Morfismos, Vol. 7, No. 2, 2003, pp. 17–45

A survey on modular Hadamard matrices [*]

Shalom Eliahou Michel Kervaire

Abstract

We provide constructions of 32-modular Hadamard matrices for every size n divisible by 4. They are based on the description of several families of modular Golay pairs and quadruples. Higher moduli are also considered, such as 48, 64, 128 and 192. Finally, we exhibit infinite families of circulant modular Hadamard matrices of various types for suitable moduli and sizes.

2000 Mathematics Subject Classification: 05B20, 11L05, 94A99.
Keywords and phrases: modular Hadamard matrix, modular Golay pair.

1 Introduction

A square matrix H of size n, with all entries ± 1, is a *Hadamard matrix* if $HH^T = nI$, where H^T is the transpose of H and I the identity matrix of size n.

It is easy to see that the order n of a Hadamard matrix must be 1, 2 or else a multiple of 4. There are two fundamental open problems about these matrices:

• Hadamard's conjecture, according to which there should exist a Hadamard matrix of every size n divisible by 4. (See [9].)

• Ryser's conjecture, stating that there probably exists no *circulant* Hadamard matrix of size greater than 4. (See [13].)

Recall that a circulant matrix is a square matrix $C = (c_{i,j})_{0 \leq i,j \leq n-1}$ of size n, such that $c_{i,j} = c_{0,j-i}$ for every i, j (with indices read mod n).

[*] **Invited article**

There are many known constructions of Hadamard matrices. However, Hadamard's conjecture is widely open. For example, the set of all currently known Hadamard matrix sizes (as of 2004) contains no arithmetic progression, and is in fact of density zero in the set of positive multiples of 4. (See [17].) The cases below 1000 which are currently open are 428, 668, 716, 764 and 892.

As for Ryser's conjecture, a lot is known, but here again the conjecture is widely open. For example, it is known that if $n > 4$ is the size of a circulant Hadamard matrix, then $n = 4 \cdot r^2$ with r odd and not a prime power. Actually further constraints on r are known, due to R. Turyn and more recently B. Schmidt [14].

In 1972, Marrero and Butson introduced the weaker notion of a *modular Hadamard matrix.* Like in the classical case, this is a square matrix H, with all entries ±1, but satisfying the above orthogonality condition only modulo some given integer m, *i.e.*

$$H \cdot H^T \equiv nI \mod m.$$

Of course, the classical Hadamard matrix conjecture has an m-modular counterpart, namely: *for every n divisible by 4, there should exist an m-modular Hadamard matrix of size n.* Even though this m-modular analogue looks much weaker than the classical one, there is a sort of converse, which rests on the following

Remark. If H is an m-modular Hadamard matrix of size n, with $n < m$, then H is an ordinary Hadamard matrix.

The proof is simple enough: the entries of $H \cdot H^T$ are at most n in absolute value. Hence, if those outside the diagonal are assumed to vanish mod m, then they must actually be zero.

With the above remark, we see that *the classical Hadamard matrix conjecture holds if and only if the modular Hadamard matrix conjecture simultaneously holds for infinitely many distinct moduli m.*

In this sense, the m-modular version of Hadamard's conjecture can be considered as an approximation to the classical one, of quality increasing with m. Currently, the highest modulus m for which the m-modular analogue of Hadamard's conjecture has been completely settled is $m = 32$. We summarize the relevant facts below.

In a series of papers, Marrero and Butson considered modular Hadamard matrices mainly with respect to moduli m which are either odd or 2 times an odd number. With respect to such moduli, sizes $n > 3$

not divisible by 4 are no longer excluded in general. For instance, they show the existence of a 6-modular Hadamard matrix of size n for every even n.

In this survey, we consider only moduli m which are divisible by 4, as this case resembles more the classical one. Indeed, *if $n > 3$ is the size of an m-modular Hadamard matrix, with m divisible by* 4*, then n itself must be divisible by* 4*,* as for ordinary Hadamard matrices. The proof is analogous to the one in the classical case, by considering congruences mod 4 rather than equalities.

As for Ryser's conjecture, the situation is somewhat different. There seems to be a very rich theory of circulant modular Hadamard matrices, which ought to be developed for its own sake. Circulant modular Hadamard matrices do exist for certain moduli and sizes greater than 4 and thus, the conjecture should rather be replaced in the modular context by the following question.

Question: For which moduli m and sizes n do there exist m-modular circulant Hadamard matrices H of size n ?

The question can be enriched by requiring that some entries of the matrix $H \cdot H^T$ be actually zero, not only zero mod m. We will introduce two such constraints, complementary in some sense, and refer to the complying matrices as being of *type* 1, *type* 2 respectively.

Informally, H will be of type 1 if any two rows of H with indices at distance $\frac{n}{2}$ are orthogonal in $\mathbf{Z}^n$, n being the order of H. On the other hand, H will be of type 2 if any two rows of H with indices at distance other than 0 and $\frac{n}{2}$ are orthogonal in $\mathbf{Z}^n$.

As we will see, there are nice infinite families of circulant modular Hadamard matrices of either type. These examples all come from number-theoretic constructions.

The complementary nature of types 1 and 2 imply that, if H is a circulant modular Hadamard matrix of both types simultaneously, then H is actually a true circulant Hadamard matrix.

Hence, investigating the possible moduli and orders of circulant modular Hadamard matrices of either type, besides being of independent interest, might shed some light on Ryser's conjecture itself.

2 Basic Definitions and Lemmas

We shall denote by $\mathrm{H}(n)$ the set of Hadamard matrices of size n, and by $\mathrm{H}_m(n)$ the set of m-modular Hadamard matrices of size n. Of course, $\mathrm{H}(n) \subset \mathrm{H}_m(n)$. Hadamard's conjecture reads $\mathrm{H}(n) \neq \emptyset$ for every n divisible by 4. Among other results, we shall see that $\mathrm{H}_{32}(n) \neq \emptyset$ for every n divisible by 4.

There are many constructions for Hadamard matrices. See the quoted surveys [4]. Here, we will mainly use three such constructions. All three use sets of complementary binary sequences, specifically pairs and quadruples. From such sets, Hadamard matrices are obtained by placing the circulant matrices derived from each sequence into suitable arrays. For convenience of the reader, this is recalled below.

2.1 The doubling lemma

We start with a very simple result.

Lemma 2.1.1 *There is a map $H_m(n) \to H_{2m}(2n)$. More specifically, if H is an m-modular Hadamard matrix of size n, then the matrix*

$$(1) \qquad H' = H \bigotimes \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} H & H \\ -H & H \end{pmatrix}$$

is a $2m$-modular Hadamard matrix of size $2n$.

Observe that the modulus has also been doubled in the process.

Proof:

$$H' \cdot H'^T = \begin{pmatrix} H & H \\ -H & H \end{pmatrix} \cdot \begin{pmatrix} H^T & -H^T \\ H^T & H^T \end{pmatrix} = \begin{pmatrix} 2H \cdot H^T & 0 \\ 0 & 2H \cdot H^T \end{pmatrix},$$

and $H \cdot H^T \equiv nI$ modulo m, *i.e.* $H \cdot H^T = nI + mX$ for some $n \times n$ integer matrix X. It follows that

$$H' \cdot H'^T = \begin{pmatrix} 2H \cdot H^T & 0 \\ 0 & 2H \cdot H^T \end{pmatrix} = 2n \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} + 2m \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}.$$

Thus $H' \cdot H'^T$ is congruent $2n$ times the identity matrix of size $2n$ modulo $2m$. $\square$

2.2 Complementary sequences

Let $A = (a_0, \ldots, a_{\ell-1})$ be a *binary sequence* of length ℓ, that is a sequence with all entries $a_i = \pm 1$. The *Hall polynomial* of A, denoted $A(z)$, is defined as $A(z) = \sum_{i=0}^{\ell-1} a_i z^i$. The kth *aperiodic correlation coefficient* $c_k(A)$ is defined as $c_k(A) = \sum_{i=0}^{\ell-1-k} a_i\, a_{i+k}$, for $0 \le k \le \ell - 1$. It is convenient to define $c_k(A) = 0$ if $k \ge \ell$.

Note that the number $c_k(A)$ arises as the coefficient of $(z^k + z^{-k})$ in the product $A(z)A(z^{-1})$ in the Laurent polynomial ring $\mathbf{Z}[z, z^{-1}]$:

$$A(z)A(z^{-1}) \;=\; c_0(A) + \sum_{k=1}^{\ell-1} c_k(A)(z^k + z^{-k}).$$

Here $c_0(A) = \ell$, the sum of the squares of the a_i which are assumed to be binary (i.e. ± 1).

A set of r binary sequences $A_1, \ldots, A_r$ is a set of *complementary sequences* if for each $k \ge 1$, the sum of the kth correlations of the sequences vanishes, that is $\sum_{j=1}^{r} c_k(A_j) = 0$ for all $k \ge 1$. (Recall our convention $c_k(A) = 0$ if k is not smaller than the length of A.)

Equivalently, using Hall polynomials, it is clear that *the binary sequences $A_1, \ldots, A_r$ form a set of complementary sequences if and only if $A_1(z)A_1(z^{-1}) + \cdots + A_r(z)A_r(z^{-1})$ equals a constant in the Laurent polynomial ring* $\mathbf{Z}[z, z^{-1}]$. In this case, the constant will simply be the sum of the respective lengths of $A_1, \ldots, A_r$.

