Uniquely Decodable Code-Division via Augmented Sylvester-Hadamard Matrices

Michel Kulhandjian and Dimitris A. Pados†
Department of Electrical Engineering
332 Bonner Hall
State University of New York at Buffalo
Buffalo, NY 14260
E-Mail: {mkk6,pados}@buffalo.edu

***Abstract*—We consider the problem of designing binary antipodal uniquely decodable (errorless) code sets for overloaded code-division multiplexing applications where the number of signals K is larger than the code length L. Our proposed errorless code set design aims at identifying the maximum number of columns that can be potentially appended to a Sylvester-Hadamard matrix of order L, while maintaining the errorless code property. In particular, we derive formally the maximum number of columns that may be appended to the Sylvester-Hadamard matrix of order $L = 8$ and use this result as a seed to produce an infinite sequence of designs in increasing L. In the noiseless transmission case, a simple algorithm is developed to uniquely decode all signals. In additive white Gaussian noise (AWGN), a slab-sphere decoding scheme can be utilized for efficient and effective decoding.**

Index Terms – Code-division multiplexing, detecting matrices, Hadamard matrices, Karystinos-Pados bound, Welch bound.

I. Introduction

Recent results in the field of optimal antipodal binary (or quaternary) code-division multiplexing addressed the problem of minimum total-squared-correlation code set design [1]-[4] and its extension to periodic and aperiodic correlations [5], [6]. With emphasis on overloaded code-division multiplexing where the number of multiplexed signals K exceeds the code (signature) length L, extendend Hadamard-matrix[1] based designs were seen to offer multiple correlation optimality (direct [1], [4], periodic [5], and aperiodic [6]).

An additional property that an overloaded code set needs to satisfy is to be "*errorless*" (uniquely decodable) in noiseless multiplexed transmission. A binary antipodal errorless code set of dimension $L \times K$ is a matrix $\mathbf{C} \in \{\pm 1\}^{L\times K}$ such that for all possible $\mathbf{x}_1 \neq \mathbf{x}_2 \in \{\pm 1\}^K$, $\mathbf{C}\mathbf{x}_1 \neq \mathbf{C}\mathbf{x}_2$. Then, in the overloaded $(K > L)$ synchronous code-division application of interest, the multiplexed signal $\mathbf{y} = A\mathbf{C}\mathbf{x} = \sum_{i=1}^{K} Ax_i\mathbf{c}_i$, where $\mathbf{c}_i \in \{\pm 1\}^L$, $i = 1, ..., K$, are the signal signatures, can be uniquely demultiplexed to recover the information bits x_i with amplitude $A > 0$.

†Corresponding author.

[1]We recall that a Hadamard matrix of size L is an $L \times L$ matrix $\mathbf{H}_L$ with elements $+1$ or 1 and mutually orthogonal columns, $\mathbf{H}_L\mathbf{H}_L^T = L\mathbf{I}_L$ where $\mathbf{I}_L$ is the size-L identity matrix. A necessary condition for a Hadamard matrix to exist is that $L \equiv 0(\mathrm{mod}4)$, except for the trivial cases of $L = 1$ or $L = 2$.

In the literature, uniquely decodable code set constructions [7]-[11] are recursive in nature and produce antipodal matrices of size $L \times A(L) + 1$ where $A(L)$ is the number of ones in the binary expansion of all positive integers less than L. An overview of existing recursive construction techniques of binary $(0, 1)$, antipodal (± 1), and ternary $(0, \pm 1)$ detecting matrices is given in [12] in a unifying framework. Size-wise, the base-line result remains Lindström's limit [13] $\lim_{L\to\infty} \frac{K_{max}(L)}{L\log_2 L} = \frac{1}{2}$ where $K_{max}(L)$ represents the maximum number of columns (signals) that a matrix can have and still be uniquely decodable.

None of the code designs in the literature considered so far the option of appending columns to Sylvester-Hadamard matrices so that the resulting code set is errorless. It is trivial to prove that for $L = 4$ the maximum number of columns that can be appended to the Sylvester-Hadamard matrix $\mathbf{H}_4$ is one. In this work, first we find formally the maximum number of columns that can be appended to the Sylvester-Hadamard matrix $\mathbf{H}_8$ (which is five, therefore $K_{max} = 13$). Then, we develop an explicit construction of antipodal matrices using the 8×13 code set as a seed to create an infinite series of code sets with dimensions $L \times A(L)+1$ and $L' \times A(L)+1+7m$ where $L = 2^p$, $p = 4, 5, ...$, and $L < L' \leq 2L$, $L' = L + 4m = 4n$, $m = 1, 2, ...$, $n = 3, 5, 7, ...$ (e.g., sets $\mathbf{C}_{12\times 20}$, $\mathbf{C}_{16\times 33}$, $\mathbf{C}_{20\times 40}$, $\mathbf{C}_{24\times 47}$, $\mathbf{C}_{28\times 56}$, $\mathbf{C}_{32\times 81}$, ... , $\mathbf{C}_{64\times 193}$, etc.). We prove that the minimum Euclidean distance of the multiplexed data $\mathbf{C}\mathbf{x}$, $\mathbf{x} \in \{\pm 1\}^K$ is 4 for $L = 2^p$ and for the noiseless multiplexing case we describe a simple recursive algorithm for errorless decoding. For additive white Gaussian noise (AWGN) channels, a slab-sphere decoding scheme [14] may provide efficient and effective decoding.

