Designs, Codes and Cryptography, 4, 327–340 (1994)


# On Sequences with Zero Autocorrelation

C. KOUKOUVINOS
*Department of Mathematics, National Technical University of Athens, Zografou 157 73, Athens, Greece*

S. KOUNIAS
*Department of Mathematics, University of Athens, Panepistemiopolis 15784, Greece*

J. SEBERRY
*Department of Computer Science, University of Wollongong, Wollongong, NSW, 2522, Australia*

C. H. YANG
*Department of Mathematical Sciences, State University of New York, Oneonta, New York 13829, USA*

J. YANG
*Department of Computer Science and Computer Science Division of Electrical Engineering, University of California, Berkeley, CA 94720, USA*

**Editor:** D. Jungnickel

*Received May 3, 1993; Revised November 24, 1993*

**Abstract.** Normal sequences of lengths $n = 18, 19$ are constructed. It is proved through an exhaustive search that normal sequences do not exist for $n = 17, 21, 22, 23$. Marc Gysin has shown that normal sequences do not exist for $n = 24$. So the first unsettled case is $n = 27$.

Base sequences of lengths $2n-1, 2n-1, n, n$ are constructed for all decompositions of $6n-2$ into four squares for $n = 2, 4, 6, \ldots, 20$ and some base sequences for $n = 22, 24$ are also given. So T-sequences (T-matrices) of length 71 are constructed here for the first time. This gives new Hadamard matrices of orders 213, 781, 1349, 1491, 1633, 2059, 2627, 2769, 3479, 3763, 4331, 4899, 5467, 5609, 5893, 6177, 6461, 6603, 6887, 7739, 8023, 8591, 9159, 9443, 9727, 9869.

## 1. Introduction

Given the sequence $A = \{a_1, a_2, \ldots, a_n\}$ of length $n$ the non-periodic autocorrelation function $N_A(s)$ is defined as

$$N_A(s) = \sum_{i=1}^{n-s} a_i a_{i+s}, \qquad s = 0, 1, \ldots, n-1. \tag{1}$$

If $A(z) = a_1 + a_2 z + \cdots + a_n z^{n-1}$ is the associated polynomial of the sequence $A$, then

$$A(z)A(z^{-1}) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_i a_j z^{i-j} = N_A(0) + \sum_{s=1}^{n-1} N_A(s)(z^s + z^{-s}), \ z \neq 0. \tag{2}$$

If $A^* = \{a_n, \ldots, a_1\}$ is the reversed sequence, then

$$A^*(z) = z^{n-1} A(z^{-1}). \tag{3}$$

Base, Turyn, Golay and normal sequences are finite sequences, with zero autocorrelation function, useful in constructing orthogonal designs and Hadamard matrices [6], in communications engineering [18], in optics and signal transmission problems [7], [11], etc.

If $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$ are two binary $(1, -1)$ sequences of length $n$ and

$$N_A(s) + N_B(s) = 0 \quad \text{for } s = 1, \ldots, n-1 \tag{4}$$

then $A, B$ are called *Golay sequences* of length $n$ (abbreviated GS($n$)). See [5], [6], [7].

From this definition and relation (2) we conclude that two $(1, -1)$ sequences of length $n$ are GS($n$) if and only if

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) = 2n, \qquad z \neq 0. \tag{5}$$

Golay sequences GS($n$) exist for $n = 2^a 10^b 26^c$ (Golay numbers) where $a, b, c$ are non-negative integers [5], [7], [8], [18].

The four sequences $A, B, C, D$ of lengths $n+p, n+p, n, n$ with entries $+1, -1$ are called *base sequences* if:

$$\begin{aligned} N_A(s) + N_B(s) + N_C(s) + N_D(s) &= \begin{cases} 0, & s = 1, \ldots, n-1 \\ 4n + 2p, & s = 0 \end{cases} \\ N_A(s) + N_B(s) &= 0, \qquad s = n, \ldots, n+p-1. \end{aligned} \tag{6}$$

Equivalently, (6) can be replaced by

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) + C(z)C(z^{-1}) + D(z)D(z^{-1}) = 4n + 2p, \quad z \neq 0 \tag{7}$$

where $A(z)$, $B(z)$, $C(z)$, $D(z)$ are the associated polynomials. Base sequences of lengths $n+1, n+1, n, n$ are denoted by BS($2n+1$). From (7) and for $p = 1$, if we set $z = 1$ we obtain

$$a^2 + b^2 + c^2 + d^2 = 4n + 2 \tag{8}$$

where $a, b, c, d$ are the sum of the elements of $A, B, C, D$ respectively. BS($2n+1$) for all decompositions of $4n+2$ into four squares for $n = 1, 2, \ldots, 24$ are given in [1], [12], [13]. Also BS($2n+1$) for $n = 25, 26, 29$ and $n = 2^a 10^b 26^c$ (Golay numbers) are given in Yang [23]. If the sequences $A, B, C, D$ are BS($2n+1$) and satisfy

$$N_{AC}(s-1) + N_{CA}(s) = 0, \qquad s = 1, \ldots, n \tag{9}$$

then they are called *Turyn sequences* (abbreviated as TS$(2n+1)$), where

$$N_{AC}(s)=\sum_{i=1}^{n-s} a_i c_{i+s}, \quad N_{CA}(s)=\sum_{i=1}^{n+1-s} c_i a_{i+s}, \qquad s=0,1,\ldots,n \tag{10}$$

are the cross-correlations.