Pairs of complementary sequences of the same length are also known as *Golay pairs.* Here, as in [6], we shall refer to quadruples of complementary sequences of the same length as *Golay quadruples.*

We shall denote by $\mathrm{GP}(n)$ the set of Golay pairs of length n, and by $\mathrm{GQ}(n)$ the set of Golay quadruples of length n. Golay pairs and quadruples may be used to construct Hadamard matrices of appropriate size. We recall these classical constructions now.

Proposition 2.2.1 *There is a map*

$$\mathrm{GP}(n) \longrightarrow \mathrm{H}(2n)$$

obtained by the following construction. Let A, B be a Golay pair of length n. Denote by A, B again the circulant matrices derived from each sequence respectively. Let

$$H \;=\; H(A, B) \;=\; \begin{pmatrix} A & B \\ -B^T & A^T \end{pmatrix}. \tag{2}$$

Then H is a Hadamard matrix of size $2n$.

Proof: A straightforward computation shows that

$$H \cdot H^T \;=\; \begin{pmatrix} AA^T + BB^T & -AB + BA \\ -B^T A^T + A^T B^T & A^T A + B^T B \end{pmatrix}.$$

Now, since A, B are circulant matrices, they commute. Hence,

$$H \cdot H^T \;=\; (A \cdot A^T + B \cdot B^T) \bigotimes \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}. \;\square$$

There is a classical construction, due to Goethals-Seidel, which associates a Hadamard matrix of size $4n$ to every Golay quadruple of length n.

First we recall what the Goethals-Seidel array is. If A, B, C and D are matrices of size n, define

$$(3) \qquad \mathrm{GS}(A, B, C, D) \;=\; \begin{pmatrix} A & -BR & -CR & -DR \\ BR & A & -D^T R & C^T R \\ CR & D^T R & A & -B^T R \\ DR & -C^T R & B^T R & A \end{pmatrix},$$

where R is the back-circulant matrix of size n defined by $R = (R_{i,j})$ with $R_{i,j} = \delta_{i+j,n+1}$ for $0 \leq i, j \leq n-1$.

Proposition 2.2.2 *There is a map*

$$\mathrm{GQ}(n) \longrightarrow \mathrm{H}(4n)$$

obtained by the following construction. Let A, B, C, D be a Golay quadruple of length n. Denote by A, B, C, D again the circulant matrices derived from each sequence respectively. Let H=GS(A, B, C, D). Then H is a Hadamard matrix of size $4n$.

The proof of the proposition uses the following properties of the matrix R. Namely, $R^2 = I, R^T = R$, and if X, Y are any two circulant matrices, then XRY^T is a symmetric matrix, *i.e.* $XRY^T = YRX^T$.

Besides the map from GP(n) to H$(2n)$ recalled above, there are other constructions associating a Hadamard matrix to a Golay pair, obtained by associating first a Golay quadruple to a Golay pair, and then using the Proposition above.

For example, if (f, g) is a Golay pair of length n, then (f, f, g, g) is a Golay quadruple of the same length n, yielding a Hadamard matrix of size $4n$. This yields a map $\mathrm{GP}(n) \longrightarrow \mathrm{H}(4n)$, not as efficient as the one above. There is a subtler classical construction, yielding this time a map from $\mathrm{GP}(n)$ to $\mathrm{H}(8n+4)$. It is obtained as follows.

Notation. If $f = (f_1, \ldots, f_\ell)$, $g = (g_1, \ldots, g_n)$ are (binary) sequences, we denote their concatenation by

$$[f; g] \quad = \quad (f_1, \ldots, f_\ell, g_1, \ldots, g_n).$$

Note that the length of $[f; g]$ is the sum of the lengths of f and g.

Proposition 2.2.3 *There are maps*

$$GP(n) \longrightarrow GQ(2n+1) \longrightarrow H(8n+4).$$

The first map associates to the Golay pair (f, g) a Golay quadruple (A, B, C, D), where

$$A = [f; 1; g], B = [f; 1; -g], C = [f; -1; g], D = [f; -1; -g].$$

Proof: Using the Hall polynomials of the respective sequences, it is straightforward to check the formula

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) + C(z)C(z^{-1}) + D(z)D(z^{-1}) \quad = \quad 4(1 + f(z)f(z^{-1}) + g(z)g(z^{-1})).$$

Thus, if $f(z)f(z^{-1}) + g(z)g(z^{-1})$ is a constant, this being the defining property of a Golay pair, then so will also be the expression $A(z)A(z^{-1})$ + $B(z)B(z^{-1})$ + $C(z)C(z^{-1})$ + $D(z)D(z^{-1})$. □

We now recall doubling constructions for Golay pairs and quadruples, that is, maps $\mathrm{GP}(n) \longrightarrow \mathrm{GP}(2n)$ and $\mathrm{GQ}(n) \longrightarrow \mathrm{GQ}(2n)$. If (f, g) is a Golay pair of length n, then $([f; g], [f; -g])$ is a Golay pair of length $2n$. If A, B, C, D is a Golay quadruple of length n, then

$$[A; B], [A; -B], [C; D], [C; -D]$$

is a Golay quadruple of length $2n$. Both statements are easy to verify.

We shall close this Section with a few comments about the lengths of Golay pairs and Golay quadruples.

For Golay pairs, it is known that $\mathrm{GP}(2^a 10^b 26^c)$ is not empty for every exponents $a, b, c \geq 0$. On the other hand, it is conjectured that no lengths other than $2^a 10^b 26^c$ may be realized as Golay pair lengths. It is easy to see that $\mathrm{GP}(n)$ is empty if n is odd and greater than 1. A theorem in [8] states that $\mathrm{GP}(n)$ is empty if n admits a divisor which is congruent to 3 mod 4. Computer searches have revealed the absence of Golay pairs of length 34, 50 and 68, and more recently of length 74 and 82 (see [2]). The smallest undecided cases now are $n = 106$ and $n = 116$.

As for Golay quadruples, there is the following

Conjecture. (Turyn, [15]) There is a Golay quadruple of length n for every positive integer n.

Because of the above-mentioned map $\mathrm{GQ}(n) \to \mathrm{GQ}(2n)$, the core of the problem is the case where n is odd. Moreover, because of the map $\mathrm{GQ}(n) \longrightarrow \mathrm{H}(4n)$, the above conjecture implies Hadamard's conjecture.

Obviously, every Golay pair A, B of length n yields a Golay quadruple A, A, B, B of the same length, and a Golay quadruple of length $2n+1$ by the map $\mathrm{GP}(n) \longrightarrow \mathrm{GQ}(2n+1)$.

2.3 Modular complementary sequences

There are modular analogues of the above notions. Let m be a positive integer. A set of r binary sequences $\{A_1, \dots, A_r\}$ is a set of *m-modular complementary sequences* if for each $k \geq 1$, the sum of the kth correlations of the sequences vanishes mod m, that is $\sum_{j=1}^{r} c_k(A_j) \equiv 0 \bmod m$ for all $k \geq 1$. This is equivalent to the statement that

$$A_1(z)A_1(z^{-1}) + \cdots + A_r(z)A_r(z^{-1})$$

equals a constant in the Laurent polynomial ring $(\mathbf{Z}/m\mathbf{Z})[z, z^{-1}]$.

In particular, we have the notion of modular Golay pairs and quadruples. We will denote by $\mathrm{GP}_m(n)$, $\mathrm{GQ}_m(n)$ the set of m-modular Golay pairs, respectively m-modular Golay quadruples, of length n.

The above constructions, associating Hadamard matrices to suitable sets of Golay sequences, work as well in the modular context.

Proposition 2.3.1 *There are maps*

$$GP_m(n) \longrightarrow H_m(2n) \text{ and } GQ_m(n) \longrightarrow H_m(4n).$$

Note that, in these maps, the modulus remains unchanged. However, for the third construction $\mathrm{GP}(n) \longrightarrow \mathrm{GQ}(2n+1) \longrightarrow \mathrm{H}(8n+4)$, we have the happy circumstance that the modulus is multiplied by 4.

Proposition 2.3.2 *There is a map* $\mathrm{G}P_m(n) \longrightarrow \mathrm{G}Q_{4m}(2n+1)$*, and hence a map* $\mathrm{GP}_m(n) \longrightarrow \mathrm{H}_{4m}(8n+4)$*.*

The multiplication of the modulus m by 4 is apparent in the proof of the last proposition of Section 2.2.

Finally, on the modular level, the doubling of Golay pairs also doubles the modulus. That is, there is a map $\mathrm{GP}_m(n) \to \mathrm{GP}_{2m}(2n)$, given by $(f,g) \mapsto ([f;g],[f;-g])$. This is easily checked using the Hall polynomials of the sequences: if $A(z) = f(z)+z^n g(z)$ and $B(z) = f(z)-z^n g(z)$, then

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) = 2(f(z)f(z^{-1}) + g(z)g(z^{-1})).$$

3 Modular Hadamard matrices

3.1 The case $m = 12$

Marrero and Butson have produced 6-modular Hadamard matrices of size n for every even positive integer n. (See [11] and [12].) Very simple matrices suffice for this purpose. It turns out that their construction yields in fact 12-modular Hadamard matrices of every size n divisible by 4.

