On the Karystinos-Pados Bounds and Optimal Binary DS-CDMA Signature Ensembles

Valery P. Ipatov, *Member, IEEE*

***Abstract*—Tightness of the Karystinos–Pados bounds was originally proved with four exceptions. In this letter, we modify the algorithm of constructing signatures removing three of these exceptions. For the fourth one the tighter bound are derived.**

***Index Terms*—Code-division-multiple-access (CDMA) signatures, Karystinos-Pados bounds, Welch bound.**

I. Introduction

In DESIGNING synchronous direct-sequence code-division-multiple-access (DS-CDMA) systems an adequate choice of a set of user signature sequences is of critical importance. In recent years considerable attention has been focused on signature sets attaining the lower *Welch bound* [1]–[3]. As shown in [1], signature sets of this sort maximize Shannon capacity of CDMA channels with Gaussian noise and Gaussian input, the latter constraint being immaterial whenever receive signal-to-noise ratio is small enough.

Let $\mathbf{S}$ be $L \times K$ matrix whose K columns are K user's signature sequences of lengths L normalized so that their energies (squared Euclidean norms) are equal to unity. The *total squared correlation* $\mathrm{TSC}(S)$ of the signature set [3] is then the sum of all $K \times K$ squared inner products (correlations) of columns of the matrix $\mathbf{S}$. According to the Welch bound [4] (properly modified to evaluate the total squared correlation [1], [2]) $\mathrm{TSC}(\mathbf{S}) \geq KM/L$ with $M = \max\{K, L\}$.

In this letter we consider binary signatures whose elements are antipodal. When M is not divisible by 4, binary signature set can not achieve the "pure" Welch bound, since matrix $\mathbf{S}$ can not have orthogonal rows ($K \geq L$) or columns ($K \leq L$) [2]. This fact stimulated the authors of [5] to produce a new version of the Welch bound, specified for binary antipodal signature alphabet. In space-saving form the Karystinos-Pados bound may be presented as

$$\mathrm{TSC}(\mathbf{S}) \geq \frac{KM}{L} + \begin{cases} 0, & M \equiv 0 \pmod 4 \\ \dfrac{m(m-1)}{L^2}, & M \equiv 1 \pmod 2 \\ \dfrac{4}{L^2}\left[\left\lfloor \dfrac{m}{2} \right\rfloor^2 + \left\lceil \dfrac{m}{2} \right\rceil^2 - m\right], & M \equiv 2 \pmod 4 \end{cases} \tag{1}$$

where $m = \min\{K, L\}$, and $\lfloor x \rfloor, \lceil x \rceil$ stand for rounding x toward zero and infinity respectively.

In [5] the Hadamard-matrix-based algorithm is also proposed to construct binary signature sets achieving the bound (1), thereby proving the tightness of the latter at least for cases where an appropriate Hadamard matrix exists. However, four exceptions are listed in [5] which are not covered by this algorithm. In our designations they are reduced to three:

$$K = L \equiv 2 \pmod 4; \qquad M = m + 1 \equiv 2 \pmod 4;$$
$$K = L \equiv 1 \pmod 4. \tag{2}$$

In Section II we show that the first two of these exceptions (three in the notation of [5]) are easily removed by a slight simplification of the algorithm of [5]. The construction is identical to that of [6] but the author could not be aware of it at the moment of submitting the letter, since [6] was published later. Discussion of the third exception in Section III results in a new bound on $\mathrm{TSC}(S)$ which is tighter than the Karystinos-Pados one.

