ISSN 0032-9460, Problems of Information Transmission, 2011, Vol. 47, No. 4, pp. 305–326. © Pleiades Publishing, Inc., 2011.
Original Russian Text © A.A. Kreshchuk, A.A. Davydov, V.V. Zyablov, 2011, published in Problemy Peredachi Informatsii, 2011, Vol. 47, No. 4, pp. 3–26.

Codes for MIMO Transmission Based on Orthogonal Sequences

A. A. Kreshchuk, A. A. Davydov, and V. V. Zyablov

Kharkevich Institute for Information Transmission Problems,
Russian Academy of Sciences, Moscow
krsch@iitp.ru adav@iitp.ru zyablov@iitp.ru

Received March 24, 2011; in final form, July 4, 2011

Abstract—We consider MIMO communication systems with Rayleigh fading. We propose a new coded modulation based on orthogonal sequences and state a new decodability condition. We introduce concepts and constructions of permutation free (PF) and permutation and repetition free (PRF) codes. We also propose a construction of PRF codes with sign manipulation, whose code rate can exceed 1. For better analysis and construction of these codes we introduce a one-to-one mapping that transforms signal matrices to vectors over a finite field. We propose construction algorithms for PF and PRF codes. We build PF and PRF codes with large cardinality, which in several case achieve the maximum cardinality. Simulation of the constructed codes and estimation of their performance was done in Simulink environment. Results show high error-correcting capability, which often reaches that of STBC codes with full transmit diversity.

DOI: 10.1134/S0032946011040016

1. INTRODUCTION

In this paper we propose a new coded modulation for MIMO (multiple-input, multiple-output) communication systems. Such systems use multiple receiving and transmitting antennas, each pair having independent path gains. Simultaneous use of multiple antennas increases the transmission rate and decreases the error probability. This kind of communication systems is also called spatial diversity systems. For further information on the diversity, see [1]. It is not sufficient to use only spatial diversity to reach high throughput. Coded modulation constructions utilizing both spatial and time diversity are called space-time codes. One of the first attempts to build an efficient full-rate space-time code was made in [2]. The technique proposed in [2] allowed to halve the number of receiving antennas by using two transmitting antennas without any loss of error-correction capability. In [3] this technique was generalized to any number of transmitting antennas, but the code rate dropped to 0.5. For a detailed review of state-of-the-art space-time codes, see [4–6].

Modern coded modulations for MIMO communication systems have small code lengths. That is why they require using an external code, which limits their applicability. The coded modulation considered in this paper was announced in [7]. It allows us to build codes of any length with proportionally increasing squared Euclidean code distance. This distance metric is equal to the energy distance between signals.

Now we describe the channel model. We consider a wireless communication system with N_T transmitting and N_R receiving antennas. Data are transmitted in blocks of length L through all the transmitting antennas simultaneously. Symbol interference is assumed to be negligible. During the transmission of one block, the channel is stationary. The channel can be described by the following expression:

$$r_j^t = \sum_{i=1}^{N_T} \alpha_{ij} s_i^t + \eta_j^t, \quad j = 1, \ldots, N_R, \quad t \in \mathbb{N}, \tag{1}$$

where s_i^t is the signal transmitted over the ith antenna at time t, r_j^t is the signal received by the jth antenna at time t, α_{ij} are statistically independent complex Gaussian random variables, and η_j^t is white Gaussian noise. The values α_{ij} are called path gains. In the general case, s_i^t are complex, but throughout this paper we assume $s_i^t = \pm 1$. The received signal r_j^t is always complex. The values $|\alpha_{ij}|$ have a Rayleigh distribution. The described channel [1,6] has the diversity order of $N_T N_R$.

The above channel is called a Rayleigh channel. This is one of models describing signal propagation in urban environments with no direct line of sight.

Rewrite (1) in a matrix form:

$$\boldsymbol{R} = \boldsymbol{S}\boldsymbol{\alpha} + \boldsymbol{\eta}. \tag{2}$$

Here $\boldsymbol{R} = \|r_j^t\|$ is an $L \times N_R$ complex matrix, $\boldsymbol{\alpha} = \|\alpha_{ij}\|$ is an $N_T \times N_R$ complex matrix, $\boldsymbol{S} = \|s_i^t\|$ is an $L \times N_T$ real matrix, and $\boldsymbol{\eta} = \|\eta_j^t\|$ is an $L \times N_R$ complex matrix. The index t in r_j^t, s_i^t, and η_j^t is a row number, and the lower index is a column number.