II. Formulation and Foundation Development

We recall that a code set $\mathbf{C} \in \{\pm 1\}^{L\times K}$ is uniquely decodable over signals $\mathbf{x} \in \{\pm 1\}^K$, $K \leq L$, if and only if for any $\mathbf{x}_1 \neq \mathbf{x}_2$, $\mathbf{C}\mathbf{x}_1 \neq \mathbf{C}\mathbf{x}_2$ or, equivalently, $\mathbf{C}(\mathbf{x}_1 - \mathbf{x}_2) \neq \mathbf{0}_{L\times 1}$. We can rewrite the unique decodability necessary and sufficient condition as $\mathsf{Null}(\mathbf{C}) \cap \{0, \pm 2\}^K = \{0\}^K$ or in an equivalent manner

$$\mathsf{Null}(\mathbf{C}) \cap \{0, \pm 1\}^K = \{0\}^K. \quad (1)$$

We are interested in this work in matrices $\mathbf{C}$ that can be written as $\mathbf{C} = [\mathbf{H}_L \mathbf{V}_L]$ where $\mathbf{V}_L \in \{\pm 1\}^{L\times(K-L)}$ and $\mathbf{H}_L$ is a Sylvester-Hadamard matrix of order $L = 2^p$, $p = 2, 3, ...$. We recall that the order-2 Sylvester-Hadamard matrix is $\mathbf{H}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $\mathbf{H}_{2^{p+1}} = \begin{bmatrix} \mathbf{H}_{2^p} & \mathbf{H}_{2^p} \\ \mathbf{H}_{2^p} & -\mathbf{H}_{2^p} \end{bmatrix}$, $p = 1, 2, ...$. Then, for any $p = 1, 2, ...$, $\mathbf{H}_{2^p}\mathbf{H}_{2^p} = 2^p \mathbf{I}_{2^p \times 2^p}$ where $\mathbf{I}_N$ is the size-N identity matrix.

By (1), for any $\mathbf{z} \in \{0, \pm 1\}^K - \{0\}^K$ we must have

$$\begin{aligned} [\mathbf{H}_L \mathbf{V}_L]\, \mathbf{z} &\neq \mathbf{0} \quad \text{or} && \text{(2a)} \\ \mathbf{H}_L \mathbf{z}_1 &\neq -\mathbf{V}_L \mathbf{z}_2 && \text{(2b)} \end{aligned}$$

where $\mathbf{z} = \left[\mathbf{z}_1^T \mathbf{z}_2^T\right]^T$, $\mathbf{z}_1 \in \{0, \pm 1\}^L$, $\mathbf{z}_2 \in \{0, \pm 1\}^{K-L}$. Obviously, there are 3^L distinct points created by the $\mathbf{H}_L$ Hadamard matrix projection $\mathbf{H}_L \mathbf{z}_1$ and up to $3^{K-L} - 1$ points created by the $\mathbf{V}_L$ matrix in the L-dimensional space by the operation $\mathbf{V}_L \mathbf{z}_2$. We need to design a matrix $\mathbf{V}_L \in \{\pm 1\}^{L\times(K-L)}$ such that no hypercube point generated by $\mathbf{V}_L$ coincides with hypercube point generated by $\mathbf{H}_L$. We shall attempt to address the following two questions: (i) What is the maximum number of columns that we can append to a given Sylvester-Hadamard $\mathbf{H}_L$ and satisfy (2b)? (ii) If we know the maximum number of columns $K - L$ that we can append, how do we design such a $\mathbf{V}_L \in \{\pm 1\}^{L\times(K-L)}$ to create the errorless code $\mathbf{C} = [\mathbf{H}_L \mathbf{V}_L]$?

The design of the optimal $\mathbf{V}_L$ (maximum number of columns) for the case $L = 4$ is simple and can be found working directly in the column space of $\mathbf{C}$ which has a total of only $2^4 = 16$ points. Four points and their corresponding antipodal points are used already by $\mathbf{H}_4$ and cannot be entered in $\mathbf{V}_4$. The remaining eight possible candidates are $[-1, 1, 1, 1]^T$, $[1, -1, 1, 1]^T$, $[1, 1, -1, 1]^T$, $[1, 1, 1, -1]^T$ and their four antipodals. Any one, but no more, of these vectors can define $\mathbf{V}_4 \in \{\pm 1\}^{4\times 1}$.

In preparation for the general construction section that follows, we present four unique decodability conditions (propositions) that we derived stemming from Eq. (2b). In the presentation, each column $\mathbf{v}_i$ in $\mathbf{V}_L = [\mathbf{v}_1, ..., \mathbf{v}_{K-L}]$ is partitioned into subvectors $\mathbf{v}_i = [\mathbf{v}_{i,0}^T, ..., \mathbf{v}_{i,M-1}^T]^T$ where $M = L/4$ and $\mathbf{v}_{i,j} \in \{\pm 1\}^4$ for $0 \leq j \leq M$.

Proposition 1 Assume $\mathbf{z}_1 \neq \mathbf{0}^L$ in (2b). The code $\mathbf{C}$ is not uniquely decodable (not errorless) if and only if

$$\begin{aligned} [\mathbf{v}_{0,0}, ..., \mathbf{v}_{N-1,0}]\, \mathbf{A}\mathbf{1}_N &= \mathbf{H}_4 \mathbf{A}_{H,0} \mathbf{1}_{N'} \\ [\mathbf{v}_{0,1}, ..., \mathbf{v}_{N-1,1}]\, \mathbf{A}\mathbf{1}_N &= \mathbf{H}_4 \mathbf{A}_{H,1} \mathbf{1}_{N'} \qquad (3) \\ \vdots \qquad\qquad & \quad \vdots \\ [\mathbf{v}_{0,M-1}, ..., \mathbf{v}_{N-1,M-1}]\, \mathbf{A}\mathbf{1}_N &= \mathbf{H}_4 \mathbf{A}_{H,M-1} \mathbf{1}_{N'} \end{aligned}$$

for some $\mathbf{A} \in \{0, \pm 1\}^{N\times N}$ that has at most one non zero entry in each column and matrices $\mathbf{A}_{H,i} \in \{0, \pm 1\}^{4\times N'}$ $i = 0, ..., M - 1$, that have at most one non zero entry in each column at the same position for all $i = 0, ..., M-1$ with values $[a_{0,j}, ..., a_{M-1,j}]^T \in \pm \mathbf{H}_M$ at column j, where $N, N' \in \mathbb{N}$, $\mathbf{1}_N = \{1\}^{N\times 1}$ and $\mathbf{1}_{N'} = \{1\}^{N'\times 1}$. □

