On 4–NPAF$(1, 2w)$ Sequences

Marc Gysin and Jennifer Seberry
Centre for Computer Security Research
Department of Computer Science
The University of Wollongong
Wollongong, NSW 2500
Australia

ABSTRACT. We give an overview on the existence of 4–NPAF $(1, 2w)$ sequences. We sketch some construction methods which give new 4–NPAF$(1, 2w)$ sequences and new orthogonal designs $OD(4n; 1, 2w)$.

1 Introduction

Definition 1 *An* orthogonal design *A, of order n, and type $(s_1, s_2, \ldots, s_u)$, denoted $OD(n; s_1, s_2, \ldots, s_u)$, on the commuting variables $(\pm x_1, \pm x_2, \ldots, \pm x_u, 0)$ is a square matrix of order n with entries $\pm x_k$, where each x_k occurs s_k times in each row and column such that the distinct rows are pairwise orthogonal.*

In other words

$$AA^T = (s_1 x_1^2 + \ldots + s_u x_u^2) I_n$$

where I_n is the identity matrix. It is known that the maximum number of variables in an orthogonal design is $\rho(n)$, the Radon number, where for $n = 2^a b$, b odd, set $a = 4c + d, 0 \leq d < 4$, then $\rho(n) = 8c + 2^d$.

Definition 2 *A* weighing matrix $W = W(n, k)$ *is a square matrix with entries 0, ± 1 having k non–zero entries per row and column and inner product of distinct rows zero. Hence, W satisfies $WW^T = kI_n$. The number k is called the weight of W. A $W(n, n)$, for $n \equiv 0 \pmod 4$, 1 or 2, whose entries are ± 1 only is called an* Hadamard matrix. *A $W(n, n-1)$ for $n \equiv 0 \pmod 4$ is equivalent to an $OD(n; 1, n-1)$ and a* skew–Hadamard matrix *or order n.*

Bulletin of the ICA, Volume 20 (1997) 6-12

There are a number of conjectures concerning weighing matrices:

Conjecture 1 (Weighing Matrix Conjecture) *There exists a weighing matrix $W(4t,k)$ for $k \in \{1,\ldots,4t\}$.*

Conjecture 2 (Skew Weighing Matrix Conjecture) *When $n \equiv 4 \pmod 8$, there exist a skew-weighing matrix (also written as an $OD(n;1,k)$) when $k \leq n-1$, $k = a^2+b^2+c^2, a,b,c$ integers except that $n-2$ must be the sum of two squares.*

Conjecture 3 *When $n \equiv 0 \pmod 8$, there exists a skew-weighing matrix (also written as an $OD(n;1,k)$) for all $k \leq n-1$.*

Definition 3 (Nonperiodic Autocorrelation Function) *Let $X = \{\{x_{11},\ldots,x_{1n}\},\{x_{21},\ldots,x_{2n}\},\ \ldots,\ldots,\ \{x_{m1},\ldots,x_{mn}\}\}$ be a family of m sequences of elements 1, 0 and -1 and length n. The* nonperiodic autocorrelation function *of the family of sequences X, denoted by N_X, is a function defined by*

$$N_X(s) = \sum_{i=1}^{n-s}(x_{1i}x_{1,i+s} + x_{2i}x_{2,i+s} + \ldots + x_{mi}x_{m,i+s}),$$

where s can range from 1 to $n-1$.

Definition 4 *The* weight $w(X_i)$ of a sequence X_i *is defined as the total number of non-zero elements in X_i. The* weight $w(X)$ of a family of sequences X *is defined as $w(X) = \sum_{i=1}^{m} w(X_i)$.*

It is well known (see for example [8] or [7]) that the sum of the squares of the row sums of sequences with zero nonperiodic autocorrelation function must add to the total weight. That is,

$$\sum_{i=1}^{m}(\sum_{j=1}^{n} x_{ij})^2 = w(X).$$

Notation 1 *Given binary or ternary sequences $S = \{s_1, s_2, \ldots, s_n\}$ and $T = \{t_1, t_2, \ldots, t_m\}$, we shall use $\bar{S}$ for the sequence S negated, S^* for the sequence S reversed and ST for the sequence T appended onto S. That is,*

$$\begin{aligned} \bar{S} &= \{-s_1, -s_2, \ldots, -s_n\}, \\ S^* &= \{s_n, \ldots, s_2, s_1\}, \\ ST &= \{s_1, \ldots, s_n, t_1, \ldots, t_m\}. \end{aligned}$$

It can be shown that negating and/or reversing one or more sequences does not affect the (non)periodic autocorrelation function.

