Designs, Codes and Cryptography, 30, 73–84, 2003

Meeting the Welch and Karystinos-Pados Bounds on DS-CDMA Binary Signature Sets

CUNSHENG DING cding@cs.ust.hk
Department of Computer Science, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China

MORDECAI GOLIN golin@cs.ust.hk
Department of Computer Science, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China

TORLEIV KLØVE Torleiv.Klove@ii.uib.no
Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong, China (on leave from the University of Bergen, Norway)

Communicated by: I. F. Blake

Received November 8, 2001; Revised March 14, 2002; Accepted March 27, 2002

Abstract. The Welch lower bound on the total-squared-correlation (TSC) of binary signature sets is loose for binary signature sets whose length L is not a multiple of 4. Recently Karystinos and Pados [6,7] developed new bounds that are better than the Welch bound in those cases, and showed how to achieve the bounds with modified Hadamard matrices except in a couple of cases. In this paper, we study the open cases.

Keywords: binary sequences, code division multiple access, codes, Welch bound, Karystinos-Pados bound

AMS Classification: 94A05, 94B60

1. Introduction

In direct-sequence code-division multiple-access (DS-CDMA) systems, multiple users are assigned individual binary antipodal signatures (spreading codes) to access a common, in time and frequency, communication channel. In conjunction with channel and receiver design specifics, the overall system performance is determined by the selection of the user signature set. Since each user signal acts as interference for the signals of other users, an appropriately designed user signature set contains signatures with low pairwise cross-correlation.

One measure of the cross-correlation properties of a signature set is the total-squared-correlation (TSC). A (K, L) signature set $\mathscr{S} = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_K\}$ is a set of K user signatures of length (processing gain) L, where $s_i \in \{-1, 1\}^L$.

The TSC of the set $\mathscr{S}$ is the sum of the squared magnitudes of all inner products between signatures:

$$\mathrm{TSC}(\mathscr{S}) = \sum_{i=1}^{K} \sum_{j=1}^{K} |\mathbf{s}_i \mathbf{s}_j^T|^2.$$

Let $\Theta(K, L)$ denote the minimum of $\mathrm{TSC}(\mathscr{S})$ over all (K, L) signature sets. We call a (K, L) signature set $\mathscr{S}$ optimal if $\mathrm{TSC}(\mathscr{S}) = \Theta(K, L)$.

For a (K, L) signature set $\mathscr{S} = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_K\}$, the corresponding signature matrix S is the matrix with rows $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_K$. We have

$$\mathrm{TSC}(\mathscr{S}) = \mathrm{trace}\Big(\big(SS^T\big)^2\Big) = \mathrm{trace}\Big(\big(S^T S\big)^2\Big).$$

Therefore, if $\mathscr{S}$ is an optimal (K, L) signature set, then the set of columns of S gives an optimal (L, K) signature set. Hence, to determine $\Theta(K, L)$ for all K and L, we only need to consider the case $K \leq L$.

The Welch bound [9] for binary signature sets states that if $K \leq L$, then $\Theta(K, L) \geq KL^2$, and it is not tight in general. Karystinos and Pados [6,7] have developed new bounds that improve the Welch bound for $L \not\equiv 0 \pmod 4$. We state their results in the following theorem.

THEOREM 1. (Karystinos and Pados). *Let $\mathscr{S}$ be a (K, L) signature set with $K \leq L$.*

i. *If* $L \equiv 0 \pmod 4$, *then* $\mathrm{TSC}(\mathscr{S}) \geq KL^2$, *with equality if and only if* $\mathbf{s}_i \mathbf{s}_j^T = 0$ *for all* $i \neq j$.

ii. *If* $L \equiv 1 \pmod 2$, *then* $\mathrm{TSC}(\mathscr{S}) \geq KL^2 + K(K-1)$, *with equality if and only if* $|\mathbf{s}_i \mathbf{s}_j^T| = 1$ *for all* $i \neq j$.

iii. *If* $L \equiv 2 \pmod 4$, *then* $\mathrm{TSC}(\mathscr{S}) \geq KL^2 + 8\binom{\lfloor K/2 \rfloor}{2} + 8\binom{\lceil K/2 \rceil}{2}$.

We repeat here the trivial proof of (i) and (ii): we have

$$\mathrm{TSC}(\mathscr{S}) = KL^2 + \sum_{i \neq j} \left| \mathbf{s}_i \mathbf{s}_j^T \right|^2.$$

We see that (i) follows immediately. Moreover, if L is odd, then $\mathbf{s}_i \mathbf{s}_j^T$ is odd. Therefore $|\mathbf{s}_i \mathbf{s}_j^T| \geq 1$ and so (ii) follows. The proof of (iii) and characterization of equality in this case is a little more involved, see Karystinos and Pados [7].

