Generalized Construction of Signature Code for Multiple-Access Adder Channel

Shan Lu, Jun Cheng, Wei Hou, and Yoichiro Watanabe
Dep. of Intelligent Information Engineering & Sciences
Doshisha University, Kyotanabe, Japan
Email: shanluxd@gmail.com, jcheng@ieee.org, etl1703@mail4.doshisha.ac.jp, watanabe@muc.doshisha.ac.jp

***Abstract*—We propose a generalized construction scheme of error-correcting signature code. We form a signature matrix whose rows become the non-zero codewords of the signature code. In the coding scheme, a signature matrix is obtained from a Hadamard matrix by replacing every element by an initial signature matrix or its associated matrix depending on the element's binary value. The proposed code has longer length, higher decodability, and larger cardinality. In this coding scheme, the initial signature matrix is in a general form and can be a signature matrix of any initial signature code. Different initial matrices provide different error-correcting signature codes, including conventional codes. This general form makes it possible to obtain error-correcting signature codes with a higher sum rate than conventional codes.**

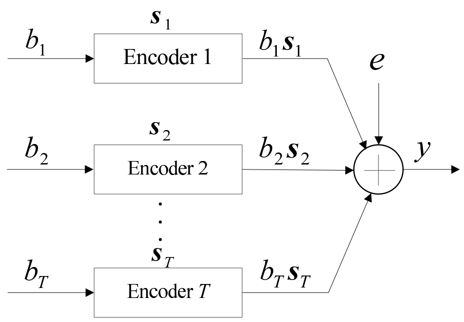

Fig. 1. Signature code in T-user noisy multiple-access adder channel

I. Introduction

In a multiple-access communication system, T users communicate with a single receiver through a multiple-access adder channel (MAAC) [1]. Multiuser coding is used to assign constituent codes C_i, $i = 1, 2, \ldots, T$ to T users so that they can communicate simultaneously with a common receiver through a MAAC, even in the presence of noise. A special case of multiuser code assigns each constituent code with two codewords, one of which is an all-zero codeword shared among all T users. The users send the all-zero codeword to indicate that they are inactive. The users who wish to be identified send their respective non-zero codewords. Combined T non-zero codewords are called a *signature code*, which is used for user identification in MAAC. For noisy MAACs, the code designed to correct errors caused by channel noise and to identify the status of users is generally called an *error-correcting* signature code.

Signature code is related to well-known problems of coin-weighting and sum-distinct sets in additive number theory [2]–[8]. Binary signature code is equivalent to Lindström's coin weighing designs [2], and a construction was given by Martirosyan and Khachatryan [3]. A unifying approach to recursively construct binary signature code was proposed by Mow [4]. Non-binary code was originally considered by Jevtić [5] [6] and extended to arbitrary code length [7]. However, the above works are restricted to signature codes in unitary minimum distance that has no capacity to correct errors.

We are constructing error-correcting signature codes. In our first attempt [9] [10], we got a binary error-correcting signature code from a Hadamard matrix, whose orthogonality provides the decodability of binary error-correcting signature code. For non-binary code, it is difficult to find such an orthogonal matrix. Based on Jevtić's integral matrix [5] [6], we previously proposed a recursive construction of non-binary error-correcting signature code [11]. However, in these previous works [9]–[11], due to their particular recursive schemes, these codes have a low sum rate.

In this paper, we propose a generalized construction scheme of error-correcting signature code and form a signature matrix whose rows are the non-zero codewords of the signature code. In our coding scheme, a signature matrix is obtained from a Hadamard matrix by replacing every element by an initial signature matrix or its associated matrix depending on the element's binary value. The initial signature matrix is in a general form and can be a signature matrix of any initial signature code. Different initial matrices produce different error-correcting signature codes, including conventional codes. This general form makes it possible to obtain error-correcting signature codes with higher sum rates than conventional codes.

II. System and Definition

A. System description

Consider a T-user multiple-access adder channel (MAAC), whose input alphabet is integer set $\mathcal{K} \triangleq \{0, 1, 2, \ldots, k\}$, where k is a positive integer. When $Z_i \in \mathcal{K}, i = 1, 2, \ldots, T$ are the channel inputs and channel output Y is given by $Y = Z_1 + Z_2 + \cdots + Z_T$, where "+" denotes the real-number addition. Output Y clearly belongs to $\{0, 1, \ldots, kT\}$. The channel is discrete and memoryless. We also assume that the transmission is synchronized.