Assume that $\boldsymbol{\eta} = \mathbf{0}$. Then $\boldsymbol{R}_1 - \boldsymbol{R}_2 = (\boldsymbol{S}_1 - \boldsymbol{S}_2)\boldsymbol{\alpha}$. Hence, we can distinguish between two different received signals $\boldsymbol{R}$ if and only if the right-hand side of the equation is nonzero. We do not want to base our criterion on the number of receiving antennas, so we assume the worst case scenario, i.e., having one receiving antenna. Then $N_R = 1$, $\boldsymbol{R}$ is a column of length L, and $\boldsymbol{\alpha}$ is a column of length N_T. Apparently, no transmission is possible in the case of $\boldsymbol{\alpha} = \mathbf{0}$. We require any two code matrices to be distinguishable when all path gains are nonzero. We state this as a desired criterion for a code.

For our code, we use a finite set $\mathcal{S}$ of $L \times N_T$ matrices $\boldsymbol{S}$ complying with the decodability condition:

$$\forall\, \boldsymbol{S}_1, \boldsymbol{S}_2 \in \mathcal{S},\ \forall\, \boldsymbol{\alpha} \in \mathbb{C}^{N_T}:\ \alpha_j \neq 0,\ \forall\, j\ \rightarrow\ \boldsymbol{S}_1\boldsymbol{\alpha} \neq \boldsymbol{S}_2\boldsymbol{\alpha}, \tag{3}$$

where α_j are elements of the column $\boldsymbol{\alpha}$.

The set $\mathcal{S}$ is considered as a *code* with *codewords* $\boldsymbol{S}$. Each column of a codeword $\boldsymbol{S} \in \mathcal{S}$ is transmitted over a separate transmitting antenna.

Condition (3) means that two different codewords can be distinguished at the receiver in case of no deep fading in the channel.

Now we introduce a definition of the MIMO code rate. The described code is nonlinear. The rate of a nonlinear code $\mathcal{S}$ of length L is defined as

$$v = \frac{\log_2 |\mathcal{S}|}{L}.$$

This definition accounts for $s_i^t = \pm 1$. In [5], the rate thus defined is called the "temporal rate."

In Sections 1–4 we consider codes whose codewords consist of columns from an ordered set of orthogonal columns. Throughout this paper, as this set we use columns of an $L \times L$ Hadamard matrix with

$$L = 2^m \geq N_T.$$

In Section 5 we modify the introduced codes. The set of columns is extended by adding their inverses.

Throughout this paper, we use a finite field of 2^m elements. However, in principle, the code construction technique could be applied to cases where L is not a power of 2.

Definition 1. A code $\mathcal{S}$ is said to be a *PRF code* (permutation and repetition free code) if no two codewords are permutations of each other and no codeword contains repeated columns.

Definition 2. A code $\mathcal{S}$ is said to be a *PF code* (permutation free code) if no two codewords are permutations of each other. Codewords of a PF code may contain repeated columns.

Lemma 1. *Let codewords $\boldsymbol{S}$ of a code $\mathcal{S}$ be columns of an $L \times L$ Hadamard matrix. Then for* (3) *to be true, it is necessary that $\mathcal{S}$ is a PF code, and it is sufficient that $\mathcal{S}$ is a PRF code.*

A proof of the lemma is given in Section 2.

Note that some PF codes do not satisfy constraint (3). Nevertheless, PF codes can be used when channel characteristics do not allow one to build a PRF code of the desired cardinality.

Hence, we introduce for MIMO communication systems a *new coded modulation*, described as a *matrix code $\mathcal{S}$*, and show that the decodability condition holds if $\mathcal{S}$ is a PRF code. With some decrease in the error-correction capability, we may let $\mathcal{S}$ be a PF code.

The *goal* of this paper is to find *construction techniques for PRF and PF codes* with sufficiently large cardinality and perform a numerical *simulation* of the constructed codes to estimate their efficiency.

To develop code construction techniques, we introduce a one-to-one *mapping of a matrix code $\mathcal{S}$ to a vector code $\mathcal{C}$*, and then use natural vector-space techniques, which proves to be efficient.

Let q be a prime or prime power. Let $\mathbb{F}_q$ denote a Galois field of q elements. Let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Let $\mathbb{F}_q^n$ denote an n-dimensional vector space over $\mathbb{F}_q$.

