On Ternary Complementary Pairs

Marc Gysin[1] and Jennifer Seberry[2]
[1]School of Information Technology
James Cook University
Townsville, QLD 4811
Australia
[2]Centre for Computer Security Research
University of Wollongong
Wollongong, NSW 2522
Australia
*

Abstract

Let $A = \{a_0, \ldots, a_{\ell-1}\}$, $B = \{b_0, \ldots, b_{\ell-1}\}$ be two finite sequences of length ℓ. Their nonperiodic autocorrelation function $N_{A,B}(s)$ is defined as:

$$N_{A,B}(s) = \sum_{i=0}^{\ell-1-s} a_i a_{i+s}^* + \sum_{i=0}^{\ell-1-s} b_i b_{i+s}^*, \quad s = 0, \ldots, \ell-1,$$

where x^* is the complex conjugate of x. If $N_{A,B}(s) = 0$ for $s = 1, \ldots, \ell - 1$ then A, B is called a complementary pair. If, furthermore, $a_i, b_i \in \{-1, 1\}$, $i = 0, \ldots, \ell-1$, or, $a_i, b_i \in \{-1, 0, 1\}$, $i = 0, \ldots, \ell-1$, then A, B is called a binary complementary pair (BCP), or, a ternary complementary pair (TCP), respectively. A BCP is also called Golay sequences. A TCP is a generalisation of a BCP. Since Golay sequences are only known to exist for lengths $n = 2^a 10^b 26^c$, $a, b, c \geq 0$, recent papers have focused on TCP's.

The purpose of this paper is to give an overview of existing constructions and techniques and present a variety of new constructions, new restrictions on the deficiencies and new computational results for TCP's. In particular:

- We give many new constructions which concatenate shorter group of sequences to obtain longer sequences. Many of these constructions can be applied recursively and lead to infinite families of TCP's.
- We give many new restrictions on TCP's of lengths ℓ and deficiencies $\delta = 2x$, where $x \equiv \ell \bmod 4$.
- We settle all the cases for existence/non–existence of TCP's of lengths $\ell \leq 20$ and weights $w \leq 40$.
- We give TCP's with minimum deficiencies for all lengths $\ell \leq 22$.

Keywords: autocorrelation function, Golay sequences, ternary complementary pair, combinatorial search–algorithm.

*This research has been carried out while the first author was at the University of Wollongong.

1 Preliminaries

Let $A = \{a_0, \ldots, a_{\ell-1}\}$, $B = \{b_0, \ldots, b_{\ell-1}\}$ be two finite sequences of length ℓ. Their *nonperiodic autocorrelation function* $N_{A,B}(s)$ is defined as:

$$N_{A,B}(s) = \sum_{i=0}^{\ell-1-s} a_i a_{i+s}^* + \sum_{i=0}^{\ell-1-s} b_i b_{i+s}^*, \quad s = 0, \ldots, \ell-1,$$

where x^* is the complex conjugate of x. If A, B have $N_{A,B}(s) = 0$, $s = 1, \ldots, \ell-1$, then A, B is called a *complementary pair*. Their *periodic autocorrelation function* $P_{A,B}(s)$ is defined as:

$$P_{A,B}(s) = \sum_{i=0}^{\ell-1} a_i a_{i+s}^* + \sum_{i=0}^{\ell-1} b_i b_{i+s}^*, \quad s = 0, \ldots, \ell-1,$$

where the subscripts are reduced modulo ℓ if necessary.

A complementary pair A, B with $a_i, b_i \in \{-1, 1\}$, $i = 0, \ldots, \ell-1$ is called a *binary complementary pair (BCP)* or *Golay sequences*. A complementary pair A, B with $a_i, b_i \in \{-1, 0, 1\}$, $i = 0, \ldots, \ell-1$ is called a *ternary complementary pair (TCP)*. Golay sequences have been extensively studied, [ElKeSa90], [Golay61], [Golay62], [SebYam92], and they are only known to exist for lengths $\ell = 2^a 10^b 26^c$, $a, b, c \geq 0$. The first unresolved cases are now $\ell = 74, 82, 106, 116, 122$. Because there are many lengths ℓ for which Golay sequences do not exist, one is motivated to generalise the definition for Golay sequences in some way and then search for the generalised case. One such possible generalisation are TCP's. The paper by [GavLem94] gives many TCP's and constructions for TCP's. The *weight $w_{A,B}$ of two sequences A and B* is defined as their total number of non–zero entries in A and B. That is,

$$w_{A,B} = N_{A,B}(0) = P_{A,B}(0).$$

The *deficiency $\delta_{A,B}$ of two sequences A and B* is defined as their total number of zero entries. That is,

$$\delta_{A,B} = 2\ell - w_{A,B}.$$

For a given length ℓ, a TCP with minimum possible deficiency is called an *optimal TCP*. Two sequences which have their zeroes in the same positions are called *disjointable sequences*. Disjointable sequences which are TCP's are important blocks in many standard constructions, see for example, Theorem 2 and Lemma 2. The following facts about $N_{A,B}$, $P_{A,B}$ and $w_{A,B}$ are well known and can be easily proven.

(i)

$$P_{A,B}(s) = N_{A,B}(s) + N_{A,B}(\ell - s), \ s = 1, \ldots, \ell-1.$$

(ii)

$$P_{A,B}(s) = P_{A,B}(\ell - s), \ s = 1, \ldots, \ell-1.$$

(iii)

$$|\sum_{i=0}^{\ell-1} a_i|^2 + |\sum_{i=0}^{\ell-1} b_i|^2 = 2\sum_{s=1}^{\ell-1} N_{A,B}(s) + w_{A,B} = \sum_{s=1}^{\ell-1} P_{A,B}(s) + w_{A,B}.$$

In particular, if A, B is a TCP, then:

(i)

$$P_{A,B}(s) = 0, \ \ s = 1, \ldots, \ell - 1.$$

(ii)

$$(\sum_{i=0}^{\ell-1} a_i)^2 + (\sum_{i=0}^{\ell-1} b_i)^2 = w_{A,B}.$$

(ii) means that the weight $w_{A,B}$ must be a sum of two squares as a *necessary but not sufficient condition* for A, B to be a TCP. From number theory (see, for example, [AdlCou95]) we know that $w_{A,B}$ is the sum of two squares if and only if every prime factor $\equiv 3 \bmod 4$ appears to an even power in the prime factorisation of $w_{A,B}$. Therefore, (i) $w_{A,B} \not\equiv 3 \bmod 4$; and; (ii) $w_{A,B} \not\equiv 6 \bmod 8$ as necessary (but not sufficient) conditions. [ElKeSa90] proved the following result which is *stronger* than (i) and (ii): The weight of a TCP (or BCP) can have no factor $\equiv 3 \bmod 4$.