The above MAAC is a noiseless channel. When it is disturbed by noise, we describe it by putting a discrete memoryless channel just after the noiseless MAAC, called a *noisy* MAAC [1] [12]. Here the discrete memoryless channel, which is set as $(kT+1)$-ary input and $(kT+1)$-ary output, is completely described by the transition probabilities for all possible input-output pairs (i,j), $0 \le i,j \le kT$.

In a T-user noisy multiple-access communication system (Fig. 1), for the ith user, codewords $\boldsymbol{s}_j$ and $\mathbf{0}^n$ are assigned, where $\boldsymbol{s}_j \in \mathcal{K}^n$, $\mathcal{K}^n$ is a set of all n-vectors (a row vector with length n) with components from $\mathcal{K}$, and $\mathbf{0}^n$ is an n-vector whose n elements are zero. Let $b_j \in \{0,1\}$ be the message data from user i to indicate user's status: inactive or active. In the absence of channel noise, the channel output vector is the sum of transmitted vectors $b_i\boldsymbol{s}_i$ $(i=1,2,\ldots,T)$. The decoder receives a vector, which is the superposition of the transmitted codewords, and attempts to identify the active users. The decodability of the signature code guarantees unique identification of all active users through the MAAC, even if the received vector is disturbed by the channel noise.

In this paper, set $\mathcal{S}=\{\boldsymbol{s}_1,\boldsymbol{s}_2,\ldots,\boldsymbol{s}_T\}$ is called a signature code. To construct an error-correcting signature code, we need to choose these T non-zero codewords such that the receiver can determine which codewords have been transmitted, even in noisy channels.

B. Definition

Next we explain some preliminary notations and definitions. The *weight* of n-vector $\boldsymbol{y}=[y_1,y_2,\ldots,y_n]$ is defined by

$$w(\boldsymbol{y})=\sum_{i=1}^{n}|y_i|,$$

where y_i is an integer. The *distance* between vectors $\boldsymbol{y}$ and $\boldsymbol{y}'$ is defined by

$$d(\boldsymbol{y},\boldsymbol{y}')=w(\boldsymbol{y}-\boldsymbol{y}').$$

Definition 1: For positive integer δ, set $\mathcal{S}=\{\boldsymbol{s}_1,\boldsymbol{s}_2,\ldots,\boldsymbol{s}_T\}$, $\boldsymbol{s}_i \in \mathcal{K}^n$, is a *$\delta$-decodable signature code* if it holds

$$w(\boldsymbol{u}X)\ge\delta \tag{1}$$

for any non-zero T-vector $\boldsymbol{u}\in\{-1,0,1\}^T$, where X is the $T\times n$ signature matrix

$$X=\begin{bmatrix}\boldsymbol{s}_1\\ \boldsymbol{s}_2\\ \vdots\\ \boldsymbol{s}_T\end{bmatrix}. \tag{2}$$

□

We denote by $(n,\delta,T)_k$ a δ-decodable $(k+1)$-ary signature code with code length n and cardinality $T \triangleq |\mathcal{S}|$. The sum rate of the signature code is $R=T/n$.

By Definition 1, the δ-decodable signature code implies that all possible 2^T sums of the transmitted vectors satisfy

$$d\left(\sum_{i=1}^{T}b_i\boldsymbol{s}_i,\sum_{i=1}^{T}b_i'\boldsymbol{s}_i\right)\ge\delta$$

for any two distinct T-vectors $\boldsymbol{b}=[b_1,b_2,\ldots,b_T]$ and $\boldsymbol{b}'=[b_1',b_2',\ldots,b_T']$, where $b_i,b_i'\in\{0,1\}$. According to multiuser coding [1] [12], a δ-decodable signature code for a noisy MAAC can correct $\lfloor(\delta-1)/2\rfloor$ or fewer errors, where notation $\lfloor p\rfloor$ stands for the greatest integer less than or equal to p. A $(n,\delta=1,T)_k$ code (or matrix) is considered *uniquely decodable* [2] [3] [7] [13] and is used for noiseless MAACs so that the decoder can uniquely identify active users.

For preparation, we describe a Hadamard matrix and define a Kronecker product.