TS$(2n+1)$ exist for $n \leq 7$, $n=12, 14$. They cannot exist for $n=10, 11, 16, 17$ and for $n=8, 9, 13, 15$, TS$(2n+1)$ might exist but an exhaustive machine search showed that they do not exist (see [1], [6, pp. 142–143]). Koukouvinos, Kounias and Sotirakoglou [13] developed an algorithm and proved through an exhaustive search that Turyn sequences do not exist for $n=18, 19, \ldots, 27$. Edmondson [3], [4] has extended this further to show they do not exist for any new order $\leq 42$, so the first unsettled case is 43.

*6-base sequences*, denoted BS$(n, n, n, n; n-1, n-1)$ of lengths $n, n, n, n, n-1, n-1$ are six sequences of $\pm 1$ with zero non-periodic autocorrelation function.

*Definition 1.* The four sequences $X, Y, Z, W$ of length $n$ with entries $0, 1, -1$ are called *T-sequences* if

$$\text{(i)} \quad |x_i|+|y_i|+|z_i|+|w_i|=1, \qquad i=1,\ldots,n \tag{11}$$

$$\text{(ii)} \quad N_X(s)+N_Y(s)+N_Z(s)+N_W(s)=\begin{cases} 0, & s=1,\ldots,n-1 \\ n, & s=0 \end{cases}$$

Yang [22] gives another name for T-sequences and calls them four-symbol $\delta$-codes. He also calls the quadruple $Q=X+Y$, $R=X-Y$, $S=Z+W$, $T=Z-W$ regular $\delta$-code of length $n$, where $X, Y, Z, W$ are T-sequences of length $n$.

If Williamson type matrices of size $w$ exist and T-sequences of length $n$ exist, then Hadamard matrices of size $4nw$ can be constructed (Cooper and (Seberry) Wallis [2]).

If $X(z)$, $Y(z)$, $Z(z)$, $W(z)$ are the associated polynomials, then from Definition 1 and (2) we see that (ii) can be replaced by

$$X(z)X(z^{-1})+Y(z)Y(z^{-1})+Z(z)Z(z^{-1})+W(z)W(z^{-1})=n, \quad z\neq 0. \tag{12}$$

We use the notation $(A/B)$ for the sequence $\{a_1, b_1, \ldots, a_n, b_n\}$ and $(A, B)$ for the sequence $\{a_1, \ldots, a_n, b_1, \ldots, b_n\}$.

## 2. On Normal Sequences

*Definition 2.* A triple $(F; G, H)$ of sequences is said to be a set of *normal sequences* for length $n$ (abbreviated as NS$(n)$) if the following conditions are satisfied.

(i) $F=(f_k)$ is a $(1,-1)$ sequence of length $n$.

(ii) $G = (g_k)$ and $H = (h_k)$ are sequences of length $n$ with entries $0, 1, -1$, such that $G + H = (g_k + h_k)$ is a $(1, -1)$ sequence of length $n$.

(iii) $N_F(s) + N_G(s) + N_H(s) = 0, s = 1, \dots, n-1$.

Condition (iii) is also equivalent to

$$F(z)F(z^{-1}) + G(z)G(z^{-1}) + H(z)H(z^{-1}) = 2n, \qquad z \neq 0. \tag{13}$$

In Theorem 1 we prove that the sequences $G$ and $H$ of Definition 2 are *quasi-symmetric*, i.e. if $g_k = 0$, then $g_{n+1-k} = 0$ and also if $h_k = 0$, then $h_{n+1-k} = 0$. This theorem means that the definition of normal sequences in [23] can be relaxed.

THEOREM 1 *If* $(F; G, H)$ *are NS(n), then*

$$\begin{aligned} g_s + g_{n-s+1} &\equiv 0 \pmod 2 \\ h_s + h_{n-s+1} &\equiv 0 \pmod 2 \end{aligned} \qquad s = 1, \dots, \left[\tfrac{n}{2}\right]$$

**Proof:** We have

$$\sum_{i=1}^{n-s}(f_i f_{i+s} + g_i g_{i+s} + h_i h_{i+s}) = 0, \qquad s = 1, \dots, n-1$$

but $f_i = \pm 1$ and so $f_i f_{i+s} = f_i + f_{i+s} - 1 + 4p$, $(p = 0, 1)$ but

$$\begin{aligned} 2(g_i g_{i+s} + h_i h_{i+s}) &= (g_i + h_i)(g_{i+s} + h_{i+s}) + (g_i - h_i)(g_{i+s} - h_{i+s}) \\ &= g_i + h_i + g_{i+s} + h_{i+s} + g_i - h_i + g_{i+s} - h_{i+s} - 2 + 4q, \\ &\quad (q = 0, 1) \\ &= 2(g_i + g_{i+s} - 1) + 4q. \end{aligned}$$

So we have

$$\begin{aligned} g_i g_{i+s} + h_i h_{i+s} &= g_i + g_{i+s} - 1 + 2q \equiv g_i + g_{i+s} - 1 \pmod 2 \\ &= h_i + h_{i+s} - 1 + 2r \equiv h_i + h_{i+s} - 1 \pmod 2 \end{aligned}$$

and so

$$\begin{aligned} f_i f_{i+s} + g_i g_{i+s} + h_i h_{i+s} &\equiv f_i + f_{i+s} + g_i + g_{i+s} - 2 \pmod 2 \\ &\equiv (f_i + f_{i+s} + g_i + g_{i+s}) \pmod 2 \end{aligned}$$

and

$$\sum_{i=1}^{n-s} f_i + \sum_{i=s+1}^{n} f_i + \sum_{i=1}^{n-s} g_i + \sum_{i=s+1}^{n} g_i \equiv 0 \pmod 2, \quad s = 1, \dots, n-1. \tag{14}$$