For any given size, let I denote the identity matrix, J the constant all-one matrix, and $K = -2I + J$, the circulant with first row $(-1, 1, \ldots, 1)$.

Proposition 3.1.1 *A* 12*-modular Hadamard matrix of size n is given by J, K or* $\begin{pmatrix} K & K \\ -K & K \end{pmatrix}$ *depending on whether $n \equiv 0, 4$ or* $8 \bmod 12$ *respectively.*

Proof: In size n, we have $J \cdot J^T = nJ$ and $K \cdot K^T = nI + (n-4)(J-I)$. This takes care of the cases $n \equiv 0, 4 \bmod 12$. Assume now $n \equiv 8 \bmod 12$, and let $H = \begin{pmatrix} K & K \\ -K & K \end{pmatrix}$ of size n. Then $H \cdot H^T =$

$\begin{pmatrix} 2KK^T & 0 \\ 0 & 2KK^T \end{pmatrix}$. Since K is of size $\frac{n}{2}$ here, we have $KK^T = \frac{n}{2}I + (\frac{n}{2} - 4)(J - I)$, and so $2K \cdot K^T = nI + (n-8)(J - I)$.

It follows that $H \cdot H^T \equiv \begin{pmatrix} nI & 0 \\ 0 & nI \end{pmatrix}$ mod 12. □

This solves the 12-modular version of Hadamard's conjecture. Obviously, more elaborate matrices will be needed for higher moduli. This is plainly illustrated in the case $m = 32$.

3.2 The solution of the 32-modular Hadamard conjecture

We shall prove the existence of a 32-modular Hadamard matrix of size 4ℓ for every positive integer ℓ. By the Doubling Lemma, it is sufficient to consider the case where ℓ is odd.

Our constructions depend on the class of ℓ mod 8, and, in contrast to [6], are all based in this paper on modular Golay pairs and quadruples.

For $\ell \equiv 1, 3$ or 7 mod 8, we shall exhibit 32-modular Golay quadruples of length ℓ. These quadruples yield 32-modular Hadamard matrices of size 4ℓ by the map $\mathrm{GQ}_m(n) \longrightarrow \mathrm{H}_m(4n)$ of Section 2 derived from the Goethals-Seidel array. For $\ell \equiv 3$ or 7 mod 8, the description of these quadruples is by direct construction, while for $\ell \equiv 1$ mod 8, they derive from 8-modular Golay pairs of length $\frac{\ell-1}{2}$, and the map $\mathrm{GP}_m(r) \longrightarrow \mathrm{GQ}_{4m}(2r+1)$ of Section 2 (with $r = \frac{\ell-1}{2}$).

In the remaining case $\ell \equiv 5$ mod 8, and more specifically for $\ell \equiv 13$ mod 16, we are so far unable to produce 32-modular Golay quadruples of length ℓ. Rather, we shall obtain 32-modular Hadamard matrices of size 4ℓ from 32-modular *Golay pairs* of length 2ℓ and the map $\mathrm{GP}_m(2\ell) \longrightarrow \mathrm{H}_m(4\ell)$ of Section 2. We observe that this construction, which works for $\ell \equiv 5$ mod 8, cannot work for $\ell \equiv 3$ or 7 mod 8, as we can prove that 32-modular Golay pairs do not exist in length congruent to 6 or 14 mod 16, as well as in length congruent to 12 mod 16, see [6]. (The existence of 32-modular Golay pairs of length 2ℓ with $\ell \equiv 1$ mod 8 remains in doubt.)

3.2.1 Modular Golay quadruples of length $\ell \equiv 1$ mod 8

Let $k = \frac{\ell-1}{8}$. We shall construct a family of 8-modular Golay pairs of length $4k$ with k free binary parameters, and then use the maps

$$\mathrm{GP}_m(r) \longrightarrow \mathrm{GQ}_{4m}(2r+1) \longrightarrow \mathrm{H}_{4m}(4(2r+1))$$

to produce the desired modular Golay quadruples and modular Hadamard matrices.

Consider an arbitrary binary sequence $h = (x_0, \dots, x_{k-1})$ say, of length k, with $x_i = \pm 1$ for all i. Obviously, the pair (h, h) is a 2-modular Golay pair of length k. By the doubling of Golay pairs, the pair (f, g) with $f = [h; h]$ and $g = [h; -h]$ is a 4-modular Golay pair of length $2k$, and the pair (A, B) with $A = [f; g]$ and $B = [f; -g]$ is an 8-modular Golay pair of length $4k$ with k free binary parameters, as desired.

In summary, with $A = [h; h; h; -h]$ and $B = [h; h; -h; h]$, the pair (A, B) is a k-parameter family of 8-modular Golay pairs of length $4k = \frac{\ell-1}{2}$.

Corollary 3.2.1 *For every $\ell \equiv 1$ mod 8, there is a k-parameter family of 32-modular Golay quadruples of length ℓ and 32-modular Hadamard matrices of size 4ℓ, where $k = \frac{\ell-1}{8}$.*

Proof: Send the above 8-modular Golay pair of length $4k = \frac{\ell-1}{2}$ to $\mathrm{GQ}_{32}(\ell)$ and $\mathrm{H}_{32}(4\ell)$ with the maps

$$\mathrm{GP}_m(r) \longrightarrow \mathrm{GQ}_{4m}(2r+1) \longrightarrow \mathrm{H}_{4m}(4(2r+1))$$

at $m = 8$ and $r = 4k = \frac{\ell-1}{2}$. □

3.2.2 Modular Golay quadruples of length $\ell \equiv 3, 7$ mod 8

Our objective here is to show that $\mathrm{GQ}_{32}(\ell) \neq \emptyset$ for $\ell \equiv 3$ mod 4. We shall need the following operation on binary sequences.

To the sequence $F = (a_0, \dots, a_k)$, we associate the new sequence $F^{\#}$, defined as

$$F^{\#} \;=\; ((-1)^k a_k, \dots, (-1)^i a_i, \dots, a_0).$$

On the level of Hall polynomials, this transformation reads simply as $F^{\#}(z) = z^k F(-z^{-1})$.

Let $r = \frac{l-3}{4}$, and set $\varepsilon = (-1)^{r-1}$. Thus, $\varepsilon = -1$ if r is even, that is if $\ell \equiv 3$ mod 8, while $\varepsilon = +1$ if $\ell \equiv 7$ mod 8. Given two (± 1)-sequences H and K of size $2r + 1$, we define a quadruple of binary sequences of length $\ell = 4r + 3$, $Q(H, K) = (A, B, C, D)$, as follows:

$$\begin{aligned} A &= [H; \varepsilon; -H^{\#}], & B &= [H; \varepsilon; -K^{\#}] \\ C &= [K; \varepsilon; -H^{\#}], & D &= [K; -\varepsilon; -K^{\#}]. \end{aligned}$$

For the binary sequences H, K described below, the associated quadruple $Q(H,K)$ turns out to be a 32-modular Golay quadruple. It is convenient to separate the cases r even and r odd.

For r even, define $H = [1^{2r+1}]$ and $K = [-1^{r+1}; 1^r]$, where $[1^{2r+1}]$ denotes the constant all 1 sequence of length $(2r+1)$, and $[-1^{r+1}]$ denotes a constant sequence of -1 repeated $(r+1)$ times.

For r odd, let $f = [1^{r-1}]$. Define

$$H = [f; -1, 1, 1; f^{\#}] \text{ and } K = [-f; 1, -1, 1; f^{\#}].$$

Since $f^{\#} = [-1, 1]^{(r-1)/2}$ in the present case, we have in fact

$$\begin{aligned} H &= [1^{r-1}; -1, 1, 1; [-1, 1]^{(r-1)/2}] \text{ and} \\ K &= [-1^{r-1}; 1, -1, 1; [-1, 1]^{(r-1)/2}]. \end{aligned}$$

In [6], we established the following result.

Theorem 3.2.2 *Let $\ell \equiv 3$ mod 4, and let H, K be the above binary sequences of length $\frac{\ell-1}{2} = 2r+1$, that is $H = [1^{2r+1}]$ and $K = [-1^{r+1}; 1^r]$ if r is even, $H = [1^{r-1}; -1, 1, 1; [-1, 1]^{(r-1)/2}]$ and $K = [-1^{r-1}; 1, -1, 1; [-1, 1]^{(r-1)/2}]$ if r is odd. Then the quadruple of binary sequences $Q(H,K) = (A,B,C,D)$ as defined above, is a 32-modular Golay quadruple of length ℓ. More precisely, we have the following formula in terms of the Hall polynomials of A,B,C,D :*

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) + C(z)C(z^{-1}) + D(z)D(z^{-1}) = 4\ell + 32 \sum_{i=1}^{[r/2]} ([r/2] - i)(z^{2i} + z^{-2i}).$$

Corollary 3.2.3 *There is a 32-modular Hadamard matrix of size 4ℓ for every positive integer $\ell \equiv 3$ mod 4.*

Proof: Send the above 32-modular Golay quadruple A, B, C, D of length ℓ to $\mathrm{H}_{32}(4\ell)$ with the map $\mathrm{GQ}_m(\ell) \longrightarrow \mathrm{H}_m(4\ell)$ of Section 2. □

Example 3.2.4 No true Hadamard matrix is known yet in size $n = 428$. But the above construction yields the following 32-modular Hadamard matrix of this size n. Let

$$\begin{aligned} A &= [1^{53}; -1; [-1, 1]^{26}; -1], \\ B &= [1^{53}; -1; [-1, 1]^{13}; [1, -1]^{13}; 1], \\ C &= [-1^{27}; 1^{26}; -1; [-1, 1]^{26}; -1], \\ D &= [-1^{27}; 1^{26}; 1; [-1, 1]^{13}; [1, -1]^{13}; 1]. \end{aligned}$$

This is a quadruple of binary sequences of length 107. For $1 \leq k \leq 106$, let $\alpha_k = c_k(A) + c_k(B) + c_k(C) + c_k(D)$ be the sum of the kth aperiodic correlation coefficients of A, B, C and D respectively. We then find $\alpha_k = 0$ for all $k \in \{1, 2, \ldots, 106\} \backslash \{2, 4, \ldots, 24\}$, and $\alpha_{2k} = 32 \cdot (13 - k)$ for k in the interval $1 \leq k \leq 12$. Thus, as claimed, (A, B, C, D) is a 32-modular Golay quadruple of length 107.