For $j\ge1$, Sylvester-type Hadamard matrix H_j with order 2^j is recursively constructed as [14]:

$$H_j=\begin{bmatrix}H_{j-1} & H_{j-1}\\ H_{j-1} & -H_{j-1}\end{bmatrix},\quad \text{with}\quad H_0=[1]. \tag{3}$$

Let U be a $T\times n$ matrix and h_{li} be an element in H_j, where l and i indicate the indices of the rows and columns, respectively. The Kronecker product between H_j and U is a $2^jT\times2^jn$ matrix obtained from H_j by replacing every element h_{li} in H_j by $h_{li}U$. Symbolically, we have

$$H_j\otimes U=[h_{li}U].$$

III. Generalized construction

In this section, we examine the generation of the construction of $(k+1)$-ary signature code for a noisy MAAC.

Before going on, we define some notations. Let A and B be $T_0\times n_0$ matrices, where the elements in A and B belong to $\mathcal{K}$. Let $[A|B]$ be a $T_0\times n_0$ matrix related to matrices A and B. We define the operation:

$$h_{li}\bar{\otimes}[A|B]\triangleq\begin{cases}A & \text{if } h_{li}=1\\ B & \text{if } h_{li}=-1.\end{cases} \tag{4}$$

We also have

$$(-h_{li})\bar{\otimes}[A|B]=h_{li}\bar{\otimes}[B|A]. \tag{5}$$

For $j\ge0$, by Sylvester-type Hadamard matrix H_j of (3), we define matrix

$$X_j\triangleq H_j\bar{\otimes}[A|B]. \tag{6}$$

Here, matrix X_j is a $2^jT_0\times2^jn_0$ matrix obtained from H_j by replacing every element "1" by A and every element "-1" by B.

The following theorem shows that matrix X_j gives a signature code with sum rate T_0/n_0:

Theorem 1: Let δ_a and δ_b be nonnegative integers, and $\delta_0=\min\{\delta_a,\delta_b/2\}$. For all non-zero vectors $\boldsymbol{u}_0\in\{-1,0,1\}^{T_0}$, if initial signature matrix A and its associated matrix B are satisfied

$$w(\boldsymbol{u}_0A)\ \ge\ \delta_a \tag{7}$$

$$w(\boldsymbol{u}_0(A-B))\ \ge\ \delta_b \tag{8}$$

then set $\mathcal{S}_j$, which is composed of rows of matrix X_j of (6), is an

$$(n_j=2^jn_0,\delta_j=2^j\delta_0,T_j=2^jT_0)_k\text{-signature code.}$$

$\square$

Proof: We prove that $\mathcal{S}_j$ is $2^j\delta_0$-decodable, i.e.,

$$w(\boldsymbol{u}_j X_j) \geq 2^j \delta_0, \text{ for } \boldsymbol{u}_j \in \{-1,0,1\}^{T_j}, \boldsymbol{u}_j \neq \mathbf{0}^{T_j}. \quad (9)$$

From the recursion of H_j, we observe that X_j also has a recursive property:

$$\begin{aligned} X_j &= H_j \bar{\otimes}[A|B] \\ &= \begin{bmatrix} H_{j-1} & H_{j-1} \\ H_{j-1} & -H_{j-1} \end{bmatrix} \bar{\otimes}[A|B] \\ &= \begin{bmatrix} X_{j-1} & X_{j-1} \\ X_{j-1} & \bar{X}_{j-1} \end{bmatrix} \end{aligned} \quad (10)$$

with $X_0 = A$, and

$$\bar{X}_{j-1} \triangleq (-H_{j-1})\bar{\otimes}[A|B] = H_{j-1}\bar{\otimes}[B|A]. \quad (11)$$

Thus, the proof is made by recursion. It is obvious the first matrix X_0 satisfies $w(\boldsymbol{u}_0 A) \geq \delta_a \geq \delta_0$. The second matrix is

$$X_1 = H_1 \bar{\otimes}[A|B] = \begin{bmatrix} A & A \\ A & B \end{bmatrix}. \quad (12)$$

Let $\boldsymbol{u}_1 = [\boldsymbol{u}_0, \bar{\boldsymbol{u}}_0] \neq \mathbf{0}^{2T_0}$, where $\boldsymbol{u}_0, \bar{\boldsymbol{u}}_0 \in \{-1,0,1\}^{T_0}$. We also have

$$\boldsymbol{u}_1 X_1 = [\boldsymbol{u}_0 A + \bar{\boldsymbol{u}}_0 A, \boldsymbol{u}_0 A + \bar{\boldsymbol{u}}_0 B].$$

We consider two cases.