Let us map the columns of an $L \times L$ Hadamard matrix $\boldsymbol{H}$ to elements of the field $\mathbb{F}_L$ taken in a fixed order. Then $\boldsymbol{H} = \|\boldsymbol{h}_0\boldsymbol{h}_1 \ldots \boldsymbol{h}_{L-1}\|$, where $\boldsymbol{h}_i$ is a column of the Hadamard matrix and $\{0, 1, \ldots, L-1\} = \mathbb{F}_L$. A codeword $\boldsymbol{S}$ composed of N_T columns of the Hadamard matrix can be expressed as

$$\boldsymbol{S} = \|\boldsymbol{h}_{i_1}\boldsymbol{h}_{i_2} \ldots \boldsymbol{h}_{i_{N_T}}\|, \quad \{i_1, i_2, \ldots, i_{N_T}\} \subset \mathbb{F}_L.$$

Now we can map each codeword $\boldsymbol{S}$ to a vector $\boldsymbol{c} \in \mathbb{F}_L^{N_T}$ whose components correspond to the column number in the Hadamard matrix. We denote this map by $\mathcal{L}$. It follows from the aforesaid that $\mathcal{L}$ is a one-to-one map which can be expressed as follows:

$$\mathcal{L}(\boldsymbol{S}) = \mathcal{L}(\|\boldsymbol{h}_{i_1}\boldsymbol{h}_{i_2} \ldots \boldsymbol{h}_{i_{N_T}}\|) = \boldsymbol{c} = (i_1, i_2, \ldots, i_{N_T}) \in \mathbb{F}_L^{N_T}. \tag{4}$$

The vectors $\boldsymbol{c}$ compose the code $\mathcal{C}$.

In the following, by PF and PRF codes we mean both codes $\mathcal{S}$, whose codewords are $L \times N_T$ matrices, and the corresponding codes $\mathcal{C} \subset \mathbb{F}_L^{N_T}$.

We develop code construction algorithms for the vector representation. Also, we construct PF and PRF codes both as subsets of Reed–Solomon (RS) codes and subsets of the vector space $\mathbb{F}_L^{N_T}$ with no connection to the RS codes.

Some results of this paper were presented without proofs in [7].

In Section 2 the maps $\mathcal{L}$ and $\mathcal{L}^{-1}$ are explored. We describe how these maps affect the distance between codewords. In Section 3 we present a general analysis of PF and PRF codes and propose techniques for their construction. In Section 4 we illustrate the efficiency of these techniques by examples of constructing specific PF and PRF codes. In Section 5 we consider a modification of PRF codes, which is called PRF codes with sign manipulation. In Section 6 we describe a maximum-likelihood decoder and analyze differences between PF and PRF codes. In Section 7 we describe a numerical simulation environment for some codes from Section 4 and show plots of the code performance versus the signal-to-noise ratio (SNR). Results of the simulation are also presented. In the Appendix we consider subsets of the field $\mathbb{F}_{2^m}$ with a fixed sum of elements, which can be used in constructing PF and PRF codes.

2. MAP $\mathcal{L}$ AND CODE DISTANCES IN $\mathcal{S}$ AND $\mathcal{L}(\mathcal{S})$

Proof of Lemma 1. First we prove the sufficiency, i.e., show that a PRF code satisfies condition (3). Let $\boldsymbol{H}$ denote an Hadamard matrix. Multiply equation (3) by the matrix $\frac{1}{L}\boldsymbol{H}^T$, where T denotes the transpose operator. The matrix $\frac{1}{L}\boldsymbol{H}^T\boldsymbol{S}_u$ is a $(0,1)$-matrix and contains exactly one 1 in each column. The position of this 1 is given by the index of the corresponding column of the matrix $\boldsymbol{S}_u$ in $\boldsymbol{H}$. Each row in $\frac{1}{L}\boldsymbol{H}^T\boldsymbol{S}_u$ either contains precisely one 1 (since $\boldsymbol{S}_u$ contains no identical columns) or is all-zero. The all-zero rows correspond to columns from $\boldsymbol{H}$ that are not present in $\boldsymbol{S}_u$. Since different matrices $\boldsymbol{S}_u$ could not be obtained from each other by permutations, there exists a column in $\boldsymbol{S}_1$ that is not present in $\boldsymbol{S}_2$. Hence, there exist an index i such that the ith row in the matrix $\frac{1}{L}\boldsymbol{H}^T\boldsymbol{S}_1$ is nonzero and the ith row in $\frac{1}{L}\boldsymbol{H}^T\boldsymbol{S}_2$ is all-zero. Since $\alpha_j \neq 0$, $\forall j$, we have $\left(\frac{1}{L}\boldsymbol{H}^T\boldsymbol{S}_1\boldsymbol{\alpha}\right)_i \neq 0$ (which is ensured by the existence of precisely one 1 in a nonzero row), while $\left(\frac{1}{L}\boldsymbol{H}^T\boldsymbol{S}_2\boldsymbol{\alpha}\right)_i = 0$, where $(\boldsymbol{e})_i$ is the ith component of the vector $\boldsymbol{e}$. Therefore, condition (3) holds.