If $\mathrm{TSC}(\mathscr{S})$ meets the bound of Theorem 1, then we say that $\mathscr{S}$ is perfect.

We give a simple lemma which will be useful later.

LEMMA 2. *If L is odd, then* $\mathrm{TSC}(\mathscr{S}) \equiv KL^2 + K(K-1) \pmod{16}$. *In particular, if* $K = L$, *then* $\mathrm{TSC}(\mathscr{S}) \equiv 1 \pmod{16}$.

Proof. Since $\mathbf{s}_i\mathbf{s}_j^T = \mathbf{s}_j\mathbf{s}_i^T$, we have

$$\mathrm{TSC}(\mathscr{S}) = KL^2 + 2 \sum_{1 \leq i < j \leq K} \left|\mathbf{s}_i\mathbf{s}_j^T\right|^2.$$

Since $\mathbf{s}_i\mathbf{s}_j^T$ is odd, $|\mathbf{s}_i\mathbf{s}_j^T|^2 \equiv 1 \pmod 8$ and so $2|\mathbf{s}_i\mathbf{s}_j^T|^2 \equiv 2 \pmod{16}$. Hence

$$\mathrm{TSC}(\mathscr{S}) \equiv KL^2 + \sum_{1 \leq i < j \leq K} 2 = KL^2 + K(K-1) \pmod{16}. \qquad \blacksquare$$

We call a signature matrix normalized if all elements in the first column and the last row are $+1$. Multiplying each element in a row or each element in a column of a signature matrix by -1 will produce another signature matrix with the same TSC. By repeating this process, any signature matrix can be changed into a normalized signature matrix with the same TSC.

A Hadamard matrix of order n is an $n \times n$ matrix H_n of $+1$'s and -1's such that $\mathbf{h}_i\mathbf{h}_j^T = 0$ for $i \neq j$ (that is, $H_nH_n^T = nI$), where $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$ are the rows of H_n. By Theorem 1(i), a Hadamard matrix is the same as a signature matrix of a perfect (n, n) signature set. Hadamard matrices are believed to exist for all orders n divisible by 4, but this has not been established in all cases. Detailed information about Hadamard matrices may be found in Hedayat et al. [4].

Karystinos and Pados [6] constructed perfect signature sets for many cases, using modifications of Hadamard matrices. We briefly describe the constructions (in our own notation). Let H_{4m} be a Hadamard matrix, let $K \leq 4m$, and let $\mathscr{S}_{K,4m}$ be a set of K rows from H_{4m}. Let

- $\mathscr{S}_{K,4m-1} \subset \{-1, 1\}^{4m-1}$ be obtained by omitting the first element from each vector in $\mathscr{S}_{K,4m}$,
- $\mathscr{S}_{K,4m+1} \subset \{-1, 1\}^{4m+1}$ be obtained by appending a 1 to each vector in $\mathscr{S}_{K,4m}$,
- $\mathscr{S}_{K,4m+2} \subset \{-1, 1\}^{4m+2}$ be obtained by appending $(1, 1)$ to $\lfloor K/2 \rfloor$ of the vectors in $\mathscr{S}_{4m}$ and $(1, -1)$ to the remaining $\lceil K/2 \rceil$ vectors of $\mathscr{S}_{K,4m}$.

Then $\mathscr{S}_{K,L}$ is a perfect (K, L) signature set for $L \in \{4m-1, 4m, 4m+1, 4m+2\}$ and $K \leq 4m$. This left open the question of optimal signature sets for the following cases when $K \leq L$:

Case 1. $L \equiv 1 \pmod 4$ and $K = L$.

Case 2. $L \equiv 2 \pmod 4$ and $K = L$ or $K = L - 1$.

The purpose of this paper is to study these open cases. Case 2 turn out to be simple, but Case 1 appears to be difficult.

2. Perfect Signature Sets for $L \equiv 2 \pmod 4$

For this case we construct perfect signature sets (provided Hadamard matrices of order $L+2$ exist). The construction is similar to the constructions of Karystinos and Pados [6,7].