Case 1. $\boldsymbol{u}_0 \neq \mathbf{0}^{T_0}, \bar{\boldsymbol{u}}_0 = \mathbf{0}^{T_0}$.

In this case, from (7), the result is immediate of that,

$$w(\boldsymbol{u}_1 X_1) = 2w(\boldsymbol{u}_0 A) \geq 2\delta_a \geq 2\delta_0.$$

Case 2. $\bar{\boldsymbol{u}}_0 \neq \mathbf{0}^{T_0}$.

Let $\epsilon_1 = [\boldsymbol{u}_0 A + \bar{\boldsymbol{u}}_0 A]$ and $\epsilon_2 = [\boldsymbol{u}_0 A + \bar{\boldsymbol{u}}_0 B]$. We also have

$$\begin{aligned} w(\boldsymbol{u}_1 X_1) &= w(\epsilon_1) + w(\epsilon_2) \\ &\geq w(\epsilon_1 - \epsilon_2) \\ &= w(\bar{\boldsymbol{u}}_0 (A - B)) \\ &\geq \delta_b \geq 2\delta_0, \end{aligned} \quad (13)$$

where the last two inequalities are satisfied from (8).

Assuming that $w(\boldsymbol{u}_{j-1} X_{j-1}) \geq 2^{j-1}\delta_0$, we prove (9). Let $\boldsymbol{u}_j$ be partitioned as

$$\boldsymbol{u}_j = [\boldsymbol{u}_{j-1}, \bar{\boldsymbol{u}}_{j-1}]$$

where $\boldsymbol{u}_{j-1}, \bar{\boldsymbol{u}}_{j-1} \in \{-1,0,1\}^{T_{j-1}}$. From (10), we have

$$\boldsymbol{u}_j X_j = [\boldsymbol{u}_{j-1} X_{j-1} + \bar{\boldsymbol{u}}_{j-1} X_{j-1}, \boldsymbol{u}_{j-1} X_{j-1} + \bar{\boldsymbol{u}}_{j-1} \bar{X}_{j-1}].$$

Since $\boldsymbol{u}_j \neq \mathbf{0}^{T_j}$ by assumption, we consider two cases.

Case 1. $\boldsymbol{u}_{j-1} \neq \mathbf{0}^{T_{j-1}}, \bar{\boldsymbol{u}}_{j-1} = \mathbf{0}^{T_{j-1}}$.

In this case, the immediate result is that

$$w(\boldsymbol{u}_j X_j) = 2w(\boldsymbol{u}_{j-1} X_{j-1}) \geq 2^j \delta_0.$$

Case 2. $\bar{\boldsymbol{u}}_{j-1} \neq \mathbf{0}^{T_{j-1}}$.

Let
$$\begin{aligned} \epsilon_1 &= [\boldsymbol{u}_{j-1} X_{j-1} + \bar{\boldsymbol{u}}_{j-1} X_{j-1}] \\ \epsilon_2 &= [\boldsymbol{u}_{j-1} X_{j-1} + \bar{\boldsymbol{u}}_{j-1} \bar{X}_{j-1}]. \end{aligned}$$

We have

$$\begin{aligned} w(\boldsymbol{u}_j X_j) &= w(\epsilon_1) + w(\epsilon_2) \\ &\geq w(\epsilon_1 - \epsilon_2) \\ &= w(\bar{\boldsymbol{u}}_{j-1}(X_{j-1} - \bar{X}_{j-1})) \\ &= w(\bar{\boldsymbol{u}}_{j-1}(H_{j-1}\bar{\otimes}[A|B] - H_{j-1}\bar{\otimes}[B|A])) \\ &= w(\bar{\boldsymbol{u}}_{j-1}(H_{j-1} \otimes (A - B))). \end{aligned} \quad (14)$$