Let A, B be a TCP and let $A^{(k,m)}$, $B^{(k,m)}$ be a pair of complex valued sequences where (for $j = 0, \ldots, \ell - 1$, $i^2 = -1$)

$$\begin{aligned} a_j^{(k,m)} &= a_j \cdot e^{2\pi ikj/m}, \\ b_j^{(k,m)} &= b_j \cdot e^{2\pi ikj/m}. \end{aligned}$$

Then $A^{(k,m)}$, $B^{(k,m)}$ is a complementary pair. For a proof consider $N_{A^{(k,m)},B^{(k,m)}}(s)$, $s = 1, \ldots, \ell - 1$. We have

$$\begin{aligned} N_{A^{(k,m)},B^{(k,m)}}(s) &= \sum_{j=0}^{\ell-1-s} a_j e^{2\pi ikj/m} a_{j+s} e^{-(2\pi ik(j+s)/m)} + \\ &\quad \sum_{j=0}^{\ell-1-s} b_j e^{2\pi ikj/m} b_{j+s} e^{-(2\pi ik(j+s)/m)} \\ &= e^{-2\pi iks/m} \sum_{j=0}^{\ell-1-s} a_j a_{j+s} + e^{-2\pi iks/m} \sum_{j=0}^{\ell-1-s} b_j b_{j+s} \\ &= N_{A,B}(s) = 0. \end{aligned}$$

The case $m = 2$ corresponds to negating every alternating element in A and B. In this case $A^{(k,2)}$, $B^{(k,2)}$ is another TCP. [Golay61] showed that there are six isomorphic transformations for a BCP A, B. These six transformation translate directly to the case of a TCP A, B. These are: (i) interchange A and B; (ii) reverse A; (iii) reverse B; (iv) negate A; (v) negate B; and; (vi) negate every alternating element in A and B. TCP's that can be transformed into one other using one or more of the above operations are said to be *equivalent*.

Notation: If A is a sequence then $\bar{A}$ denotes the sequence A with each of its elements negated and $A^{'}$ denotes the sequence A reversed.

2 Multiplications of TCP's

In this section, longer sequences are obtained by concatenating shorter groups of sequences in a certain way. We call such constructions as "multiplications". The following lemma is a result of applying one of the well known Golay constructions, [Golay61], to multiply (or concatenate) TCP's. This construction was originally given for BCP's.

Lemma 1 *Let M, N and P, Q be TCP's of length ℓ and r respectively, then*

$$\begin{aligned} X &= \{m_1 \times P, n_1 \times Q, m_2 \times P, n_2 \times Q, \ldots, \ldots, m_\ell \times P, n_\ell \times Q\} \\ Y &= \{-n_\ell \times P, m_\ell \times Q, -n_{\ell-1} \times P, m_{\ell-1} \times Q, \ldots, \ldots, -n_1 \times P, m_1 \times Q\} \end{aligned}$$

is a TCP of length $2\ell r$.

We shift the sequences X and Y r positions: X by appending r zeros and Y by prefacing with r zeros to obtain the following new powerful construction.

Theorem 1 *Let A, B be a disjointable TCP 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*

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

$U = X+Y$, $V = X-Y$. Then X, Y and U, V are both TCP's of length $(2\ell+1)r$ and U, V have weight $w_{U,V} = w_{A,B} w_{M,N}$.

Proof. Follows directly from Lemma 1 and the construction. □

Note that because of the construction, U and V are disjointable. This means that the above construction can be applied recursively by setting either $A_{new} = U$, $B_{new} = V$ or $M_{new} = U$, $N_{new} = V$.

Example 1 (We replace 1 by '+' and -1 by '–'.)
Let $\ell = 9$, $M = + + + + 0 + - - +$, $N = + + - - 0 + - + -$. Let $P = \frac{1}{2}(A+B)$ and $Q = \frac{1}{2}(A-B)$ be a TCP of length r, let 0 denote the sequence of r zeros. Now

```
X = P  Q  P  Q  P -Q  P -Q  0  0  P  Q -P -Q -P  Q  P -Q  0
Y = 0  P  Q -P -Q  P -Q -P  Q  0  0  P  Q  P  Q -P  Q -P  Q

U = P  A  A -B  B  B  B -A  Q  0  P  A -B  B -B -B  A -A  Q
V = P -B  B  A  A -A  A  B -Q  0  P -B -A -A -A  A  B  B -Q,
```

and X, Y and U, V are TCP's of length $n = 19r$ and $w_{U,V} = 16 w_{A,B}$.

Remark: The construction in Theorem 1 can be generalised by shifting X and Y $(2k+1)r$ positions and prefacing/appending $(2k+1)r$ zeroes. The TCP's U, V obtained will have lengths $(2\ell + 2k + 1)r$ and weights $w_{U,V} = w_{A,B} w_{M,N}$. Theorem 1 is the case $k = 0$.

We restate a theorem from [GerSeb79] that originally has been given by R.J. Turyn.

Theorem 2 *Let A, B and M, N be TCP's of length n and and r, respectively. Assume that A, B are disjointable and let $P = \frac{1}{2}(A+B)$, $Q = \frac{1}{2}(A-B)$. Let '$\times$' denote the Kronecker–product. Let*

$$\begin{aligned} U &= P \times M + Q \times N', \\ V &= P \times N - Q \times M'. \end{aligned}$$

Then U, V is a TCP of length nr and weight $\frac{1}{2} w_{A,B} w_{M,N}$. U, V will be disjointable if M, N are disjointable.

