PARTIAL UNIT MEMORY CODES ON THE BASE OF SUBCODES OF HADAMARD CODES

A. E. Ashikhmin and V. V. Ziablov
Institute for Problems of Information Transmission
Russian Academy of Sciences
Ermolova 19, Moscow GSP-4, 101447, Russia

Abstract

The partial memory codes on the base of subcodes of nonlinear Hadamard codes are proposed. It is shown that they have better parameters than partial memory codes based on linear block codes.

1 Introduction

Unit memory (UM) codes are well known [1]. Here we consider the partial unit memory (PUM) codes and code with partial memory two [2] on the base of subcodes of nonlinear Hadamard codes. Although ensembles of nonlinear PUM codes were already considered [3], up to now there is no example in which nonlinear PUM codes have better performances than linear PUM codes. Here we present two examples of this kind.

2 Constructing of nonlinear partial memory codes

We will construct nonlinear partial memory codes on the base of regular trellis with the following properties. Each node in the i-th column is connected with each node in the (i+1)-th column by branches; each branch is labelled with a binary vector of length n. The number of the branches coming from one node to another node is the same, the sets of such branches we call bunches. The vectors on the branches leaving from or coming to any node can be obtained by adding a certain vector to the vectors on the branches leaving from or coming to the zero node. Each path from left to right through this trellis specifies a codeword of a nonlinear partial memory code. Note that the above trellis is almost the trellis corresponding to a linear partial memory code, e.g. the trellis corresponding to a unit memory convolutional code. The only difference between them is that in the case of a linear partial memory code vectors on the branches leaving the zero node and vectors on the branches coming to the zero node are codewords of some linear block codes, whereas in the case of a nonlinear partial memory code these vectors are codewords

of some nonlinear block codes. We will denote nonlinear partial memory code by $(n, M_0|M_1)$, where n is length of the vectors on the branches, M_0 is the number of the branches leaving from or coming to any node of the trellis, and M_1 is the number of the nodes in a column of the trellis. Hence M_0/M_1 is the number of codewords in a bunch.

We will introduce the following notations. Let $Q = \{\mathbf{q}^{(0)}, ..., \mathbf{q}^{(M-1)}\}$ be (n, M) nonlinear block code of block length n and cardinality M and let $\mathbf{q}^{(0)}, ..., \mathbf{q}^{(M-1)}$ be its codewords. Let us introduce an operation $\triangleright$ that maps an index $x \in \{0, \ldots, M-1\}$ into the corresponding codeword $\mathbf{q}^{(x)}$ from Q, i.e. $x \triangleright Q = \mathbf{q}^{(x)}$. Let $Q_1, Q_2, \ldots Q_l$ be $(n, M_1), (n, M_2), \ldots (n, M_l)$ nonlinear block codes respectively. Let us introduce a sum Q of $Q_1, Q_2, \ldots Q_l$ as follows

$$Q = \{\mathbf{q}^{(0)}, ..., \mathbf{q}^{(M_1 M_2 \ldots M_l - 1)}\} = \begin{bmatrix} Q_1 \\ Q_2 \\ \vdots \\ Q_l \end{bmatrix} =$$

$$= \{\mathbf{q}_1^{(i)} + \mathbf{q}_2^{(j)} + \ldots + \mathbf{q}_l^{(k)} : i = 0, \ldots, M_1 - 1; j = 0, \ldots, M_2 - 1; \ldots; k = 0, \ldots, M_l - 1\}.$$

Then an operation $\triangleright$ mapping the indexes $x^{(1)} \in \{0...M_1 - 1\}, x^{(2)} \in \{0...M_2 - 1\}, \ldots,$ $x^{(l)} \in \{0...M_l - 1\}$ into the codeword from Q is determined by the following way:

$$(x^{(1)}, x^{(2)}, \ldots, x^{(l)}) \triangleright Q = x^{(1)} \triangleright Q_1 + x^{(2)} \triangleright Q_2 \ldots + x^{(l)} \triangleright Q_l.$$