Proposition 2 Assume $\mathbf{z}_1 \neq \mathbf{0}^L$ in (2b). If

$$\begin{aligned} \beta_{0,0}\mathbf{v}_{0,0} \odot ... \odot \beta_{N-1,0}\mathbf{v}_{N-1,0} &= \alpha_0 \mathbf{h}_j \\ \beta_{0,1}\mathbf{v}_{0,1} \odot ... \odot \beta_{N-1,1}\mathbf{v}_{N-1,1} &= \alpha_1 \mathbf{h}_j \qquad (4) \\ \vdots \qquad\qquad & \quad \vdots \\ \beta_{0,M-1}\mathbf{v}_{0,M-1} \odot ... \odot \beta_{N-1,M-1}\mathbf{v}_{N-1,M-1} &= \alpha_{M-1} \mathbf{h}_j \end{aligned}$$

is not true for all $[\alpha_0, ..., \alpha_{M-1}]^T \in \mathbf{H}_M$, $\mathbf{h}_j \in \mathbf{H}_4$, $\beta_{i,j} \in \{0, 1\}$, $0 \leq i \leq N - 1$, $0 \leq j \leq M - 1$, $\beta_{0,0} = \beta_{0,1} = ... = \beta_{0,M-1}$, $\beta_{1,0} = \beta_{1,1} = ... = \beta_{1,M-1}$, ..., $\beta_{N-1,0} = \beta_{N-1,1} = ... = \beta_{N-1,M-1}$, where the $\odot$ operator denotes element by element multiplication of $\mathbf{v}_{i,j}$ vectors, then (2b) is satisfied. □

Proposition 3 Assume $\mathbf{z}_1 = \mathbf{0}^L$ in (2b). The code $\mathbf{C}$ is not uniquely decodable if and only if

$$\begin{aligned} [\mathbf{v}_{0,0}, ..., \mathbf{v}_{N-1,0}]\, \mathbf{A}\mathbf{1}_N &= \mathbf{0} \\ [\mathbf{v}_{0,1}, ..., \mathbf{v}_{N-1,1}]\, \mathbf{A}\mathbf{1}_N &= \mathbf{0} \qquad (5) \\ \vdots \qquad\qquad & \quad \vdots \\ [\mathbf{v}_{0,M-1}, ..., \mathbf{v}_{N-1,M-1}]\, \mathbf{A}\mathbf{1}_N &= \mathbf{0} \end{aligned}$$

for some $\mathbf{A} \in \{0, \pm 1\}^{N\times N}$ where $N \in \mathbb{N}$, $\mathbf{1} = \{1\}^{4\times 1}$, $\mathbf{0} = \{0\}^{4\times 1}$ and $\mathbf{A}$ has at most one ± 1 entry in each column. □

Proposition 4 Assume $\mathbf{z}_1 = \mathbf{0}^L$ in (2b). If

$$\begin{aligned} \beta_{0,0}\mathbf{v}_{0,0} \odot ... \odot \beta_{N-1,0}\mathbf{v}_{N-1,0} &= \alpha \mathbf{1} \\ \beta_{0,1}\mathbf{v}_{0,1} \odot ... \odot \beta_{N-1,1}\mathbf{v}_{N-1,1} &= \alpha \mathbf{1} \qquad (6) \\ \vdots \qquad\qquad & \quad \vdots \\ \beta_{0,M-1}\mathbf{v}_{0,M-1} \cdots \odot \beta_{N-1,M-1}\mathbf{v}_{N-1,M-1} &= \alpha \mathbf{1} \end{aligned}$$

is not true for all $\alpha \in \{\pm 1\}$, $\beta_{i,j} \in \{0, 1\}$, $0 \leq i \leq N - 1$, $0 \leq j \leq M - 1$, $\beta_{0,0} = \beta_{0,1} = ... = \beta_{0,M-1}$, $\beta_{1,0} = \beta_{1,1} = ... = \beta_{1,M-1}$, $\beta_{N-1,0} = \beta_{N-1,1} = ... = \beta_{N-1,M-1}$, where $\odot$ operator denotes element by element multiplication of $\mathbf{v}_{i,j}$ vectors, then (2b) is satisfied. □

III. Errorless Code Set Construction

We begin by trying to find the maximum number of columns that can be appended to the Sylvester-Hadamard matrix $\mathbf{H}_8$ while maintaining the unique decodability property. We introduce the notation $\mathbf{H}_4 = [\mathbf{h}_0, \mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3]$, $[\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3] \triangleq \left[[-1, 1, 1, 1]^T, [1, -1, 1, 1]^T, [1, 1, -1, 1]^T, [1, 1, 1, -1]^T\right]$, and the negation function $\mathbf{x}^- \triangleq -\mathbf{x}$. Table I lists the vectors $\mathbf{h}_0, ..., \mathbf{h}_3, \mathbf{a}_0, .., \mathbf{a}_3$ in their direct and negated form along with their corresponding elements in the extended $GF(2^4)$ field with primitive polynomial $\alpha^4 + \alpha + 1 = 0$ and negation function $\alpha^- = \alpha^5$. The summation among all the elements in the extended $GF(2^4)$ field is equivalent to elementwise multiplication of corresponding binary antipodal vectors.