The matrix $H = \mathrm{GS}(A, B, C, D)$ is therefore a 32-modular Hadamard matrix of size 428 (see Figure 1). It is amusing to observe that among the $91378 = \binom{428}{2}$ entries of the strict upper triangular part of $H \cdot H^T$, there are 86242 entries which are strictly 0, while the remaining 5136 non-zero ones consist of 428 entries of the form $32k$ for each $1 \leq k \leq 12$.

Actually, any row in H is orthogonal to exactly 403 other rows in H. For example, the 25 rows *not orthogonal* to the first row are the rows in position 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104 and 106.

One last remark concerning the determinant of H. Recall the theorem of Hadamard [9] stating that the determinant of any real matrix M of size n with entries from the interval $[-1, 1]$ satisfies the inequality $|det(M)| \leq n^{n/2}$. Moreover, the equality $|det(M)| = n^{n/2}$ holds true if and only if M is a Hadamard matrix. Here, in the above example H of size $n = 428$, we have $n^{\alpha n} < |det(H)| < n^{\beta n}$, with $\alpha = 0.347$ and $\beta = 0.348$.

3.2.3 The case $\ell \equiv 5$ mod 8

We know only one way to obtain 32-modular Hadamard matrices of size 4ℓ for $\ell \equiv 5 \bmod 8$. Namely, from 32-modular Golay pairs of length $2\ell \equiv 10 \bmod 16$ and the map $\mathrm{GP}_m(2\ell) \longrightarrow \mathrm{H}_m(4\ell)$.

The relevant modular Golay pairs are somewhat involved, and are best described through their Hall polynomials.

Let $k = \frac{\ell - 5}{8}$. Define $S(z) = \sum_{i=0}^{k-1} (-1)^i z^{4i}$. Let x_0, x_1 be two binary parameters, and define the pair of polynomials $U(z), V(z)$ as follows:

$$\begin{aligned} U(z) &= (x_0 + x_1 z + x_0 z^2) S(z) + (-1)^k (x_0 - x_1 z - x_0 z^2) z^{4k} \\ &\quad + (-1)^k (x_0 - x_1 z + x_0 z^2) S(z) z^{4(k+1)}, \\ V(z) &= \textstyle\sum_{i=0}^{2k} (-1)^i z^{4i} \ + \ z^{8k+2}. \end{aligned}$$

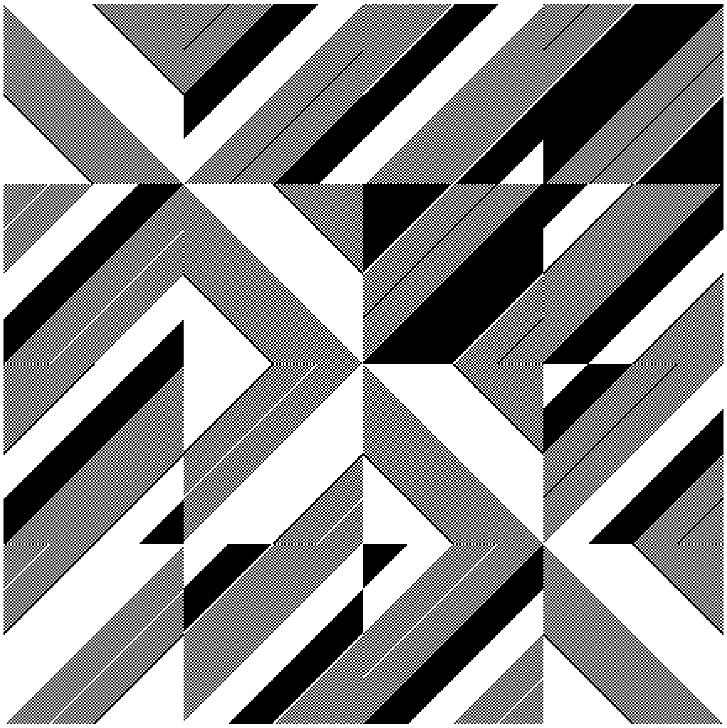

Figure 1: *A* 32*-modular* Hadamard *matrix of size* 428 *(white pixels represent* +1 *and black pixels represent* −1*)*

Finally, let $x_3 = \pm 1$ be a third free binary parameter, and define $A(z), B(z)$ as follows:

$$\begin{aligned} A(z) &= U(z) + x_3 z^3 V(z) + z^{16k+9}(U(z^{-1}) - x_3 z^{-3} V(z^{-1})), \\ B(z) &= U(z) + x_3 z^3 V(z) - z^{16k+9}(U(z^{-1}) - x_3 z^{-3} V(z^{-1})). \end{aligned}$$

In [6], we prove the following result.

Theorem 3.2.5 *For every $\ell \equiv 5$ mod 8, the above polynomials $A(z), B(z)$ are the respective Hall polynomials of a 3-parameter 32-modular Golay pair A, B of length $2\ell = 16k + 10$.*

In this theorem, the total correlation $A(z)A(z^{-1}) + B(z)B(z^{-1})$, which we abbreviate $A\overline{A} + B\overline{B}$, is given by the formula

$$A\overline{A} + B\overline{B} \;=\; 32k + 20 + 32\sum_{i=1}^{k-1}(-1)^i(k-i)(z^{4i} + z^{-4i}). \tag{4}$$

Example 3.2.6 We get true Golay pairs of length 10 for $k = 0$ and true Golay pairs of length 26 for $k = 1$. Let now $k = 2$. There are no Golay pairs of length $2\ell = 16k + 10 = 42$, because 42 has a divisor congruent to 3 mod 4 (see [8]). However, setting $x_0 = x_1 = x_3 = 1$ for simplicity in the pair given by the above theorem, we get a 32-modular Golay pair A, B of length 42, namely

$$\begin{aligned} A \;&=\; {+}{+}{+}{+}{-}{-}{-}{-}{+}{-}{-}{+}{+}{-}{+}{-}{-}{+}{-}{+}{-}{+}{-}{-}{+}{-} \\ &\quad\; {+}{+}{-}{+}{-}{-}{-}{+}{+}{-}{-}{-}{-}{+}{+}{+}, \end{aligned}$$

$$\begin{aligned} B \;&=\; {+}{+}{+}{+}{-}{-}{-}{-}{+}{-}{-}{+}{+}{-}{+}{-}{-}{+}{-}{+}{+}{+}{+}{+}{-}{+} \\ &\quad\; {-}{-}{+}{-}{+}{+}{+}{-}{-}{+}{+}{+}{+}{-}{-}{-}\,. \end{aligned}$$

Remarkably, this pair is almost a true Golay pair of length 42, as it satisfies $c_i(A) + c_i(B) = 0$ for all $1 \leq i \leq 41$ with the sole exception of $i = 4$, for which $c_4(A) + c_4(B) = -32$.

More generally, the formula (4) shows that only $(k-1)/(16k+8)$ of the correlations sums $c_i(A) + c_i(B)$ are non-zero. On the other hand, we know that a pair (A, B) with $k \geq 2$ as in the above Theorem can never be an actual Golay pair even with an arbitrary (binary) polynomial $S(z) = \sum_{i=0}^{k-1} u_i z^{4i}$. (See [8], Lemma 4.7 and the remark at the end of Section 1.2 in [6].)

Corollary 3.2.7 *There exist* 32*-modular Hadamard matrices of size* 4ℓ *for every positive integer* $\ell \equiv 5$ *mod* 8*.*

Proof: Send the above 32-modular Golay pair A, B of length 2ℓ to $H_{32}(4\ell)$ with the map $\mathrm{GP}_m(2\ell) \longrightarrow \mathrm{H}_m(4\ell)$ of Section 2. $\Box$

Corollary 3.2.8 *There exist* 128*-modular Hadamard matrices of size* $16\ell + 4$ *for every positive integer* $\ell \equiv 5$ *mod* 8*.*

Proof: Send the above 32-modular Golay pair A, B of length 2ℓ to $H_{128}(16\ell+4)$ with the maps $\mathrm{GP}_m(2\ell) \longrightarrow \mathrm{GQ}_{4m}(4\ell+1) \longrightarrow \mathrm{H}_{4m}(16\ell+4)$ of Section 2. □

Example 3.2.9 Currently, no Hadamard matrices of size $4r$ are known for $r = 789, 853$ and 917. These are the only undecided cases with $r \leq 1000$ and $r \equiv 21 \bmod 32$. However, *there exist* 128-*modular Hadamard matrices in size* $4r$ *for* $r = 789, 853$ *and* 917. Indeed, let $\ell = \frac{r-1}{4}$. Then $\ell \equiv 5 \bmod 8$, and the conclusion follows from the second corollary above.