If A, B is a TCP of length ℓ and 0_m is a sequences of m zeroes $m \geq 0$, then it is easy to see that $A0_mB$, $A0_m\bar{B}$ is a TCP of length $2\ell + m$. This is a standard construction and it is a special case of a family of constructions which are given in the following lemma.

Lemma 2 *Let X, Y and M, N be TCP's of lengths n and r respectively. Let 0_m be a sequence of m zeros ($m \geq 0$). Let*

$$\begin{aligned} A &= M \times X \quad 0_m \quad N' \times Y \\ B &= N \times X \quad 0_m \quad \bar{M}' \times Y, \end{aligned}$$

$$\begin{aligned} C &= M \times X \quad N' \times Y \quad 0_m \quad N \times X \quad \bar{M}' \times Y \\ D &= M \times X \quad N' \times Y \quad 0_m \quad \bar{N} \times X \quad M' \times Y, \end{aligned}$$

$$\begin{aligned} E &= M \times X \quad N \times Y' \quad 0_m \quad M \times Y \quad N \times \bar{X}' \\ F &= M \times X \quad N \times Y' \quad 0_m \quad M \times \bar{Y} \quad N \times X', \end{aligned}$$

$$\begin{aligned} G &= M \times X \quad \bar{N}' \times X \quad 0_m \quad N \times Y \quad M' \times Y \\ H &= M \times X \quad N' \times X \quad 0_m \quad N \times Y \quad \bar{M}' \times Y, \end{aligned}$$

$$\begin{aligned} I &= M \times X \quad M \times \bar{Y}' \quad 0_m \quad N \times Y \quad N \times X' \\ J &= M \times X \quad M \times Y' \quad 0_m \quad N \times Y \quad N \times \bar{X}'; \end{aligned}$$

and if M and N are disjointable, let $P = \frac{1}{2}(M+N)$, $Q = \frac{1}{2}(M-N)$, and let

$$\begin{aligned} U &= P \times X + Q \times Y \quad 0_m \quad P \times \bar{Y}' + Q \times X' \\ V &= P \times X + Q \times Y \quad 0_m \quad P \times Y' + Q \times \bar{X}'. \end{aligned}$$

Then A, B and U, V are TCP's of lengths $2nr + m$ and weights $w_{X,Y} w_{M,N}$, and C, D; E, F; G, H and I, J are TCP's of lengths $4nr + m$ and weights $2w_{X,Y} w_{M,N}$.

Proof. Follows directly from the construction. Examples can be constructed using the sequences with length $n = 7$ and weight 10 to show the inequivalence of these constructions. □

Remark: The two constructions yielding the TCP's C, D and E, F are almost identical except that the roles (but not the positions in the Kronecker product) for M, N and X, Y are exchanged. The same statement is true for the TCP's G, H and I, J.

[GavLem94], Page 525, gives an important construction how disjointable sequences A, B of a TCP can be padded with an appropriate number of zeroes,

reversed and "hooked onto each other" to get a BCP. This construction can be generalised in a straightforward manner to yield TCP's. In particular, if A, B is a disjointable TCP of length ℓ and weight $w_{A,B}$ and A (and therefore B) can be padded with m zeroes at the end such that the resulting sequence $\tilde{A}$ satisfies $\tilde{a}_i = 0$ if[1] $\tilde{a}_{\ell+m-1-i} \neq 0$, then $\tilde{A}+\tilde{B}'$, $\tilde{A}-\tilde{B}'$ is a TCP of length $\ell+m$ and weight $2w_{A,B}$.

The construction in Theorem 7, in [GavLem94] starts with a BCP A, B, lets $P = \frac{1}{2}(A+B)$, $Q = \frac{1}{2}(A-B)$ and then obtains a new TCP where the length is multiplied by 3 and the weight is multiplied by $2\frac{1}{2}$ by concatenating A, B, P and Q and reversed and/or negated versions of A, B, P and Q appropriately. A few remarks are now in order: (i) the construction generalises directly to the case of a disjointable TCP. (ii) When trying to find other similar constructions that also give TCP's, one needs to make sure that (iia) the total number of A's in the new sequences equals the total number of B's and the total number of P's equals the total number of Q's; and; (iib) when considering the nonperiodic autocorrelation function, the sequences A, B, P and Q which are the building blocks of the longer sequences can be treated as if they were normal variables with one exception: shifting the sequences into each other is not commutative. For example, shifting the sequence A into the sequence B is not the same as shifting the sequence B into the sequence A. In such cases some of the sequences may need to be reversed appropriately in order to get the desired results. (iii) There are many inequivalent such constructions that give TCP's and from (ii) it should be clear that it is easy to search for such constructions either "by hand" (if there are only very few concatenations) or by computer if there are more concatenations involved.

For the remainder of this section we denote such constructions by a multiplication of type (m, f), if the initial length of the TCP is multiplied by m and its weight by f. It is desirable to find multiplications of type $(m, f = m)$ rather than type $(m, f < m)$. Because the final weight also needs to be a sum of two squares and from the preliminaries, we immediately derive that the following multiplications (m, f) are *not* possible for the following f's: $2f = 3, 6, 7, \ldots$. More precisely, multiplications of the type (m, f) are not possible, if in the prime factorisation of $2f$ there is an prime factor $\equiv 3 \bmod 4$ appearing to an odd power. Hence, for example, multiplications of the type $(3, 3)$ or $(7, 7)$ are not possible. Table 1 gives some multiplications. More multiplications and more details can be found in [GysSeb96].

3 Restrictions on the Deficiencies for TCP's

3.1 Equations Modulo 4

Suppose A, B is a TCP. Then from their nonperiodic autocorrelation function we can derive two useful facts: (i) the number of ± 1–terms arising from $N_{A,B}(s)$ must be even for *each* $s = 1, \ldots, \ell - 1$ since otherwise $N_{A,B}(s) = 0$ is not possible. (ii) The nonlinear equations $N_{A,B}(s)$ can be changed into linear equations by

[1] This "if" is the only difference from the construction in [GavLem94]. In [GavLem94] this "if" is an "if and only if" and subsequently yielded a BCP and not a TCP.

