Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 47 (2001)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: CIRCULANT MODULAR HADAMARD MATRICES
Autor: Eliahou, Shalom / Kervaire, Michel
Kapitel: 3. Circulant modular Hadamard matrices of type 2
DOI: https://doi.org/10.5169/seals-65430

Equivalently, this "remainder" $R(z)$ can be written

$$(11)\quad R(z) = 2\sum_{\nu=1}^{\frac{p-1}{2}}(z^{4\nu} + z^{-4\nu}) + \left\{\sum_{\nu=1}^{p}(z^{2\nu-1} + z^{-(2\nu-1)}) + z^p + z^{-p}\right\} \varepsilon_0\,\varepsilon_1\,.$$

The (periodic) correlations of $H(z)$ in degrees $\equiv 2 \mod 4$ are strictly zero. This includes in particular the correlation of degree $2p$. Hence, the modular Hadamard matrix associated with the sequence (polynomial) of the Theorem is indeed of type 1 as asserted. The correlations in degrees $\equiv 0 \mod 4$ are $2(p-1)$. Note that the correlation in degree p is $2(p-1)\,\varepsilon_0\,\varepsilon_1$ because z^p+z^{-p} also appears in the sum $\sum_{\nu=1}^{p}(z^{2\nu-1} + z^{-(2\nu-1)})$ for $\nu = \frac{p+1}{2}$.

REMARK. It seems probable, from computer-assisted experimentation, that $p-1$ may be the maximum modulus for a modular circulant Hadamard matrix of type 1 and size $4p$. However, the power of 2 dividing $p-1$ is certainly not always maximal as the power of 2 dividing the modulus of a modular CHM of type 1 and size $4p$. There are many values of p (where p is prime and satisfies $p \equiv 9 \mod 16$) for which a variant of the formula for $H(z)$ in the above Theorem yields a 16-modular CHM. The first few such values of p are $p = 73,\ 89,\ 233,\ \ldots$. On the other hand, it seems for example that indeed no 16-modular, type 1 CHM of size $4p$ exists for $p = 41$.

We hope to come back on the general question of 16-modular circulant Hadamard matrices of type 1 in a future publication.

3. CIRCULANT MODULAR HADAMARD MATRICES OF TYPE 2

In this section we produce circulant modular Hadamard matrices of type 2 and size $n = 2(q+1)$, where q is an arbitrary odd prime power. The existence of such objects is a corollary of a theorem from the 1971 paper [DGS].

We are grateful to Roland Bacher for valuable discussions about some unpublished work of his which helped in obtaining the following result.

THEOREM 2. *For every $n = 2(q+1)$, where q is an odd prime power, there exists a binary sequence $X = (x_0, \ldots, x_{n-1})$ with $x_i = \pm 1$ for all i $(0 \le i \le n-1)$, such that $\gamma_k(X) = 0$ for all $k \neq 0, \frac{n}{2}$. In other words,* circ(X) *is a circulant modular Hadamard matrix of type 2 and size n.*

Proof. Set $x_{\frac{n}{2}} = x_0 = 1$ and $x_{\frac{n}{2}+i} = -x_i$ for all $i = 1, 2, \ldots, \frac{n}{2} - 1$. The sequence $X = (x_1, x_2, \ldots, x_{n-1})$ is therefore determined by its subsequence $Y = (x_1, x_2, \ldots, x_{\frac{n}{2}-1})$.

We have $\gamma_0(X) = n$, $\gamma_{\frac{n}{2}}(X) = 4 - n$, and

$$\gamma_k(X) = 2(\alpha_k(Y) - \alpha_{\frac{n}{2}-k}(Y))$$

for all $k = 1, 2, \ldots, \frac{n}{2} - 1$ as easily checked, where α_k is the kth *aperiodic* correlation coefficient. Of course, $\gamma_{n-k}(X) = \gamma_k(X)$ for all $k = 1, 2, \ldots, \frac{n}{2} - 1$.

In order to prove the theorem, it therefore suffices to exhibit a binary sequence $Y = (x_1, x_2, \ldots, x_{\frac{n}{2}-1})$ of length $\frac{n}{2} - 1 = q$, satisfying the equation $\alpha_k(Y) - \alpha_{\frac{n}{2}-k}(Y) = 0$ for every $k = 1, 2, \ldots, \frac{n}{2} - 1$.

For this purpose, we recall the notion of a *negacyclic* matrix, introduced by Delsarte, Goethals and Seidel in their paper [DGS].

By definition it is simply a matrix of the form

$$\begin{pmatrix} u_0 & u_1 & \ldots & \ldots & u_r \\ -u_r & u_0 & u_1 & \ldots & u_{r-1} \\ -u_{r-1} & -u_r & u_0 & \ddots & u_{r-2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ -u_1 & -u_2 & \ldots & -u_r & u_0 \end{pmatrix}$$

which we will denote by $NC(u_0, u_1, \ldots, u_r)$.

Explicitly, the entries $c_{i,j}$ of the matrix $NC(u_0, u_1, \ldots, u_r)$ are

$$c_{i,j} = \begin{cases} u_{j-i} & \text{if } 0 \le i \le j \le r, \\ -u_{r-i+j+1} & \text{if } 0 \le j < i \le r. \end{cases}$$

It is very easy to see that the binary sequence $Y = (x_1, x_2, \ldots, x_{\frac{n}{2}-1})$ satisfies $\alpha_k(Y) - \alpha_{\frac{n}{2}-k}(Y) = 0$ for every $k = 1, 2, \ldots, \frac{n}{2} - 1$ if and only if the negacyclic matrix $C = NC(0, x_1, \ldots, x_{\frac{n}{2}-1})$ is a conference matrix, that is if $C \cdot C^t = (\frac{n}{2} - 1)I$.

Now, Delsarte, Goethals and Seidel have explicitly constructed negacyclic conference matrices of every size of the form $q + 1$, where $q = p^f$ with p an odd prime and f a positive integer, in Section 7 of [DGS]. These negacyclic conference matrices are equivalent to the usual Paley conference matrices based on the quadratic character $\chi \colon \mathbf{F}_q^* \to \{\pm 1\}$ of the finite field $\mathbf{F}_q$. □

NOTE. After having submitted the present paper for publication, we came across the Thèse d'Habilitation of Philippe Langevin (Toulon). There, a concept which is closely related to our type 2 sequences is studied. P. Langevin uses the terminology "almost perfect sequences" and his treatment also relies on [DGS].

Thus, we now find it preferable to drop the type 1 / type 2 terminology and rather call *enhanced modular* the modular matrices of type 1. We intend to use this new designation in future publications on the subject.

BIBLIOGRAPHY

[DGS] DELSARTE, P., J.M. GOETHALS and J.J. SEIDEL. Orthogonal matrices with zero diagonal, II. *Canad. J. Math. 23* (1971), 816–832.

[R] RYSER, H.J. *Combinatorial Mathematics.* Carus Monograph 14. Math. Assoc. of America, 1963.

(Reçu le 18 juillet 2000)

Shalom Eliahou

Département de Mathématiques
LMPA Joseph Liouville
Université du Littoral Côte d'Opale
Bâtiment Poincaré
50, rue Ferdinand Buisson, B.P. 699
F-62228 Calais
France
e-mail: eliahou@lmpa.univ-littoral.fr

Michel Kervaire

Département de Mathématiques
Université de Genève
2-4, rue du Lièvre
B.P. 240
CH-1211 Genève 24
Suisse
e-mail: Michel.Kervaire@math.unige.ch