II. Binary Signature Set Construction

The algorithm works whenever $M - 1$ is not a multiple of 4 and a Hadamard matrix exists of an order which is the least a multiple of 4 greater than M. If M or $M - 3$ are multiples of 4 it coincides with the one in [5], We therefore dwell only on the case $M \equiv 2 \pmod 4$. Let w_i denote weight, i.e., the number of negative elements, of the ith row of the binary matrix. Suppose a Hadamard matrix of the order $N = M + 2$ exists and, if $w_1 \neq 0$, multiply all its rows element-wise by the first row. The matrix obtained is again a Hadamard one whose first row has zero weight, i.e., consists only of elements $+1$, while all the other rows are of weight $N/2$ due to their orthogonality to the first row. Rearranging the columns we arrive at a Hadamard matrix $\mathbf{H}$ whose first $N/2$ columns start with two-element prefix $+1, +1$, while the rest of the columns have the prefix $+1, -1$. Select $\lfloor m/2 \rfloor$ and $\lceil m/2 \rceil$ columns correspondingly out of the first and second halves of the columns of $\mathbf{H}$ and then exclude the two-element prefixes of the selected columns to arrive at the $M \times m$ matrix $\mathbf{S}_0$. It is readily seen that after dropping the prefixes any inner product of two different columns in $\mathbf{H}$ either remains zero (if the prefixes removed are different) or changes to -2 when the prefixes are the same. Now normalize $\mathbf{S}_0$ by dividing it by $\sqrt{L}$ and transpose the resulting matrix if $K > L$ (using the "row-column equivalence" of the sums of the squared inner products [3]). In the binary matrix $\mathbf{S}$ thus produced

$$\lfloor m/2 \rfloor(\lfloor m/2 \rfloor - 1) + \lceil m/2 \rceil(\lceil m/2 \rceil - 1)$$

Manuscript received June 21, 2003. The associate editor coordinating the review of this letter and approving it for publication was Prof. S. W. Kim.

The author is with the Department of Information Technology, University of Turku, 20520 Turku, Finland (e-mail: valery.ipatov@utu.fi).

Digital Object Identifier 10.1109/LCOMM.2004.823428

correlations of columns are equal to $-2/\sqrt{L}$, so that $\mathrm{TSC}(\mathbf{S})$ equals the minimum predicted by (1). Thus $\mathbf{S}$ is the desired matrix whose columns are binary signatures meeting the bound (1). Thereby 2 of the 3 exceptions (2) (three of four in the notation of [5]) are eliminated, and the tightness of bounds found in [5] appears to be true for any $M \equiv 2 \pmod 4$ with the only stipulation of existence of an appropriate Hadamard matrix, any relations between K and L being irrelevant.

III. Bounds for Case $K = L \equiv 1 \pmod 4$

Let us now show that in the case $K = L \equiv 1 \pmod 4$ the bound (1) ramifies further depending on the specific value of K. Since the correlations of columns of binary square matrix $\mathbf{S}$ of the odd order K can only take on the values $1, \pm 1/K, \pm 3/K, \ldots$, the three least candidate values of $\mathrm{TSC}(\mathbf{S})$ are

$$\mathrm{TSC}(\mathbf{S}) = K + \frac{K-1}{K} + \frac{16l}{K^2} \tag{3}$$

where $l = 0, 1, 2$ is the number of pairs of columns with correlation $\pm 3/K$, the rest of all nonunity correlations being $\pm 1/K$.

Proposition 1: There are two necessary conditions of existence $K = L \equiv 1 \bmod 4$ binary signatures satisfying (3)

$$K = 2(x(x+1) + 2(l - 2t)) + 1 \tag{4}$$

$$K = 2(y(y+1) + 2(s - 2u)) + 1 \tag{5}$$

where x, y, t, s, u are integers; $x, y = 0, 1, \ldots$; $0 \le t, u \le l = 0, 1, 2$; $s = 0$ if $l = 0, 1$ and $s = 0, 1$ if $l = 2$.

Proof: Since $K \ge 5 \ge 2l + 1$, a column in $\mathbf{S}$ exists which does not enter any pair with correlation $\pm 3/K$. Deleting this column leads to $K \times (K-1)$ matrix $\mathbf{S}_1$ with

$$\mathrm{TSC}(\mathbf{S}_1) = K - 1 + \frac{(K-1)(K-2)}{K^2} + \frac{16l}{K^2}. \tag{6}$$

Let us calculate $\mathrm{TSC}(\mathbf{S}_1)$ in terms of row inner products. Due to "row–column equivalence", l is the number of pairs of rows (as well as columns) in $\mathbf{S}$ having the correlation $\pm 3/K$, all other pairs of different rows having correlation $\pm 1/K$. After discarding any one column in $\mathbf{S}$, row inner products change from $\pm 1/K$ to 0 or $\pm 2/K$ and from $\pm 3/K$ to $\pm 2/K$ or $\pm 4/K$. It is clear that the number t of row pairs in $\mathbf{S}_1$ whose inner product is $\pm 4/K$ can not exceed l: $t \le l = 0, 1, 2$. Denote the number of rows in $\mathbf{S}_1$ having even weight by n and take into account that with row length $K - 1 \equiv 0 \pmod 4$ an inner product $\pm 2/K$ occurs only for rows i, j whose weights w_i, w_j are of different parities. Allowing for the changing squared norms of rows from 1 to $(K-1)/K$ as a result of column elimination and counting the number of all possible row inner products in $\mathbf{S}_1$, we obtain