In the next Section, we shall actually obtain a 192-modular Hadamard matrix of size $4 \cdot 917$.

3.3 Other moduli

We shall exhibit a few more modular Hadamard matrices in sizes for which, as above, no true Hadamard matrices are known yet.

The modulus $m = 48$

We start by constructing 48-modular Golay pairs of length $24k + 2$ for every positive integer k. (See [6], Section 1.5.) Define $S(z) = \sum_{i=0}^{k-1} (-1)^i z^{12i}$. Let x_0, x_1 be two binary parameters, and define the pair of polynomials $U(z), V(z)$ as follows :

$$\begin{aligned} U(z) &= \{x_0(1 + z^2 - z^4 + z^6 - z^8 - z^{10}) + x_1(z + z^5 + z^9)\}S(z), \\ V(z) &= (1 - z^4 + z^8)S(z) \ + \ z^{12k-2}. \end{aligned}$$

Finally, let x_3 be a third free binary parameter, and define $A(z), B(z)$ as follows :

$$\begin{aligned} A(z) &= U(z) + x_3 z^3 V(z) + z^{24k+1}(U(z^{-1}) - x_3 z^{-3} V(z^{-1})), \\ B(z) &= U(z) + x_3 z^3 V(z) - z^{24k+1}(U(z^{-1}) - x_3 z^{-3} V(z^{-1})). \end{aligned}$$

We prove the following result in [6].

Theorem 3.3.1 *For every* $\ell \equiv 1$ *mod* 12, *the above polynomials* $A(z), B(z)$ *are the respective Hall polynomials of a* 3-*parameter* 48-*modular Golay pair* A, B *of length* $2\ell = 24k + 2$.

Example 3.3.2 For $k = 1$, this construction yields true Golay pairs of length 26. Let now $k = 2$. There are no Golay pairs of length $2\ell = 24k + 2 = 50$, as revealed by an exhaustive computer search. (See [1].) However, setting $x_0 = x_1 = x_3 = 1$ in the pair given by the above theorem, we get a 48-modular Golay pair A, B of length 50, namely

$$\begin{aligned} A \;=\;& ++++-++--+-+----+--++-+-+- \\ & ++-+---++-----+-+++--+++, \end{aligned}$$

$$\begin{aligned} B \;=\;& ++++-++--+-+----+--++-+--- \\ & --+-+++--+++++-+---++---, \end{aligned}$$

where + stands for +1 and − for −1. This pair satisfies $c_i(A) + c_i(B) = 0$ for all $1 \leq i \leq 49$ with the sole exception of $i = 12$, for which $c_{12}(A) + c_{12}(B) = -48$.

Corollary 3.3.3 *There exist* 48*-modular Hadamard matrices of size* $48k + 4$ *and* 192*-modular* Hadamard *matrices of size* $192k + 20$ *for every positive integer* k*.*

Proof: Send the above 48-modular Golay pair A, B of length $2\ell = 24k + 2$ to $H_{48}(4\ell)$ and to $H_{192}(16\ell + 4)$ with the maps $\mathrm{GP}_m(2\ell) \longrightarrow \mathrm{H}_m(4\ell)$ and $\mathrm{GP}_m(2\ell) \longrightarrow \mathrm{GQ}_{4m}(4\ell + 1) \longrightarrow \mathrm{H}_{4m}(16\ell + 4)$ of Section 2, respectively. □

Example 3.3.4 There exist 192-modular Hadamard matrices of size $4 \cdot 917$. Indeed, take $k = 19$ in the above 192-modular construction. There also exist 48-modular Hadamard matrices of size $4 \cdot 721$ and $4 \cdot 853$ (with $k = 60$ and $k = 71$ in the above 48-modular construction, respectively.) These three sizes, $4 \cdot 721, 4 \cdot 853$ and $4 \cdot 917$, are all undecided cases for true Hadamard matrices.

The moduli $m = 2^t$

We have proved above that $\mathrm{H}_{32}(n) \neq \emptyset$ for every positive integer n divisible by 4. Using the map $\mathrm{H}_m(n) \longrightarrow \mathrm{H}_{2m}(2n)$, we see that $\mathrm{H}_{64}(n) \neq \emptyset$ for every n divisible by 8, and more generally that $\mathrm{H}_{2^{t+3}}(n) \neq \emptyset$ for every $t \geq 3$ and every n divisible by 2^t.

However, with further constructions, we shall obtain 64-modular and 128-modular Hadamard matrices of some (but unfortunately not all) sizes $n \equiv 4 \bmod 8$.

Recall from Section 3.2.1 that, if h is an arbitrary binary sequence of length k, then the pair (h, h) is a k-parameter 2-modular Golay pair of length k. In other terms, $\mathrm{GP}_2(k) \neq \emptyset$ for every positive integer k. By the doubling of Golay pairs, that is, by the map $\mathrm{GP}_m(n) \longrightarrow \mathrm{GP}_{2m}(2n)$, which doubles both length and modulus, we readily obtain the following statements.

Proposition 3.3.5 *$GP_{2^t}(2^{t-1}k) \neq \emptyset$ for every positive integers t and k.*

Corollary 3.3.6 *There exist 2^{t+2}-modular Hadamard matrices of size $n = 4 \cdot (2^t k + 1)$ for every positive integers t, k.*

Proof: Use the maps $\mathrm{GP}_m(n) \longrightarrow \mathrm{GQ}_{4m}(2n+1) \longrightarrow \mathrm{H}_{4m}(4\cdot(2n+1))$ of Section 2. $\square$

Example 3.3.7 No Hadamard matrices of size $4 \cdot 721$ are known yet. Now, $721 = 2^4 \cdot 45 + 1$. Thus, the above result, with $t = 4$, yields a 64-modular Hadamard matrix of size $4 \cdot 721$. (We already had a 48-modular Hadamard matrix of size $4 \cdot 721$. See the case $m = 48$ above.)

We recall one last construction of modular Golay pairs.

Proposition 3.3.8 *(*[6]*) There are* 16*-modular Golay pairs of length* $8k + 2$ *for every integer* $k \geq 0$.

Proof: For $k = 0$, the pair $A(z) = 1 + z, B(z) = 1 - z$ will do. Assume now $k \geq 1$. Choose polynomials $f(z) = \sum_{i=0}^{k-1} x_i z^{4i}$, $g(z) = \sum_{i=0}^{k-1} y_i z^{4i}$ with arbitrary $x_i = \pm 1$, $y_i = \pm 1$ for $i = 0, 1, \ldots, k-1$. Let also $w = \pm 1$ be chosen arbitrarily. Further, let $F(z) = z^{-(4k-1)} f(z) + z^{4k-1} f(z^{-1})$ and $G(z) = z^{-(4k-1)} g(z) - z^{4k-1} g(z^{-1})$. A 16-modular Golay pair, of length $8k + 2$, is given by

$$\begin{aligned} A(z) &= \{(1 + z^3)F(z) + (z + z^2)G(z) + w(z - z^2)\}z^{4k-1} \\ B(z) &= \{(1 - z^3)F(z) + (z - z^2)G(z) + w(z + z^2)\}z^{4k-1}.\square \end{aligned}$$

Corollary 3.3.9 *There exist 2^{t+6}-modular Hadamard matrices of size $n = 4 \cdot (2^{t+3}k + 2^{t+1} + 1)$ for every integers $t, k \geq 0$.*

Proof: Since $\mathrm{GP}_{16}(8k+2) \neq \emptyset$, it follows by successive doubling that $\mathrm{GP}_{2^{t+4}}(2^{t+3}k + 2^{t+1}) \neq \emptyset$, for every $t \geq 0$. Using again the maps $\mathrm{GP}_m(n) \longrightarrow \mathrm{GQ}_{4m}(2n+1) \longrightarrow \mathrm{H}_{4m}(4 \cdot (2n+1))$ of Section 2, it follows that the sets $\mathrm{GP}_{2^{t+6}}(2^{t+4}k + 2^{t+2} + 1)$ and $\mathrm{H}_{2^{t+6}}(4 \cdot (2^{t+4}k + 2^{t+2} + 1))$ are both non-empty, for every $t, k \geq 0$. $\square$

Example 3.3.10 It is not known whether Hadamard matrices of size $4 \cdot \ell$ exist for $\ell = 789, 853, 917$ and 933. These four values of ℓ are congruent to 5 mod 16. The above corollary, with $t = 0$, therefore yields 64-modular Hadamard matrices of size $4 \cdot 789$, $4 \cdot 853$, $4 \cdot 917$ and $4 \cdot 933$. Note that only the case $4 \cdot 933$ is really of interest here, as we had already obtained 128-modular Hadamard matrices of size $4 \cdot 789$, $4 \cdot 853$ and $4 \cdot 917$ in Section 3.2.3.

