1996

Multiplication of ternary complementary pairs

Marc Gysin

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Multiplication of ternary complementary pairs

Abstract

We present a computer-search method for concatenating or "multiplying" binary or ternary complementary pairs. All multiplications by a particular number *m* are considered. The computer-search method is new and leads to a large set of new results. The results and equivalences are discussed and some applications and numerical consequences are shown.

Disciplines

Physical Sciences and Mathematics

Publication Details

Gysin M and Seberry J, Multiplication of ternary complementary pairs, Australasian Journal of Combinatorics, 14 (1996), 165-180.

Multiplications of Ternary Complementary Pairs

Marc Gysin and Jennifer Seberry

Centre for Computer Security Research,
Department of Computer Science,
The University of Wollongong,
Wollongong, NSW 2500
Australia

Abstract

We present a computer-search method for concatenating or "multiplying" binary or ternary complementary pairs. All multiplications by a particular number m are considered. The computer-search method is new and leads to a large set of new results. The results and equivalences are discussed and some applications and numerical consequences are shown.

1 Introduction

The definition of the nonperiodic autocorrelation function is given as follows.

Definition 1 (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 2 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 $w(X) = \sum_{i=1}^{m} w(X_i)$.

Australasian Journal of Combinatorics 14 (1996), pp.165-180

It is well known (see for example [9] or [11]) 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,

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

Example 1 (We replace 1 by '+' and -1 by '$-$')
Consider the TCP

$$\begin{aligned} A &= ++-++0-0-+++, \\ B &= +++-+0+0-+-- \end{aligned}$$

We have $(\sum_{i=1}^{12} a_i)^2 + (\sum_{i=1}^{12} b_i)^2 = 4^2 + 2^2 = 20 = w(A,B)$.

Sequences with the properties mentioned above can be used for constructing weighing matrices (see also Section 5). A weighing matrix is defined as follows.

Definition 3 A *weighing matrix* $W = W(n,k)$ is a square matrix with entries $0, \pm 1$ 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 $n \equiv 0(\text{mod } 4)$, 1 or 2, whose entries are ± 1 only is called *an Hadamard matrix.* A $W(n, n-1)$ for $n \equiv 0(\text{mod } 4)$ is equivalent to an orthogonal design $OD(n; 1, n-1)$ and a *skew-Hadamard matrix* or order n.

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* $n \equiv 4(\mathit{mod}\ 8)$*, 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* $n \equiv 0(\mathit{mod}\ 8)$*, there exist a skew-weighing matrix (also written as an* $OD(n;1,k)$*) for all* $k \leq n-1$.

In Seberry and Zhang [12] weighing matrices of order $4t$ and weight $2t$ are discussed and they are found to exist for all orders less than 4000 for which Hadamard matrices are known.

Furthermore, sequences with zero (non)periodic autocorrelation function are of the interest in different research areas. For example:

- Communications Theory (sending a signal to a remote object and overlapping it with the signal reflected to measure the distance);

- Coding Theory (sequences with zero (non)periodic autocorrelation function have a constant Hamming distance to the periodically shifted versions of themselves);
- Cryptography (pseudo–random sequences); and
- Combinatorics (sequences with zero (non)periodic autocorrelation function are related to orthogonal designs, Hadamard matrices, weighing matrices, difference sets, block designs, ...).

Two sequences G and H with entries 1, -1 and zero nonperiodic autocorrelation function are called *Golay sequences* or *a binary complementary pair (BCP).* These sequences have been extensively studied (see for example [2] and [11]) and they are only known to exist for lengths $n = 2^a 10^b 26^c$, $a, b, c \geq 0$. The first unresolved cases are now $n = 74, 82, 106, 116, 122$. Two sequences M and N with entries 1, 0 and -1 and zero nonperiodic autocorrelation function are called *a ternary complementary pair (TCP).* A TCP is a generalisation of a BCP. [6] and [3] give examples and an overview on the existence of TCP's with minimal number of zeros.

Sequences with zero (non)periodic autocorrelation function are hard to find, since for longer lengths n the growth of candidate sequences is exponential in n.

There are different methods to obtain longer sequences by concatenating (or "multiplying") shorter sequences. Standard constructions and theorems give one method (see for example [6]). Another possibility is to perform a computer–search for all multiplications by a particular number and a particular weight, this is described in this paper.