The aforesaid also means that, to satisfy (3), the code $\mathcal{S}$ *must* be a PF code. To prove this, we can take the all-one column as $\boldsymbol{\alpha}$. If $\boldsymbol{S}_2$ is a permutation of $\boldsymbol{S}_1$, then, obviously, condition (3) is violated. △

Note that the proof of Lemma 1 can easily be generalized to any set of orthogonal columns.

Recall that each column of a codeword $\boldsymbol{S} \in \mathcal{S}$ is transmitted over a separate antenna. Therefore, each element of a codeword $\mathcal{L}(\boldsymbol{S})$ corresponds to one antenna.

The decodability requirement imposes several constraints on a code $\mathcal{L}(\mathcal{S})$. A PRF code $\mathcal{S}$ cannot have codewords with the same set of columns. For a code $\mathcal{L}(\mathcal{S})$, this results in the absence of codewords with the same set of elements. The absence of repeated columns in codewords of $\mathcal{S}$ results in the absence of repeated symbols in codewords of $\mathcal{L}(\mathcal{S})$.

Let us examine how the map $\mathcal{L}$ affects distances between codewords. We use the Euclidean metric for the matrices and the Hamming metric in the field $\mathbb{F}_L^{N_T}$.

The Euclidean distance between two distinct columns of an $L \times L$ Hadamard matrix equals $\sqrt{\frac{L}{2}\cdot 2^2 + \frac{L}{2}\cdot 0^2} = \sqrt{2L}$. Take two codewords $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{L}(\mathcal{S})$ with Hamming distance d. Then the squared Euclidean distance between the matrices $\mathcal{L}^{-1}(\boldsymbol{c}_1)$ and $\mathcal{L}^{-1}(\boldsymbol{c}_2)$ equals the sum of the squared distances between the columns; i.e.,

$$d_E^2(\mathcal{L}^{-1}(\boldsymbol{c}_1), \mathcal{L}^{-1}(\boldsymbol{c}_2)) = 2Ld.$$

Hence, $d_E(\mathcal{L}^{-1}(\boldsymbol{c}_1), \mathcal{L}^{-1}(\boldsymbol{c}_2)) = \sqrt{2dL}$.

According to [5], the Euclidean distance is a good measure of the code performance when the *SNR is low.* We will optimize our code for this situation.

The squared Euclidean distance is the energy distance between codewords. There is a well-known expression [6] for this distance:

$$d_E^2(\boldsymbol{S}_1, \boldsymbol{S}_2) = \operatorname{tr}\left[(\boldsymbol{S}_1 - \boldsymbol{S}_2)^H(\boldsymbol{S}_1 - \boldsymbol{S}_2)\right],$$

where tr is the matrix trace operator and H denotes Hermitian conjugation.

In [6], a choice criterion based on the Euclidean distance was called the trace criterion. We will use this criterion in constructing the coded modulation.

In the literature (see, e.g., [6]) one can find other criteria for constructing space-time codes: the rank criterion and determinant criterion. We do not use these criteria in the present paper, since they are better suited for high values of the SNR.

Note that the error-correction capability depends not only on the minimum code distance but also on the whole distance spectrum. To summarize all the aforesaid, we will construct PF and PRF codes of length N_T over the field $\mathbb{F}_L$ with a "good" Hamming distance spectrum.

3. SOME APPROACHES TO CONSTRUCTING PERMUTATION FREE CODES

3.1. Basic Concepts and Definitions

Let $[n,k,d]_q$ be a linear code of length n and dimension k with minimum distance d over the field $\mathbb{F}_q$. Denote by $(n,M,d)_q$ a nonlinear code over $\mathbb{F}_q$ of length n and cardinality M with minimum distance d.