With the above formulation, we describe the columns of $\mathbf{V}_L$, $\mathbf{v}_i$, $i = 0, ..., K - L - 1$, as two-dimensional finite field vectors $\mathbf{f}_i = [f_{i,0} f_{i,1}]^T$, $f_{i,0}, f_{i,1} \in \{0, 1, \alpha, ..., \alpha^{14}\}$, $i = 0, ..., K - L - 1$, $L = 8$. By Propositions 2 and 4, no vector subset of $[\mathbf{f}_0, \mathbf{f}_1, .., \mathbf{f}_{K-L-1}]$ can be

TABLE I
$GF(2^4)$ FIELD EQUIVALENCE

Antipodal	Polynomial	Power
$\mathbf{h}_0$	0	0
$\mathbf{h}_2$	1	1
$\mathbf{h}_1$	α	α
$\mathbf{h}_0^-$	α^2	α^2
$\mathbf{a}_1$	α^3	α^3
$\mathbf{h}_3$	$\alpha+1$	α^4
$\mathbf{h}_1^-$	$\alpha^2+\alpha$	α^5
$\mathbf{a}_1^-$	$\alpha^3+\alpha^2$	α^6
$\mathbf{a}_2$	$\alpha^3+\alpha+1$	α^7
$\mathbf{h}_2^-$	α^2+1	α^8
$\mathbf{a}_3$	$\alpha^3+\alpha$	α^9
$\mathbf{h}_3^-$	$\alpha^2+\alpha+1$	α^{10}
$\mathbf{a}_3^-$	$\alpha^3+\alpha^2+\alpha$	α^{11}
$\mathbf{a}_2^-$	$\alpha^3+\alpha^2+\alpha+1$	α^{12}
$\mathbf{a}_0$	$\alpha^3+\alpha^2+1$	α^{13}
$\mathbf{a}_0^-$	α^3+1	α^{14}