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

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

ST denotes the sequence T appended onto S and S/T (for $m = n$) means the sequence T is interleaved into the sequence S. That is,

$$\begin{aligned} ST &= \{s_1, \ldots, s_n, t_1, \ldots, t_m\}, \\ S/T &= \{s_1, t_1, s_2, t_2, \ldots, s_n, t_n\}. \end{aligned}$$

It can be shown that negating and/or reversing one or more sequences does not affect the (non)periodic autocorrelation function. Therefore, if A, B is a TCP then, for example, A^*, $\bar{B}$ is a TCP as well. The two TCP's A, B and A^*, $\bar{B}$ are said to be *equivalent.*

2 Multiplication of Sequences "by Hand"

A trivial multiplication is the multiplication by 2. It can easily be carried out by hand. Given a TCP A, B of length n, one way to multiply by 2 is to let

$$\begin{aligned} X &= A\ B, \\ Y &= A\ \bar{B}. \end{aligned}$$

Now X and Y is a TCP of length $2n$.

In order to prove that X and Y is a TCP, we have to show that $N_X(s) + N_Y(s) = 0,\ s = 1, \ldots, 2n-1$. We have,

$$\left.\begin{aligned} N_X(s) &= \textstyle\sum_{i=1}^{n-s} a_i a_{i+s} + \sum_{i=1}^{s} a_{n-s+i} b_i + \sum_{i=1}^{n-s} b_i b_{i+s}, \\ N_Y(s) &= \textstyle\sum_{i=1}^{n-s} a_i a_{i+s} - \sum_{i=1}^{s} a_{n-s+i} b_i + \sum_{i=1}^{n-s} b_i b_{i+s}, \end{aligned}\right\} s = 1, \ldots, n-1;$$

and

$$\left.\begin{aligned} N_X(s) &= \textstyle\sum_{i=1}^{2n-s} a_i b_{s-n+i}, \\ N_Y(s) &= -\textstyle\sum_{i=1}^{2n-s} a_i b_{s-n+i}, \end{aligned}\right\} s = n, \ldots, 2n-1.$$

Therefore, $N_X(s) + N_Y(s) = 2N_A(s) + 2N_B(s),\ s = 1, \ldots, n-1$ and $N_X(s) + N_Y(s) = 0$, otherwise. Since $N_A(s) + N_B(s) = 0,\ s = 1, \ldots, n-1,\ N_X(s) + N_Y(s) = 0,\ s = 1, \ldots, n-1$. Hence, $N_X(s) + N_Y(s) = 0,\ s = 1, \ldots, 2n-1$.

Observe the way we preserved zero nonperiodic autocorrelation. We have zero nonperiodic autocorrelation because we put the same number of A's and B's into X and Y, and because in X A is shifted into B and in Y A is shifted into $\bar{B}$. Therefore, if we multiply a TCP A and B of length n by longer lengths m, we basically only have to take care about two conditions:

(i) the number of A's and B's has to be the same in the new sequences; and

(ii) we have to make sure that the mixed terms, obtained when shifting different sequences into each other, add to zero.

Note that in the above example interleaving can be applied to form another TCP X_2 and Y_2. We let

$$\begin{aligned} X_2 &= A/B, \\ Y_2 &= A/\bar{B} \end{aligned}$$

and observe that X_2, Y_2 have zero nonperiodic autocorrelation function. The proof works similar as above.

Definition 4 (Crosscorrelation) The *crosscorrelation of two sequences A and B* is defined by:

$$N_{AB}(s) = \begin{cases} \sum_{i=1}^{s} a_{n-s+i} b_i, & s = 1, \ldots, n, \\ \sum_{i=1}^{2n-s} a_i b_{s-n+i} & s = n+1, \ldots, 2n-1, \\ 0 & \text{otherwise.} \end{cases}$$

Note that $N_{AB}(s)$ means "the sequence A is shifted into the sequence B" and $N_{BA}(s)$ means "the sequence B is shifted into the sequence A". Clearly,

$$\begin{aligned} N_{AB}(s) + N_{A\bar{B}}(s) &= 0, \text{ and} \\ N_{AB}(s) &\neq N_{BA}(s). \end{aligned}$$

That is, when adding the terms from the crosscorrelations from the sequence A shifted into the sequence B and the sequence A shifted into the sequence $\bar{B}$ we get zero. However, shifting the sequence A into the sequence B and shifting the sequence B into the sequence A, does not generally give terms which add to zero.

Condition (ii) above can now be reformulated: the crosscorrelations have to add to zero for $s = 1, \ldots, mn-1$. Of course we only have to check that the crosscorrelations are zero for $s = 1, n+1, 2n+1, \ldots, (m-1)n+1$, and we can then conclude that the crosscorrelations are zero for all $s = 1, \ldots, mn-1$.

This formalism and simplification allows us to multiply "by hand" for special and easy cases and to implement the above rules on computer and carry out exhaustive searches for small values of m.