Let H_{L+2} be a normalized Hadamard matrix. Any column of H_{L+2}, except the first contains an equal number of 1's and -1's (since H_{L+2}^T is also a Hadamard matrix). For $K \le L$, let $\mathscr{T}_1$ be a set of $\lfloor K/2 \rfloor$ rows from H_{L+2} which starts with $(1,1)$ and $\mathscr{T}_2$ a set of $\lceil K/2 \rceil$ rows from H_{L+2} which starts with $(1,-1)$. For $k=1,2$, let $\mathscr{S}_k \subset \{-1,1\}^L$ be the set of vectors obtained by deleting the first two elements of the vectors in $\mathscr{T}_k$, and let $\mathscr{S} = \mathscr{S}_1 \cup \mathscr{S}_2$. If $\mathbf{s}_i$ and $\mathbf{s}_j$ are distinct vectors of $\mathscr{S}$, then $\mathbf{s}_i\mathbf{s}_j^T = -2$ if they belong to the same $\mathscr{S}_k$, and $\mathbf{s}_i\mathbf{s}_j^T = 0$ otherwise. Hence

$$\sum_{i=1}^{L}\sum_{j=1}^{L}|\mathbf{s}_i\mathbf{s}_j^T|^2 = KL^2 + 4\left\lfloor\frac{K}{2}\right\rfloor\left(\left\lfloor\frac{K}{2}\right\rfloor - 1\right) + 4\left\lceil\frac{K}{2}\right\rceil\left(\left\lceil\frac{K}{2}\right\rceil - 1\right),$$

that is, the signature set is perfect.

THEOREM 3. *If* $L \equiv 2 \pmod 4$ *and there exists a Hadamard matrix of order* $L+2$, *then perfect* (K, L) *signature sets exist for all* $K \le L$.

3. Signature Sets for $L \equiv 1 \pmod 4$

We now consider (L,L) signature sets for $L \equiv 1 \pmod 4$. For $L=5$ and $L=13$ perfect (L,L) signature sets do exist, we give constructions below. However, perfect (9, 9) signature sets do not exist; a proof of this is given in an appendix. By Lemma 2, for a (9, 9) signature set we have $\mathrm{TSC} = 9^3 + 9 \cdot 8 + 16a$ for some integer $a \ge 0$. In fact there do not exist (9, 9) signature sets with $\mathrm{TSC} = 9^3 + 9 \cdot 8 + 16a$ for any $a \in \{0,1,2\}$. Such a set would have $|\mathbf{s}_i\mathbf{s}_j^T| = 3$ for exactly a pairs (i,j) where $i<j$ and $|\mathbf{s}_i\mathbf{s}_j^T| = 1$ for the remaining pairs with $i<j$. It is a simple task to check by computer that this is not possible. A (9, 9) signature set with $\mathrm{TSC} = 9^3 + 9 \cdot 8 + 16 \cdot 3 = 849$ do exist, a construction is given below. Hence, $\Theta(9,9) = 849$.

The example (9, 9) is important because it shows that Karystinos and Pados's bound is not sharp for (L,L) set in general. Therefore, it is of interest to find constructions of (L,L) signature sets, even if they are not perfect. In this section we consider various constructions of (L,L) signature sets. For all L, except $L=5$ and $L=13$, the corresponding values of the TSC are above the Karystinos-Pados bound, but we can not decide if they are optimal or not (except for $L=9$).

3.1. *Shortening Hadamard Matrices*

One possible construction is to delete three elements from the rows of a normalized Hadamard matrix of order $L+3$. It is easy to show that this results in a signature set where

$$\mathrm{TSC} \geq L^3 + 3(L-1)(L-2).$$

Since our next construction gives signature sets with lower TSC, we omit the details of the proof.

3.2. *Extending Hadamard Matrices*

Let H be a Hadamard matrix of order $L-1$, let $\mathbf{a}, \mathbf{b} \in \{-1,1\}^{L-1}$, and $c \in \{-1,1\}$. Consider the $L \times L$ matrix

$$S(H,\mathbf{a},\mathbf{b},c) = \left[\begin{array}{c|c} \mathbf{a}^T & -H \\ \hline c & \mathbf{b} \end{array}\right],$$

and let $\mathscr{S}_{H,\mathbf{a},\mathbf{b},c}$ be the set of rows of this matrix. We want to find the minimum of $\mathrm{TSC}(\mathscr{S}_{H,\mathbf{a},\mathbf{b},c})$ over all Hadamard matrices H of order $L-1$ and all $\mathbf{a}, \mathbf{b}, c$. Normalizing $S(H,\mathbf{a},\mathbf{b},c)$ we get a matrix $S(H',\mathbf{1},\mathbf{1},1)$ where H' is again a Hadamard matrix. Hence, we can assume without loss of generality that $\mathbf{a}=\mathbf{b}=\mathbf{1}$ and $c=1$. We write $\mathscr{S}_H = \mathscr{S}_{H,\mathbf{1},\mathbf{1},1}$.