of the form $[c,c]^T$, $[c^-,c]^T$, $[c,c^-]^T$, $[c^-,c^-]^T$ where $c \in \{0,1,\alpha,\alpha^2,\alpha^4,\alpha^5,\alpha^8,\alpha^{10}\}$. Consider all $2^8 = 256$ possible antipodal columns of $\mathbf{C}$ reduced down to 128 by the column-sign equivalence property. Organize the 128 vectors into three types of matrices, $\mathbf{A}$, $\mathbf{D}$, $\mathbf{G}$ as well as $\mathbf{H}_8$ as given below: $\mathbf{A}_1 = \begin{bmatrix} \alpha^{13} & \alpha^{14} & \alpha^3 & \alpha^3 & \alpha^7 & \alpha^7 & \alpha^9 & \alpha^9 \\ 0 & 0 & \alpha^8 & 1 & \alpha^5 & \alpha & \alpha^{10} & \alpha^4 \end{bmatrix}$, $\mathbf{A}_2 = \begin{bmatrix} \alpha^3 & \alpha^6 & \alpha^{13} & \alpha^{13} & \alpha^7 & \alpha^7 & \alpha^9 & \alpha^9 \\ 0 & 0 & \alpha^8 & 1 & \alpha^{10} & \alpha^4 & \alpha & \alpha^5 \end{bmatrix}$, $\mathbf{A}_3 = \begin{bmatrix} \alpha^7 & \alpha^{12} & \alpha^{13} & \alpha^{13} & \alpha^3 & \alpha^3 & \alpha^9 & \alpha^9 \\ 0 & 0 & \alpha^5 & \alpha & \alpha^{10} & \alpha^4 & \alpha^8 & 1 \end{bmatrix}$, $\mathbf{A}_4 = \begin{bmatrix} \alpha^9 & \alpha^{11} & \alpha^{13} & \alpha^{13} & \alpha^3 & \alpha^3 & \alpha^7 & \alpha^7 \\ 0 & 0 & \alpha^{10} & \alpha^4 & \alpha & \alpha^5 & \alpha^8 & 1 \end{bmatrix}$, $\mathbf{A}_5 = \begin{bmatrix} 0 & 0 & 1 & \alpha^8 & \alpha & \alpha^5 & \alpha^4 & \alpha^{10} \\ \alpha^{13} & \alpha^{14} & \alpha^3 & \alpha^3 & \alpha^7 & \alpha^7 & \alpha^9 & \alpha^9 \end{bmatrix}$, $\mathbf{A}_6 = \begin{bmatrix} 0 & 0 & 1 & \alpha^8 & \alpha & \alpha^5 & \alpha^4 & \alpha^{10} \\ \alpha^3 & \alpha^6 & \alpha^{13} & \alpha^{13} & \alpha^9 & \alpha^9 & \alpha^7 & \alpha^7 \end{bmatrix}$, $\mathbf{A}_7 = \begin{bmatrix} 0 & 0 & 1 & \alpha^8 & \alpha & \alpha^5 & \alpha^4 & \alpha^{10} \\ \alpha^7 & \alpha^{12} & \alpha^9 & \alpha^9 & \alpha^{13} & \alpha^{13} & \alpha^3 & \alpha^3 \end{bmatrix}$, $\mathbf{A}_8 = \begin{bmatrix} 0 & 0 & 1 & \alpha^8 & \alpha & \alpha^5 & \alpha^4 & \alpha^{10} \\ \alpha^9 & \alpha^{11} & \alpha^7 & \alpha^7 & \alpha^3 & \alpha^3 & \alpha^{13} & \alpha^{13} \end{bmatrix}$, $\mathbf{D}_1 = \begin{bmatrix} 0 & 0 & 1 & \alpha^8 \\ 1 & \alpha^8 & 0 & 0 \end{bmatrix}$, $\mathbf{D}_2 = \begin{bmatrix} 0 & 0 & 1 & \alpha^5 \\ 1 & \alpha^5 & 0 & 0 \end{bmatrix}$, $\mathbf{D}_3 = \begin{bmatrix} 0 & 0 & \alpha^4 & \alpha^{10} \\ \alpha^4 & \alpha^{10} & 0 & 0 \end{bmatrix}$, $\mathbf{D}_4 = \begin{bmatrix} \alpha^{13} & \alpha^3 & \alpha^7 & \alpha^9 \\ \alpha^{13} & \alpha^3 & \alpha^7 & \alpha^9 \end{bmatrix}$, $\mathbf{D}_5 = \begin{bmatrix} \alpha^{13} & \alpha^3 & \alpha^7 & \alpha^9 \\ \alpha^3 & \alpha^{13} & \alpha^9 & \alpha^7 \end{bmatrix}$, $\mathbf{D}_6 = \begin{bmatrix} \alpha^{13} & \alpha^3 & \alpha^7 & \alpha^9 \\ \alpha^7 & \alpha^9 & \alpha^{13} & \alpha^3 \end{bmatrix}$, $\mathbf{D}_7 = \begin{bmatrix} \alpha^{13} & \alpha^3 & \alpha^7 & \alpha^9 \\ \alpha^9 & \alpha^7 & \alpha^3 & \alpha^{13} \end{bmatrix}$, $\mathbf{G}_1 = \begin{bmatrix} \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^9 \\ \alpha^9 & \alpha^{12} & \alpha^6 & \alpha^{14} \end{bmatrix}$, $\mathbf{G}_2 = \begin{bmatrix} \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^9 \\ \alpha^7 & \alpha^{11} & \alpha^{14} & \alpha^6 \end{bmatrix}$, $\mathbf{G}_3 = \begin{bmatrix} \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^9 \\ \alpha^3 & \alpha^{14} & \alpha^9 & \alpha^{12} \end{bmatrix}$, $\mathbf{G}_4 = \begin{bmatrix} \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^9 \\ \alpha^{13} & \alpha^6 & \alpha^{12} & \alpha^{11} \end{bmatrix}$, $\mathbf{G}_5 = \begin{bmatrix} \alpha & \alpha & 1 & 1 \\ \alpha^8 & 1 & \alpha^5 & \alpha \end{bmatrix}$, $\mathbf{G}_6 = \begin{bmatrix} \alpha^4 & \alpha^4 & 1 & 1 \\ \alpha^8 & 1 & \alpha^{10} & \alpha^4 \end{bmatrix}$, $\mathbf{G}_7 = \begin{bmatrix} \alpha^4 & \alpha^4 & \alpha & \alpha \\ \alpha^5 & \alpha^1 & \alpha^{10} & \alpha^4 \end{bmatrix}$, $\mathbf{H}_8 = \begin{bmatrix} 0 & \alpha & 1 & \alpha^4 & 0 & \alpha & 1 & \alpha^4 \\ 0 & \alpha & 1 & \alpha^4 & \alpha^2 & \alpha^5 & \alpha^8 & \alpha^{10} \end{bmatrix}$. No two vectors from the same matrix can be included in the construction of $\mathbf{V}_8$, since they will coincide with the $[c,c]^T$, $[c^-,c]^T$, $[c,c^-]^T$, $[c^-,c^-]^T$ forms, $c \in \{0,1,\alpha,\alpha^2,\alpha^4,\alpha^5,\alpha^8,\alpha^{10}\}$. Certainly, $\mathbf{H}_8$ (and $\mathbf{H}_8^-$) cannot be included in our design set either. It can be shown that under field summation $\mathbf{A}_{i_0} + \mathbf{A}_{i_1} = \mathbf{D}_{j_0}$ or $\mathbf{G}_{8-j_0}$, $\mathbf{A}_{i_2} + \mathbf{D}_{j_1} = \mathbf{A}_{i_3}$, $\mathbf{D}_{j_2}+\mathbf{D}_{j_3} = \mathbf{G}_{j_4}$ and $\mathbf{G}_{j_5}+\mathbf{G}_{j_6} = \mathbf{G}_{j_7}$ where $i_n \in \{1,...,8\}$, $0 \le n \le 3$, and $j_m \in \{1,...,7\}$, $0 \le m \le 7$. This result establishes that the maximum number of vectors that we can append to $\mathbf{H}_8$ and have uniquely decodable code $\mathbf{C}$ is five. The possible $\mathbf{V}_8$ matrices with $K - L = 5$ columns where $K = A(8) + 1 = 13$ can be constructed from $(\mathbf{A},\mathbf{A},\mathbf{A},\mathbf{D},\mathbf{G})$, $(\mathbf{A},\mathbf{A},\mathbf{D},\mathbf{D},\mathbf{D})$, $(\mathbf{A},\mathbf{A},\mathbf{D},\mathbf{D},\mathbf{G})$, $(\mathbf{A},\mathbf{A},\mathbf{D},\mathbf{G},\mathbf{G})$, $(\mathbf{A},\mathbf{D},\mathbf{D},\mathbf{D},\mathbf{D})$, $(\mathbf{A},\mathbf{D},\mathbf{D},\mathbf{D},\mathbf{G})$, $(\mathbf{A},\mathbf{D},\mathbf{D},\mathbf{G},\mathbf{G})$, and $(\mathbf{A},\mathbf{D},\mathbf{G},\mathbf{G},\mathbf{G})$ combinations only.

Next, we are ready to propose a general $L \times [A(L)+1]$ code set design[2] when $L = 2^p$, $p = 3,4,...$. Choose[3] $\mathbf{V}_8 = \begin{bmatrix} \alpha^{13} & 1 & \alpha & \alpha^{13} & \alpha^3 \\ 0 & 0 & 0 & \alpha^{13} & \alpha^{3-} \end{bmatrix}$ and then recursively construct

$$\mathbf{V}_L = \begin{bmatrix} \mathbf{V}_{L/2} & \mathbf{V}_{L/2} & \mathbf{R} \\ \mathbf{V}_{L/2} & \mathbf{V}_{L/2}^- & \mathbf{0}_{L/2} \end{bmatrix} \tag{7}$$