Note that these rules do not only apply for TCP's. For example [9] starts with four special sequences A, B, C and D with zero nonperiodic autocorrelation function to get

$$\begin{array}{rcccc} X & = & AC & 00 & B^*0, \\ Y & = & BD & 00 & \bar{A}^*0, \\ Z & = & 00 & A\bar{C} & 0D^*, \\ W & = & 00 & B\bar{D} & 0\bar{C}^*, \end{array}$$

(where 0 and 00 are sequences of zeros of different lengths).

Now X, Y, Z and W are sequences with zero nonperiodic autocorrelation function. Observe that the basic rules for shifting apply in the same manner as above. However, there are some additional rules when shifting reversed sequences into other sequences. One of these rules is for example:

$$N_{AB}(s) = N_{B^*A^*}(s)$$

That is, shifting the sequence A into the sequence B is the same as shifting the sequence B reversed into the sequence A reversed.

Another way of multiplying, given a TCP A, B of length n with zeros in the same positions, is to let $P = \frac{1}{2}(A+B)$ and $Q = \frac{1}{2}(A-B)$. Note that P and Q is now a T,CP as well. A, B, P and Q have then to be concatenated appropriately. For example, we let

$$\begin{array}{rcccc} X & = & \bar{P} & A & Q, \\ Y & = & P & B & Q. \end{array}$$

If we shift by $s = 1, \ldots, n$, we have

$$\begin{aligned} N_X(s) + N_Y(s) &= N_{\bar{P}}(s) + N_P(s) + N_A(s) + N_B(s) + N_Q(s) + N_Q(s) + \\ & N_{\bar{P}A}(s) + N_{AQ}(s) + N_{PB}(s) + N_{BQ}(s). \end{aligned}$$

The first six terms add to zero because A, B; P, Q; and $\bar{P}$, Q are all TCP's. Therefore,

$$N_X(s) + N_Y(s) = N_{\bar{P}A}(s) + N_{AQ}(s) + N_{PB}(s) + N_{BQ}(s),$$

which we rewrite as

$$\begin{aligned} N_X(s) + N_Y(s) &= \frac{1}{2}(-N_{AA}(s) - N_{BA}(s) + N_{AA}(s) - \\ & N_{AB}(s) + N_{AB}(s) + N_{BB}(s) + N_{BA}(s) - N_{BB}(s)). \end{aligned}$$

These terms add to zero by "cancelling each other out".

If we shift by $s = n+1, \ldots, 2n$, we have

$$\begin{aligned} N_X(s) + N_Y(s) &= N_{\bar{P}A}(s) + N_{AQ}(s) + N_{PB}(s) + N_{BQ}(s) + \\ & N_{\bar{P}Q}(s-n) + N_{PQ}(s-n). \end{aligned}$$

Clearly, the first four terms again add to zero. Similarly, the last two terms add to zero.

Finally, if we shift by $s = 2n+1, \ldots, 3n-1$, we get

$$N_X(s) + N_Y(s) = N_{\bar{P}Q}(s-n) + N_{PQ}(s-n),$$

which of course is zero again.

Therefore, $N_X(s) + N_Y(s) = 0$, $s = 1, \ldots, 3n-1$, and so X and Y is a TCP of length $3n$.

The general rules are quite simple and straightforward to implement.

3 Multiplication of Sequences on the Computer

Preliminary conditions:

We start with a TCP A, B of length n with zeros in the same positions. We let $P = \frac{1}{2}(A+B)$ and $Q = \frac{1}{2}(A-B)$. Observe that P and Q have zero nonperiodic autocorrelation function and $w(P,Q) = \frac{1}{2}w(A,B)$. We try to find longer TCP's X and Y by concatenating A, B, P and Q appropriately.

There are two important parameters for the computer-search:

1. The number m with which we multiply the sequences; and
2. the number $\frac{1}{2}f$ with which we multiply the initial weight $w(A, B)$.

We also define:

$$a = \sum_{i=1}^{n} a_i,\ b = \sum_{i=1}^{n} b_i,\ x = \sum_{i=1}^{nm} x_i,\ y = \sum_{i=1}^{nm} y_i,$$

where a_i, b_i, x_i and y_i are the individual elements of the sequences A, B, X and Y respectively.