4 Circulant modular Hadamard matrices

4.1 Introduction

According to Ryser's conjecture, there probably exists no circulant Hadamard matrix of size $n > 4$. In contrast, the modular level reveals interesting families of examples [5]. These families are all based on the quadratic and biquadratic characters of finite fields, and will be exhibited below. Thus, it would seem appropriate to rephrase the problem as follows.

Question: For what moduli m and sizes n do there exist m-modular circulant Hadamard matrices of size n ?

Definition 4.1.1 Let $s = \{x_0, x_1, \ldots, x_{n-1}\} \in \{\pm 1\}^n$ be a binary sequence of size n. The kth periodic correlation coefficient $\gamma_k(s)$ of s, for $0 \leq k \leq n-1$, is defined as $\gamma_k(s) = \sum_{i=0}^{n-1} x_i x_{i+k}$, where the indices are read modulo n.

Observe that $\gamma_0(s) = n$, and that $\gamma_{n-k}(s) = \gamma_k(s)$ for $1 \leq k \leq n-1$. Also, setting $s(z) = \sum_{i=0}^{n-1} s_i z^i$, we have the formula $s(z)s(z^{-1}) = n + \sum_{k=1}^{n-1} \gamma_k(s) z^k$ in the quotient ring $\mathbf{Z}[z]/(z^n - 1)$. Finally, if $H = circ(s)$ is the circulant matrix with first row s, then obviously the matrix $H \cdot H^T$ has $\gamma_{j-i}(s)$ as entry with position i, j. Thus, H will be an m-modular circulant Hadamard matrix if and only if $\gamma_k(s) \equiv 0 \bmod m$ for all $1 \leq k \leq \frac{n}{2}$.

The most obvious examples of circulant modular Hadamard matrices with a large modulus are

$$J = circ(1, \cdots, 1) \text{ and } K = -2I + J = circ(-1, 1, \cdots, 1)$$

of size n. We have $J \cdot J^T = nJ$ and $K \cdot K^T = nI + (n-4)(J-I)$. Thus, J is a circulant n-modular Hadamard matrix, and K is a circulant $(n-4)$-modular Hadamard matrix, both of size n.

More elaborate examples have the property that some of their periodic correlation coefficients are actually 0, not only 0 mod m. We introduce the following definition.

Definition 4.1.2 Let $s \in \{\pm 1\}^n$ be a binary sequence of size n, with n even. We say that s is *of type 1* if $\gamma_{\frac{n}{2}}(s) = 0$. We say that s is *of type 2*if $\gamma_1(s) = \ \ldots\ = \gamma_{\frac{n}{2}-1}(s) = 0$. This definition extends quite naturally to circulant binary matrices. A circulant binary matrix H is of type i (with $i = 1$ or 2) if its first row is of type i (equivalently, if any of its rows is of type i).

Remark 4.1.3 Ryser's conjecture is equivalent to saying that there are no binary sequences of length greater than 4 which are simultaneously of type 1 and of type 2.

Circulant modular Hadamard matrices of type 1 and type 2 were introduced in [6]. After finding that "type 2" was equivalent with the notion of "almost perfect sequence", we thought of abandoning the term "type 2", and replacing the term "type 1" by "enhanced". But we now choose to restore the type 1 / type 2 terminology, essentially because of the symmetry in the definition. We ask a little indulgence from the reader for these terminological meanderings.

Example 4.1.4 Here is a binary sequence of length 8 and type 2. Let $s = (1, 1, 1, -1, 1, -1, -1, 1)$. Then $\gamma_1(s) = \gamma_2(s) = \gamma_3(s) = 0$, showing that s is indeed a sequence of type 2. Additionally, $\gamma_4(s) = -4$. Taking H to be the circulant matrix with first row s, we have:

$$H = \begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 \end{pmatrix},$$

and

$$H \cdot H^T = \begin{pmatrix} 8 & 0 & 0 & 0 & -4 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 & -4 & 0 & 0 \\ 0 & 0 & 8 & 0 & 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 & 0 & -4 \\ -4 & 0 & 0 & 0 & 8 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 & 0 & 8 & 0 & 0 \\ 0 & 0 & -4 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & -4 & 0 & 0 & 0 & 8 \end{pmatrix}.$$

Another example of a binary sequence of length 8 and type 2 is provided by $t = (1, 1, 1, -1, 1, 1, 1, -1)$. In this case we have $\gamma_1(t) = \gamma_2(t) = \gamma_3(t) = 0$ and $\gamma_4(t) = 8$.

For every odd prime $p \equiv 1 \bmod 4$, we will exhibit circulant $(p-1)$-modular Hadamard matrices of type 1 and length $4p$. Then, turning our attention to moduli which are powers of 2, we will exhibit 16-modular Hadamard matrices of type 1 and length $4p$ for every odd prime $p \equiv 9 \bmod 16$ for which 2 is a fourth power mod p. Finally, we will recall a classical construction from Delsarte, Goethals and Seidel which implies that there is a circulant $(n-4)$-modular Hadamard matrix of type 2 for every size n of the form $n = 2(p^r + 1)$ where p is prime.

4.2 Circulant $(p-1)$-modular Hadamard matrices of type 1 and size $4p$

As announced above, we shall construct a circulant $(p-1)$-modular Hadamard matrix of type 1 and size $4p$, for every prime number $p \equiv 1 \bmod 4$. It is convenient to do so by exhibiting the Hall polynomial of its first row.

Consider the set $S = \{1, \ldots, p-1\}$ and its partition $S = S_0 \cup S_1$, where S_0 is the subset of squares mod p, and S_1 the subset of non-squares mod p. Of course, we have $|S_0| = |S_1| = \frac{p-1}{2}$. Let $g_0(z)$ denote the generating function of S_0. That is, $g_0(z) = \sum_{i \in S_0} z^i$.

Similarly, let $g_1(z) = \sum_{i \in S_1} z^i$ be the generating function of S_1. Note that, since $S = S_0 \coprod S_1$, we have $g_0(z) + g_1(z) = \sum_{i=1}^{p-1} z^i$.

Let $x_0, x_1, x_2, x_3 \in \{\pm 1\}$ be four free binary parameters, and consider the polynomial

$$h(z) = x_0(1+z^{2p})(1+g_0(z^2)) + x_1(1+z^{2p})z^p g_0(z^2) +$$
$$x_2(1-z^{2p})g_1(-z^2) + x_3(1-z^{2p})z^p(1+g_1(-z^2)),$$

viewed as an element in the quotient ring $\mathbf{Z}[z]/(z^{4p}-1)$.

As it turns out, when expressing $h(z)$ in the form $\sum_{i=0}^{4p-1} a_i z^i$, we have $a_i = \pm 1$ for all $0 \leq i \leq 4p-1$.

In [5], we prove the following result.

Theorem 4.2.1 *Let $p \equiv 1$ mod 4 be a prime number. Let $h(z) \in \mathbf{Z}[z]/(z^{4p}-1)$ be the above polynomial,*

$$h(z) = x_0(1+z^{2p})(1+g_0(z^2)) + x_1(1+z^{2p})z^p g_0(z^2) +$$
$$x_2(1-z^{2p})g_1(-z^2) + x_3(1-z^{2p})z^p(1+g_1(-z^2)).$$

Then $h(z)$ is the Hall polynomial of a 4-parameter binary sequence h of length $4p$, with the property that circ*(h) is a circulant $(p-1)$-modular Hadamard matrix of type 1 and size $4p$.*

The proof of the theorem in [5] is obtained by computing $h(z)h(z^{-1})$ explicitly in the ring $\mathbf{Z}[z]/(z^{4p}-1)$.

We find the following expression:

$$h(z)h(z^{-1}) = 4p + (p-1)R(z),$$

where $R(z) = 2\sum_{i=1}^{p-1} z^{4i} + x_0x_1(\sum_{i=1}^{2p} z^{2i-1} + z^p + z^{3p})$.

Given that $h(z)h(z^{-1}) = 4p + \sum_{j=1}^{4p-1} \gamma_j(h) z^j$, the above expression shows that the gcd of the periodic correlation coefficients $\gamma_i(h)$ of h for $i = 1, ..., 4p-1$, is equal to $p-1$. Note also that $\gamma_{2p} = 0$, showing that h is a binary sequence of type 1. Thus, as stated, *circ*(h) is a circulant $(p-1)$-modular Hadamard matrix of type 1 and size $4p$.

Example 4.2.2 Let $p = 5$. The non-zero squares mod 5 are 1 and 4. Therefore $S_0 = \{1, 4\}$, $g_0(z) = z + z^4$ and $g_1(z) = z^2 + z^3$. Finally,

$$h(z) \equiv x_0(1 + z^2 + z^8 + z^{10} + z^{12} + z^{18}) + x_1(z^3 + z^7 + z^{13} + z^{17})+$$

$$x_2(z^4 - z^6 - z^{14} + z^{16}) + x_3(z + z^5 + z^9 - z^{11} - z^{15} - z^{19}) \text{ mod } (z^{20} - 1),$$

so $h(z)$ is the Hall polynomial of the binary sequence

$$\begin{aligned} h \ = \ & (x_0, x_3, x_0, x_1, x_2, x_3, -x_2, x_1, x_0, x_3, x_0, -x_3, x_0, \\ & x_1, -x_2, -x_3, x_2, x_1, x_0, -x_3). \end{aligned}$$

The periodic correlation coefficients $\gamma_i = \gamma_i(h)$ for $i = 1, ..., 10$ are the following: $\gamma_1 = \gamma_3 = \gamma_7 = \gamma_9 = 4x_0x_1, \gamma_2 = \gamma_6 = \gamma_{10} = 0, \gamma_4 = \gamma_8 = 8, \gamma_5 = 8x_0x_1$.