(m, f)	Example
$(3, 2)$	$PA\bar{Q}$ $\bar{P}B\bar{Q}$
$(3, 2\frac{1}{2})$	AQB $\bar{A}PB$
$(4, 2\frac{1}{2})$	$PQA\bar{Q}$ $\bar{P}BP\bar{Q}$
$(5, 4)$	$PA\bar{A}B\bar{Q}$ $\bar{P}\bar{A}\bar{B}B\bar{Q}$
$(5, 4)$	$PB\bar{A}BQ$ $P\bar{A}\bar{B}\bar{A}\bar{Q}$
$(5, 4)$	$PAA\bar{A}Q$ $\bar{P}B\bar{B}\bar{B}Q$

Table 1: Multiplications of TCP's.

considering the following identity for $x, y \in \{-1, 1\}$: $xy + 1 \equiv x + y \bmod 4$. We call these equations *(reduced) equations modulo* 4 and denote them by $\tilde{N}_{A,B}(s)$. Clearly $\tilde{N}_{A,B}(s) \equiv 0 \bmod 4$, $s = 1, \ldots, \ell - 1$. The equations modulo 4 are linear and hence much easier to handle than the original ones.

Notice that neither converse is true, that is, the number of ± 1–terms arising from the nonperiodic autocorrelation function being even does *not* imply $N_{A,B}(s) = 0$ neither does $\tilde{N}_{A,B}(s) \equiv 0 \bmod 4$. Hence, (i) and (ii) can only be used for non–existence results.

Two more remarks on $\tilde{N}_{A,B}(s)$: (iia) Consider, say, $a_i + 2a_j + a_k \equiv 0 \bmod 4$, this equation can be simplified to $a_i + a_k \equiv 2 \bmod 4$. The general rule is that every term appearing twice on the left hand side can be omitted by adding 2 to the right hand side. (iib) each $\tilde{N}_{A,B}(s)$ gives "one bit" of information. The maximum amount of information we can gain is $\ell - 1$ bits in the (very unlikely) case that all the $\tilde{N}_{A,B}(s)$ are linearly independent.

Confirmation of known results:

BCP's of odd length do not exist: Assume the contrary, that is, there is a BCP of an odd length. Then any of the following additions $\tilde{N}_{A,B}(s) + \tilde{N}_{A,B}(\ell - s) \equiv 0 \bmod 4$, $s = 1, \ldots, \ell - 1$ with the above rules gives $0 \equiv 2 \bmod 4$, a contradiction.

A TCP of length $\ell > 3$ and deficiency $\delta = 1$ does not exist: Again we assume the contrary, that is a TCP with the above properties does exist. From remark (i) above it follows that the length ℓ must be odd and the zero must be in the middle of one sequence, say A. Again considering $\tilde{N}_{A,B}(s) + \tilde{N}_{A,B}(\ell - s) \equiv 0 \bmod 4$, for $s = 1, \ldots, \ell - 1$, one can show that the sequence A is symmetric, that is, $a_k = a_{\ell-1-k}$. Using $\tilde{N}_{A,B}(s)$, one can also show that B is skew–symmetric, that is, $b_k = -b_{\ell-k-1}$. However, this is a little bit more involved and details are

given in [GavLem94]. Finally, these symmetry conditions are used in the *original equations* $N_{A,B}(s)$ to show that a TCP with the above properties can not exist. Details are again given in [GavLem94].

New results:

New results obtained via equations modulo 4 are described in Section 3.2.

3.2 Restrictions for $\delta = 2x$, where $x \equiv \ell \bmod 4$ and Restrictions for $\delta = 3$

The equations modulo 4 led us to the following theorem. A proof is given in Appendix B.

Theorem 3 *Let A, B be two ternary sequences of length ℓ, let $\delta_{A,B} = 2x$, where $x \equiv \ell \bmod 4$ and assume A, B are disjointable. Let $\mathcal{T} = \sum_{a_i=0} i$.*

Now if $\ell \equiv 2 \bmod 4$ and $\mathcal{T} \equiv 0 \bmod 2$, then A and B cannot have zero periodic autocorrelation function.

Remark: The non–existence result in Theorem 3 is also valid if A and B are two ternary sequences and one can be shifted cyclically such that the shifted versions of A and B satisfy all the preconditions of the theorem.

Corollary 1 *Let A, B be two ternary sequences of length ℓ, let $\delta_{A,B} = 2x$, where $x \equiv \ell \bmod 4$ and assume A, B are disjointable. Let $\mathcal{T} = \sum_{a_i=0} i$.*

Now if

(i) $\ell \equiv 0 \bmod 4$ *and* $\mathcal{T} \equiv 1 \bmod 2$*; or;*

(ii) $\ell \equiv 1 \bmod 4$ *and* $\mathcal{T} \equiv 1 \bmod 2$*; or;*

(iii) $\ell \equiv 2 \bmod 4$ *and* $\mathcal{T} \equiv 0 \bmod 2$*; or;*

(iv) $\ell \equiv 3 \bmod 4$ *and* $\mathcal{T} \equiv 0 \bmod 2$*;*

then A, B can not be a TCP.

Proof. Assume the contrary, that is, there exists a TCP A, B, which fulfills either (i), (ii), (iii) or (iv) of the corollary. Now another TCP $\tilde{A}$, $\tilde{B}$ can be obtained by padding A, B with m zeroes, where m is the smallest non–negative residue equivalent to $2 - x \bmod 4$. Now $\tilde{A}$, $\tilde{B}$ have length $\tilde{\ell} \equiv 2 \bmod 4$ and it is easy to see that they also fulfill all the other preconditions of Theorem 3. Since $\tilde{A}$, $\tilde{B}$ have zero nonperiodic autocorrelation function they also have zero periodic autocorrelation function. This is a contradiction to Theorem 3. □

Remark: Two ternary sequences A, B of length $\ell \equiv x \bmod 4$ and $\delta_{A,B} = 2x + 2$ can neither have zero periodic nor zero nonperiodic autocorrelation function since $w_{A,B} \equiv 6 \bmod 8$.