Sign '+' denotes component-wise modulo-2 addition of vectors. Matrices of type:

$$\begin{bmatrix} Q_1 \\ Q_2 \\ \vdots \\ Q_l \end{bmatrix}$$

we will call quasi-generator matrices. Then the quasi-generator matrix of nonlinear PUM code on the base of codes $Q_{00} = (n, M_0/M_1), Q_{01} = (n, M_1)$, and $Q_{11} = (n, M_1)$ is determined as follows

$$G = \begin{bmatrix} Q_{00} & \\ Q_{01} & Q_{11} \end{bmatrix}. \tag{1}$$

The l-th vector $\mathbf{v}_{i,j,l}$ belonging to the bunch coming from node i to node j is determined as follows:

$$\mathbf{v}_{i,j,l} = q_{11}^{(i)} + q_{01}^{(j)} + q_{00}^{(l)}; i, j = 0, \ldots, M_1 - 1; l = 0, \ldots, M_0/M_1 - 1.$$

An output vector $\mathbf{z_i}$ of length n at discrete time i is calculated from the rule

$$\mathbf{z_i} = (x_i^{(0)}, x_i^{(1)}) \triangleright \begin{bmatrix} Q_{00} \\ Q_{01} \end{bmatrix} + x_{i-1}^{(1)} \triangleright Q_{11},$$

where $x_i^{(0)} \in \{0, \ldots, M_0/M_1 - 1\}$ and $x_i^{(1)} \in \{0, \ldots, M_1 - 1\}$ are indexes at discrete time i and $x_{i-1}^{(1)} \in \{0, \ldots, M_1 - 1\}$ is an index at discrete time $i-1$.

From the description of encoding procedure one can see that matrices Q_{00}, Q_{01}, and Q_{11} are used instead of generator matrices of a partial unit memory convolutional code, indexes $x_i^{(0)}$ and $x_i^{(1)}$ are analogs of information vectors and mapping $\triangleright$ is used instead of multiplication of an information vector by a generator matrix.

The quasi-generator matrix of nonlinear code with partial memory two on the base of codes $Q_{00}, Q_{01}, Q_{02}, Q_{11}$, and Q_{22}, is determined in a similar manner

$$G = \begin{bmatrix} Q_{00} & & \\ Q_{01} & Q_{11} & \\ Q_{02} & & Q_{22} \end{bmatrix}. \tag{2}$$

An output vector $\mathbf{z_i}$ of length n at discreet time i is calculated from the rule

$$\mathbf{z_i} = (x_i^{(0)}, x_i^{(1)}, x_i^{(2)}) \triangleright \begin{bmatrix} Q_{00} \\ Q_{01} \\ Q_{02} \end{bmatrix} + x_{i-1}^{(1)} \triangleright Q_{11} + x_{i-2}^{(2)} \triangleright Q_{22}.$$

2.1 Construction 1

Now we shall construct a $(12, 24|12)$-nonlinear PUM code with free distance 12 and growth of profile distance $\alpha = 2$. Let A be a matrix obtained from the order 12 Hadamard matrix of the Paley type by removing the all-zero row and the all-zero column

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Let $A^* = [a_{11}, a_{10}, ..., a_1]$, where a_i is the i-th column of A, that is we take columns of A in the inverse order. We form two different Hadamard matrices H_{12}, H_{12}^* as follows

$$H_{12} = \begin{bmatrix} 0 & \mathbf{0} \\ \mathbf{0^t} & A \end{bmatrix}, H_{12}^* = \begin{bmatrix} 0 & \mathbf{0} \\ \mathbf{0^t} & A^* \end{bmatrix}.$$

Then we form the codes Q_{00}, Q_{01}, and Q_{11} as follows

$$Q_{00} = \{(0,0,0,0,0,0,0,0,0,0,0,0),(1,1,1,1,1,1,1,1,1,1,1,1)\},$$

the codewords of Q_{01} are rows of H_{12} and the codewords of Q_{11} are rows of H_{12}^*. It is easy to see that free distance of the nonlinear partial unit memory code with generator matrix (1) equals 12. The minimum distance of the code with generator matrix

$$Q = \begin{bmatrix} Q_{00} \\ Q_{01} \\ Q_{11} \end{bmatrix}$$

equals 2, and hence growth of profile distance $\alpha = 2$. Thus we obtained a $(12, 24|12)$-nonlinear PUM code with $d_{free} = 12$ and $\alpha = 2$. Since the values M_0 and M_1 of any linear partial unit memory code are equal to some powers of 2 it is obvious that linear $(12, 24|12)$ code does not exist. Moreover, the $(12, 16|8)$-linear PUM code is also not known.