where $\mathbf{V}_{L/2}$ is the $L/2 \times [A(L/2)+1-L/2]$ matrix constructed in the previous step, $\mathbf{R} = [\mathbf{r}_0,...,\mathbf{r}_{M-1}]^T$ with $\mathbf{r}_i = \left[\bar{\mathbf{0}}_{4i}^T, \alpha^{13}, 1, \alpha, \mathbf{0}_{4(M-1-i)}^T\right]^T$, $0 \le i \le M-1$, $M = L/8$, $\bar{\mathbf{0}}_q$ is the q-dimensional column vector with all elements zero from the extended field $GF(2^4)$, except at the qth position which is 0^-, $\mathbf{0}_t$ is an extended field $GF(2^4)$ all-zero t-dimensional column vector and $\mathbf{0}_{L/2}$ is an $L/2 \times (L/2-1)$ all-zero extended field $GF(2^4)$ matrix. By either Propositions 2 and 4 or Propositions 1 and 3, the resulting code construction $\mathbf{C}_{L\times A(L)+1} = [\mathbf{H}_L \mathbf{V}_L]$ is errorless and of maximum known size $K = A(L)+1$ (to the very best of our knowledge there is no other known construction algorithm that offers size higher than $A(L)+1$ for a given L). The minimum Euclidean distance among vectors $\mathbf{y} = \mathbf{Cx}$ can be found to be equal to 4. The derivation is omitted herein due to lack of space.

Finally, we conclude this paper with an extension of our design to the case $L' = 0(\text{mod}4)$ and $L' \neq 2^p$, $p = 1,2,...$. First, find the largest $L = 2^p$ such that $L < L' \le 2L$. Then, design $\mathbf{V}_L$ according to (7). Find $m \in \{1,2,...\}$ such that $L' = L + 4m$ and extend $\mathbf{V}_L$ to

$$\mathbf{V}_{L'} = \begin{bmatrix} \mathbf{V}_L & \mathbf{0}_L \\ \mathbf{0}' & \mathbf{R}' \end{bmatrix} \tag{8}$$

where $\mathbf{0}_L$ of dimensions $L \times 3m$ and $\mathbf{0}'$ of dimensions $m \times [A(L)+1-L]$ are all-zero matrices from the extended field $GF(2^4)$ and $\mathbf{R}' = \left[\mathbf{r}_0',...,\mathbf{r}_{m-1}'\right]^T$ with $\mathbf{r}_i' = \left[\mathbf{0}_{3i}^T, \alpha^{13}, 1, \alpha, \mathbf{0}_{3(m-1-i)}^T\right]^T$, $0 \le i \le m-1$. The matrix $\mathbf{C}_{L'\times[L'+A(L)+1-L+7m]} = [\mathbf{H}_{L'}' \mathbf{V}_{L'}]$ is our proposed errorless code set where $\mathbf{H}_{L'}'$ is created by the first L' rows and columns of the Sylvester-Hadamard matrix $\mathbf{H}_{2L}$ of order $2L$. Compared with other recursive methods, our method in (8) produces errorless codes[4] $\mathbf{C}$ of dimension $L' = 0(\text{mod}4) \in (L = 2^p, 2^{p+1}]$, and size $K = [L' + A(L) + 1 - L + 7m]$

[2]Since $L = 2^p$, $K = A(L)+1 = p2^{p-1}+1$, $p = 3,4,...$.

[3]In this design, $\mathbf{V}_8$ is chosen from the $(\mathbf{A},\mathbf{D},\mathbf{D},\mathbf{D},\mathbf{G})$ combination.

[4]Note that all of our antipodal errorless code sets $\mathbf{C}_{L\times K}$ can be directly converted to errorless "optical" code sets $\{0,1\}^{L\times K}$, $\mathbf{C}_{optical} = (\mathbf{J}+\mathbf{C})/2$ where $\mathbf{J}$ is the $L \times K$ all-one matrix. The proof that $\text{Null}(\mathbf{C}_{optical}) \cap \{0,\pm 1\}^K = \{0\}^K$ is trivial. However, it is not necessarily true that optical errorless code sets can be converted to errorless antipodal code sets.

that is lower than $A(L')+1$ that constructions in [7]-[12] can achieve for certain $L' = 0(\mathrm{mod}4)$ values. Such constructions, however, require derivation/knowledge of smaller size errorless constructions, while our design in (8) is Sylvester-Hadamard explicit.

IV. Multiuser decoding algorithms

In the following, we describe a recursive algorithm to decode all multiplexed signals in the absence of noise. Suppose that K signals contribute ± 1 information bits and

$$\mathbf{y} = \mathbf{C}\mathbf{x} = \sum_{i=1}^{K} x_i \mathbf{c}_i \tag{9}$$

where $\mathbf{y} \in \{-K, ..., 0, ..., K\}^L$ is the multiplexed signal vector, $\mathbf{C} \in \{\pm 1\}^{L\times K}$ is the proposed code set, $\mathbf{c}_i \in \{\pm 1\}^K$ is the ith signal signature, $i = 1, \cdots, K$, and $\mathbf{x} \in \{\pm 1\}^K$ is the information bit vector. By the design of $\mathbf{C}$, equation (9) has the property that all possible 2^K bit-weighted sums of the $\mathbf{c}_i$ signatures are distinct. This means that we can recover $\mathbf{x}$ uniquely and correctly from $\mathbf{y}$. Consider the following equation

$$\mathbf{r} = \frac{1}{2}(\mathbf{y} + \mathbf{C}\mathbf{1}_{K\times 1}) = \mathbf{C}\mathbf{x}' \tag{10}$$

where $\mathbf{1}_{K\times 1}$ is the all-one vector and $\mathbf{x}' \in \{0,1\}^{K\times 1}$ is the affine transformation of $\mathbf{x}$. Solution of (9) is equivalent to solving (10). Let $n_1 = L - 4(i-1)$, $n_2 = n_1 - L/2$, $n_3 = n_1 + L/2$, $n_4 = L/2 + 4i$, $n_5 = n_4 - 4$, $n_6 = 4i$, $n_7 = n_6 - 4$ and $n_8 = n_4 + L/2$, for $i = 1$ to $L/8$. The demultiplexing algorithm is given in direct implementation form in Table II.