We are looking for four ternary sequences A, B, C, C of lengths m, m, n, n ($m \geq n$) and weight w where A, B, C, C have zero nonperiodic autocorrelation function. That is,

$$N_A(s) + N_B(s) + 2N_C(s) = 0, \ s = 1, \ldots, m-1, \text{and } c_i = 0, \ i > n.$$

From these sequences we can form the sequences $X = AB$, $Y = A\bar{B}$, $Z = C0C^*$ and $W = Ca\bar{C}^*$, $a \neq 0$. X, Y, Z, W are called *4-NPAF$(1, 2w)$ sequences.*

Lemma 1 *If there are sequences A, B, C, C of length m, m, n, n ($m \geq n$) and weight w, then there is an orthogonal design $OD(4p; 1, 2w)$, where $p \geq max(2m, 2n+1)$.*

Proof. Given A, B and C take the 4–NPAF$(1, 2w)$ sequences AB, $A\bar{B}$, $C0C^*$, $Ca\bar{C}^*$ as the first rows of length $p \geq \max(2m, 2n+1)$ (if necessary append zeros) of four circulant matrices which can be used in the Goethals–Seidel array to form an $OD(4p; 1, 2w)$. □

2 Existence of Sequences of Type A,B,C,C

We performed exhaustive searches on the computer for sequences of type A,B,C,C for particular weights and lengths. The results are presented in Table 1. In the table, 1 is replaced by '+' and -1 by '−'. Where the weight could not be written as $a^2 + b^2 + 2c^2$ (a, b, c being the row sums of A, B, C respectively), we write "n/e", meaning that sequences for this particular weight cannot exist. "n/f" means that there were no sequences found subjected to complete search for some lengths m and n. However, sequences may exist for longer lengths.

We also construct sequences of type A,B,C,C from Golay sequences and ternary complementary pairs (TCP's).

Lemma 2 *If there are Golay sequences or ternary complementary pairs of lengths ℓ and weight u, then there are sequences of type A,B,C,C of*

(i) *lengths $m = n = \ell$ and weight $w = 2u$; and*

(ii) *lengths $m = \ell + 1$, $n = \ell$ and weight $w = 2u + 2$.*

Proof. Given Golay sequences or a ternary complementary pair X, Y of length n and weight w take the four sequences

(i) $A = X$, $B = X$, $C = Y$; or

(ii) $A = \{X, 1\}$, $B = \{X, -1\}$, $C = Y$.

Now A,B,C,C have the desired properties. □

m	n	Weight	Sequences
5	4	17	$+++-+, ++0--, ++-+$
5	4	18	$++++-, -+++-, ++-+$
5	5	19	$+++--, +-0+-, +++-+$
5	5	20	$+++--, +-++-, +++-+$
7	5	21	$++-+-++, ++0+--, ++0-+$
7	6	22	$+++-+0-, +-+--0+, ++0-+$
7	6	23	$++-0+-+, -+++--+, ++0+-$
8	6	24	$++++-++-, ++-+---+, ++00-+$
9	7	25	$+0++0-+0+, +-+0++0--, +++-0+-$
9	9	25	$++00+-+0+, ++-+--00+, +0+00++--$
7	6	26	$+++-++-, +-+++-+, -++++-$
7	7	26	$++++--+, +++-+-+, +++-0+-$
9	7	27	$++00+-+0+, ++-+++00-, +++--+-$
9	8	27	$++0+0+--, ++-000--+,$ $++-+-0++$
7	7	28	$+++-++-, ++-+-+-, ++++--+$
8	7	28	$++-++-0+, -+++--0+, ++++-+-$
		29	n/f
		30	n/e
9	8	31	$+++-++--+, -+++0-+-+, +-+++++0-$
10	8	31	$+++++0--+-, ++0-++-0-+,$ $++-+-0++$
8	8	32	$+++-+---, -+++--+, +++-++-+$
9	8	33	$+++--+--+, +++-0+---,$ $+++-+-++$
9	8	34	$++++--+--, ++-++---+,$ $+++-+-++$
11	10	35	$+++0+0+0+--, ++-0++-0--+,$ $++0+-+-\div++$

Table 1. Sequences of type A,B,C,C found via computer.

Corollary 1 *There are sequences of type A,B,C,C of*

(i) *lengths $m = n = 2^a10^b26^c$ and weight $w = 4 \times 2^a10^b26^c$; and*

(ii) *lengths $m = 2^a10^b26^c+1$, $n = 2^a10^b26^c$ and weight $w = 4\times2^a10^b26^c + 2$,*

$a, b, c \geq 0$.

Proof. Take Golay sequences in the above constructions. □

[1] and [4] present many new TCP's of length n and weight w. Hence, we get many new sequences of type A,B,C,C, many new 4–NPAF$(1, 4w)$ and 4–NPAF$(1, 4w + 4)$ sequences and many new $OD(8n + 4; 1, 4w)$ and

$OD(8n+8;1;4w+4)$. These results are summarised in Table 2. The table indicates the two constructions from Lemma 2. [3] multiplies (or concatenates) the length and the weight of a TCP (where the two sequences have their zeros in the same positions) by certain small numbers which again leads to new TCP's and new sequences of type A,B,C,C. In particular multiplication is possible for the following parameters

$$(m,f) = (3,4),(3,5),(4,5),(5,8),(6,8),(6,10),(7,8),(7,10),$$

where m indicates the multiplier of the length and $\frac{1}{2}f$ the multiplier of the weight. For example, $(m,f) = (3,5)$ means that we can multiply the length of a given TCP (or Golay sequences) by 3 and the weight by $2\frac{1}{2}$.
The multiplication $(m,f) = (3,5)$ leads to new results.