The excess of a Hadamard matrix H is the sum of all its elements, we denote it by $\sigma(H)$. Note that $\sigma(H) = \mathbf{1}H\mathbf{1}^T$. Let $\sigma(n)$ denote the maximal excess of a Hadamard matrix of order n. This quantity was first studied by Best [1]. He showed that if Hadamard matrices of order n exist, then

$$\frac{n^2}{2^n}\binom{n}{n/2} \leq \sigma(n) \leq n^{3/2}. \tag{1}$$

He determined the first few values:

n	4	8	12	16	20	24
$\sigma(n)$	8	20	36	64	80	112

The maximal excess of Hadamard matrices has been studied by a number of authors since and we mention a couple of the results.

Hammer et al. [3] showed that for $n = 2^{2m}$ we have $\sigma(n) = n^{3/2}$.

For $n = 4m(m+1)$, Kounias and Farmakis [8] improved Best's upper bound to $4m^2(2m+3)$, and for odd $m \leq 19$ it has been shown that this bound can be reached.

THEOREM 4. *Let H be a Hadamard matrix of order n. Then*

$$\mathrm{TSC}(\mathscr{S}_H) = (n+1)^3 + n(3n+1) - 4\sigma(H).$$

Proof. Let $\mathscr{S}_H = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_n, \mathbf{s}_{n+1} = \mathbf{1}\}$. For all i we have

$$|\mathbf{s}_i\mathbf{s}_i^T|^2 = (n+1)^2. \tag{2}$$

If $i \neq j$ and $1 \leq i,j \leq n$ then

$$|\mathbf{s}_i\mathbf{s}_j^T| = |1 + \mathbf{h}_i\mathbf{h}_j^T| = 1. \tag{3}$$

Since the transpose of a Hadamard matrix is again a Hadamard matrix we get

$$\sum_{i=1}^{n} h_{ij}h_{ik} = \begin{cases} n, & \text{if } j = k \\ 0, & \text{if } j \neq k, \end{cases}$$

and so

$$\sum_{i=1}^{n} (\mathbf{1h}_i^T)^2 = \sum_{i=1}^{n}\sum_{j=1}^{n} h_{ij} \sum_{k=1}^{n} h_{ik} = \sum_{j=1}^{n}\sum_{k=1}^{n}\sum_{i=1}^{n} h_{ij}h_{ik} = n^2. \tag{4}$$

For $1 \leq j \leq n$ we have $\mathbf{s}_{n+1}\mathbf{s}_j^T = 1 - \mathbf{1h}_j^T$ and so

$$\sum_{j=1}^{n} (\mathbf{s}_{n+1}\mathbf{s}_j^T)^2 = n - 2\sum_{j=1}^{n} \mathbf{1h}_j^T + \sum_{j=1}^{n} (\mathbf{1h}_j^T)^2 = n - 2\sigma(H) + n^2. \tag{5}$$

Combining (2)–(5) we get

$$\begin{aligned}\sum_{i=1}^{n+1}\sum_{j=1}^{n+1} |\mathbf{s}_i\mathbf{s}_j^T|^2 &= \sum_{i=1}^{n+1} |\mathbf{s}_i\mathbf{s}_i^T|^2 + 2\sum_{1\leq i<j\leq n} |\mathbf{s}_i\mathbf{s}_j^T|^2 + 2\sum_{j=1}^{n} |\mathbf{s}_{n+1}\mathbf{s}_j^T|^2 \\ &= (n+1)(n+1)^2 + n(n-1) + 2n - 4\sigma(H) + 2n^2 \\ &= (n+1)^3 + n(3n+1) - 4\sigma(H). \qquad \blacksquare\end{aligned}$$

Theorem 4 immediately gives the following result.

THEOREM 5. *For $K = L \equiv 1 \pmod 4$, if Hadamard matrices of order $L-1$ exist, then there exists an (L, L) signature set $\mathscr{S}$ with*

$$\mathrm{TSC}(\mathscr{S}) = L^3 + (L-1)(3L-2) - 4\sigma(L-1).$$

EXAMPLE 1. *It is known that* $\sigma(4) = 8$. *Hence, there exists a (5, 5) signature set* $\mathscr{S}$ *with*

$$\mathrm{TSC}(\mathscr{S}) = 5^3 + 4 \cdot 13 - 4 \cdot 8 = 5^3 + 5 \cdot 4,$$

that is, a perfect (5,5) signature set exists.