$$\mathrm{TSC}(\mathbf{S}_1) = \frac{K(K-1)^2 + 8n(K-n) + 32t}{K^2}. \tag{7}$$

Equating the right-hand sides of expressions (6) and (7) and solving the equation thereby produced in K gives

$$K = 2(n \pm \sqrt{n - 2(l - 2t)}) + 1.$$

Since K is natural we put $n - 2(l - 2t) = x^2$ where x is a nonnegative integer, which results in (4), the minus sign in the preceding expression having been ignored, since $x(x+1)$ and $x(x-1)$ generate the same series of integers when $x = 0, 1, \ldots$.

To prove condition (5), let us return to matrix $\mathbf{S}$ and delete in it a column entering a column pair with correlation $\pm 3/K$. In the $K \times (K-1)$ matrix $\mathbf{S}_2$ thus obtained there are no column pairs with correlation $\pm 3/K$ if $l = 0, 1$ and no more than one such pair if $l = 2$. Designating the number of such pairs by s, the number of rows in $\mathbf{S}_2$ whose inner product is $\pm 4/K$ by u and repeating exactly all the steps described above we arrive at (5), thereby completing proof of the proposition. (Q.E.D.)

Since K should obey both conditions (4) and (5) integers x and y are tied to each other by the equation

$$x(x+1) - y(y+1) = 2(s - l) + 4(t - u) \tag{8}$$

where again $0 \le t, u \le l = 0, 1, 2$; $s = 0$, if $l = 0, 1$ and $s = 0, 1$, if $l = 2$. Under substitution $l = 0$ $\mathrm{TSC}(\mathbf{S})$ (3) coincides with the bound (1) and in (8), (4), and (5) only zero values of s, t, u are allowed. Thereby we have proved the following necessary condition.

Proposition 2: $K = L \equiv 1 \pmod 4$ binary signatures meeting the bound (1) may exist only for values $K = 2x(x+1) + 1 = 5, 13, 25, 41, 61, \ldots$

The signature ensemble attaining the bound (1) for $K = 5$ is trivial and consists of five cyclic shifts of the properly normalized sequence $(++++-)$. Less obvious but still simple is the construction of the signatures for $K = 13$: they are 13 cyclic shifts of binary sequence formed on the basis of (13, 4, 1) Singer difference set [6], [7]. Nothing is known so far (at least to the author) about the existence of the sets in question for further K from the list above.

Proposition 3: The only size K allowing existence of $K = L \equiv 1 \pmod 4$ binary signatures having minimum $\mathrm{TSC}(\mathbf{S})$ defined by (3) with $l = 1$ is $K = 17$.

Proof: When $l = 1$, trying substitutions $s = 0$ and $t, u = 0, 1$ in (8) and finding its integer solutions for x, y leaves only two possibilities: $K = 5, 17$, of which the first is discarded due to the existence of the set with lower $\mathrm{TSC}(\mathbf{S})$. (Q.E.D.)

Finally, for $l = 2$ solving (8) under s, t, u running over their ranges (all values of K covered with $l = 0, 1$ excluded) leads to the following statement.

Proposition 4: $K = L \equiv 1 \pmod 4$ binary signatures having a minimum $\mathrm{TSC}(\mathbf{S})$ defined by (3) with $l = 2$ may exist only for $K = 9, 21, 49, 69$ or $K = 2x(x+1) - 7, x \ge 4$.