Similarly, if we set $s-1$ instead of $s$, we have

$$\sum_{i=1}^{n-s+1} f_i + \sum_{i=s}^{n} f_i + \sum_{i=1}^{n-s+1} g_i + \sum_{i=s}^{n} g_i \equiv 0 \pmod 2, \; s = 2, \ldots, n. \tag{15}$$

From (14) and (15) ((15) - (14)) we obtain

$$f_{n-s+1} + f_s + g_{n-s+1} + g_s \equiv 0 \pmod 2, \; s = 2, \ldots, n-1. \tag{16}$$

The relation (16) is still valid and for $s = n$, because

$$f_1 f_n + g_1 g_n + h_1 h_n = 0$$

but $f_s + f_{n-s+1} \equiv 0 \pmod 2$, and so from (16) we obtain

$$g_s + g_{n-s+1} \equiv 0 \pmod 2, \qquad s = 1, \ldots, \left[\frac{n}{2}\right].$$

Similarly, using the same argument as before, we obtain

$$h_s + h_{n-s+1} \equiv 0 \pmod 2, \qquad s = 1, \ldots, \left[\frac{n}{2}\right].$$

■

In Theorem 2 we prove that if $L = A + B$ is a sequence of real numbers with symmetric $A$ and skew $B$, then

$$L(z)L(z^{-1}) = A(z)A(z^{-1}) + B(z)B(z^{-1}), \text{ for all } \; z \neq 0.$$

THEOREM 2 *If $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$ are two sequences of length n, where n is even, A is symmetric i.e. $a_i = a_{n+1-i}$, B is skew symmetric i.e. $b_i = -b_{n+1-i}$ and $L = \{l_1, \ldots, l_n\}$, $l_i = a_i + b_i$, then*

$$L(z)L(z^{-1}) = A(z)A(z^{-1}) + B(z)B(z^{-1}), \quad z \neq 0.$$

**Proof:** Since $A$ is symmetric and $B$ is skew symmetric we have for $n = 2m$, writing $X^*$ for the reverse of the sequence $X$,

$$A = (A_1, A_1^*), \qquad B = (B_1, -B_1^*),$$

where $A_1 = \{a_1, \ldots, a_m\}$, $B_1 = \{b_1, \ldots, b_m\}$.

So we have

$$\begin{aligned} A(z) &= A_1(z) + z^m A_1^*(z) &= A_1(z) + z^{2m-1} A_1(z^{-1}) \\ B(z) &= B_1(z) - z^m B_1^*(z) &= B_1(z) - z^{2m-1} B_1(z^{-1}) \end{aligned}$$

and

$$\begin{aligned} A(z)B(z^{-1}) &= \left(A_1(z) + z^{2m-1} A_1(z^{-1})\right)\left(B_1(z^{-1}) - z^{-2m+1} B_1(z)\right) \\ &= A_1(z)B_1(z^{-1}) + z^{2m-1} A_1(z^{-1}) B_1(z^{-1}) \\ &\quad - z^{-2m+1} A_1(z) B_1(z) - A_1(z^{-1}) B_1(z) \\ &= -\left(A_1(z^{-1}) + z^{-2m+1} A_1(z)\right)\left(B_1(z) - z^{2m-1} B_1(z^{-1})\right) \\ &= -A(z^{-1})B(z) \end{aligned}$$

or

$$\begin{aligned} L(z)L(z^{-1}) &= (A(z)+B(z))\left(A(z^{-1})+B(z^{-1})\right) \\ &= A(z)A(z^{-1})+A(z)B(z^{-1})+B(z)A(z^{-1})+B(z)B(z^{-1}) \\ &= A(z)A(z^{-1})+B(z)B(z^{-1}). \end{aligned}$$

■

In Theorem 3 we prove that from a given pair of Golay sequences GS(n): $(F, H)$, we can obtain two sets of normal sequences, $(F;\, H,\, O_n)$ and $(F;\, L,\, M)$, where $L$ and $M$ are respectively the symmetric and skew parts of $H$. Therefore, a set of normal sequences can be regarded as a generalization of a pair of Golay sequences.

THEOREM 3 *If $F$, $H$ are Golay sequences of length $n$, then the following two sets*

(i) $(F;\, H,\, O_n)$,

(ii) $(F;\, L,\, M)$

*are $NS(n)$, where $L$ and $M$ are respectively the symmetric and skew parts of $H$.*

**Proof:**

(i) The sequences $F$, $H$ and $O_n$ (a sequence of $n$ zeros) satisfy the conditions (i) and (ii) of Definition 2. Also we have

$$\begin{aligned} F(z)F(z^{-1})+H(z)H(z^{-1})+O_n(z)O_n(z^{-1}) &= F(z)F(z^{-1})+H(z)H(z^{-1}) \\ &= 2n. \end{aligned}$$

