1. Introduction

L'Enseignement Mathématique, t. 47 (2001), p. 103–114

CIRCULANT MODULAR HADAMARD MATRICES

by Shalom ELIAHOU*) and Michel KERVAIRE

1. INTRODUCTION

Besides Hadamard's conjecture proper, one of the major open problems concerning Hadamard matrices is Ryser's conjecture, according to which there are no circulant Hadamard matrices of size greater than 4; cf. [R].

In the light of Ryser's conjecture, it might prove interesting to consider the weaker notion of a circulant *modular* Hadamard matrix, and ask for what moduli and sizes such matrices happen to exist.

On the one hand, one hopes that non-existence results may shed some light on Ryser's conjecture. On the other hand, computer experimentation reveals the existence of families of modular circulant Hadamard matrices of given sizes and moduli with intriguing patterns. In the present note we exhibit one such infinite family with a large modulus m.

NOTATION. Let $X = (x_0, x_1, \ldots, x_{n-1})$ be a sequence of even size n, with $x_i = \pm 1$ for all $i = 0, \ldots, n-1$. We denote the k-th periodic correlation coefficient of X by

$$\gamma_k(X) = \sum_{i=0}^{n-1} x_i x_{i+k} ,$$

where the subscripts are read modulo n, for every k $(0 \leq k \leq n-1)$.

Clearly, $\gamma_k(X)$ is the dot product of X with its k-th left shift $\sigma_k(X)$, where $\sigma_k(X) = (x_k, x_{k+1}, \ldots, x_{k+n-1})$, again with indices read modulo n. Observe that $\gamma_0(X) = n$ and that $\gamma_{n-k}(X) = \gamma_k(X)$ for $k = 1, \ldots, n-1$.

*) During the preparation of this paper, the first author partially benefited from a research contract with the Fonds National Suisse pour la Recherche Scientifique.

A *circulant matrix* $\mathrm{circ}(X)$ is associated to X. The rows of $\mathrm{circ}(X)$ are the shifts $\sigma_{-k}(X), k = 0, \ldots, n-1$ of the sequence X.

Of course, the conjunction of the conditions $\gamma_k(X) = 0$ for all $k = 1, \ldots, \frac{n}{2}$ is equivalent to $H = \mathrm{circ}(X)$ being a circulant Hadamard matrix, while $\gamma_k(X) \equiv 0 \mod m$ for all $k = 1, \ldots, \frac{n}{2}$ means that $H = \mathrm{circ}(X)$ is an m-modular circulant Hadamard matrix.

There are two trivial examples of circulant modular Hadamard matrices with a large modulus. One is the constant all-one matrix $J = \mathrm{circ}(1, \ldots, 1)$. The matrix J is an n-modular circulant Hadamard matrix (CHM for short) of size n.

The other example is $J' = \mathrm{circ}(-1, 1, \ldots, 1) = J - 2I$, where I is the identity matrix of size n. Here, $J' \cdot (J')^t = nI + (n-4)(J - I)$, whence J' is an $(n-4)$-modular CHM of size n.

In order to exhibit interesting examples of circulant modular Hadamard matrices, we shall require that some of the correlations $\gamma_k(X)$ be actually zero, not only zero modulo m.

Using the notation $H(z) = \sum_{i=0}^{n-1} x_i z^i \in \mathbf{Z}[z]/(z^n - 1)$ as usual, the correlations $\gamma_k = \gamma_k(X)$ arise as coefficients in the identity

$$H(z)H(z^{-1}) = n + \sum_{k=1}^{\frac{n}{2}-1} \gamma_k(z^k + z^{-k}) + \gamma_{\frac{n}{2}} z^{\frac{n}{2}} \in \mathbf{Z}[z]/(z^n - 1), \tag{1}$$

where $\mathbf{Z}[z]/(z^n - 1)$ may be viewed as the group ring $\mathbf{Z}C_n$ of the cyclic group of order n generated by z.

The special position of $\gamma_{\frac{n}{2}}$ in this formula suggests that it be treated separately, as in the following (tentative) definition.

DEFINITION. Let $H = \mathrm{circ}(X)$ be an m-modular circulant Hadamard matrix of even size n. We say that H is *of type* 1 if $\gamma_{n/2}(X) = 0$. We say that H is *of type* 2 if $\gamma_k(X) = 0$ for all $k \neq 0, \frac{n}{2}$.

Ryser's conjecture amounts to saying that, in size greater than 4, *there is no circulant modular Hadamard matrix which is simultaneously of types* 1 *and* 2.

Even though the constraints for type 2 seem to be much stronger than the one for type 1, this may not necessarily be so. Consider, for example, the case of size $n = 20$ and modulus $m = 16$. Let

$$X = (1,1,1,-1,1,-1,-1,-1,-1,1,1,-1,-1,1,-1,1,1,1,1,-1).$$

Then, quite surprisingly perhaps, circ(X) is a 16-modular CHM of type 2, as X satisfies the equalities $\gamma_k(X) = 0$ for all $k \neq 0, 10$, and $\gamma_{10}(X) = -16$.

However, it follows from formula (1) above that there is no 16-modular CHM of type 1 in size 20. Indeed, for $n = 20$, substituting $z = 1$ in formula (1) with $\gamma_{10} = 0$ yields $H(1)^2 = 20 + 2\sum_{k=1}^{9} \gamma_k$.

The condition $\gamma_k \equiv 0 \mod 16$ for $k = 1, \ldots, 9$ would imply $(H(1)/2)^2 \equiv 5 \mod 8$, contradicting the fact that 5 is not a square modulo 8. Hence, the condition $\gamma_{10}(X) = 0$ alone forbids the other correlation coefficients of X, at positive indices k, to vanish simultaneously modulo 16.

The same argument shows that for q odd with $q \not\equiv 1 \mod 8$, there is no 16-modular CHM of length $4q$ satisfying $\gamma_{2q} \equiv 0 \mod 32$.

In this note, we exhibit (in the next section) a 4-parameter family of $(p-1)$-modular circulant Hadamard matrices of type 1 and of size $4p$ for every prime number p such that $p \equiv 1 \mod 4$.

As to circulant modular Hadamard matrices of type 2, it turns out that they can be obtained from a well known paper of Delsarte, Goethals and Seidel [DGS]. This is explained in Section 3.

2. A FAMILY OF $(p-1)$-MODULAR CIRCULANT HADAMARD MATRICES OF SIZE $4p$.

Let p be a *prime* satisfying $p \equiv 1 \mod 4$. We are going to prove the existence of $(p-1)$-modular circulant Hadamard matrices of type 1 and size $4p$. We give explicitly below the first row $(x_0, x_1, \ldots, x_{4p-1})$ of such a matrix as a polynomial $H(z) = \sum_{i=0}^{4p-1} x_i z^i \in \mathbf{Z}C_{4p} = \mathbf{Z}[z]/(z^{4p}-1)$, where all coefficients x_i equal ± 1 and $H(z)H(z^{-1}) \equiv 4p$ modulo $(p-1)\mathbf{Z}C_{4p}$. In order to write down $H(z)$ we need some notation.

Let $S_0 \subset [1, p-1] \cup [p+1, 2p-1]$ be the set of squares modulo $2p$, which are prime to p. Note that if s is a square mod p, then s is also a square mod $2p$. Indeed, if there exists c such that $c^2 = s + kp$ and k is odd, then $(c+p)^2 = c^2 + 2cp + p^2 = s + 2cp + (k+p)p \equiv s \mod 2p$.