From (1) we have $\sigma(L-1) \leq (L-1)^{3/2}$. *Hence, for* $L \geq 9$, *we have*

$$L^3 + (L-1)(3L-2) - 4\sigma(L-1) > L^3 + L(L-1),$$

and so, if perfect (L, L) *signature sets exist, they can not be constructed in this way for* $L \geq 9$.

EXAMPLE 2. *It is known that* $\sigma(8) = 20$. *Hence, the minimal TSC we obtain for a (9, 9) signature set* $\mathscr{S}$ *by this method is*

$$\mathrm{TSC}(\mathscr{S}) = 9^3 + 8 \cdot 25 - 4 \cdot 20 = (9^3 + 9 \cdot 8) + 48.$$

As explained above, this is in fact optimal (but not perfect).

EXAMPLE 3. *It is known that* $\sigma(12) = 36$. *Hence, the minimal TSC we obtain for a (13, 13) signature set* $\mathscr{S}$ *by this method is*

$$\mathrm{TSC}(\mathscr{S}) = 13^3 + 12 \cdot 37 - 4 \cdot 36 = (13^3 + 13 \cdot 12) + 144.$$

As we will show by another construction, this is not optimal (actually, a perfect signature set exists).

3.3. Signature sets and codes

The problem we study can be rephrased in term of binary codes. For two n-tuples $\mathbf{a}$, $\mathbf{b}$ of the same length, the Hamming distance between $\mathbf{a}$ and $\mathbf{b}$, denoted $d_H(\mathbf{a}, \mathbf{b})$ is the number of positions where they differ. The Hamming weight of $\mathbf{a}$ is the number of non-zero elements of $\mathbf{a}$.

A binary (L, M) code $\mathscr{C}$ is a subset of $\{0, 1\}^L$ with M elements. The elements of $\mathscr{C}$ are called codewords. The minimum distance of $\mathscr{C}$ is the smallest Hamming distance between distinct codewords.

The distance distribution of $\mathscr{C}$ is the sequence $A_0, A_1, \ldots, A_L$, where

$$A_i = \frac{|\{(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathscr{C} \text{ and } d_H(\mathbf{a}, \mathbf{b}) = i\}|}{M}.$$

In particular, $A_0 = 1$. In this notation, the minimum distance is the least positive d such that $A_d \neq 0$.

The (invertible) mapping ϕ defined by $\phi(0) = 1$ and $\phi(1) = -1$ can be extended to vectors and codes to get a $1 - 1$ correspondence between codes and signature sets. If

$\mathbf{c}_1, \mathbf{c}_2 \in \{0,1\}^L$ and $\mathbf{s}_i = \phi(\mathbf{c}_i)$, then

$$\mathbf{s}_1\mathbf{s}_2^T = L - 2d_H(\mathbf{s}_1, \mathbf{s}_2) = L - 2d_H(\mathbf{c}_1, \mathbf{c}_2).$$

Hence we get the following relation.

THEOREM 6. *Let $\mathscr{C}$ be an (L, L) code with distance distribution $A_0, A_1, \ldots, A_L$. Then*

$$\mathrm{TSC}(\phi(\mathscr{C})) = L\sum_{i=0}^{L} A_i(L-2i)^2 = L\sum_{j=0}^{(L-1)/2} (A_{\frac{L-1}{2}-j} + A_{\frac{L+1}{2}+j})(2j+1)^2.$$

In particular, $\phi(\mathscr{C})$ is perfect if and only if $A_i = 0$ for $i \notin \{0, L-1/2, L+1/2\}$.

Remark 1. As noted above, if S is a (L, L) signature matrix, multiplying each element in a row or each element in a column of S by -1 will produce a signature matrix S' with the same TSC. Hence, we may assume without loss of generality that $\mathbf{1}$ belongs to $\mathscr{S}$ and that all the remaining signatures have a majority of elements which are $+1$. This means that $\mathbf{0} \in \psi(\mathscr{S})$ and that $w_H(\psi(\mathbf{s})) < L/2$ for all $\mathbf{s} \in \mathscr{S}$. In particular, if $\mathscr{S}$ is perfect, then $\mathscr{C} = \psi(\mathscr{S})\backslash\{\mathbf{0}\}$ is a constant weight code; all codewords have weight $(L-1)/2$. Moreover, the distance between any two codewords of $\mathscr{C}$ is even and it is in $\{(L-1)/2, (L+1)/2\}$ so it must be $(L-1)/2$ (since $(L+1)/2$ is odd). Hence the code is also equidistant. The size of the code $\mathscr{C}$ is $L-1$. The best general upper bound on equidistant constant weight codes with these parameters turns out to be $L+1$ (see Fu et al. [2]) and so perfect signature sets give rise to codes which are almost best possible. On the other hand, the bounds can not be used to rule out the existence of such codes for any L.