4.3 Circulant 16-modular Hadamard matrices of type 1

Our objective is to construct circulant 16-modular Hadamard matrices of type 1 and size $4p$, where p is an odd prime. According to the Lemma below, this is only possible for $p \equiv 1$ mod 8, that is $p \equiv 1$ or 9 mod 16. When $p \equiv 1$ mod 16, the $(p - 1)$-modular construction of Section 4.2 already provides us with the desired sort of matrices, as $p - 1$ is divisible by 16.

In this Section we consider the remaining case $p \equiv 9$ mod 16. We shall present a partial solution to our construction problem, which works in the case where 2 is a fourth power mod p (for example $p = 73$ or 89). For those primes $p \equiv 9$ mod 16 where 2 is not a fourth power mod p (for example $p = 41$ or 137), we do not know how to construct 16-modular circulant Hadamard matrices of type 1 and size $4p$. Quite possibly, none exists in this case.

We start with the promised result restricting the possible sizes of circulant 16-modular Hadamard matrices of type 1.

Lemma 4.3.1 *Let $r \geq 1$ be a natural number, and assume there exists a circulant 16-modular Hadamard matrix of type 1 and size $4r$. Then $r \equiv 0$, 1 or 4 mod 8.*

Proof: Let $h(z)$ be the Hall polynomial of the first row h of a circulant 16-modular Hadamard matrix of type 1 and size $4r$. In the quotient ring $\mathbf{Z}[z](z^{4r} - 1)$, we have the general formula $h(z)h(z^{-1}) = 4r + \sum_{k=1}^{2r-1} \gamma_k(z^k + z^{-k}) + \gamma_{2r}z^{2r}$, where the γ_k are the periodic correlation coefficients of the sequence h. Setting $z = 1$ in the above formula, we get $h(1)^2 = 4r + 2\sum_{k=1}^{2r-1} \gamma_k + \gamma_{2r}$. Now, $\gamma_{2r} = 0$ by the type 1 hypothesis, and $\gamma_k \equiv 0 \bmod 16$ for all $1 \leq k \leq 2r-1$. It follows that $h(1)^2 = 4r + 32\theta$ for some integer θ. Thus $h(1)$ is even, and dividing by 4 we get $r = (h(1)/2)^2 + 8\theta$. The conclusion follows as the only squares mod 8 are 0, 1 and 4. As a side remark, note that the same argument would still work under the weaker hypothesis $\gamma_{2r} \equiv 0 \bmod 32$ instead of $\gamma_{2r} = 0$. □

Let p be a prime such that $p \equiv 1 \bmod 8$. As in Section 4.2, consider the set $S = \{1, \ldots, p-1\}$ and its partition $S = S_0 \cup S_1$, where S_0 is the subset of squares mod p, and S_1 the subset of non-squares mod p. For our purposes here, we need to refine this partition as follows.

Let $\rho : S \to \mathbf{F}_p^*$ denote the natural projection of S into the multiplicative group $\mathbf{F}_p^*$ of non-zero elements of the finite field $\mathbf{F}_p$.

Let $c \in \mathbf{F}_p^*$ denote a generator of that group, that is an element of multiplicative order $p-1$.

Given that the squares in $\mathbf{F}_p^*$ consist of the subgroup $\langle c^2 \rangle$ generated by c^2, we have $S_0 = \rho^{-1}(\langle c^2 \rangle)$ and $S_1 = \rho^{-1}(c\langle c^2 \rangle)$, where $c\langle c^2 \rangle$ is the other coset of $\langle c^2 \rangle$ in $\mathbf{F}_p^*$.

Consider now the subgroup $\Gamma = \langle c^4 \rangle \subset \mathbf{F}_p^*$. Thus, Γ is the only subgroup of order $(p-1)/4$ in $\mathbf{F}_p^*$. The four cosets of Γ in $\mathbf{F}_p^*$ are $\Gamma, c\Gamma, c^2\Gamma$ and $c^3\Gamma$, and of course they partition $\mathbf{F}_p^*$ into four pieces of equal size $(p-1)/4$. This partition refines the earlier one into squares and non-squares, as $\Gamma \cup c^2\Gamma = \langle c^2 \rangle$.

Transporting back the above partition to S by ρ^{-1}, we shall denote $S_{00} = \rho^{-1}(\Gamma), S_{10} = \rho^{-1}(c\Gamma), S_{01} = \rho^{-1}(c^2\Gamma)$ and $S_{11} = \rho^{-1}(c^3\Gamma)$.

In this way, we obtain the promised refinement of the partition $S = S_0 \cup S_1$, as $S_0 = S_{00} \cup S_{01}$ and $S_1 = S_{10} \cup S_{11}$. The four subsets $S_{u,v}$ all have cardinality $(p-1)/4$.

For $u, v = 0, 1$, we shall denote by $g_{u,v}(z)$ the generating function of $S_{u,v}$, that is $g_{u,v}(z) = \sum_{i \in S_{u,v}} z^i$. Note that $g_{00}(z) + g_{01}(z) + g_{10}(z) + g_{11}(z) = \sum_{i=1}^{p-1} z^i$.

Note also that $g_0(z) = g_{00}(z) + g_{01}(z)$ and $g_1(z) = g_{10}(z) + g_{11}(z)$, where $g_0(z)$ and $g_1(z)$ are the generating functions defined and used in Section 4.2.

Let $x_0, x_1, x_2, x_3 \in \{\pm 1\}$ be four free binary parameters, and consider the polynomial

$$h(z) = x_0(1+z^{2p})(1-g_{00}(z^2)-g_{01}(z^2))+x_1(1+z^{2p})z^p(g_{00}(z^2)-g_{01}(z^2))+$$
$$x_2(1-z^{2p})(g_{10}(-z^2)-g_{11}(-z^2))+x_3(1-z^{2p})z^p(1-g_{10}(-z^2)-g_{11}(-z^2)),$$

viewed as an element in the quotient ring $\mathbf{Z}[z]/(z^{4p}-1)$. As for the corresponding polynomial in Section 4.2, when expressing $h(z)$ in the form $\sum_{i=0}^{4p-1} a_i z^i$, we have $a_i = \pm 1$ for all $0 \leq i \leq 4p-1$.

In [7], we prove the following result.

Theorem 4.3.2 *Let $p \equiv 1$ mod 8 be a prime number. Furthermore, let $h(z) \in \mathbf{Z}[z]/(z^{4p}-1)$ be the above polynomial*

$$h(z) = x_0(1+z^{2p})(1-g_{00}(z^2)-g_{01}(z^2))+x_1(1+z^{2p})z^p(g_{00}(z^2)-g_{01}(z^2))+$$

$$x_2(1-z^{2p})(g_{10}(-z^2)-g_{11}(-z^2))+x_3(1-z^{2p})z^p(1-g_{10}(-z^2)-g_{11}(-z^2)).$$

Then $h(z)$ is the Hall polynomial of a 4-parameter binary sequence h of length $4p$, with the property that circ*(h) is a circulant 8-modular* Hadamard *matrix of type 1 and size $4p$. Moreover, the matrix* circ*(h) is a circulant 16-modular Hadamard matrix if and only if $p \equiv 9$ mod 16 and 2 is a fourth power mod p.*

The periodic correlations γ_k in $h(z)h(z^{-1}) = 4p+\sum_{k=1}^{2p-1}\gamma_k(z^k+z^{-k})$ are explicitly determined in [7], using Jacobi sums. They depend on the decomposition $p = a^2+b^2$ with b even, a odd and the sign of a normalized by the requirement $a \equiv 1$ mod 4.

With this normalization, the correlations γ_k, are all equal to $\pm(p-9)$, $\pm 2(a+3)$, or $\pm 2b$ for $k = 1, \ldots, 2p-1$. Furthermore, $\gamma_{2p} = 0$ showing that h is of type 1.

By a theorem of Gauss, a prime $p \equiv 1$ mod 8 is of the form $p = a^2+b^2$ with b divisible by 8 if and only if 2 is a fourth power modulo p. If follows that if $p \equiv 9$ mod 16 and 2 is a fourth power modulo p, then necessarily $a \equiv -3$ mod 8 and $b \equiv 0$ mod 8. Thus, in this case, all the periodic correlations $\gamma_k(h)$ for $k = 1, \ldots, 2p-1$ are divisible by 16, and $circ(h)$ is a circulant 16-modular Hadamard matrix of type 1 and size $4p$.