Equation (1) says that:

$$\begin{aligned} a^2 + b^2 &= w(A, B), & (2) \\ x^2 + y^2 &= \frac{1}{2} f w(A, B). & (3) \end{aligned}$$

We can write $x = \frac{k_1}{2}a + \frac{k_2}{2}b$ and $y = \frac{k_3}{2}a + \frac{k_4}{2}b$ with k_1, k_2, k_3, k_4 integers. This is because X and Y are concatenations of A, B, P and Q and $\sum_{i=1}^{n} p_i = \frac{1}{2}(a + b)$ and $\sum_{i=1}^{n} q_i = \frac{1}{2}(a - b)$. Therefore,

$$\begin{aligned} x^2 + y^2 &= (\frac{k_1}{2}a + \frac{k_2}{2}b)^2 + (\frac{k_3}{2}a + \frac{k_4}{2}b)^2 \\ &= a^2\frac{k_1^2 + k_3^2}{4} + b^2\frac{k_2^2 + k_4^2}{4} + ab\frac{k_1k_2 + k_3k_4}{4} \\ &= \frac{1}{2}f(a^2 + b^2). \end{aligned}$$

Hence,

$$\frac{k_1^2 + k_3^2}{4} = \frac{k_2^2 + k_4^2}{4} = \frac{1}{2}f, \tag{4}$$

and,

$$(k_1 = k_4 \wedge k_2 = -k_3) \vee (k_1 = -k_4 \wedge k_2 = k_3). \tag{5}$$

From (4) we see that $2f$ (and f) must be the sum of two squares. [1] shows that f is the sum of two squares if and only if f has no square–free factor $\equiv 3 (\text{mod } 4)$. We restate this in the following lemma.

Lemma 1 *We can multiply the weight by $\frac{1}{2}f$ only if f has no square-free factor $\equiv 3(mod\ 4)$.*

Corollary 1 *Multiplying the weight with*

$$\frac{1}{2}f = 1\frac{1}{2}, 3, 3\frac{1}{2}, 5\frac{1}{2}, 6, 7, 7\frac{1}{2}, 9\frac{1}{2}, \ldots$$

is not possible.

The search:

The computer–search starts with the same number of sequences A and B and another number of sequences P and Q. These two numbers can be deduced from m and f.

The algorithm now has to concatenate A, B, P and Q and reversed and/or negated versions of A, B, P and Q to find sequences X and Y such that:

- X and Y have both the length mn; and
- X and Y have zero nonperiodic autocorrelation function.

The algorithm can be described as follows:

1. From m and f determine the number of A's and B's and the number of P's and Q's that will be available to form X and Y.
2. Go through all possibilities for forming X and Y by concatenating the A's, B's, P's and Q's available such that X and Y both have length mn.
3. For each configuration obtained, go through all possibilities for negating/not negating individual A's, B's, P's and Q's in X and Y such that Equations (4) and (5) are satisfied.
4. For each configuration obtained, go through all possibilities for reversing/not reversing individual A's, B's, P's and Q's in X and Y.
5. Test the nonperiodic autocorrelation function for each configuration obtained by the above steps. If it is zero for all possible $s = 1, \ldots mn - 1$, then X and Y is a TCP with the desired properties.

Observe Equations (4) and (5). These are important conditions that allow us to reduce the search–space drastically. When testing the nonperiodic autocorrelation function, we of course only have to consider the crosscorrelations for $s = 1.n + 1, \ldots, (m-1)n + 1$.

The algorithm can also skip equivalent configurations. Equivalence is described below.

4 Results and Brief Discussion

Equivalences:

Equivalent configurations are a consequence of the following facts:

- The sequences A and B are interchangeable.

- The sequences X and Y are interchangeable.
- Negating and/or reversing A and/or B and then take the negated and/or reversed version of A and/or B as input to the algorithm, does not affect the nonperiodic autocorrelation function being zero.
- Negating and/or reversing X and/or Y does not affect the nonperiodic autocorrelation function being zero.

A lot of other equivalences can be formed by combining the above ones. When designing the algorithm and considering final results, it seemed to be almost impossible to recognise and filter out all such equivalences.

Example 2 Consider the multiplication by $m = 3$ and $f = 5$. From Table 1 we conclude that

$$\begin{aligned} X &= AQB, \\ Y &= \bar{A}PB \end{aligned}$$

is a possible multiplication. By letting $A_1 = \bar{A}$, $B_1 = B$ (note that if A, B is a TCP, then A_1, B_1 is a TCP as well) we get

$$\begin{aligned} P_1 &= \tfrac{1}{2}(A_1 + B_1) &&= \tfrac{1}{2}(B - A) &&= \bar{Q}, \\ Q_1 &= \tfrac{1}{2}(A_1 - B_1) &&= \tfrac{1}{2}(-A - B) &&= \bar{P}, \end{aligned}$$

and

$$\begin{aligned} X_1 &= A_1Q_1B_1 &&= \bar{A}\bar{P}B, \\ Y_1 &= \bar{A}_1P_1B_1 &&= A\bar{Q}B. \end{aligned}$$

Hence,

$$\begin{aligned} X &= \bar{A}\bar{P}B, \\ Y &= A\bar{Q}B. \end{aligned}$$

is another possible multiplication for the same parameters m and f.