Let $\bar{\boldsymbol{u}}_{j-1} = [\bar{\boldsymbol{u}}_{j-1,1}, \ldots, \bar{\boldsymbol{u}}_{j-1,l}, \ldots, \bar{\boldsymbol{u}}_{j-1,2^{j-1}}]$, where $\bar{\boldsymbol{u}}_{j-1,l} \in \{-1,0,1\}^{T_0}$. Let $\boldsymbol{\beta}_l \triangleq \bar{\boldsymbol{u}}_{j-1,l}(A - B)$, $l = 1, 2, \ldots, 2^{j-1}$. We have

$$\begin{aligned} & w(\bar{\boldsymbol{u}}_{j-1}(H_{j-1} \otimes (A - B))) \\ &= w(\sum_{l=1}^{2^{j-1}} h_{l1}\boldsymbol{\beta}_l, \ldots, \sum_{l=1}^{2^{j-1}} h_{li}\boldsymbol{\beta}_l, \ldots, \sum_{l=1}^{2^{j-1}} h_{l2^{j-1}}\boldsymbol{\beta}_l), \end{aligned} \quad (15)$$

where h_{li} is the element in the ith row and the jth column.

Next we introduce $2^{j-1} \times n_0$ matrix:

$$\Phi \triangleq \begin{bmatrix} \sum_{l=1}^{2^{j-1}} h_{l1}\boldsymbol{\beta}_l \\ \sum_{l=1}^{2^{j-1}} h_{l2}\boldsymbol{\beta}_l \\ \vdots \\ \sum_{l=1}^{2^{j-1}} h_{l2^{j-1}}\boldsymbol{\beta}_l \end{bmatrix} = H_{j-1}^{\mathrm{T}} \begin{bmatrix} \boldsymbol{\beta}_1 \\ \boldsymbol{\beta}_2 \\ \vdots \\ \boldsymbol{\beta}_{2^{j-1}} \end{bmatrix}. \quad (16)$$

Multiplying both sides by Hadamard matrix H_{j-1} for (16), we have

$$H_{j-1}\Phi = 2^{j-1} \begin{bmatrix} \boldsymbol{\beta}_1 \\ \boldsymbol{\beta}_2 \\ \vdots \\ \boldsymbol{\beta}_{2^{j-1}} \end{bmatrix}. \quad (17)$$

Since we assume $\bar{\boldsymbol{u}}_{j-1} \neq \mathbf{0}^{T_{j-1}}$, without loss of generality, there exists at least a non-zero vector such that $\bar{\boldsymbol{u}}_{j-1,l_0} \neq \mathbf{0}^{T_0}$. From (8), it holds that

$$w(\boldsymbol{\beta}_{l_0}) = w(\bar{\boldsymbol{u}}_{j-1,l_0}(A - B)) \geq \delta_b. \quad (18)$$

The weight of the l_0th row vector of matrix $H_{j-1}\Phi$ is

$$\sum_{n=1}^{n_0} |\sum_{i=1}^{2^{j-1}} h_{l_0 i}\phi_{in}| = 2^{j-1} w(\boldsymbol{\beta}_{l_0}) \geq 2^{j-1}\delta_b \geq 2^j \delta_0$$

where ϕ_{in} is the element in the ith row and the nth column of matrix Φ. Thus, we have

$$\begin{aligned} w(\boldsymbol{u}_j X_j) &= \sum_{i=1}^{2^{j-1}} \sum_{n=1}^{n_0} |\phi_{in}| \\ &= \sum_{n=1}^{n_0} \sum_{i=1}^{2^{j-1}} |h_{l_0 i}\phi_{in}| \\ &\geq \sum_{n=1}^{n_0} |\sum_{i=1}^{2^{j-1}} h_{l_0 i}\phi_{in}| \\ &\geq 2^j \delta_0. \end{aligned} \quad (19)$$

Here, the second equality holds because all of the elements in H_{j-1} are either -1 or 1. This proves the theorem. $\square$

We now consider a variation of matrices A and B.

Let $A' = \begin{bmatrix} O \\ A \end{bmatrix}$ and B' be $(T^*+T_0)\times n_0$ matrices, where O is a $T^* \times n_0$ zero matrix and A is a $T_0 \times n_0$ matrix. Let

$$X'_j = H_j \bar{\otimes} [A'|B']. \tag{20}$$

We have the following corollary.