(ii)

$$L=(l_k), \quad \text{where } l_k=\begin{cases} h_k & \text{if } h_k=h_{n+1-k} \\ 0 & \text{if } h_k=-h_{n+1-k} \end{cases}$$

$$M=(m_k), \quad \text{where } m_k=\begin{cases} h_k & \text{if } h_k=-h_{n+1-k} \\ 0 & \text{if } h_k=h_{n+1-k} \end{cases}$$

i.e. $L$ and $M$ are respectively the symmetric and skew parts of $H$. Then $H(z) = L(z)+M(z)$, $H(z)H(z^{-1}) = L(z)L(z^{-1})+M(z)M(z^{-1})$ and so we have

$$\begin{aligned} F(z)F(z^{-1})+L(z)L(z^{-1})+M(z)M(z^{-1}) &= F(z)F(z^{-1})+H(z)H(z^{-1}) \\ &= 2n. \end{aligned}$$

■

In Theorem 4 we prove that we can obtain sets of normal sequences NS($2m+1$): $(A/C;\, B/O_m,\, O_{m+1}/D)$ from Turyn sequences TS($2m+1$): $(A,\, B;\, C,\, D)$ with lengths $m+1, m+1, m, m$. Where for even $m$ $A$ is symmetric and $C$ skew, and for odd $m$ $A$ is skew and $C$ symmetric. TS($2m+1$) can be written as:

1. For $m$ odd

$$A=\{A_1, -A_1^*\}, \qquad B=\{b_1, B_1, -B_1^*, b_1\},$$
$$C=\left\{C_1, c_{\frac{m+1}{2}}, C_1^*\right\}, \quad D=\left\{D_1, d_{\frac{m+1}{2}}, D_1^*\right\}$$

where

$$\begin{aligned} A_1 &= \{a_1, \ldots, a_{\frac{m+1}{2}}\}, \ B_1 = \{b_2, \ldots, b_{\frac{m+1}{2}}\}, \\ C_1 &= \left\{c_1, \ldots, c_{\frac{m-1}{2}}\right\}, \ D_1 = \left\{d_1, \ldots, d_{\frac{m-1}{2}}\right\} \end{aligned}$$

2. For $m$ even

$$\begin{aligned} &A = \{A_1, a_{\frac{m}{2}+1}, A_1^*\}, \quad B = \{b_1, B_1, b_{\frac{m}{2}+1}, B_1^*, -b_1\}, \\ &C = \{C_1, -C_1^*\}, \qquad D = \{D_1, -D_1^*\} \end{aligned}$$

where

$$\begin{aligned} &A_1 = \{a_1, \ldots, a_{\frac{m}{2}}\}, \quad B_1 = \{b_2, \ldots, b_{\frac{m}{2}}\}, \\ &C_1 = \{c_1, \ldots, c_{\frac{m}{2}}\}, \quad D_1 = \{d_1, \ldots, d_{\frac{m}{2}}\}. \end{aligned}$$

THEOREM 4 *If $A, B, C, D$ are Turyn sequences of lengths $m+1, m+1, m, m$ (TS(2m+1)), i.e.*

(i) $A(z)A(z^{-1}) + B(z)B(z^{-1}) + C(z)C(z^{-1}) + D(z)D(z^{-1}) = 4m + 2$

(ii) $A(z)C(z^{-1}) + zC(z)A(z^{-1}) = 0$

*for all $z \neq 0$.*

*Then the sequences $F = A/C$, $G = B/O_m$, $H = O_{m+1}/D$ are $NS(2m+1)$, where*

$$\begin{aligned} A/C &= \{a_1, c_1, a_2, c_2, \ldots, a_m, c_m, a_{m+1}\} \\ B/O_m &= \{b_1, 0, b_2, 0, \ldots, b_m, 0, b_{m+1}\} \\ O_{m+1}/D &= \{0, d_1, 0, d_2, \ldots, 0, d_m, 0\} \end{aligned}$$

**Proof:**

$$\begin{aligned} &F = A/C, &&\text{so } F(z) = A(z^2) + zC(z^2) \\ &G = B/O_m, &&\text{so } G(z) = B(z^2) \\ &H = O_{m+1}/D, &&\text{so } H(z) = zD(z^2). \end{aligned}$$

So we have

$$\begin{aligned} &F(z)F(z^{-1}) + G(z)G(z^{-1}) + H(z)H(z^{-1}) \\ &= A(z^2)A(z^{-2}) + C(z^2)C(z^{-2}) + B(z^2)B(z^{-2}) + D(z^2)D(z^{-2}) \\ &\quad + zC(z^2)A(z^{-2}) + z^{-1}A(z^2)C(z^{-2}) \\ &= 4m + 2. \end{aligned}$$

■

Normal sequences do not exist for $n = 2^{2a-1}(8b + 7)$, $a, b$ non-negative integers as the numbers $4^a(8b + 7)$ cannot be written as the sum of three squares. In particular $n \neq 14, 30, 46, 56, 62, 78, 94, \ldots$ It is known that NS(6) does not exist. Yang [23] has given these sequences for $n = 3, 5, 7, 9, 11, 12, 13, 15, 25, 29$ and he notes they exist for $n = 2^a 10^b 26^c$ (Golay numbers).

NS($n$) have not been found for $n \geq 17$ (except $n = 25, 29$ and $g$ where $g$ is a Golay number). This means we can construct T-sequences of length $(2n + 1)t$, if a new set of NS($n$) can be found, where $t = 2s + 1$ is the length of base sequences (BS($2s + 1$)).

In this paper we construct NS($n$) for $n = 18, 19$. It is also proved through an exhaustive search that NS($n$) do not exist for $n = 17, 21, 22, 23$. Marc Gysin [9], [10] has shown that normal sequences do not exist for $n = 24$. Hence the first unsettled case is $n = 27$.