The equivalences of the type in Example 2 can be stated as a lemma.

Lemma 2 *Multiplications which can be obtained by interchanging*

(i) A with $\bar{A}$ and P with $\bar{Q}$; or

(ii) B with $\bar{B}$ and P with Q,

are equivalent.

Proof. The first class of equivalences is shown in Example 2. For the second class let

$$A_1 = A,\ B_1 = \bar{B}.$$

Now

$$P_1 = \frac{1}{2}(A_1 + B_1) = \frac{1}{2}(A - B) = Q,\ Q_1 = \frac{1}{2}(A_1 - B_1) = \frac{1}{2}(A + B) = P.$$

□

Results:

m	f	Examples	m	f	Examples
3	4	$PA\bar{Q}$ $\bar{P}B\bar{Q}$	6	10	$AB^*QP^*B\bar{A}^*$ $\bar{A}B^*\bar{Q}P^*\bar{B}\bar{A}^*$
3	5	AQB $\bar{A}PB$	6	10	$A^*Q^*B^*BP\bar{A}$ $\bar{A}^*\bar{Q}^*\bar{B}^*BP\bar{A}$
4	5	$PQA\bar{Q}$ $\bar{P}BP\bar{Q}$	7	8	$PP\bar{P}A\bar{Q}\bar{Q}\bar{Q}$ $\bar{P}\bar{P}\bar{P}BQ\bar{Q}\bar{Q}$
5	8	$PA\bar{A}B\bar{Q}$ $\bar{P}\bar{A}\bar{B}B\bar{Q}$	7	8	$PPQ\bar{A}P\bar{Q}\bar{Q}$ $\bar{P}\bar{P}\bar{Q}\bar{B}P\bar{Q}\bar{Q}$
5	8	$PB\bar{A}BQ$ $P\bar{A}\bar{B}\bar{A}\bar{Q}$	7	8	$PQ\bar{P}B\bar{Q}P\bar{Q}$ $\bar{P}\bar{Q}\bar{P}\bar{A}QP\bar{Q}$
5	8	$PAA\bar{A}Q$ $\bar{P}B\bar{B}\bar{B}Q$	7	10	$A\bar{Q}AQ\bar{Q}\bar{Q}B$ $\bar{A}\bar{P}\bar{P}PB\bar{P}B$
6	8	$\bar{Q}\bar{A}PQBP$ $\bar{Q}\bar{A}P\bar{Q}\bar{B}\bar{P}$	7	10	$\bar{Q}\bar{A}APQBP$ $\bar{Q}\bar{A}P\bar{Q}B\bar{B}\bar{P}$
6	8	$\bar{Q}^*\bar{A}^*P^*PBQ$ $\bar{Q}^*\bar{B}^*\bar{P}^*P\bar{A}\bar{Q}$	7	10	$PQA\bar{A}BP\bar{Q}$ $\bar{P}\bar{Q}\bar{A}\bar{B}BP\bar{Q}$
6	8	$\bar{Q}P^*\bar{A}B^*PQ^*$ $\bar{Q}\bar{P}^*\bar{A}\bar{B}^*P\bar{Q}^*$	7	10	$\bar{Q}P\bar{Q}AAB\bar{P}$ $Q\bar{A}BB\bar{P}\bar{Q}\bar{P}$
6	8	$PP\bar{A}B\bar{Q}Q$ $P\bar{P}\bar{A}\bar{B}\bar{Q}\bar{Q}$	7	10	$P\bar{Q}P\bar{A}BAQ$ $PB\bar{A}\bar{B}\bar{Q}\bar{P}\bar{Q}$
6	10	$\bar{A}APQBB$ $\bar{A}\bar{A}P\bar{Q}B\bar{B}$	7	10	$P\bar{B}QPBA\bar{Q}$ $\bar{P}B\bar{A}\bar{Q}PA\bar{Q}$
6	10	$AQB\bar{A}PB$ $\bar{A}\bar{Q}\bar{B}\bar{A}PB$	7	10	$\bar{P}APA\bar{Q}BQ$ $P\bar{A}\bar{P}B\bar{Q}BQ$

Table 1: Multiplications obtained via computer.

Table 1 shows some results obtained. Shorter multiplications ($m = 3, 4$) were a matter of seconds or minutes on the computer while longer multiplications ($m = 7$) took several CPU–days of computer–time. Clearly, the growth of the search–space is exponential in m.