Remark 2. A code $\mathscr{C}$ is said to be self-complementary if $\mathbf{x} \in \mathscr{C}$ implies $\bar{\mathbf{x}} \in \mathscr{C}$, where $\bar{\mathbf{x}} = \mathbf{x} + \mathbf{1}$ denotes the complement of $\mathbf{x}$. From the theorem above we see that if $\mathscr{S}$ is perfect, then the code $\psi(\mathscr{S}) \cup (\mathbf{1} + \psi(\mathscr{S}))$ is self-complementary of size $2L$. Moreover, its minimum distance is $(L-1)/2$ since $\mathbf{c}_1, \mathbf{c}_2 \in \psi(\mathscr{S}), \mathbf{c}_1 \neq \mathbf{c}_2$, implies that

$$d_H(\mathbf{1}+\mathbf{c}_1, \mathbf{1}+\mathbf{c}_2) = d_H(\mathbf{c}_1, \mathbf{c}_2) \in \left\{\frac{L-1}{2}, \frac{L+1}{2}\right\},$$

$$d_H(\mathbf{c}_1, \mathbf{1}+\mathbf{c}_2) = L - d_H(\mathbf{c}_1, \mathbf{c}_2) \in \left\{\frac{L+1}{2}, \frac{L-1}{2}\right\}.$$

Hence, a perfect signature set gives a self-complementary code with size close to the best upper bound (the Gray-Rankin bound).

3.4. Signature Sets from Binary Functions

THEOREM 7. *Let $G = \{g_1, g_2, \ldots, g_L\}$ be an Abelian group of order L and let $f : G \to \{-1, 1\}$ be a binary function on G. Let $\mathscr{S}$ be the (L, L) signature set*

$$\mathscr{S} = \{\mathbf{s}_g = (f(g_1 + g), f(g_2 + g), \ldots, f(g_L + g)) \mid g \in G\}.$$

Then

$$\mathrm{TSC}(\mathscr{S}) = L \sum_{h \in G} (C_f(h))^2,$$

where

$$C_f(x) = \sum_{y \in G} f(x + y) f(y),$$

is the autocorrelation of f.

Proof. We have

$$\mathbf{s}_g \mathbf{s}_h^T = \sum_{i=1}^{L} f(g_i + g) f(g_i + h) = \sum_{j=1}^{L} f(g_j + g - h) f(g_j) = C_f(g - h).$$

Hence

$$\mathrm{TSC}(\mathscr{S}) = \sum_{g \in G} \sum_{h' \in G} (C_f(g - h'))^2 = \sum_{g \in G} \sum_{h \in G} (C_f(h))^2 = L \sum_{h \in G} (C_f(h))^2. \qquad \blacksquare$$

Consider the following special case. An m-subset D of G is called an (L, m, λ) difference set if the differences $x - y$ take on each nonzero element of G exactly λ times when (x, y) ranges over all distinct pairs in $D \times D$. D is called cyclic if G is cyclic. If D is an (L, m, λ) difference set of G, then $G \backslash D$ is an $(L, L - m, L - 2m + \lambda)$ difference set.

Define $f_D : G \to \{-1, +1\}$ by

$$f_D(h) = \begin{cases} -1, & \text{if } h \in D \\ +1, & \text{if } h \notin D. \end{cases}$$

Then $C_{f_D}(h) = L - 4(m - \lambda)$ for $h \neq 0$. Since $m(m - 1) = \lambda(L - 1)$, we have $L - 4(m - \lambda) = 1$ if and only if

$$(L, m, \lambda) = (2u(u + 1) + 1, u^2, u(u - 1)/2), \tag{6}$$

or

$$(L, m, \lambda) = (2u(u + 1) + 1, (u + 1)^2, (u + 1)(u + 2)/2). \tag{7}$$

If D is a difference set with parameters (7), then $G\backslash D$ is a difference set with parameters (6). Hence it is sufficient to consider one of these sets of parameters. Theorem 7 gives the following result.