Lemma 3 *If there is a TCP of length ℓ and weight w (where the two sequences have their zeros in the same positions), then there are sequences of type A,B,C,C of*

(i) *lengths $m = n = 3\ell$ and weight $5w$; and*

(ii) *lengths $m = 3\ell+1$, $n = 3\ell$ and weight $5w+2$.*

Proof. Given a TCP S, T of length ℓ (where S and T have their zeros in the same positions), let $P = \frac{1}{2}(S+T)$, $Q = \frac{1}{2}(S-T)$ and let

$$\begin{aligned} X &= SQB, \\ Y &= \bar{S}PB. \end{aligned}$$

Now X, Y is a TCP of length 3ℓ and weight $2\frac{1}{2}w$ (see [3]) and we can apply Lemma 2 to get the desired sequences of type A,B,C,C. □

There are TCP's with the parameters in Table 2 with zeros in the same positions. Hence, we get many new sequences of type A,B,C,C and weights $5w$ and $5w+2$ (where w is the initial weight of the TCP) and many 4–NPAF$(1,10w)$ and 4–NPAF$(1,10w+4)$ sequences. In the last step, we get new $OD(24n+4;1,10w)$ and $OD(24n+8;1,10w+4)$ (where n is the initial length of of the TCP).
Finally, in Table 3, we present some other sequences of type A,B,C,C which fill in some of the gaps for weights $w \leq 50$.

3 Numerical Consequences

Table 4 shows the parameters of the orthogonal designs $OD(4p;1,2w)$ obtained by the above constructions via sequences of type A,B,C,C.

TCP length	TCP weight	A,B,C,C lengths	A,B,C,C weight
5	8	5,5/6,5	16/18
6	10	6,6/7,6	20/22
7	10	7,7/8,7	20/22
8	16	8,8/9,8	32/34
9	16	9,9/10,9	32/34
10	20	10,10/11,10	40/42
11	16	11,11/12,11	32/34
12	20	12,12/13,12	40/42
13	20	13,13/14,13	40/42
14	26	14,14/15,14	52/54
15	20	15,15/16,15	40/42
16	32	16,16/17,16	64/66
17	32	17,17/18,17	64/66
18	32	18,18/19,18	64/66
19	32	19,19/20,19	64/66
20	40	20,20/21,20	80/82

Table 2. From TCP's to sequences of type A,B,C,C.

m	n	Weight	Sequences
11	11	37	$++---+++-+-$, $+-+++0++++-$, $+0+00--+--+$
11	11	44	$+-+-+----++$, $+--+++-++++$, $++++-+--++-$

Table 3. Some other sequences of type A,B,C,C.

References

[1] A. Gavish and A. Lempel, On Ternary Complementary Sequences, *IEEE Transactions on Information Theory* **40**, 2 (1994), 522–526.

[2] A.V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York–Basel, 1979.

[3] M. Gysin and J. Seberry, Multiplications of ternary complementary pairs, to be published.

[4] M. Gysin and J. Seberry, On ternary complementary pairs, to be published.

[5] C. Koukouvinos, S. Kounias, J. Seberry, C.H. Yang and J. Yang, Multiplication of sequences with zero autocorrelation, *Australasian Journal of Combinatorics* **10** (1994), 5–15.

[6] C. Koukouvinos, S. Kounias, J. Seberry, C.H. Yang and J. Yang, On sequences with zero autocorrelation, *Designs, Codes and Cryptography* **4** (1994), 327–340.

[7] C. Koukouvinos and J. Seberry, On weighing matrices, *Utilitas Mathematica* **43** (1993), 101–127.

[8] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, in *Contemporary Design Theory - a Collection of Surveys*, eds J. Dinitz and D.R. Stinson, John Wiley and Sons, New York, (1992), 431–560.

p	w	How
11	16	Table 3
10	17	Table 2
10	18	Table 2
11	19	Table 2
11	20	Table 2
14	21	Table 2
14	22	Table 2 and 3
14	23	Table 2
16	24	Table 2
18	25	Table 2
14	26	Table 2
18	27	Table 2
15	28	Table 2
18	31	Table 2
17	32	Table 2 and 3
18	33	Table 2
18	34	Table 2 and 3
22	35	Table 2
23	37	Table 3
21	40	Table 3
22	42	Table 3
23	44	Table 3
37	50	Table 3 and multiplication by $(m, f) = (3, 5)$
29	52	Table 3
30	54	Table 3
33	64	Table 3
34	66	Table 3
41	80	Table 3
42	82	Table 3
61	100	Table 3 and multiplication by $(m, f) = (3, 5)$
62	102	Table 3 and multiplication by $(m, f) = (3, 5)$

Table 4. An orthogonal design $OD(4p; 1, 2w)$ exists.