Table 1 gives rise to many new TCP's. These multiplications can be applied to any BCP or TCP A, B with zeros in the same positions. The multiplications in general lead to TCP's since P and Q are ternary sequences. Some of these new TCP's will have their zeros in the same positions which means that we can apply these multiplications recursively.

Example 3 We apply the multiplication

$$\begin{aligned} X &= \bar{P}APA\bar{Q}BQ, \\ Y &= P\bar{A}\bar{P}B\bar{Q}BQ \end{aligned}$$

to the TCP

$$\begin{aligned} A &= --+0-0-, \\ B &= --+0+0+ \end{aligned}$$

of length $n = 7$ and weight $w = 10$. Now

$$\begin{aligned} P &= --+0000, \\ Q &= 0000-0-; \end{aligned}$$

and

$$\begin{aligned} X &= ++-0000--+0-0---+0000--+ \\ &\quad 0-0-0000+0+--+0+0+0000-0-, \\ Y &= --+0000++-0+0+++-0000--+ \\ &\quad 0+0+0000+0+--+0+0+0000-0-\,. \end{aligned}$$

X, Y is now a TCP of length $7n = 49$ and weight $5w = 50$. Observe that for this case X and Y have their zeros in the same positions, therefore, any multiplication of the table can be (re)applied to X and Y.

Some multiplications are a result of an extended standard construction which has first been presented in [6]:

Theorem 1 *Let A, B be a TCP (with zeros in the same positions) of length r. Let $P = \frac{1}{2}(A+B)$, $Q = \frac{1}{2}(A-B)$ (that is, P and Q is a TCP) and let M, N be a TCP of length ℓ. Let 0_r denote the sequence of r zeros and let*

$$\begin{aligned} U &= \{m_1 \times P, n_1 \times Q, m_2 \times P, n_2 \times Q, \ldots, \ldots, m_\ell \times P, n_\ell \times Q, 0_r\} \\ V &= \{0_r, -n_\ell \times P, m_\ell \times Q, -n_{\ell-1} \times P, m_{\ell-1} \times Q, \ldots, \ldots, -n_1 \times P, m_1 \times Q\}, \end{aligned}$$

$X = U + V$, $Y = U - V$. Then U, V and X, Y are both TCP's of length $(2\ell+1)r$.

Example 4 Let $M = ++$ and $N = +-$, let A, B, P, Q, 0_r be as above. Now

$$\begin{aligned} U &= PQP\bar{Q}0_r, \\ V &= 0_rPQ\bar{P}Q, \end{aligned}$$

and

$$\begin{aligned} X &= PAA\bar{A}Q, \\ Y &= P\bar{B}BB\bar{Q} \end{aligned}$$

are TCP's of length $5r$ and weight $4 \times w(A, B)$.

Hence, X and Y can be obtained by the above standard construction *as well as* the exhaustive computer–search.

Other multiplications obtained are a result of applying "shorter" multiplications appropriately. For example, starting with $X = PA\bar{Q}$, $Y = \bar{P}B\bar{Q}$, some of the multiplications by $m = 6$ and $f = 8$ can be obtained by applying the "shorter" multiplications by $m = 3$ and $f = 4$ twice and then concatenating these results together. The TCP

$$\begin{aligned} X_{new} &= XY &= PA\bar{Q}\bar{P}B\bar{Q}, \\ Y_{new} &= X\bar{Y} &= PA\bar{Q}P\bar{B}Q \end{aligned}$$

is obtained in this way. We can obtain another TCP X_{new_2}, Y_{new_2} by applying a special kind of interleaving '&'. $X\&Y$ is the sequence Y interleaved into the sequence X blockwise. That is,

$$\begin{aligned} X_{new_2} &= X\&Y &= P\bar{P}AB\bar{Q}\bar{Q}, \\ Y_{new_2} &= X\&\bar{Y} &= PPA\bar{B}\bar{Q}Q. \end{aligned}$$

Note that for this special type of interleaving we have to know the length of the initial sequences that formed X and Y.

There is a large set of results for which none of the above constructions apply. That is, these results can neither be obtained by (known) standard constructions nor can they be shown to be they equivalent to others. For example

$$\begin{aligned} X &= \bar{Q}\bar{B}ABP\bar{Q}P, \\ Y &= \bar{Q}\bar{P}\bar{Q}\bar{A}BA\bar{P} \end{aligned}$$

is such a result.

The question which arises immediately, is, whether there are other unknown standard constructions that lead to these results or whether these multiplications occur "randomly".