Corollary 1: Let δ_a and δ_b be nonnegative integers, and $\delta_0 = \min\{\delta_a, \delta_b/2\}$. For all vectors $[\boldsymbol{u}^*, \boldsymbol{u}^a]$, where $\boldsymbol{u}^* \in \{-1,0,1\}^{T^*}$, $\boldsymbol{u}^a \in \{-1,0,1\}^{T_0}$, if matrices A' and B' satisfy

$$\begin{aligned} w([\boldsymbol{u}^*, \boldsymbol{u}^a]A') \geq \delta_a, &\quad \text{for } \boldsymbol{u}^a \neq \mathbf{0}^{T_0} \\ w([\boldsymbol{u}^*, \boldsymbol{u}^a](A'-B')) \geq \delta_b, &\quad \text{for } [\boldsymbol{u}^*, \boldsymbol{u}^a] \neq \mathbf{0}^{T^*+T_0} \end{aligned} \tag{21}$$

then set $\mathcal{S}'_j$, which is composed of rows of matrix X'_j of (20) with the first T^* all-zero rows removed, is a

$$(2^j n_0, 2^j\delta_0, 2^j(T_0+T^*)-T^*)_k\text{-signature code.}$$

□

Since the proof closely resembles that of Theorem 1, we omit it but give an intuitive explanation. By Theorem 1, for any non-zero vector $\boldsymbol{u}^a_j$, it holds that

$$w([\boldsymbol{u}^*_j, \boldsymbol{u}^a_j]\begin{bmatrix} O \\ X_j \end{bmatrix}) \geq 2^j\delta_0$$

i.e., $w(\boldsymbol{u}^a_j X_j) \geq 2^j\delta_0$. where X_j is a sub-matrix of X'_j formed by removing the first T^* all-zero rows from X'_j.

IV. Signature codes

Theorem 1 and Corollary 1 show that given any δ_0-decodable code, with constraints (8) or (21), a $2^j\delta_0$-decodable code is obtained. Now we give two particular constructions.

A. $(k+1)$-ary signature code

For any integer k, let $\ell = \lfloor \log_2 k \rfloor$, and define a $(\ell+1)\times 1$ matrix $\boldsymbol{a} = [2^0, 2^1, \cdots, 2^{\ell-1}, k]$. Note that matrix $\boldsymbol{a}^{\mathrm{T}}$ is uniquely decodable [5], i.e., $w(\boldsymbol{u}\boldsymbol{a}^{\mathrm{T}}) \geq 1$ with $\boldsymbol{u} \neq \mathbf{0}^{\ell+1}, \boldsymbol{u} \in \{-1,0,1\}^{\ell+1}$. Next we give a $(k+1)$-ary signature code from initial signature matrix $\boldsymbol{a}^{\mathrm{T}}$.

Construction I: Let $A = \boldsymbol{a}^{\mathrm{T}}$ and $B = \mathbf{0}^{\ell+1}$ by Theorem 1. Set $\mathcal{S}_j$, which is composed of rows of matrix X_j, is a

$$(2^j, 2^{j-1}, (\ell+1)2^j)_k\text{-signature code}$$

since $w(\boldsymbol{u}A) \geq 1$ and $w(\boldsymbol{u}(A-B)) \geq 1$. □

We show an example to understand the coding procedure.

Example 1: Let $k = 5$. Obviously, $\ell = 2$. First matrix $A = [1,2,5]^{\mathrm{T}}$. The second matrix is

$$X_1 = \begin{bmatrix} 1 & 1 \\ 2 & 2 \\ 5 & 5 \\ 1 & 0 \\ 2 & 0 \\ 5 & 0 \end{bmatrix}.$$

The third matrix is

$$X_2 = \begin{bmatrix} 1&1&1&1 \\ 2&2&2&2 \\ 5&5&5&5 \\ 1&0&1&0 \\ 2&0&2&0 \\ 5&0&5&0 \\ 1&1&0&0 \\ 2&2&0&0 \\ 5&5&0&0 \\ 1&0&0&1 \\ 2&0&0&2 \\ 5&0&0&5 \end{bmatrix},$$

which gives a $(4,2,12)_5$-signature code:

$$\mathcal{S}_2 = \{1111, 2222, 5555, 1010, 2020, 1100, 2200, 5500, 1001, 2002, 5005\}.$$

□

Remark 1: The signature code in Construction I is originally from vector $\boldsymbol{a}^{\mathrm{T}}$, which is uniquely decodable for any positive integer k. It should be emphasized that a better choice may exist than $\boldsymbol{a}^{\mathrm{T}}$ for a particular value of k. For instance, for k=7, uniquely decodable matrix $A = [3,5,6,7]^{\mathrm{T}}$ gives a signature code with a sum rate of 4, which exceeds $\boldsymbol{a}^{\mathrm{T}} = [1,2,7]^{\mathrm{T}}$.