Example 2 (i) Disjointable TCP's of lengths $\ell = 5, 9, 13, 17, \ldots$ and deficiency $\delta = 2$ and their zeroes in positions k, k odd, do not exist.

(ii) TCP's of lengths $4, 8, 12, 16, \ldots$ and deficiency $\delta = 2, 10, 18, 26, \ldots$ do not exist.

Lemma 3 Let A, B be a TCP of length ℓ and assume that its deficiency $\delta_{A,B} = 3$, then

(i) $\ell \equiv 2 \bmod 4$ and if $\ell = 4m + 2$ then (without loss of generality) $a_m = a_{\ell-m-1} = b_{\frac{\ell}{2}} = 0$.

Furthermore, if $a = \sum_{j=0}^{\ell-1} a_j$, $b = \sum_{j=0}^{\ell-1} b_j$, $a_{even} = \sum_{j \text{ even}} a_j$, $a_{odd} = \sum_{j \text{ odd}} a_j$, $b_{even} = \sum_{j \text{ even}} b_j$, $b_{odd} = \sum_{j \text{ odd}} b_j$, and $\ell = 4m + 2$ then

(ii) $a^2 + b^2 = 8m + 1$;

(iii) $a \equiv 0 \bmod 4$;

(iv) $b \equiv b_0 \bmod 4$;

(v) $a_k + a_{\ell-1-k} + b_k + b_{\ell-1-k} \equiv 2 \bmod 4$, for $k = 0, \ldots, m-1$;

(vi) furthermore, if the decomposition of $w_{A,B}$ into two squares is unique up to order and sign, then $a_{even} = a$ and $a_{odd} = 0$, or, $a_{even} = 0$ and $a_{odd} = a$;

(vii) furthermore, if the decomposition of $w_{A,B}$ into two squares is unique up to order and sign, then $b_{even} = b$ and $b_{odd} = 0$;

(viii) $m \geq 6$;

Lemma 3, (i) has also been given in [GavLem94].

Proof.

(i) Follows from the ± 1 terms arising from $N_{A,B}(s)$, the only possibility to have an even number of ± 1 terms for $s = 1, \ldots, \ell - 1$ is the one given above.

(ii) $a^2 + b^2 = w_{A,B} = 8m + 1$.

(iii) b is odd, hence $b^2 \equiv 1 \bmod 8$, since $a^2 + b^2 \equiv 1 \bmod 8$, we must have $a \equiv 0 \bmod 4$.

(iv) Consider $\tilde{N}_{A,B}(\frac{\ell}{2}) \equiv 0 \bmod 4$. This equations yields $a + b - b_0 \equiv 0 \bmod 4$. Hence, together with (iii) $b \equiv b_0 \bmod 4$.

(v) Follows from $\tilde{N}_{A,B}(\ell - 1) \equiv 0 \bmod 4, \ldots, \tilde{N}_{A,B}(\ell - m) \equiv 0 \bmod 4$.

(vi) Consider the equivalent TCP C, D which is obtained from A, B by alternating every second element. Clearly C, D must also satisfy (iii) which gives restriction (vi).

(vii) As (vi) and taking into account that b_{even} has an odd number of ± 1 terms (and b_{odd} an even number of ± 1 terms). Hence, $b_{even} \neq 0$.

(viii) Follows from an exhaustive computer–search through all possible candidate sequences.

□

Two sequences with zero periodic autocorrelation function and $\delta = 3$ exist: We did not find any TCP with $\delta = 3$. Two ternary sequences with zero *periodic* autocorrelation function and $\delta = 3$ do exist as the following sequences A, B of length $\ell = 10$ show:

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

4 Computational Results and Numerical Consequences

4.1 A Combinatorial Search–Algorithm for TCP's

Let A, B be a TCP and let $A^{(k,m)}$, $B^{(k,m)}$ be as in Section 1 and let $a^{(k,m)} = \sum_{i=0}^{\ell-1} a_i^{(k,m)}$, $b^{(k,m)} = \sum_{i=0}^{\ell-1} b_i^{(k,m)}$. Now $A^{(k,m)}$, $B^{(k,m)}$ are a complementary pair and hence, $|a^{(k,m)}|^2 + |b^{(k,m)}|^2 = w_{A,B}$. Notice that $|a^{(k,m)}|^2$ and $|b^{(k,m)}|^2$ are two non–negative real values. This property can be used to drastically improve the performance of a combinatorial search–algorithm that is trying to find TCP's of a given length ℓ and weight $w_{A,B}$. Suppose the algorithm has a certain *candidate* sequence A which may is a member of a TCP A, B. The algorithm can now test if

$$|a^{(k,m)}|^2 > w_{A,B}$$

for *any* integer values k, m. If this test is positive, then (since $|b^{(k,m)}|^2 \geq 0$) A can not be a member of such a TCP. Notice that this process does *not* involve the inspection of any candidate sequence B.

Remarks: (i) If $m = \ell$ and the sequences A and B are interpreted as a signal then $|a^{(k,\ell)}|^2$, $|b^{(k,\ell)}|^2$ can be interpreted as the magnitudes of the discrete Fourier transform of A and B. (ii) This algorithm can easily be adapted such that the above test works for any families of sequences with constant periodic (or nonperiodic) autocorrelation function. (iii) We are indebted to R. Fletcher, [Fletcher97] who mentioned this test to us for sequences with constant periodic autocorrelation function.

4.2 Computational Results and Numerical Consequences

The above algorithm enabled us to search through all candidate TCP's of length $\ell \leq 20$ and weight $w \leq 40$. TCP's that both started and/or ended with a zero element were not counted. The existence/non–existence results for TCP's with these parameters are given in Appendix A. We were also able to search for optimal TCP's up to length $\ell = 22$. For lengths 2 to 22 these are given in Table 2. Optimal TCP's up to length $\ell = 12$ and for $\ell = 14$ are also given in [GavLem94]. In Table 2 "$C(l, d, z)$" means that the TCP for the given length ℓ and deficiency $\delta_{A,B}$ can be obtained via the standard construction (Lemma 2) with a TCP of length l and and deficiency d and insertion of z zeroes. Instead of asking for the minimum deficiency δ for a given length ℓ, one could also ask for the minimum length ℓ for a given weight w. The results in Appendix A and some further

searches allowed us to answer these questions for some instances. The answers are given in Table 3. "∞" means that there is no TCP for the given weight w.