Therefore we know these sequences

(i) exist for $n \in \{1, 2, \ldots, 5, 7, 8, \ldots, 13, 15, 16, 18, 19, 20, 25, 26, 29, 32, \ldots\}$;

(ii) do not exist for $n \in \{6, 14, 17, 21, 22, 23, 24, 30, 46, 56, 62, 78, 94, \ldots\}$.

(iii) $n \in \{27, 28, 31, \ldots, \}$ are undecided.

We now formally prove Theorem 5:

THEOREM 5 *If $(F; G, H)$ are NS(n), then the following $(1, -1)$ sequences $A = (F, 1)$, $B = (F, -1)$, $C = G + H$, $D = G - H$ of lengths $n + 1, n + 1, n, n$ respectively are BS(2n+1) and vice versa.*

**Proof:** We have

$$\begin{aligned} A(z) &= F(z) + z^n \\ B(z) &= F(z) - z^n \\ C(z) &= G(z) + H(z) \\ D(z) &= G(z) - H(z) \end{aligned} \tag{17}$$

From (17) we obtain

$$\begin{aligned} &A(z)A(z^{-1}) + B(z)B(z^{-1}) + C(z)C(z^{-1}) + D(z)D(z^{-1}) \\ &= (F(z) + z^n)(F(z^{-1}) + z^{-n}) + (F(z) - z^n)(F(z^{-1}) - z^{-n}) \\ &\quad + (G(z) + H(z))(G(z^{-1}) + H(z^{-1})) + (G(z) - H(z))(G(z^{-1}) - H(z^{-1})) \\ &= 2(F(z)F(z^{-1}) + G(z)G(z^{-1}) + H(z)H(z^{-1})) + 2 \\ &= 4n + 2, \end{aligned}$$

i.e. $A, B, C, D$ are BS($2n + 1$).

The converse of the theorem is immediate from the first part and need not be proved separately. ■

We carried out a computer search by appropriately modifying the algorithm given in [13]. The original searches were carried out on an IBM 4361 running VM/CMS at the University of Thessalonica, Greece in 1989.

**Results:** With the application of our algorithm and using Theorem 5, the following normal sequences NS($n$) have been found for $n = 18$ and 19.

$$\begin{aligned} n = 18.\quad & F = (+ + + + + - - + + - - + - + + - + -) \\ & G = (+00 - 0 - 00 + +00 + 0 + 00+) \\ & H = (0 + +0 - 0 + +00 + -0 - 0 - +0) \end{aligned}$$

$$\begin{aligned} n = 19.\quad & F = (+ - - + + + - - - - + + + + + + + - +) \\ & G = (00 - 0 + - + 0 + - + 0 + + - 0 + 00) \\ & H = (- + 0 - 000 + 000 + 000 + 0 - +) \end{aligned}$$

where + stands for 1 and − for −1.

We note that these normal sequences of lengths 18 and 19 are unique up to equivalence.

Also with the application of our algorithm it is proved through an exhaustive search that normal sequences do not exist for $n = 17, 21, 22, 23$.

## 3. On Base Sequences

We give a formal proof of a well-known result.

THEOREM (Turyn [18]) *If $X, Y, Z, W$ are $(1, -1)$ sequences of lengths $n, n, n$ and $n - 1$ respectively and satisfy the condition*

$$N_X(s) + N_Y(s) + 2N_Z(s) + 2N_W(s) = 0, \qquad s \neq 0$$

*i.e. if the sequences $X, Y, Z, Z; W, W$ are 6-base sequences $(6-BS(n, n, n, n; n-1, n-1))$ then the following $(1, -1)$ sequences*

$$A = (Z; W), \qquad B = (Z; -W), \qquad C = X, \qquad D = Y,$$

*of lengths $2n - 1, 2n - 1, n, n$ respectively are base sequences $(BS(3n - 1))$.*

**Proof:** We have

$$\begin{aligned} A(z) &= Z(z) + z^n W(z) \\ B(z) &= Z(z) - z^n W(z) \\ C(z) &= X(z) \\ D(z) &= Y(z) \end{aligned} \tag{18}$$

Since $X, Y, Z, Z; W, W$ are 6-BS$(n, n, n, n; n - 1, n - 1)$ we have

$$X(z)X(z^{-1}) + Y(z)Y(z^{-1}) + 2Z(z)Z(z^{-1}) + 2W(z)W(z^{-1}) = 6n - 2, \quad z \neq 0. \tag{19}$$

From (18) we obtain

$$\begin{aligned}
&A(z)A(z^{-1}) + B(z)B(z^{-1}) + C(z)C(z^{-1}) + D(z)D(z^{-1}) \\
&= \left(Z(z) + z^n W(z)\right)\left(Z(z^{-1}) + z^{-n} W(z^{-1})\right) \\
&\quad + \left(Z(z) - z^n W(z)\right)\left(Z(z^{-1}) - z^{-n} W(z^{-1})\right) \\
&\quad + X(z)X(z^{-1}) + Y(z)Y(z^{-1}) \\
&= X(z)X(z^{-1}) + Y(z)Y(z^{-1}) + 2Z(z)Z(z^{-1}) + 2W(z)W(z^{-1}) \\
&= 6n - 2, \qquad z \neq 0 \quad \text{(because of (19))},
\end{aligned}$$

i.e. $A, B, C, D$ are BS$(3n-1)$. ■

*Remark 1.* We note that from the $6 - BS(24, 24, 24, 24; 23, 23)$ $X$, $Y$, $Z$, $Z$, $W$, $W$, T-sequences (T-matrices) $T_1 = (Z, 0_{47})$, $T_2 = (0_{24}, W, 0_{24})$, $T_3 = (0_{47}, (X + Y)/2)$, and $T_4 = (0_{47}, (X - Y)/2)$, of length 71 are constructed here for the first time ($0_t$ is the sequence of $t$ zeros). These give new Hadamard matrices of orders 213, 781, 1349, 1491, 1633, 2059, 2627, 2769, 3479, 3763, 4331, 4899, 5467, 5609, 5893, 6177, 6461, 6603, 6887, 7739, 8023, 8591, 9159, 9443, 9727, 9869 see also [15] and [16, p. 452, pp. 481–482]).