Now let H_{24}, H_{24}^* be formed from Sylvester's rule

$$H_{24} = \begin{bmatrix} H_{12} & H_{12} \\ H_{12} & -H_{12} \end{bmatrix}, H_{24}^* = \begin{bmatrix} H_{12}^* & H_{12}^* \\ H_{12}^* & -H_{12}^* \end{bmatrix}.$$

And let codes Q_{00}, Q_{01}, and Q_{11} be formed as follows: Q_{00} consists from all-zero word and all-one word of length $n = 24$, the codewords of Q_{01} are rows of H_{24} and the codewords of Q_{11} are rows of H_{24}^*. Thus we obtain $(24, 48|24)$-nonlinear PUM code with $d_{free} = 24$ and $\alpha = 4$. It is clear that we can continue this process and obtain $(12i, 24i|12i)$-nonlinear PUM codes, $i \geq 1$, with $d_{free} = 12i$, and $\alpha = 2i$.

2.2 Construction 2

Now we consider a nonlinear code with partial memory two. Let H_{12} be Hadamard matrix of order 12 and let $\mathbf{h}_i$ be the i-th row of H_{12}. We form the codes $Q_{00}, Q_{01}, Q_{02}, Q_{11}$, and Q_{22} as follows

$$Q_{00} = \{(0,0,0,0,0,0,0,0,0,0,0,0),(1,1,1,1,1,1,1,1,1,1,1,1)\},$$

$$Q_{01} = \{\mathbf{h}_0, \mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3\}, Q_{02} = \{\mathbf{h}_0, \mathbf{h}_4, \mathbf{h}_5, \mathbf{h}_6\},$$

$$Q_{11} = \{\mathbf{h}_0, \mathbf{h}_7, \mathbf{h}_8, \mathbf{h}_9\}, Q_{01} = \{\mathbf{h}_0, \mathbf{h}_{10}, \mathbf{h}_{11}, \mathbf{h}_{10} + \mathbf{h}_{11}\}.$$

From the results of [2] it follows that free distance of a code with quasi-generator matrix (2) can be estimated as follows

$$d_{free} \geq min\{d_m, d_s + d_e + 2d_o\},$$

where

$$d_m = d_{min}\begin{bmatrix} Q_{00} & & \\ Q_{01} & Q_{11} & \\ Q_{02} & & Q_{22} \\ & Q_{00} & \\ & Q_{01} & Q_{11} \\ & & Q_{00} \end{bmatrix}, d_s = d_{min}\begin{bmatrix} Q_{00} \\ Q_{01} \\ Q_{02} \end{bmatrix}, d_e = d_{min}\begin{bmatrix} Q_{00} \\ Q_{11} \\ Q_{22} \end{bmatrix}, d_o = d_{min}\begin{bmatrix} Q_{00} \\ Q_{01} \\ Q_{02} \\ Q_{11} \\ Q_{22} \end{bmatrix}.$$

In our case $d_m = 12, d_s = 4, d_e = 4, d_o = 2$, hence $d_{free} = 12$. It was found with computer that $\alpha = 8/5$. Thus we obtain $(12, 32|16)$-nonlinear code with partial memory two with $d_{free} = 12$ and $\alpha = 8/5$. Note that the best known linear code with partial memory two and $d_{free} = 12$ is $(12, 16|8)$ code. So, we get one additional information bit without decreasing free distance.

References

[1] C.Thommesen and J.Justesen, Bounds on Distance and Error Exponents of Unit Memory Codes, IEEE Trans.Inform.Theory, vol.IT-29, pp.637-649, sep., 1983.

[2] U.Dettmar,U.K.Sorger,D.N,Gevorkian,V.V.Ziablov, An Extention of Partial Unit Memory Codes, Proc. , The third international colloquium on coding theory, Dilijian,1990.

[3] V.V.Ziablov,S.A.Shavgulidze,M.G.Shanidze, Bounds on Free Euclidean Distance for Various Systems of Modulation and Coding, Problems of Control and Information Theory, Vol.17(6),pp.345-356, 1988.