In Table 2, the TCP's of length 12, 15 and 18 can be "hooked onto each other" as described in Section 1 to give TCP's of length $\ell = 22, 28, 34$ and deficiences $\delta = 4$. The TCP of length $\ell = 22$ and deficiency $\delta = 4$ has been proven optimal via exhaustive computer–search through candidate sequences of smaller deficiencies. The other TCP's may or may not be optimal. Let A, B be a TCP with $\delta_{A,B} \geq 3$. In this case, the zeroes are usually in the same positions of different sequences. But this is not always so as the following example of a TCP A, B with $\delta_{A,B} = 4$ shows:

$$\begin{aligned} A &= +0+000+, \\ B &= +++--+-. \end{aligned}$$

All the TCP's (except the one of length $\ell = 3$) in Table 2 are disjointable. Hence, they can be applied in Theorem 2 to give new TCP's. Since the new TCP's obtained are also disjointable, Theorem 2 can be applied recursively yielding the following corollary.

Corollary 2 There are TCP's of lengths

$$\ell = 2^{a+c+f+i+n} 3^{c+2e+j+m} 5^{b+f+j} 7^{d+i+m} 11^{g+n} 13^{h} 17^{k} 19^{l}$$

and weights

$$w = 2^{1+a+2b+3e+f+3g+h+4k+4l+2m+2n} 5^{c+d+f+h+m+n} 13^{i+j}$$

for all integers $a, b, c, d, e, f, g, h, i, j, k, l, m, n \geq 0$.

Remark: TCP's of different lengths and smaller deficiencies may be obtained by, for example, appending a zero to a TCP of length $\ell = 10$ and deficiency $\delta = 0$ and, in the construction, counting this as a TCP of length 11 and deficiency $\delta = 2$ and then removing possible initial and/or final runs of zeroes in the final TCP's.

5 Conclusion and Further Research

The two sizes minimum deficiency δ for a given length ℓ (Table 2) and minimum length ℓ for a given weight w (Table 3) display a rather "wild and erratic behaviour". This is not surprising from a combinatorialist's point of view. Nevertheless, the standard construction in Lemma 2 often yields optimal TCP's. It is natural to ask whether there are multiplications or standard constructions that give only optimal TCP's. We conjecture that the answer to this question is a negative one.

The case $\delta = 3$ and TCP's is not settled yet. Lemma 3 provides some restrictions but it would be much more satisfactory to have a TCP with $\delta = 3$ or have a non–existence proof for such TCP's.

Theorem 3 states that two sequences with deficiency $\delta = 4, 12, 20, \ldots$ and certain properties cannot have zero periodic autocorrelation function. Since the periodic

ℓ	$\delta_{A,B}$	Example	Remarks
2	0	$++,\ +-$	Golay sequences
3	1	$++-,\ +0+$	only example of $\delta = 1$
4	0	$+++-,\ ++-+$	Golay sequences
5	2	$++0+-,\ ++0-+$	$C(2,0,1)$
6	2	$+++0-+,\ -+-0++$	also via $C(3,1,0)$
7	4	$+0+0-++,\ +0+0+--$	$C(3,1,1)$
8	0	$++++++--+,$ $++--+-+-$	Golay sequences
9	2	$+-++0+++-,$ $+-++0----+$	$C(4,0,1)$
10	0	$+++++-+--+,$ $++--+++-+-$	Golay sequences
11	6	$+0+-+0+0-++,$ $+0-++0+0---$	also via $C(4,0,3)$
12	4	$-+++0++--+0+,$ $-+++0+-++-0-$	give optimal TCP of length 22, $\delta = 4$
13	6	$-+++0+0+--+0+,$ $-+++0+0-++-0-$	also via $C(6,2,1)$
14	2	$+0++++--+++-+-,$ $-0-++++-++--+-$	give BCP of length 26
15	4	$++-+++++-0-+-0+,$ $++-+++---0+-+0-$	give TCP of length 28, $\delta = 4$
16	0	$++++++---++--+-+,$ $++++--+++-++-+-+-$	Golay sequences
17	2	$+++++--0+-+--++-,$ $++--++++0+--+-+-+$	also via $C(8,0,1)$
18	4	$+0++++-+--+--++0-,$ $+0+-+-++++---++-0+$	also via $C(8,0,2)$
19	6	$+++++--+000++--+-+-,$ $+++++--+000--++-+-+$	$C(8,0,3)$
20	0	$++++++--+$ $++--+++-+-,$ $++++++--+$ $--++----+-+$	Golay sequences
21	2	$++++++--+0$ $++--+++-+-,$ $++++++--+0$ $--++----+-+$	$C(10,0,1)$
22	4	$+-+-++++0-+$ $++0+--+---++,$ $++++++--0--$ $+-0++---++-$	also via $C(10,0,2)$

Table 2: Optimal TCP's for lengths ℓ, $2 \le \ell \le 22$.

w	1	2	3	4	5	6	7	8	9	10
ℓ	1	1	∞	2	3	∞	∞	4	∞	6
w	11	12	13	14	15	16	17	18	19	20
ℓ	∞	∞	9	∞	∞	8	13	∞	∞	10
w	21	22	23	24	25	26	27	28	29	30
ℓ	∞	∞	∞	∞	18	14	∞	∞	> 20	∞
w	31	32	33	34	35	36	37	38	39	40
ℓ	∞	16	∞	> 20	∞	∞	> 20	∞	∞	20

Table 3: Minimum lengths ℓ for a given weight w.

autocorrelation function being zero is a *weaker* requirement than the nonperiodic autocorrelation function being zero, non–existence for certain sequences with periodic autocorrelation function being zero is a *stronger* result. It, for example, also implies that there are no weighing matrices (definition of weighing matrices not given in this paper) constructed from two circulants with certain properties.