THEOREM 7 *Suppose there are four* $(1, -1)$ *sequences* $X$, $Y$, $Z$, $W$ *of lengths* $n, n, n, n-1$ *respectively which satisfy the condition*

$$N_X(s) + N_Y(s) + 2N_Z(s) + 2N_W(s) = 0, \qquad s \neq 0.$$

*Then* $n$ *can only be even or 1. If* $n$ *is even,* $x + y \equiv 2 \pmod 4$ *where* $x, y$ *are the sum of the elements of sequences* $X$ *and* $Y$ *respectively. Further*

$$x_s x_{n-s+1} + y_s y_{n-s+1} = 0, \qquad s = 2, \ldots, \left[\frac{n}{2}\right].$$

**Proof:** Write $X = \{x_i\}$, $Y = \{y_i\}$, $Z = \{z_i\}$, $i = 1, 2, \ldots, n$, $W = \{w_j\}$, $j = 1, 2, \ldots, n-1$. We consider the autocorrelation function and use the fact that if $x, y$ are $\pm 1$, $x + y \equiv xy + 1 \pmod 4$. $N(n-1) = x_1 x_n + y_1 y_n + 2z_1 z_n = 0$. Hence

$$x_1 + y_1 + x_n + y_n - 2 + 2z_1 z_n \equiv 0 \pmod 4$$

$$x_1 + y_1 + x_n + y_n \equiv 0 \pmod 4 \tag{20}$$

$$N(n-2) = x_1 x_{n-1} + x_2 x_n + y_1 y_{n-1} + y_2 y_n + 2z_1 z_{n-1} + 2z_2 z_n + 2w_1 w_{n-1}$$

Hence

$$x_1 + y_1 + x_2 + y_2 + x_{n-1} + y_{n-1} + x_n + y_n \equiv 2 \pmod 4$$

and using (20) we have

$$x_2 + y_2 + x_{n-1} + y_{n-1} \equiv 2 \pmod 4. \tag{21}$$

$N(n-3)$ gives

$$x_1 + x_2 + x_3 + y_1 + y_2 + y_3 + x_{n-2} + x_{n-1} + x_n + y_{n-2} + y_{n-1} + y_n \equiv 0 \bmod 4)$$

and hence

$$x_3 + y_3 + x_{n-2} + y_{n-2} \equiv 2 \pmod 4.$$

Assume that for $t > 1, t < \left[\frac{n}{2}\right]$

$$x_t + y_t + x_{n-t+1} + y_{n-t+1} \equiv 2 \pmod 4.$$

Then noting $N(n-t)$, for $t < \left[\frac{n}{2}\right]$, is

$$\begin{aligned} x_1 + \cdots + x_t + y_1 + \cdots y_t + x_{n-t+1} + \cdots + x_n + y_{n-t+1} + \cdots + y_n \\ \equiv 2(t-1) \pmod 4 \end{aligned}$$

we consider $N(n-t-1)$ which gives, after noting that the $Z$ and $W$ sequences contribute $2t+1$ terms each twice or a total of 2(mod 4),

$$x_1 + \cdots + x_{t+1} + y_1 + \cdots + y_{t+1} + x_{n-t} + \cdots + x_n + y_{n-t} + \cdots + y_n \equiv 2t \pmod 4.$$

Using the assumption we have

$$x_{t+1} + y_{t+1} + x_{n-t} + y_{n-t} \equiv 2 \pmod 4 \tag{22}$$

for $t > 1, t \leq \left[\frac{n}{2}\right]$.

Now suppose $n = 2k+1$ then $N(k+1)$ where $t = k$ is

$$\begin{aligned} x_1 + \cdots + x_k + y_1 + \cdots + y_k + x_{k+2} + \cdots + x_{2k+1} + y_{k+2} + \cdots + y_{2k+1} \\ \equiv 2(k-1) \pmod 4. \end{aligned}$$

then, as before, we get

$$x_k + y_k + x_{k+2} + y_{k+2} \equiv 2 \pmod 4.$$

However for $n = 2k+1$ and $t = k+1$ we have $N(k)$ is

$$\begin{aligned} x_1 + \cdots + x_{k+1} + y_1 + \cdots + y_{k+1} + x_{k+1} + \cdots + x_{2k+1} + y_{k+1} + \cdots + y_{2k+1} \\ \equiv 2 \pmod 4 \end{aligned}$$

which gives, under the assumption,

$$x_{k+1} + y_{k+1} + x_{k+1} + y_{k+1} \equiv 2 \pmod 4,$$

which is impossible. So $n$ is not odd and $> 1$.