5 Numerical Consequences and Applications

Multiplications of four sequences A,B,C,D:

Note that if there are four ternary sequences A, B, C and D with zero nonperiodic autocorrelation function and with A, B and C, D having their zeros in the same positions respectively, then all the above multiplications can be applied to A, B and C, D.

Example 5 Given four sequences A, B, C, D of length n and weight w with the properties mentioned above, the multiplication

$$\begin{aligned} X &= PA\bar{Q}, \\ Y &= \bar{P}B\bar{Q} \end{aligned}$$

can be applied as follows to A, B, C and D. We let

$$\begin{aligned} P_1 &= \tfrac{1}{2}(A+B), & Q_1 &= \tfrac{1}{2}(A-B), \\ P_2 &= \tfrac{1}{2}(C+D), & Q_2 &= \tfrac{1}{2}(C-D). \end{aligned}$$

Now

$$\begin{aligned} X &= P_1 A \bar{Q}_1, \\ Y &= \bar{P}_1 B \bar{Q}_1, \\ Z &= P_2 C \bar{Q}_2, \\ W &= \bar{P}_2 D \bar{Q}_2, \end{aligned}$$

and X, Y, Z, W are four sequences of length $3n$ and weight $2w$ with zero nonperiodic autocorrelation function.

Hence, all the multiplications apply to four sequences (with zeros in the appropriate positions) as well.

Weighing matrices:

Weighing matrices can be constructed by using four sequences of length n and weight w with zero (non)periodic autocorrelation function. These four sequences serve to generate four circulant matrices, say M_1, M_2, M_3, M_4, with the following property:

$$M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T = wI_n,$$

where I_n is the identity matrix of order n. Now M_1, M_2, M_3, M_4 can be used in the Goethals–Seidel array (for details of the construction see for example [4] or [11]) to form a $W(4n, w)$.

If we have four sequences with zero nonperiodic autocorrelation function, we can either put them directly into the four matrices M_1, M_2, M_3, M_4, or *first* multiply them, *and then* form M_1, M_2, M_3, M_4 which are then used in the Goethals–Seidel array to construct the weighing matrices. There are many families of four sequences with zero nonperiodic autocorrelation function known. Other families of four sequences with the desired properties can be easily formed from TCP's. If we have, for example, a TCP A, B of length n and weight w, then $X = A$, $Y = A$, $Z = B$, $W = B$ are four sequences with zero nonperiodic autocorrelation function which can be used in the constructions mentioned above to form weighing matrices. Since we can always append an arbitrary number of zeros to each of the four sequences before constructing M_1, M_2, M_3, M_4, we only consider "shortest" multiplications (that is, with minimum m) for each f. All the other multiplications do not to lead to any new order or weight for the weighing matrices or they are trivial. In particular, we concentrate on the following multiplications (m, f):

$(1,2)$	"no multiplication",
$(3,5)$	multiply the weight by $2\frac{1}{2}$.

The constructions and the resulting parameters are described in the following lemmas.

Lemma 3 *There is a weighing matrix*

$$W(4n+4+4x, 4n+2) \text{ and } W(12n+12+4x, 10n+5),$$

where $x \geq 0$, *and* $n \in \{1, 2, \ldots, 30\} \cup \{2^a 10^b 26^c | a, b, c \geq 0\}$.

Proof. Take base sequences of lengths $n+1$, $n+1$, n, n and weight $4n+2$ and multiply them as indicated above. Since base sequences do exist for $n \in \{1, 2, \ldots, 30\} \cup \{2^a 10^b 26^c | a, b, c \geq 0\}$ ([7]) and since we can always append an arbitrary number x or $x+1$ of zeros to each sequence before constructing M_1, M_2, M_3, M_4, we get weighing matrices with the above parameters. □

Lemma 4 *There is a weighing matrix*

$$W(4n+4x, w) \text{ and } W(12n+4x, 2\frac{1}{2}w),$$

where $x \geq 0$, *and*

$$\begin{aligned}(n,w) \in\ & \{(5,16),(5,18),(5,20),(7,22),(8,24),(7,26),(7,28),\\ & (11,44),(14,52),(15,54)\}\\ \cup\ & \{(2^a 10^b 26c, 2 \times 2^a 10^b 26^c) | a,b,c \geq 0\}\\ \cup\ & \{(2^a 10^b 26^c + 1, 2 \times 2^a 10^b 26^c + 2) | a,b,c \geq 0\}.\end{aligned}$$