Many patterns and structures occur in TCP's and multiplications obtained via computer. Some of these patterns deserve to be further examined and may lead to other new theorems and a deeper understanding of TCP's and combinatorial designs or sequences.

Acknowledgment

Supported by the ARC grants A49131885 and A9130102, The University of Wollongong and the Centre for Computer Security Research.

References

[AdlCou95] A. Adler and J.E. Coury, *The Theory of Numbers*, Jones and Bartlett Publishers International, London, United Kingdom, 1995.

[ElKeSa90] 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.

[Fletcher97] R. Fletcher, Manuscripts and personal communications, 1997.

[GavLem94] A. Gavish and A. Lempel, On ternary complementary sequences, *IEEE Transactions on Information Theory*, 40, 2, 522–526, 1994.

[Golay61] M.J.E. Golay, Complementary series, *IRE Trans. Information Theory* IT–7, 82–87, 1961.

[Golay62] M.J.E. Golay, Note on Complementary series, *Proc. of the IRE* 84, 1962.

[GerSeb79] A.V. Geramita and J.Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York – Basel, 1979.

[GysSeb96] M. Gysin and J. Seberry, Multiplications of ternary complementary pairs, *Australasian Journal of Combinatorics*, 14, 165–180, 1996.

[Koukouvinos98] C. Koukouvinos, On ternary complementary sequences, *Bulletin of the Institute of Combinatorial Applications*, 22, 99–101, 1998.

[KouSeb93] C. Koukouvinos and J. Seberry, On weighing matrices, *Utilitas Mathematica*, 43, 101–127, 1993.

[KouSeb99] C. Koukouvinos and J. Seberry, New weighing matrices constructed using two sequences with zero autocorrelation function – a review, accepted for publication in *Journal of Statistical Planning and Inference*.

[1KKSYY91] 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.

[2KKSYY91] 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.

[Schroeder84] M.R. Schroeder, *Number Theory in Science and Communication*, Springer–Verlag, New York, 1984.

[SebYam92] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, *Contemporary Design Theory – a Collection of Surveys*, eds. J. Dinitz and D.R. Stinson, John Wiley and Sons, New York, 431–560, 1992.

A Existence Results for TCP's of Lengths $\ell \leq 20$ and Weights $w \leq 40$

In Table 4 and 5 we give the existence results for TCP's of length $\ell \leq 20$ and weight $w \leq 40$. The following abbreviations are used. **YG**: yes, Golay sequences; **YFG**: yes, standard construction (Lemma 2) with Golay sequences of weight $\frac{w}{2}$; **Y**: yes, via computer–search; **YFT**: yes, standard construction (Lemma 2) with a TCP of smaller length of weight $\frac{w}{2}$; **YFTI**: yes, from a TCP of the same weight and by interleaving zeroes (for example, if $\{a_0, a_1, \ldots, a_{l-1}\}$, $\{b_0, b_1, \ldots, b_{l-1}\}$ is a TCP of length l, then $\{a_0, 0, a_1, 0, \ldots, 0, a_{l-1}\}$, $\{b_0, 0, b_1, 0, \ldots, 0, b_{l-1}\}$ is a TCP of length $2l-1$); **YHT**: yes, by "hooking" a TCP of length $\frac{\ell+2}{2}$ and weight $\frac{w}{2}$ "onto each other"; **N**: no, via exhaustive computer–search; **N1**: no, deficiency $\delta = 1$ and $\ell > 3$; **NSQ**: no, not the sum of two squares; **NW**: no, weight has a factor $\equiv 3 \bmod 4$. Sequences that both started and/or ended in zero were not counted. Sequences that were obtained via computer–search (that is, Y–entries below) can be accessed via the WWW on http://www.cs.jcu.edu.au/ marc/TCP/tcpres.html.

B Proof Of Theorem 3

Proof. Assume that A, B are two disjointable sequences of length $\ell \equiv 2 \bmod 4$ and deficiency $\delta_{A,B} = 4, 12, 20, \ldots$. Assume that $\mathcal{T} = \sum_{a_i=0} i \equiv 0 \bmod 2$. We are to show that such sequences can not have zero periodic autocorrelation function. Assume the contrary, that is, assume that there exist two sequences A, B with

w, ℓ	2	3	4	5	6	7	8	9	10
4	YG	YFG	YFG	YFG	YFG	YFG	YFG	YFG	YFG
5		Y	N	YFTI	N	YFTI	N	YFTI	N
6		NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
7			NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
8			YG	YFG	YFG	YFG	YFG	YFG	YFG
9				NW	NW	NW	NW	NW	NW
10				N	YFT	YFT	YFT	YFT	YFT
11					NSQ	NSQ	NSQ	NSQ	NSQ
12					NSQ	NSQ	NSQ	NSQ	NSQ
13						N1	N	Y	N
14						NSQ	NSQ	NSQ	NSQ
15							NSQ	NSQ	NSQ
16							YG	YFG	YFG
17								N1	N
18								NW	NW
19									NSQ
20									YG

Table 4: Existence of TCP's for lengths $2 \leq \ell \leq 10$ and weights $4 \leq w \leq 20$

the above properties and $P_{A,B}(s) = 0$, $s = 1, \ldots, \ell - 1$. Since, $P_{A,B}(s) = 0$, $s = 1, \ldots, \ell - 1$, the equations modulo 4, denoted by $\tilde{P}_{A,B}(s)$ must also be 0, $s = 1, \ldots, \ell - 1$.