For $n = 2k$ we see that (22) means exactly three of $x_{t+1}$, $y_{t+1}$, $x_{n-t}$, $y_{n-t}$ are one and one is minus one or exactly three are minus one and one is one, in either case we have, by induction,

$$x_s x_{n-s+1} + y_s y_{n-s+1} = 0, \qquad s = 2, \ldots, \left[\frac{n}{2}\right].$$

The remark that for $n$ even, $x + y \equiv 2 \pmod 4$ where $x$, $y$ are the sum of the elements of sequences $X$ and $Y$ respectively follows immediately from the equations (20) and (22).

■

*Remark 2.* BS$(3n-1)$ for all decompositions of $2(3n-1)$ into four squares for $n = 2, 4, \ldots, 20$ are given in Table 1. Some BS$(3n-1)$ for $n = 22, 24$ are also given in Table 1. These results were found by computer search using an appropriately modified

*Table 1.* Sequences $X, Y, Z, W$ which give base sequences BS$(3n-1)$ where $A = Z; W$, $B = Z; -W$, $C = X$, $D = Y$ of lengths $2n-1, 2n-1, n, n$.

| Length | Sums of Squares | Sequences |
|---|---|---|
| n | $2t = 2(3n-1)$<br>$= a^2 + b^2 + c^2 + d^2$ | |
| 2 | $0^2 + 0^2 + 1^2 + 3^2$ | $X = Y = (+-), Z = (++), W = (+)$ |
| 4 | $0^2 + 2^2 + 3^2 + 3^2$ | $X = (-+++), Y = (-+-+), Z = (-++-), W = (+++)$ |
| 6 | $1^2 + 1^2 + 4^2 + 4^2$ | $X = (++-+++), Y = (+-++++),$<br>$Z = (--+-++), W = (-+++-)$ |
| | $1^2 + 2^2 + 2^2 + 5^2$ | $X = (+--+++), Y = (+-++-+),$<br>$Z = (-+++-+), W = (++++-)$ |
| 8 | $0^2 + 1^2 + 3^2 + 6^2$ | $X = (-+++++++), Y = (+---+++-),$<br>$Z = (-+-++++-), W = (+-++--+)$ |
| 10 | $1^2 + 2^2 + 2^2 + 7^2$ | $X = (----++++++), Y = (-+-++-+-++),$<br>$Z = (+++--++-++), W = (-+++-+-++)$ |
| | $0^2 + 0^2 + 3^2 + 7^2$ | $X = (---+-++++-), Y = (+---+++--+),$<br>$Z = (-+--++-+++), W = (++-+-++++)$ |
| 12 | $1^2 + 2^2 + 4^2 + 7^2$ | $X = (--+++-+-++++),$<br>$Y = (-++--++-+-++),$<br>$Z = (++++--++-+-+),$<br>$W = (-++++++--+-)$ |
| | $2^2 + 4^2 + 5^2 + 5^2$ | $X = (--+++++-+-++),$<br>$Y = (-+++--+--+++),$<br>$Z = (--+-++-+++--),$<br>$W = (++++-+++-+-)$ |
| 14 | $1^2 + 4^2 + 4^2 + 7^2$ | $X = (---+++++-+++-+),$<br>$Y = (-++--+-+++++-+),$<br>$Z = (++++---++-++-+),$<br>$W = (+++-+++--+-+-)$ |
| | $4^2 + 4^2 + 5^2 + 5^2$ | $X = (-+++-+-+++-++-),$<br>$Y = (++--++++-+-+-+),$<br>$Z = (----++++-++--+),$<br>$W = (+++-++++-+--+)$ |
| | $1^2 + 3^2 + 6^2 + 6^2$ | can be obtained by changing the signs of<br>odd elements of each sequence in<br>$2t = 82 = 1^2 + 4^2 + 4^2 + 7^2$ |

*Table 1. Continued.*

| Length | Sums of Squares | Sequences |
|---|---|---|
| n | $2t = 2(3n - 1)$<br>$= a^2 + b^2 + c^2 + d^2$ | |
| 16 | $2^2 + 4^2 + 5^2 + 7^2$ | $X = (+ + - + + + + + - + + - - - + -)$,<br>$Y = (- + - + - - - + + + + - + + - +)$,<br>$Z = (+ - + + + + - - - + + + + + - +)$,<br>$W = (- + + + - + + + - - + - - + -)$ |
| | $0^2 + 3^2 + 6^2 + 7^2$ | can be obtained by changing the signs of<br>odd elements of each sequence in<br>$2t = 94 = 2^2 + 4^2 + 5^2 + 7^2$ |
| 18 | $1^2 + 1^2 + 2^2 + 10^2$ | $X = (+ + + + - - + + + + + + + - + + + -)$,<br>$Y = (+ - + - + + - - - + + + + - + - + -)$,<br>$Z = (- - - + - + + - + + - + - - + + + -)$,<br>$W = (+ - - - - - + + - + + + - + + + -)$ |
| | $1^2 + 4^2 + 5^2 + 8^2$ | can be obtained by changing the signs of<br>odd elements of each sequence in<br>$2t = 106 = 1^2 + 1^2 + 2^2 + 10^2$ |
| | $2^2 + 2^2 + 7^2 + 7^2$ | $X = (+ + + + + + - - - + - - + + + - - -)$,<br>$Y = (- - + - + + - - + + + + - - + + - +)$,<br>$Z = (- + - - + + + - + + - + + + - - - -)$,<br>$W = (+ + + + - + + - + - + + + - + - +)$ |
| 20 | $3^2 + 3^2 + 6^2 + 8^2$ | $X = (+ + + - + + + + + + - - + + - + - + + -)$,<br>$Y = (- - - - + + + - + + + + + - + - + + + +)$,<br>$Z = (- + - + - + - - + - + + + + - - + + - -)$,<br>$W = (+ + + + + - - - + - - + + - + - - + +)$ |
| | $0^2 + 1^2 + 6^2 + 9^2$ | can be obtained by changing the signs of<br>odd elements of each sequence in<br>$2t = 118 = 3^2 + 3^2 + 6^2 + 8^2$ |
| 22 | $0^2 + 0^2 + 7^2 + 9^2$ | $X = (- - - - + + + - + + - + - - + + + + - + - -)$,<br>$Y = (- - - + - - - + + + - - + + + + + + - - + -)$,<br>$Z = (- - + + - + + + + + + - + + - + - + + + - +)$,<br>$W = (+ + - + + - - - + - + - + - - + + + + - -)$ |
| 24 | $1^2 + 2^2 + 4^2 + 11^2$ | $X = (+ + + + - - - + - + + - + + - + - + - + + - - -)$,<br>$Y = (+ + + + - + + - - + + + + - + - - + - - - + + -)$,<br>$Z = (+ - - + + + - + + + - - - - + + - + + - + + + +)$,<br>$W = (+ + + + - + + - + + + - + - + - + - - - - + +)$ |