Proof. Take four sequences of type A,B,C,C (that is, A, B, C, C have zero nonperiodic autocorrelation function) of lengths n, n, p, p, $n \geq p$ and weight w, where A, B have their zeros in the same positions. We can again append x or $x+n-p$ zeros to each sequence before constructing M_1, M_2, M_3 and M_4. The sequences of type A,B,C,C with the desired properties are shown to exist for the above parameters (n,w) in [5], and they can be constructed for

$$\begin{aligned}(n,w) \in\ & \{(2^a 10^b 26^c, 2 \times 2^a 10^b 26^c) | a,b,c \geq 0\}\\ \cup\ & \{(2^a 10^b 26^c + 1, 2 \times 2^a 10^b 26^c + 2) | a,b,c \geq 0\}\end{aligned}$$

from Golay sequences. □

Lemma 5 *There is a weighing matrix*

$$\begin{aligned}&W(4n+4x, 2w), && W(4n+4+4x, 2w+2), && W(8n+4+4x, 4w+1),\\ &W(12n+4x, 5w), && W(12n+4+4x, 5w+2), && W(24n+4+4x, 10w+1),\end{aligned}$$

where $x \geq 0$, *and*

$$(n,w) \in \{(6,10),(14,26)\} \cup \{(2^a 10^b 26^c, 2 \times 2^a 10^b 26^c) | a,b,c \geq 0\}.$$

Proof. Take a TCP A, B of length n and weight w with zeros in the same positions. We can now take the four sequences A, B, A, B of lengths n and weight $2w$ and carry out the same constructions as above. This explains the first column of weighing matrices of the lemma. For the second column, consider the sequences X, Y, X, Y of lengths mn and weight fw which are obtained by multiplying A and B by (m, f). We now let

$$E = \{X, 1\}, \ F = \{X, -1\}, \ G = H = Y,$$

and we take E, F, G, H (with x or $x+1$ zeros appended) as the first rows of the circulant matrices M_1, M_2, M_3, M_4. Finally, for the third column, we take X, Y as above and form

$$S = \{X, 0, X\}, \ T = \{X, 0, \bar{X}\}, \ U = \{Y, 0, Y^*\}, \ V = \{Y, a, \bar{Y}^*\}, \ a \neq 0.$$

Now S, T, U, V (with x zeros appended) have zero nonperiodic autocorrelation function and they serve to construct M_1, M_2, M_3, M_4. Since TCP's do exist for $n = 2^a 10^b 26^c$ and $w = 2n$ and for $(n, w) \in \{(6, 10), (14, 26)\}$ (for the last two pairs of (n, w) see [3] or [6]), we get the weighing matrices with the required parameters. □

In some cases, we can of course multiply more than once before constructing M_1, M_2, M_3, M_4. For example, we can multiply by $(m_1, f_1) = (2, 4)$ an arbitrary number of times, before finally multiplying by $(m_2, f_2) = (3, 5)$. Such kind of combined multiplications lead to other weighing matrices which are not listed in the above lemmas. Clearly, if we multiply more than once, the sequences in the intermediate steps must have their zeros in the same positions.

6 Conclusion and Further Research

A computer–search for obtaining longer TCP's from shorter ones has been presented. When testing the nonperiodic autocorrelation function, only the crosscorrelations of sequences and no single values of s had to be considered. The search led to many new and interesting results. Some of these results may be obtained by applying other already known constructions or by applying "shorter" multiplications more than once. Others turned out to be equivalent with previously found ones. However, there was a large set of configurations which was completely new or for which there is no construction method known. More research could be done in this direction.

The computer–search was easy to implement. This kind of computer–search could be adapted to find multiplications for any family of sequences with zero nonperiodic autocorrelation function.

References

[1] H. Davenport, The higher Arithmetic: An introduction to the theory of numbers, Harper and Brothers, New York, 1960.

[2] S. Eliahou, M. Kervaire and B. Saffari, A new restriction on the lengths of Golay complementary sequences, *Journal of Combinatorial Theory A*, 55, 49–59, 1990.

[3] A. Gavish and A. Lempel, On ternary complementary sequences, *IEEE Transactions on Information Theory*, 40, 2, 522–526, 1994.

[4] J-M. Goethals and J.J. Seidel, Orthogonal matrices with zero diagonal, *Canad. J. Math.*, 19, 1001–1010, 1967.

[5] M. Gysin and J. Seberry, On 4-NPAF$(1, 2w)$ sequences, to be published.

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

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

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

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

[10] J. Seberry, The skew–weighing matrix conjecture, *University of Indore Research J. Science*, 7, 1–7, 1982.

[11] 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, 431–560, 1992.

[12] J. Seberry and X-M. Zhang, Semi Williamson type matrices and the W(2n,n) conjecture, *J. Comb. Math. and Comb. Computing*, 11, 65–71, 1992.

(Received 23/11/95)