In the case of AWGN, we can efficiently use the slab-sphere decoding algorithm [14] to recover the signals. To illustrate the behavior of our proposed errorless code sets, we consider the overloaded system $\mathbf{C}_{8\times 13}$ in Fig. 1 constructed by equation (7). The performance of the code set in terms of average bit-error-rate (BER) over all K signals versus common signal SNR is plotted in Fig. 2. It can be argued that the proposed errorless code set design of overload-gain 62% can be potentially utilized in code-division multiplexing even under slab-sphere decoding. Fig. 3 shows our errorless $\mathbf{C}_{16\times 33}$ design (overload-gain 106%). The average BER study is given in Fig. 4 and shows most appealing error rate under maximum-likelihood (ML) decoding (but not under slab-sphere decoding).

$$\mathbf{C}_{8\times 13} = \begin{bmatrix} + & + & + & + & + & + & + & + & - & + & + & - & + \\ + & - & + & - & + & - & + & - & + & + & - & + & - \\ + & + & - & - & + & + & - & - & + & - & + & + & + \\ + & - & - & + & + & - & - & + & + & - & - & + & + \\ + & + & + & + & - & - & - & - & + & + & + & - & - \\ + & - & + & - & - & + & - & + & + & + & + & + & + \\ + & + & - & - & - & - & + & + & + & + & + & + & - \\ + & - & - & + & - & + & + & - & + & + & + & + & - \end{bmatrix}$$

Fig. 1. Errorless signature code set for an overloaded system with codelength $L = 8$ and code size $K = 13$.

TABLE II

Noiseless Decoding Algorithm

1) Initialize input $\mathbf{r} = \frac{1}{2}(\mathbf{y} + \mathbf{C}\mathbf{1})$.
2) For $i = 1$ to $L/8$, do;
   2a) Compute $m_{n_3-1} = \mathbf{r}(n_1) + \mathbf{r}(n_1 - 1) - [\mathbf{r}(n_2) + \mathbf{r}(n_2 - 1))]$;
   if $(m_{n_3-1} \mod 4) = 2$, then set $x'_{n_3-1} := 1$; otherwise $x'_{n_3-1} := 0$.
   2b) Compute $m_{n_3-2} = \mathbf{r}(n_1) + \mathbf{r}(n_1 - 2) - [\mathbf{r}(n_2) + \mathbf{r}(n_2 - 2)]$;
   if $(m_{n_3-2} \mod 4) = 2$, then set $x'_{n_3-2} := 1$; otherwise $x'_{n_3-2} := 0$.
   2c) Compute $m_{n_3-3} = \mathbf{r}(n_1) + \mathbf{r}(n_1 - 3)[\mathbf{r}(n_2) + \mathbf{r}(n_2 - 3)] - 2(x'_{n_3-1} + x'_{n_3-2})$;
   if $(m_{n_3-3} \mod 4) = 2$, then set $x'_{n_3-3} := 1$; otherwise $x'_{n_3-3} := 0$.
3) For $i = 1$ to $L/8 - 1$, do;
   3a) Compute $m_{n_8} = \mathbf{r}(n_4 + 1) + \mathbf{r}(n_5 + 1) - [\mathbf{r}(n_6 + 1) + \mathbf{r}(n_7 + 1)] - 2(x'_{n_7+1} + x'_{n_6+1})$;
   if $(m_{n_8} \mod 4) = 2$, then $x'_{n_8} := 1$; otherwise $x'_{n_8} := 0$.
4) Set $\mathbf{r}_1 := \mathbf{r} - \mathbf{C}_{K-L/2:K}\mathbf{x}'_{K-L/2:K}$, $\mathbf{r}_2 := (\mathbf{r}_{1,1:L/2} + \mathbf{r}_{1,L/2+1:L})/2$ and $\mathbf{r}_3 := (\mathbf{r}_{1,1:L/2} - \mathbf{r}_{1,L/2+1:L})/2$.
5) Run algorithm from Step 1 initialized at $\mathbf{r}_2$ and $\mathbf{r}_3$ with dimension $L/2$ until all K unknown elements of $\mathbf{x}'$ are found.

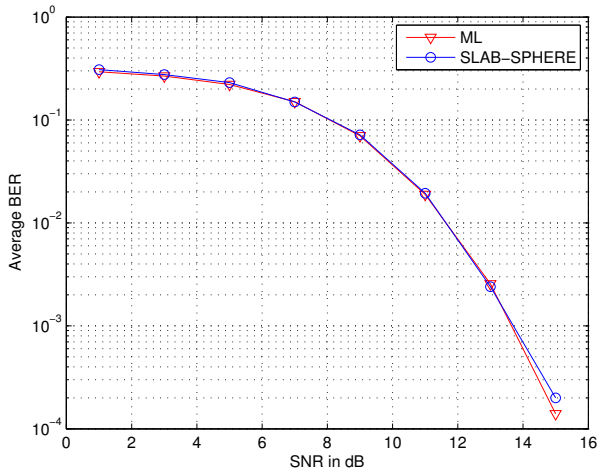

Fig. 2. BER versus SNR for the errorless code system with $L = 8$ and $K = 13$.

References

[1] 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.

[2] C. Ding, M. Golin, and T. Kløve, "Meeting the Welch and Karystinos-Pados bounds on DS-CDMA binary signature sets," *Des., Codes Cryptogr.*, vol. 30, pp. 73-84, Aug. 2003.

[3] V. P. Ipatov, "On the Karystinos-Pados bounds and optimal binary DS-CDMA signature ensembles," *IEEE Commun. Lett.*, vol. 8, pp. 81-83, Feb. 2004.