algorithm from that described in [13]. The results for $n = 4, 6, 8$ were first given in [18]. We recall that BS$(3n - 1)$ can be used to construct $T$-sequences of lengths $3n - 1$ and Hadamard matrices of order $4(3n - 1)$.

## References


1. Cohen, G., Rubie, D., Seberry, J., Koukouvinos, C., Kounias, S., and Yamada, M. 1989. A survey of base sequences, disjoint complementary sequences and $OD(4t; t, t, t, t)$. *J. Combin. Math. Combin. Comput.* 5:69–104.
2. Cooper, J., and Wallis, J. 1972. A construction for Hadamard arrays. *Bull. Austr. Math. Soc.* 7:269–277.

3. Edmondson, G. M. 1991. *More Non-existent Turyn Sequences*. Masters Thesis, University College, University of NSW, Australian Defence Force Academy, Canberra.
4. Edmondson, G. M., Seberry, J., and Anderson, M. R. 1994. On the existence of Turyn sequences of length less than 43. *Math. Comput.* 62:351–362.
5. Eliahou, S., Kervaire, M., and Saffari, B. 1990. A new restriction on the lengths of Golay complementary sequences. *J. Combin. Th. (Ser. A)* 55:49–59.
6. Geramita, A. V., and Seberry, J. 1979. *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*. New York: Marcel Dekker.
7. Golay, M. J. E. 1961. Complementary series. *IRE Trans. Information Theory* IT-7:82–87.
8. Golay, M. J. E. 1962. Note on Complementary series. *Proc. of the IRE* 84.
9. Gysin, M. 1993. *On Normal and Near-Yang Sequences*. M.Sc. Thesis, University of Wollongong.
10. Gysin, M., and Seberry, J. In press. New results with near-Yang sequences. *Bull. Institute of Comb. Appl.*
11. Harwit, M., and Sloane, N. J. A. 1979. *Hadamard Transform Optics*. New York: Academic Press.
12. Koukouvinos, C., Kounias, S., and Seberry, J. 1990a. Further results on base sequences, disjoint complementary sequences, $OD(4t; t, t, t, t)$ and the excess of Hadamard matrices. *Ars Combinatoria* 30:241–256.
13. Koukouvinos, C., Kounias, S., and Sotirakoglou, K. 1990b. On base and Turyn sequences. *Mathematics of Computation* 55:825–837.
14. Kounias, S., Koukouvinos, C., and Sotirakoglou, K. 1991. On Golay sequences. *Discrete Mathematics* 92:177–185.
15. Koukouvinos, C., and Seberry, J. 1992. Constructing Hadamard matrices from orthogonal designs. *Austral. J. Comb.* 6:267–278.
16. Seberry, J., and Yamada, M. 1992. Hadamard matrices, sequences, and block designs. In D. J. Stinson and J. Dinitz, editors, *Contemporary Design Theory—A Collection of Surveys*, pp. 431–560. John Wiley and Sons.
17. Seberry Wallis, J. 1975. Construction of Williamson type matrices. *J. Linear and Multilinear Algebra* 3:197–207.
18. Turyn, R. J. 1974. Hadamard matrices, Baumert-Hall units, four symbol sequences, pulse compressions and surface wave encodings. *J. Combin. Theory (Ser. A)* 16:313–333.
19. Yang, C. H. 1979. Hadamard matrices, finite sequences and polynomials defined on the unit circle. *Math. Comput.* 33:688–693.
20. Yang, C. H. 1982. Hadamard matrices and $\delta$-codes of length $3n$. *Proc. Amer. Math. Soc.* 85:480–482.
21. Yang, C. H. 1983a. Lagrange identity for polynomials and $\delta$-codes of lengths $7t$ and $13t$. *Proc. Amer. Math. Soc.* 88:746–750.
22. Yang, C. H. 1983b. A composition theorem for $\delta$-codes. *Proc. Amer. Math. Soc.* 89:375–378.
23. Yang, C. H. 1989. On composition of four-symbol $\delta$-codes and Hadamard matrices. *Proc. Amer. Math. Soc.* 107:763–776.