COROLLARY 8. *For $u \geq 1$, if there exists a difference set with parameters (6), then there exists a perfect $(2u(u+1)+1, 2u(u+1)+1)$ signature set.*

EXAMPLE 4. *For $u = 1$ we get $2u(u+1)+1 = 5$, and there exists a $(5, 1, 0)$ difference set in $\mathbf{Z}_5$, namely $D = \{0\}$. Hence a perfect $(5, 5)$ signature set exists.*

EXAMPLE 5. *For $u = 2$ we get $2u(u+1)+1 = 13$, and there exists a $(13, 4, 1)$ difference set in $\mathbf{Z}_{13}$, namely $D = \{0, 1, 3, 9\}$. Hence a perfect $(13, 13)$ signature set exists.*

It is known that for $3 \leq u \leq 6$, difference sets with parameters (6) do not exist [5]. For $u \geq 7$ the existence of such difference sets is an open question.

4. Concluding Remarks

The constructions given by Karystinos and Pados [6,7], and the constructions given in this paper show that the Karystinos-Pados bound is sharp, for all cases, except $K = L \equiv 1 (\mathrm{mod}\ 4)$.

The case $K = L \equiv 1 (\mathrm{mod}\ 4)$ is more involved. For $L = 5$ and $L = 13$, the Karystinos-Pados bound is sharp, for $L = 9$ it is not. For $L \geq 17$ the question is open. The best general construction we have is by extending a Hadamard matrix (Theorem 4). However, for the case $L = 13$ a better construction was obtained using difference sets (Corollary 8).

Appendix: Proof that Perfect (9, 9) Signature Sets do not Exist

Since a perfect (9, 9) signature set is equivalent to a (9, 8, 4) equidistant constant weight code; suppose that such a code exists. We will show that this gives a contradiction. It is sufficient to consider the code up to equivalence, that is, permutation of positions. When we do this, we write w.l.o.g (without loss of generality).

W.l.o.g the first two codewords are

$$\mathbf{c}_1 = (11\ 11\ 00\ 000), \qquad \mathbf{c}_2 = (11\ 00\ 11\ 000).$$

For any codeword $\mathbf{c}$, we will group the elements into 4 groups, having 2, 2, 2, and 3 bits respectively. We denote these groups by $\mathbf{c}^{(i)}$, $i = 1, 2, 3, 4$. Hence

$$\mathbf{c} = (\mathbf{c}^{(1)} \mid \mathbf{c}^{(2)} \mid \mathbf{c}^{(3)} \mid \mathbf{c}^{(4)}).$$

Denote the weight of $\mathbf{c}^{(i)}$ by w_i. Then

$$w_1 + w_2 + w_3 + w_4 = w_H(\mathbf{c}) = 4,$$
$$(2 - w_1) + (2 - w_2) + w_3 + w_4 = d_H(\mathbf{c}_1, \mathbf{c}) = 4,$$
$$(2 - w_1) + w_2 + (2 - w_3) + w_4 = d_H(\mathbf{c}_2, \mathbf{c}) = 4.$$

Solving these equations we get

$$w_2 = w_3 = 2 - w_1 \quad \text{and} \quad w_4 = w_1.$$

Hence, up to equivalence, there are 3 possible choices for $\mathbf{c}$:

$$(00\ 11\ 11\ 000), \quad (10\ 10\ 10\ 100), \quad (11\ 00\ 00\ 110).$$

We say that $\mathbf{c}$ is of type a if $w_H(\mathbf{c}^{(1)}) = a$. The potential codeword of type 0 is unique. The potential codeword of type 2 is unique, except for the place of the 0 in group 4. In particular, the distance between them is eight. Hence the code can not contain codewords of both types 0 and 2. Therefore, at least five of the eight codewords of the code are of type 1.

We now consider five such codewords $\mathbf{c}_i$, $i = 3, 4, 5, 6, 7$, of type 1. Since $\mathbf{c}_i^{(1)} = (10)$ or (01), we may assume w.l.o.g. that $\mathbf{c}_i^{(1)} = (10)$ for $i = 3, 4, 5$. Similarly, w.l.o.g. $\mathbf{c}_3^{(2)} = \mathbf{c}_4^{(2)} = (10)$. Let $a_i = d_H(\mathbf{c}_3^{(i)}, \mathbf{c}_4^{(i)})$ for $i = 1, 2, 3, 4$. Then

$$a_1 + a_2 + a_3 + a_4 = 4, \quad a_1 = a_2 = 0, \quad a_3, a_4 \in \{0, 2\},$$

and so $a_3 = a_4 = 2$. Hence, w.l.o.g.,

$$\mathbf{c}_3 = (10\ 10\ 10\ 100), \qquad \mathbf{c}_4 = (10\ 10\ 01\ 010).$$

Let $b_i = d_H(\mathbf{c}_3^{(i)}, \mathbf{c}_5^{(i)})$ for $i = 1, 2, 3, 4$ and $b_4' = d_H(\mathbf{c}_4^{(4)}, \mathbf{c}_5^{(4)})$. Then

$$b_1 + b_2 + b_3 + b_4 = d_H(\mathbf{c}_3, \mathbf{c}_5) = 4,$$
$$b_1 + b_2 + (2 - b_3) + b_4' = d_H(\mathbf{c}_4, \mathbf{c}_5) = 4.$$