Remark 2: The following choice might also exist:

$$A = \begin{bmatrix} k & k \\ (\boldsymbol{k}^{\ell+1})^{\mathrm{T}} & (\boldsymbol{k}^{\ell+1})^{\mathrm{T}} - \boldsymbol{a}^{\mathrm{T}} \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 0 \\ (\mathbf{0}^{\ell+1})^{\mathrm{T}} & \boldsymbol{a}^{\mathrm{T}}, \end{bmatrix}$$

where $\boldsymbol{k}^{\ell+1}$ is an $(\ell+1)$-vector whose elements are all k. This choice gives the conventional $(k+1)$-ary error-correcting signature code in [11]. Due to the $(\ell+2)\times 2$ initial matrix, the code in [11] has a lower sum rate of $(\ell+2)/2$ than the code in Construction I for $k > 1$.

B. binary signature code

Before the construction, we give some definitions. For $t \geq 1$, we define matrices

$$A'_t = \begin{bmatrix} O_{t-1} & O_{t-1} \\ A'_{t-1} & A'_{t-1} \\ A'_{t-1} & B'_{t-1} \end{bmatrix} \tag{22}$$

and

$$B'_t = \begin{bmatrix} I_{t-1} & O_{t-1} \\ B'_{t-1} & B'_{t-1} \\ B'_{t-1} & A'_{t-1} \end{bmatrix} \tag{23}$$

with $A'_0 = [1]$ and $B'_0 = [0]$, where I_{t-1} is a $2^{t-1}\times 2^{t-1}$ identity matrix and O_{t-1} is a $2^{t-1}\times 2^{t-1}$ zero matrix. Matrices A'_t and B'_t have $T(t) = (t+2)2^{t-1}$ rows and $n(t) = 2^t$ columns.

It follows that

$$A'_t - B'_t = \begin{bmatrix} -I_{t-1} & O_{t-1} \\ H_{t-1} & H_{t-1} \\ H_{t-1} & -H_{t-1} \end{bmatrix}.$$

[1] showed that

$$w(\boldsymbol{u}_t(A'_t - B'_t)) \geq 1 \tag{24}$$

for $\boldsymbol{u}_t \in \{-1,0,1\}^{T(t)}$, and $\boldsymbol{u}_t \neq \mathbf{0}^{T(t)}$.

Note the weight of A'_t. In A'_i, sub-matrices O_{i-1} have 2^{i-1} all-zero rows. The number of all-zero rows in A'_t is the accumulation of the all-zero rows in O_{i-1} for $i = 1, 2, \ldots, t$, i.e.

$$T^*(t) = 1 + 2 + \cdots + 2^{t-1} = 2^t - 1.$$

Since we are only interested in the remaining (non-zero) rows of A'_t, we show by recursion that

$$w([\boldsymbol{u}_t^*, \boldsymbol{u}_t^a]A'_t) \geq 1 \tag{25}$$

for $\boldsymbol{u}_t^a \in \{-1,0,1\}^{T(t)-T^*(t)}$ and $\boldsymbol{u}_t^a \neq \mathbf{0}^{T(t)-T^*(t)}$.

It is obvious that $w([u_1^*, \boldsymbol{u}_1^a]A'_1) \geq 1$ for $\boldsymbol{u}_1^a \in \{-1,0,1\}^2$ and $\boldsymbol{u}_1^a \neq \mathbf{0}^2$.

Assuming that

$$w([\boldsymbol{u}_{t-1}^*, \boldsymbol{u}_{t-1}^a]A'_{t-1}) \geq 1$$

for any non-zero vector $\boldsymbol{u}_{t-1}^a \in \{-1,0,1\}^{T(t-1)-T^*(t-1)}$. Let $A_t = H_2 \otimes [A'_{t-1}|B'_{t-1}]$. Note that A_t is the sub-matrix of A'_t of (22). Since $w([\boldsymbol{u}_{t-1}^*, \boldsymbol{u}_{t-1}^a](A'_{t-1} - B'_{t-1})) \geq 1$ ((24)), by Corollary 1, $w([\boldsymbol{u}_{t-1}^*, \boldsymbol{u}_t^a]A_t) \geq 1$ for $\boldsymbol{u}_t^a \in \{-1,0,1\}^{T(t)-T^*(t)}$ and $\boldsymbol{u}_t^a \neq \mathbf{0}^{T(t)-T^*(t)}$. Thus, we obtain (25).