Example 4.3.3 The smallest prime $p \equiv 9$ mod 16 for which 2 is a fourth power mod p is $p = 73 = (-3)^2+8^2$. Setting $x_0 = x_1 = x_2 = x_3 = 1$ in the above formula for $h(z)$, we get the following binary sequence h, for which $circ(h)$ is a 16-modular Hadamard matrix of type 1 and size 292 :

$+ + - - - - - + - + - + - - - + - - - - + - + - - - + -$
$+ - + + - - - - - + - + + + + + - - - + - - - + - - - +$
$+ + + + - - + + - + - - + + - + - + - + - + - - + + - +$

$- - + + - + - + - - + + - - - + - - + + - + - + - + - -$
$+ - - + - - - - - - - - - - - - - - - + + - - + + + - +$
$- - - - - + + + - - - + - - - + + - - + + - - + - - - +$
$- - - - - - - + - - - + + - - + - - - + - - + + - - - -$
$- - + + - + - + - - + - - - - + + - - + - + - - - + - +$
$+ - - + - - + - - - + + + + - + - - - - - - - + - - + +$
$+ - - + - - - + - - + + + - + - - - + + + - - + - - - +$
$- - - + - - - + - - - +.$

4.4 Circulant modular Hadamard matrices of type 2

We are seeking binary sequences s of even length n with the property that $\gamma_1(s) = \ \dots \ = \gamma_{\frac{n}{2}-1}(s) = 0$. In this way, *circ*$(s)$ will be a circulant m-modular Hadamard matrix of type 2, with $m = \gamma_{\frac{n}{2}}(s)$.

These sequences were first introduced by J.Wolfmann [16] in 1992, and are called *almost perfect sequences*. See also Langevin [10]. (Recall that a sequence s of length $n \equiv 0 \bmod 4$ is *perfect* if it satisfies $\gamma_i(s) = 0$ for all $1 \leq i \leq n/2$. This is equivalent to *circ*(s) being a circulant Hadamard matrix. Hence, Ryser's conjecture amounts to saying that there is no perfect sequence of length $n \equiv 0 \bmod 4$ with $n > 4$.)

Almost perfect sequences are known in all lengths n of the form $n = 2(q+1)$ where q is an odd prime power, and are believed not to exist in other lengths. This follows from a theorem by Delsarte, Goethals and Seidel, establishing the existence of a negacyclic conference matrix of order $q+1$ for every odd prime power q. For convenience of the reader, this is recalled below.

Definition 4.4.1 A *conference matrix* C is a square matrix of size n, with entries 0 on the diagonal and ±1 elsewhere, satisfying the condition $C \cdot C^T {=} (n-1)I$.

Definition 4.4.2 A *negacyclic matrix* N is a square matrix of the form

$$N = NC(u_0, u_1, \dots, u_r) = \begin{pmatrix} u_0 & u_1 & \dots & \dots & u_r \\ -u_r & u_0 & u_1 & \dots & u_{r-1} \\ -u_{r-1} & -u_r & u_0 & \dots & u_{r-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -u_1 & -u_2 & \dots & -u_r & u_0 \end{pmatrix}.$$

Example 4.4.3 As an illustration of both concepts simultaneously, here is a negacyclic conference matrix of size 6:

$$C = \begin{pmatrix} 0 & 1 & 1 & 1 & -1 & 1 \\ -1 & 0 & 1 & 1 & 1 & -1 \\ 1 & -1 & 0 & 1 & 1 & 1 \\ -1 & 1 & -1 & 0 & 1 & 1 \\ -1 & -1 & 1 & -1 & 0 & 1 \\ -1 & -1 & -1 & 1 & -1 & 0 \end{pmatrix}.$$

Theorem 4.4.4 *(Delsarte-Goethals-Seidel,* [3]*) Let q be an odd prime power. Then there exists a negacyclic conference matrix of size $q+1$.*

Proof: (Sketch) Let g be a primitive element of the finite field $\mathbf{F}_{q^2}$, that is, a generator of the group $\mathbf{F}^*_{q^2}$ of non-zero elements.

Let $A = \begin{pmatrix} 0 & -g^{q+1} \\ 1 & g+g^q \end{pmatrix}$, with entries in the subfield $\mathbf{F}_q$ as $g \cdot g^q$ and $g+g^q$ are the norm and trace of g, respectively.

Let

$$v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The $q+1$ vectors $A^i \cdot v, 0 \leq i \leq q$, are pairwise independent over $\mathbf{F}_q$. Define the matrix C of size $q+1$ by

$$C_{i,j} = \chi(det(A^i \cdot v, A^j \cdot v))$$

for $0 \leq i,j \leq q$, where $\chi : \mathbf{F}_q \to \{0, \pm 1\}$ is the quadratic character of $\mathbf{F}^*_q$, extended by $\chi(0) = 0$.

Then C has entries 0 on the diagonal, and ± 1 elsewhere. Moreover, C is a conference matrix, that is $C \cdot C^T = qI$. Finally, let Γ be the alternating diagonal matrix $\Gamma = diag(1, -1, \ldots, 1, -1)$ of size $q+1$. As it turns out, the product $\Gamma \cdot C$ is a *negacyclic* conference matrix of size $q+1$, as desired. See [3] for more details. □

Theorem 4.4.5 *Let q be an odd prime power, and let $n = 2(q+1)$. There exists a binary sequence s of length n and of type 2, i.e. satisfying $\gamma_1(s) = \ldots = \gamma_{\frac{n}{2}-1}(s) = 0$. Moreover, $\gamma_{\frac{n}{2}}(s) = 4 - n$.*

Proof: Given a binary sequence $s' = (x_1, x_2, \ldots, x_q)$ of length q, define the sequence $s = [1; s'; 1; -s']$ of length $n = 2q+2$. An easy calculation shows that $\gamma_{n/2}(s) = 4 - n$, and that $\gamma_k(s) = 2(c_k(s') -$

$c_{q+1-k}(s'))$ for all $1 \leq k \leq q$, where $c_k(s') = \sum_{j=1}^{q-k} x_j x_{j+k}$ denote the k^{th} *aperiodic* correlation coefficient of the sequence s'. Thus, the sequence s will be of type 2 if and only if $c_k(s') = c_{q+1-k}(s')$ for all $1 \leq k \leq q$.

Now, the latter condition on s' is equivalent to the negacyclic matrix $N = NC(0, x_1, x_2, \ldots, x_q)$ being a conference matrix, as the dot product of the ith row and the $(i+k)$th row of N is equal to $c_k(s') - c_{q+1-k}(s')$. By the result of Delsarte, Goethals and Seidel, there exists a negacyclic conference matrix $C = NC(0, y_1, \ldots, y_q)$ of size $q+1$. Let $s' = (y_1, \ldots, y_q)$, and $s = [1; s'; 1; -s']$. From the above discussion, it follows that s is a binary sequence of type 2 and length n, as desired. □

Acknowledgement

The first author gratefully acknowledges partial support from the Fonds National Suisse de la Recherche Scientifique during the preparation of this paper.

Shalom Eliahou
Département de Mathématiques,
Université du Littoral Côte d'Opale,
Bâtiment Poincaré, 50 rue Ferdinand Buisson, B.P. 699, 62228 Calais, France,
eliahou@lmpa.univ-littoral.fr

Michel Kervaire
Département de Mathématiques,
Université de Genève,
2 rue du Lièvre, B.P. 240, 1211 Genève 24, Suisse.
Michel.Kervaire@math.unige.ch

References

[1] Terry H. A.; Ralph G. S., *Golay sequences*, Lect. Notes Math., **622** (1977), 44-54.

[2] Borwein P. B.; Ferguson R. A., *A complete description of Golay pairs for lengths up to 100*, Math. Comput., **47** (2004), 967-985.

[3] Delsarte P.; Goethals J.-M.; Seidel J., *Orthogonal matrices with zero diagonal. II*, Can. J. Math., **XXIII** (1971), 816-832.

[4] Dinitz J. H.; Stinton D. R., Contemporary Design Theory, A Collection of Surveys, Wiley-Interscience Publication, 1992.

[5] Eliahou S.; Kervaire M., *Circulant Modular Hadamard matrices*, Ens. Math., **47** (2001), 103-114.

[6] Eliahou S.; Kervaire M., *Modular Sequences and Modular matrices*, J. of Comb. Designs, **9** (2001), 187-214.

[7] Eliahou S.; Kervaire M., *Circulant 16-modular Hadamard matrices and Jacobi sums*, J. Comb. Theory, **100** (2002), 116-135.

[8] Eliahou S.; Kervaire M.; Saffari B., *On Golay polynomial pairs*, Adv. Applied Math., **12** (1991), 235-292.

[9] Hadamard J., *Résolution d'une question relative aux déterminants*, Bulletin des Sciences Mathématiques, **17** (1893), 240-246.

[10] Langevin P., *Almost perfect binary functions*, App. Alg. Eng. Comm. Comp., **4** (1993), 95-102.

[11] Marrero O.; Butson A. T., *Modular Hadamard matrices and related designs*, J. Comb. Theory, **15** (1973), 257-269.

[12] Marrero O.; Butson A. T., *Modular Hadamard matrices and related designs, II*, Can. J. Math., **XXIV** (1972), 1100-1109.

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

[14] Schmidt B., *Cyclotomic integers and finite geometry*, J. of the Amer. Math. Soc., **12** (1999), 929-952.

[15] Turyn R. J., *Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression and surface wave encoding*, J. Comb. Theory, **16** (1974), 313-333.

[16] Wolfmann J., *Almost perfect autocorrelation sequences*, IEEE Trans. Inform. Theory, **38** (1992), 1412-1418.

[17] Van Lint J. H.; Wilson R. M., A course in combinatorics, Cambridge University Press, 1992.