Write $\frac{\delta_{A,B}}{2} = 4m + 2$ and let

$$\begin{aligned} \mathcal{S}_{even} &= \{i \mid a_i = 0,\ i \text{ even}\}, \\ \mathcal{S}_{odd} &= \{i \mid a_i = 0,\ i \text{ odd}\}. \end{aligned}$$

Since $\mathcal{T} \equiv 0 \bmod 2$, $|\mathcal{S}_{even}| \equiv |\mathcal{S}_{odd}| \equiv 0 \bmod 2$. Since $\delta_{A,B} = 4, 12, 20, \ldots$, $|\mathcal{S}_{even}| + |\mathcal{S}_{odd}| \equiv 2 \bmod 4$. Consider now the equations $\tilde{P}_{A,B}(2) \equiv 0 \bmod 4$, $\tilde{P}_{A,B}(4) \equiv 0 \bmod 4, \ldots, \tilde{P}_{A,B}(\frac{\ell-2}{2}) \equiv 0 \bmod 4$ and

$$\tilde{P}_{A,B}(2) + \tilde{P}_{A,B}(4) + \ldots + \tilde{P}_{A,B}(\frac{\ell-2}{2}) \equiv 0 \bmod 4. \tag{1}$$

(Assume that the equations modulo 4 are written such that the LHS contains all the variable–terms and the RHS contains all the constant–terms.) If now $i_u - i_v \not\equiv s \not\equiv i_j - i_k \bmod \ell$, $i_u, i_v \in \mathcal{S}_{even}$, $i_j, i_k \in \mathcal{S}_{odd}$ then $\tilde{P}_{A,B}(s) \equiv 0 \bmod 4$ can be written as

$$\begin{aligned} a_{i_0-s} + a_{i_0+s} + \ldots + a_{i_{4m+2-1}-s} + a_{i_{4m+2-1}+s} \quad &+ \\ b_{i_0-s} + b_{i_0+s} + \ldots + b_{i_{4m+2-1}-s} + b_{i_{4m+2-1}+s} \quad &\equiv \quad 0 \bmod 4, \end{aligned}$$

where $i_0, \ldots, i_{4m+2-1} \in \mathcal{S}_{even} \cup \mathcal{S}_{odd}$ and the subscripts are reduced modulo ℓ if necessary and the subscripts are not necessarily all distinct (and all the terms on the LHS are not equal to zero). If s can be written d_1 times as a difference in

w, ℓ	11	12	13	14	15	16	17	18	19	20
4	YFG	YFG	YFG	YFG	YFG	YFG	YFG	YFG	YFG	YFG
5	YFTI	N	YFTI	N	YFTI	N	YFTI	N	YFTI	N
6	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
7	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
8	YFG	YFG	YFG	YFG	YFG	YFG	YFG	YFG	YFG	YFG
9	NW	NW	NW	NW	NW	NW	NW	NW	NW	NW
10	YFT	YFT	YFT	YFT	YFT	YFT	YFT	YFT	YFT	YFT
11	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
12	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
13	Y	N	N	Y	Y	N	YFTI	N	Y	N
14	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
15	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
16	YFG	YFG	YFG	YFG	YFG	YFG	YFG	YFG	YFG	YFG
17	N	N	Y	Y	Y	N	N	N	N	N
18	NW	NW	NW	NW	NW	NW	NW	NW	NW	NW
19	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
20	N	YFT	YFT	YFT	YFT	YFT	YFT	YFT	YFT	YFT
21	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
22	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
23		NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
24		NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
25			N1	N	N	N	N	Y	Y	Y
26			N	Y	Y	YHT	N	YFT	YFT	YFT
27				NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
28				NSQ	NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
29					N1	N	N	N	N	N
30					NSQ	NSQ	NSQ	NSQ	NSQ	NSQ
31						NSQ	NSQ	NSQ	NSQ	NSQ
32						YG	YFG	YFG	YFG	YFG
33							NSQ	NSQ	NSQ	NSQ
34							N	N	N	N
35								NSQ	NSQ	NSQ
36								NW	NW	NW
37									N1	N
38									NSQ	NSQ
39										NW
40										YG

Table 5: Existence of TCP's for lengths $11 \leq \ell \leq 20$ and weights $4 \leq w \leq 40$

$\mathcal{S}_{even}$ mod ℓ and d_2 times as a difference in $\mathcal{S}_{odd}$ mod ℓ, then $\tilde{P}_{A,B}(s) \equiv 0 \bmod 4$ can be written as

$$\begin{aligned} a_{i_0-s} + a_{i_0+s} + \ldots + a_{i_{4m+2-1}-s} + a_{i_{4m+2-1}+s} \quad &+ \\ b_{i_0-s} + b_{i_0+s} + \ldots + b_{i_{4m+2-1}-s} + b_{i_{4m+2-1}+s} \quad &\equiv \quad 2 \cdot (d_1 + d_2) \bmod 4, \end{aligned}$$

where the subscripts are as above (and now some of the terms on the LHS are zero). Consider now (1) which is obtained by adding all the previous considered equations. It is easy to see that on the LHS in (1) each (non–negative) variable a_i, b_i, with i even, occurs $|\mathcal{S}_{even}|$ times. Similarly each (non–negative) variable a_i, b_i, with i odd, occurs $|\mathcal{S}_{odd}|$ times. Since $|\mathcal{S}_{even}| \equiv |\mathcal{S}_{odd}| \equiv 0 \bmod 2$, the LHS of (1) is equivalent to 0 mod 4. The RHS of (1) is equivalent to $2 \cdot (d_{tot_1} + d_{tot_2}) \bmod 4$ where d_{tot_1} is the total number of solutions to $i - k \equiv 2, 4, \ldots, \frac{\ell-2}{2} \bmod \ell$, $i, k \in \mathcal{S}_{even}$ and d_{tot_2} is the total number of solutions to $i - k \equiv 2, 4, \ldots, \frac{\ell-2}{2} \bmod \ell$, $i, k \in \mathcal{S}_{odd}$. We have

$$\begin{aligned} d_{tot_1} &= \frac{|\mathcal{S}_{even}|}{2} \cdot (|\mathcal{S}_{even}| - 1), \\ d_{tot_2} &= \frac{|\mathcal{S}_{odd}|}{2} \cdot (|\mathcal{S}_{odd}| - 1), \end{aligned}$$

and since $|\mathcal{S}_{even}| + |\mathcal{S}_{odd}| \equiv 2 \bmod 4$, $d_{tot_1} + d_{tot_2} \equiv 1 \bmod 2$. Hence, the RHS of (1) is equivalent to 2 mod 4. This is a contradiction and concludes the proof. □