Since $b_1 = 0$ and $b_2, b_3, b_4, b_4' \in \{0, 2\}$, there are two possible solutions, and for each solution the corresponding $\mathbf{c}_5$ is uniquely determined; we denote the two alternatives by $\mathbf{c}_{5,A}$ and $\mathbf{c}_{5,B}$:

b_1	b_2	b_3	b_4	b_4'	
0	2	2	0	2	$\mathbf{c}_{5,A} = (10\ 01\ 01\ 100)$
0	2	0	2	0	$\mathbf{c}_{5,B} = (10\ 01\ 10\ 010)$.

However, $\{\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_{5,A}\}$ and $\{\mathbf{c}_4, \mathbf{c}_3, \mathbf{c}_{5,B}\}$ are equivalent (switch elements 4 and 5 and also elements 6 and 7). Hence, w.l.o.g. $\mathbf{c}_5 = \mathbf{c}_{5,A}$, that is

$$\mathbf{c}_5 = (10\ 01\ 01\ 100).$$

Let $\mathbf{c}$ be another codeword of type 1, and let $d_i = d_H(\mathbf{c}_3^{(i)}, \mathbf{c}^{(i)})$ for $i = 1, 2, 3, 4$ and $d_4' = d_H(\mathbf{c}_4^{(4)}, \mathbf{c}^{(4)})$. Then

$$\begin{aligned} d_1 + d_2 + d_3 + d_4 &= d_H(\mathbf{c}_3, \mathbf{c}) = 4, \\ d_1 + d_2 + (2 - d_3) + d_4' &= d_H(\mathbf{c}_4, \mathbf{c}) = 4, \\ d_1 + (2 - d_2) + (2 - d_3) + d_4 &= d_H(\mathbf{c}_5, \mathbf{c}) = 4. \end{aligned}$$

Again $d_1, d_2, d_3, d_4, d_4' \in \{0, 2\}$, and we see that there are two solutions, the corresponding $\mathbf{c}$ is uniquely determined in each case:

d_1	d_2	d_3	d_4	d_4'	
0	2	0	2	0	$\mathbf{c} = (10\ 01\ 10\ 010)$
2	0	2	0	2	$\mathbf{c} = (01\ 10\ 01\ 100)$.

Since the distance between these two potential codewords is eight, they can not both belong to the code. Hence, the code can have only four codewords of type 1, contradicting our earlier observation that the code needs to have at least five such codewords.

References

1. M. Best, The excess of a Hadamard matrix, *Indag. Math.*, Vol. 39, No. (5) (1977) pp. 357–361.
2. F. W. Fu, T. Kløve, Y. Luo and V. K. Wei, On equidistant constant weight codes, *Proc. of the Intern. Workshop on Coding and Cryptography*, D. Augot and C. Carlet (eds.), Paris, January 8–12 (2001) pp. 225–232.
3. J. Hammer, R. Levingston and J. Seberry, A remark on the excess of Hadamard matrices and orthogonal designs, *Ars Combin.*, Vol. 5 (1978) pp. 237–254.
4. A. S. Hedayat, N. J. A. Sloane and J. Stufken, *Orthogonal arrays: theory and applications*, Springer-Verlag, New York (1999).
5. D. Jungnickel, *Difference sets, Contemporary Design Theory: A Collection of Surveys*, J. Dinitz and D. R. Stinson (eds.), John Wiley & Sons (1992) pp. 241–324.
6. G. N. Karystinos and D. A. Pados, New bounds on the total-squared-correlation and perfect design of DS-CDMA binary signature sets, *Proc. IEEE Intern. Conf. on Telecommunications*, Bucharest, Romania, Vol. 3. (2001) pp. 260–265.
7. G. N. Karystinos and D. A. Pados, New bounds on the total-squared-correlation and perfect design of DS-CDMA binary signature sets, *IEEE Trans. Communications*, Vol. 51 (2003) pp. 48–51.
8. S. Kounias and N. Farmakis, On the excess of Hadamard matrices, *Discrete Math.*, Vol. 68 (1988) pp. 59–69.
9. L. R. Welch, Lower bounds on the maximum cross correlation of signals, *IEEE Trans. Inform. Theory*, Vol. 20 (1974) pp. 397–399.