Based on (24) and (25), from Corollary 1, we have the following construction of a binary signature code:

Construction II: Set $\mathcal{S}_j$, which is composed of rows of matrix

$$X'_j = H_j \bar{\otimes} [A'_t|B'_t]$$

where the first $2^t - 1$ rows were removed, is a

$$(2^{j+t}, 2^{j-1}, (t+2)2^{j+t-1} - 2^t + 1)_k\text{-signature code.}$$

□

The sum rate of the above binary signature code is

$$R = \frac{(t+2)2^{j+t-1} - 2^t + 1}{2^{j+t}} > 1, \quad j, t \geq 1.$$

This means that it is higher than that of the code in Construction I when $k = 1$.

V. Conclusion

We proposed a generalized construction scheme of error-correcting signature code. In our coding scheme, a signature matrix is obtained from a Hadamard matrix by replacing every element by an initial signature matrix or its associated matrix depending on the element's binary value. The initial signature matrix is in a general form and can be a signature matrix of any initial signature code. Different initial matrices give different error-correcting signature codes, including conventional codes. This general form makes it possible to obtain error-correcting signature codes with a higher sum rate than conventional codes.

Acknowledgment

This work was partly supported by JSPS KAKENHI (24300030) Grant-in-Aid for Scientific Research (B).

References

[1] S. C. Chang and E. J. Weldon, Jr., "Coding for T-user multiple-access channels," *IEEE Trans. Inform. Theory*, vol. IT-25, no. 6, pp. 684–691, Nov. 1979.

[2] B. Lindström, "Determining subsets by unramified experiments," in *A Survey of statistical Design and Linear Models*, ed. J. N. Srivastava, North-Holland, New York, 1975.

[3] S. S. Martirosyan and G. G. Khachatryan, "Construction of signature codes and the coin weighing problem," *Probl. Inform. Transm.*, vol. IT-25, pp. 334-335, Oct.-Dec. 1989.

[4] W. H. Mow, "Recursive constructions of detecting matrices for multiuser coding: a unifying approach," *IEEE Trans. Inform. Theory*, vol. IT-55, no. 1, pp. 93-98, Jan. 2009.

[5] D. Jevtić, "On families of sets of integral vectors whose representatives form sum-distinct sets," *SIAM J. Discrete Math.*, vol. 8, no. 4, pp. 652-660, Nov. 1995.

[6] D. Jevtić, "Disjoint uniquely decodable codebooks for noiseless synchronized multiple-access adder channels generated by integer sets," *IEEE Trans. Inform. Theory*, vol. IT-38, No. 3, pp. 1142–1146, May 1992.

[7] J. Cheng and Y. Watanabe, "T-user code with arbitrary code length for multiple-access adder channel," *IEICE Trans. Fundamentals*, vol. E82-A, no. 10, pp. 2011–2016, Oct. 1999.

[8] D. Jevtić, "On sum distinct sets of integral vectors," ARS Combinatoria, vol. 45, pp. 87-95, April 1997.

[9] J. Cheng, K. Kamoi, and Y. Watanabe, "Error-correcting signature code for multiple-access adder channel," *2005 Int. Symposium on Information and Theory* (*ISIT2005*), pp. 2036-2039, Sept. 4–9, 2005, Adelaide, Australia.

[10] J. Cheng, K. Kamoi, and Y. Watanabe, "User identification by signature code for noisy multiple-access adder channel," *2006 Int. Symposium on Information and Theory* (*ISIT2006*), pp. 1974-1977, July 9–14, 2006, Seattle, USA.

[11] J. Cheng, K. Kamoi, and Y. Watanabe, "Error-correcting non-binary signature code for multiple-access adder channel," *2007 Int. Symposium on Information and Theory* (*ISIT2007*), pp. 2571-2574, June 24–29, 2007, Nice, France.

[12] J. Cheng and Y. Watanabe, "Multi-user k-ary code for noisy multiple-access adder channel," *IEEE Trans. Inform. Theory*, vol. IT-47, no. 6, pp. 2603-2607, Sept. 2001.

[13] T. Bohman, "A sum packing problem of Erdős and the Conway–Guy sequence," *Proc. Amer. Math. Soc.*, vol. 124, no. 12, pp. 3627–3636, Dec. 1996.

[14] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands: North-Holland, 1977.