[4] Ming Li, S. N. Batalama, D. A. Pados, and J. D. Matyas "The maximum squared correlation, total asymptotic efficiency, and sum capacity of minimum-TSC quaternary signature sets," *IEEE Trans. Commun.*, vol. 57, pp. 3662-3672, Dec. 2009.

[5] H. Ganapathy, D. A. Pados, and G. N. Karistinos "New bounds and optimal binary signature sets - Part I: Periodic Total Squared Correlation," *IEEE Trans. Commun.*, vol. 59, pp. 1123-1132, Apr. 2011.

[6] H. Ganapathy, D. A. Pados, and G. N. Karistinos "New bounds and optimal binary signature sets - Part II: Aperiodic total squared correlation," *IEEE Trans. Commun.*, vol. 59, pp. 1411-1420, May 2011.

[7] P. Pad, F. Marvasti, K. Alishahi, and S. Akbari, "A class of errorless codes for overloaded synchronous wireless and optical CDMA systems," *IEEE Trans. Inform. Theory*, vol. 55, pp. 2705-2715, June 2009.

$$\mathbf{C}_{16\times 33} = \begin{bmatrix}
+ & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & - & + & + & - & + & - & + & + & - & + & - & + & + & - & + & + & + \\
+ & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - & + & + & - & + & - & + & + & - & + & - & + & + & - & - & + & + & + \\
+ & + & - & - & + & + & - & - & + & + & - & - & + & + & - & - & + & - & + & + & + & + & - & + & + & + & - & + & - & + & + & + & + \\
+ & - & - & + & + & - & - & + & + & - & - & + & + & - & - & + & + & - & - & + & + & + & - & - & + & + & + & - & - & - & + & + & + \\
+ & + & + & + & - & - & - & - & + & + & + & + & - & - & - & - & + & + & + & + & - & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & - & + & - & - & + & - & + & + & - & + & - & - & + & - & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + & - \\
+ & + & - & - & - & - & + & + & + & + & - & - & - & - & + & + & + & + & + & + & - & + & + & + & + & - & + & + & + & + & + & - & + \\
+ & - & - & + & - & + & + & - & + & - & - & + & - & + & + & - & + & + & + & + & - & + & + & + & + & - & + & + & + & + & + & - & - \\
+ & + & + & + & + & + & + & + & - & - & - & - & - & - & - & - & - & + & + & - & + & + & - & - & + & - & + & + & + & + & + & + & + \\
+ & - & + & - & + & - & + & - & - & + & - & + & - & + & - & + & + & - & + & + & - & + & - & - & - & + & + & + & + & + & + & + & + \\
+ & + & - & - & + & + & - & - & - & - & + & + & - & - & + & + & + & - & + & + & + & - & + & - & - & + & + & + & + & + & + & + & + \\
+ & - & - & + & + & - & - & - & + & + & - & - & + & + & - & + & + & + & - & + & + & + & - & + & + & - & + & + & + & + & + & + & + \\
+ & + & + & + & - & - & - & - & - & - & - & + & + & + & + & + & + & + & + & - & - & - & - & - & + & + & + & + & + & + & + & + & + \\
+ & - & + & - & - & + & - & + & - & + & + & + & - & + & - & + & + & + & + & + & - & - & - & - & - & + & + & + & + & + & + & + & + \\
+ & + & - & - & - & - & + & + & - & - & + & + & + & - & - & + & + & + & + & - & - & - & - & - & + & + & + & + & + & + & + & + & + \\
+ & - & - & + & - & + & + & - & - & + & + & - & + & - & - & + & + & + & + & + & - & - & - & - & - & + & + & + & + & + & + & + & + \end{bmatrix}$$

Fig. 3. Errorless signature code set for an overloaded system with codelength $L = 16$ and code size $K = 33$.

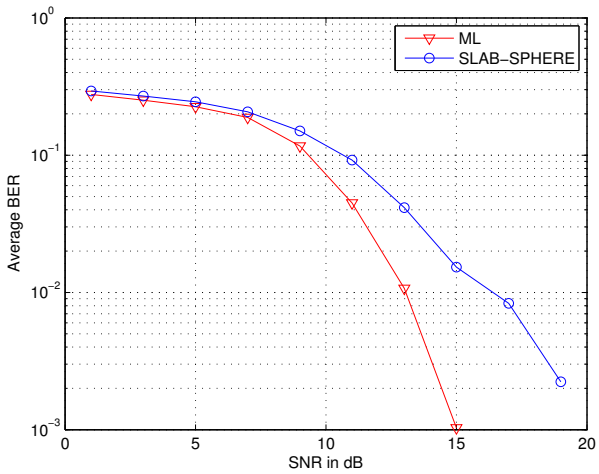

Fig. 4. BER versus SNR for the errorless code system with $L = 16$ and $K = 33$.

[8] Y. W. Wu and S. C. Chang, "Coding scheme for synchronous-CDMA systems," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1064-1067, May 1997.

[9] G. H. Khachatrian and S. S. Martirossian, "A new approach to the design of codes for synchronous-CDMA systems," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1503-1506, Sept. 1995.

[10] G. H. Khachatrian and S. S. Martirossian, "Code construction for the T-user noiseless adder channel," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1953-1957, Sept. 1998.

[11] S. S. Martirossian and G. H. Khachatrian, "Construction of signature codes and the coin weighing problem," in *Probl. Peredachi Inf.*, vol. 25, no. 4, pp. 96-97, Sept. 1989.

[12] W. H. Mow , "Recursive constructions of detecting matrices for multiuser coding: A unifying approach," *IEEE Trans. Inform. Theory*, vol. 55, pp. 93-98, Jan. 2009.

[13] B. Lindström, "On a combinatorial problem in number theory," in *Can. Math. Bull.*, vol. 8, pp. 477-490, 1965.

[14] Kai-Kit Wong, A. Pulraj, and R. D. Murch, "Efficient high-performance decoding for overloaded MIMO antenna systems," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 1833-1843, May 2007.