In fact, $K = 9$ should be removed from this list. Indeed, when $l = 2, K = 9$ (4) gives $t = 0, x = 0 \Rightarrow n = 2(l - 2t) = 4$, i.e., normalized row correlations of $\mathbf{S}_1$ take on only values $0, \pm 1/4$, four rows being of even and five of odd weight. This in turn entails the orthogonality of any rows having weights of equal parity. After multiplying all rows symbol-wise by the first one and rearranging the columns (and if necessary the rows), matrix $\mathbf{S}_1$ may be transformed into $\mathbf{S}'_1$ having the same row correlations, with the first four rows being four Walsh-Hadamard functions (scaled by $1/3$) and the other rows having odd weights as before. Since each of five odd-weight rows has a squared correlation $1/16$ with each of four Walsh–Hadamard function en-

tering $\mathbf{S'}_1$, it is easily deduced that the sum of its squared correlations with the other four Walsh-Hadamard functions not entering $\mathbf{S'}_1$ will be $3/4$, possible values of every correlation being only $\pm 1/4$ and $\pm 3/4$ (the latter follows from the evenness of the weights of Walsh–Hadamard functions). The sum $3/4$ can be derived from these values squared if exactly one correlation is $\pm 3/4$ leaving the rest equal to $\pm 1/4$. There are five such rows altogether but only four Walsh–Hadamard functions not entering $\mathbf{S'}_1$. Therefore, at least two odd-weight rows have correlation $\pm 3/4$ with the same Walsh–Hadamard function. Calculating their inner product in the Walsh-Hadamard basis gives $\pm 9/16$ plus seven terms assuming values $\pm 1/16$. Obviously, this never results in zero, in contradiction with the orthogonality of the odd-weight rows of $\mathbf{S'}_1$. This proves the nonexistence of 9 binary signatures having a total squared correlation given by (3) with $l = 2$. The same fact is proved in [6] with the support of a computer search.

We can now note that the next in magnitude value of $\mathrm{TSC}(\mathbf{S})$ corresponds to a substitution $l = 3$ in (3) (one column pair with correlation $\pm 5/K$, the rest having correlations $\pm 1/K$, produces equal $\mathrm{TSC}(\mathbf{S})$). Then combining what was obtained for $l = 0, 1, 2, 3$ derives the new bound

$$\mathrm{TSC}(\mathbf{S}) \geq K + \frac{K-1}{K} + \begin{cases} 0, & K = 2x(x+1)+1, \quad x \geq 1 \\ \dfrac{16}{K^2}, & K = 17 \\ \dfrac{32}{K^2}, & K = 21, 49, 69 \text{ or} \\ & K = 2x(x+1)-7, \quad x \geq 4 \\ \dfrac{48}{K^2}, & \text{other } K \equiv 1 \pmod 4. \end{cases} \tag{9}$$

A simple example of a set of 9 signatures of length 9 achieving the bound (9) can be found in [6].

IV. Conclusion

Using an algorithm of the elimination of columns of the Hadamard matrix, we have demonstrated that the Karystinos–Pados bound is tight, whenever $M = \max\{K, L\} \equiv 2 \pmod 4$ and a Hadamard matrix of size $M + 2$ exists, thereby removing doubts as to three out of four cases referred to in [5]. For the fourth case $K = L \equiv 1 \pmod 4$ a new version of bound is derived, improving the estimation of the total squared correlation from below for the majority of values K.

References

[1] M. Rupf and J. L. Massey, "Optimum sequence multisets for synchronous code-division multiple-access channels," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1261–1266, July 1994.

[2] D. V. Sarwate, "Meeting the Welch bound with equality," in *Proc. Sequences and Their Applications (SETA'98)*, C. Ding, T. Helleseth, and H. Niederreiter, Eds., London, U.K., 1999.

[3] J. L. Massey and T. Mittelholzer, "Welch's bound and sequence sets for code-division multiple-access systems," in *Sequences II, Methods in Communication, Security, and Computer Sciences*, R. Capocelli, A. De Santis, and U. Vaccaro, Eds. New York: Springer-Verlag, 1993.

[4] R. L. Welch, "Lower bound on the maximum cross-correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397–399, May 1974.

[5] G. N. Karystinos and D. A. Pados, "New bounds on the total squared correlation and optimum design of DS-CDMA binary signature sets," *IEEE Trans. Commun.*, vol. 51, pp. 48–51, Jan. 2003.

[6] C. Ding, M. Golin, and T. Klove, "Meeting the Welch and Karystinos-Pados bounds on DS-CDMA binary signature sets," *Designs, Coding, and Cryptography*, vol. 30, pp. 73–84, Aug. 2003.

[7] L. D. Baumert, *Cyclic Difference Sets*. New York: Springer-Verlag, 1971.