Definition 3. (i) A *PF code* is a set of words none of which is a permutation of another. We denote an $(n,M,d)_q$ PF code by $(n,M,d)_q^{\mathrm{PF}}$. Given n, d, and q, we denote the maximum possible cardinality of a PF code by $M_q^{\mathrm{PF}}(n,d)$. A *maximal PF code* is a code with cardinality $M_q^{\mathrm{PF}}(n,d)$.

(ii) A PF code whose codewords do not contain repeated symbols is called a *PRF code.* We denote an $(n,M,d)_q$ PRF code by $(n,M,d)_q^{\mathrm{PRF}}$. Given n, d, and q, we denote the maximum possible cardinality of a PRF code by $M_q^{\mathrm{PRF}}(n,d)$. A *maximal PRF code* is a code with cardinality $M_q^{\mathrm{PRF}}(n,d)$.

(iii) Consider subcodes of an $[n,n-d+1,d]_q$ RS code. A subcode is called a *PF subcode* or a *PRF subcode* if it is a PF or PRF code, respectively. Let $\overline{M}_q^{\mathrm{PF}}(n,d)$ and $\overline{M}_q^{\mathrm{PRF}}(n,d)$ denote the maximum cardinality of PF and PRF subcodes, respectively. A *maximal PF subcode* and a *maximal PRF subcode* are subcodes with cardinalities $\overline{M}_q^{\mathrm{PF}}(n,d)$ and $\overline{M}_q^{\mathrm{PRF}}(n,d)$, respectively.

Throughout this paper we assume that $n \le q$.

Note that a PRF code is a repetition free (RF) code. These codes were described in [8, 9]. But in those papers, permutations of symbols in codewords were not forbidden.

Let $a = (a_1, a_2, \ldots, a_n)$ be an n-dimensional vector over $\mathbb{F}_q$.

If $\sum\limits_{i=1}^{n} a_i = s \in \mathbb{F}_q$, then the vector a is called an *$(n,s)_q$-vector.* If *all components* of an $(n,s)_q$-vector are *different*, then it is called an *$(n,s)_q^{\mathrm{RF}}$-vector*, or just an *RF vector.* Thus, for an $(n,s)_q^{\mathrm{RF}}$-vector a we have

$$\sum_{i=1}^{n} a_i = s \in \mathbb{F}_q, \qquad a_i \ne a_j \quad \text{for} \quad i \ne j.$$

Let $u = (u_1, u_2, \ldots, u_n)$ be an n-dimensional vector over $\mathbb{F}_q$. Following [10, Section 5.6], by a *composition* of the vector u we call the following q-dimensional vector over the alphabet $\{0, 1, \ldots, n\}$:

$$\operatorname{comp}(u) = \operatorname{comp}(u_1, u_2 \ldots, u_n) = (v_0, v_1, \ldots, v_{q-1}) = (v_0(u), v_1(u), \ldots, v_{q-1}(u)),$$

where $v_i = v_i(u)$ is the number of components u_j equal to i. Obviously, $\sum\limits_{i=0}^{q-1} v_i(u) = n$.

The 2*nd-order composition* of an n-dimensional vector u over $\mathbb{F}_q$ is defined as the following $(n+1)$-dimensional vector over the alphabet $\{0, 1, \ldots, q-1\}$:

$$\begin{aligned}\operatorname{comp}^{(2)}(u) = \operatorname{comp}(\operatorname{comp}(u)) &= \operatorname{comp}(v_0(u), v_1(u), \ldots, v_{q-1}(u)) \\ &= (V_0, V_1, \ldots, V_n) = (V_0(u), V_1(u), \ldots, V_n(u)),\end{aligned}$$

where $V_i = V_i(u)$ is the number of components $v_j(u)$ equal to i. It is obvious that

$$V_i(u) \ge 0, \qquad \sum_{i=0}^{n} V_i(u) = q, \qquad \sum_{i=0}^{n} iV_i(u) = n, \qquad V_0 \ge q-n. \tag{5}$$

The symmetric group S_n of degree n with cardinality $n!$ (composed of all permutations on n elements) partitions the vector space $\mathbb{F}_q^n$ into disjoint orbits. In what follows, we consider only these orbits. Values of the parameters n and q will be clear from the context.

The length (cardinality) of an orbit lies in the range $1, \ldots, n!$. The number and lengths of orbits depend on the values of n and q.

