combin. Theory* Ser. A **80** (1997), 13–78.

[3] J. F. DILLON: Some really beautiful Hadamard matrices, *Cryptogr. Commun.*, **2** (2010), 271–292.

[4] J. F. DILLON and H. DOBBERTIN: New difference sets with Singer parameters, *Finite Fields Appl.* **10** (2004), 342–389.

[5] K. J. HORADAM: Hadamard Matrices and Their Applications, *Princeton University press, Princeton, NJ*, 2007.

[6] D. E. KNUTH: Dancing links, in *Millennial Perspectives in Computer Science*, J. Davies, B. Roscoe, and J. Woodcock, Eds., Palgrave Macmillan, Basingstoke, 2000, pp. 187–214.

[7] W. DE LAUNEY and D. FLANNERY: Algebraic Design Theory, *American Mathematical Society, Providence, RI*, 2011.

[8] R. A. LIEBLER: The inversion formula, *J. Combin. Math. Combin. Comput.*, **13** (1993), 143-160.

[9] M. MATOLCSI, J. RÉFFY and F. SZÖLLŐSI: Construction of complex Hadamard matrices via tiling abelian groups, *OSID* **14** (2007) (in print)

[10] A. POTT: Finite Geometry and Character Theory, *Springer Verlag, Berlin*, 1995.

[11] S. SZABÓ: Topics in Factorization of Abelian Groups, *Birkhäuser Verlag*, 2004.