Let $O^w(a) = O^w(a_1, a_2, \ldots, a_n)$ denote an orbit containing the word $a = (a_1, a_2, \ldots, a_n)$, where $a_i \in \mathbb{F}_q$. The word $a = (a_1, a_2, \ldots, a_n)$ is called an orbit generator. Any word contained in an orbit can be viewed as its generator. If $\sum\limits_{i=1}^{n} a_i = s \in \mathbb{F}_q$, then the orbit $O^w(a_1, a_2, \ldots, a_n)$ is also called an $(n, s)_q$-*orbit*, and its generator $(a_1, a_2, \ldots, a_n)$ is an $(n, s)_q$-*vector*.

Let $O(v) = O(v_0, v_1, \ldots, v_{q-1})$ denote an orbit whose generator has the composition $v = (v_0, v_1, \ldots, v_{q-1})$. All words of the orbit have the same composition, and the orbit is composed of all words with this composition. We call this composition the *orbit composition*. The length of the orbit $O(v_0, v_1, \ldots, v_{q-1})$ is equal to the number of n-dimensional vectors over $\mathbb{F}_q$ with composition $(v_0, v_1, \ldots, v_{q-1})$; i.e.,

$$|O(v_0, v_1, \ldots, v_{q-1})| = \binom{n}{v_0, v_1, \ldots, v_{q-1}} = \frac{n!}{v_0!\, v_1! \ldots v_{q-1}!}. \tag{6}$$

We define the *structure of an orbit* to be the 2nd-order composition of its generator. Let $O^{(2)}(V) = O^{(2)}(V_0, V_1, \ldots, V_n)$ denote an orbit whose generator has 2nd-order composition $V = (V_0, V_1, \ldots, V_n)$. Let $T(V_0, V_1, \ldots, V_n)$ be the set of orbits with structure $(V_0, V_1, \ldots, V_n)$. The number of orbits $N_O(V_0, V_1, \ldots, V_n)$ in this set equals the number of q-dimensional vectors over the alphabet $\{0, 1, \ldots, n\}$ with composition $(V_0, V_1, \ldots, V_n)$; i.e.,

$$N_O(V_0, V_1, \ldots, V_n) = \frac{q!}{V_0!\, V_1! \ldots V_n!}. \tag{7}$$

Taking (6) into account, the length of any orbit in the set $T(V_0, V_1, \ldots, V_n)$ is

$$|O^{(2)}(V_0, V_1, \ldots, V_n)| = \frac{n!}{(0!)^{V_0} (1!)^{V_1} \ldots (n!)^{V_n}} = \frac{n!}{\prod\limits_{i=0}^{n} (i!)^{V_i}}. \tag{8}$$

In essence, relation (8) is relation (6) written with grouped multipliers.

The total number $N_\Sigma(n, q)$ of orbits of the group S_n in the space $\mathbb{F}_q^n$ equals the number of combinations of q things n at a time with repetitions:

$$N_\Sigma(n, q) = \binom{q + n - 1}{n}. \tag{9}$$

3.2. Upper Bounds for PF Codes

Lemma 2. *A PF code $(n, M, d)_q^{\mathrm{PF}}$ can include at most one word from each orbit of the group S_n regardless of the orbit structure.*

Corollary 1. *For any distance d, for the maximum possible cardinality of an $(n, M, d)_q^{\mathrm{PF}}$ code we have*

$$M_q^{\mathrm{PF}}(n, d) \le \binom{q + n - 1}{n}.$$

Proof. Apply Lemma 2 and equation (9). △

Lemma 3. *Fix an element $a \in \mathbb{F}_q$. Consider q orbits with generators of the form $(\underbrace{a, \ldots, a}_{n-1}, b)$, where $b \in \mathbb{F}_q$ and the equality $a = b$ is allowed. Let W denote the number of words in these orbits that belong to an $(n, M, 2)_q^{\mathrm{PF}}$ code C with code distance* 2.

(i) *If the word $(\underbrace{a, \ldots, a}_{n-1}, a)$ belongs to C, then $W = 1$.*

(ii) *If the word $(\underbrace{a, \ldots, a}_{n-1}, a)$ does not belong to C, then $W \le n$. Furthermore, all words that are generators of orbits contained in the code are of the forms $(\underbrace{a, \ldots, a}_{n-1}, b)$, $(\underbrace{a, \ldots, a}_{n-2}, b, a)$, $(\underbrace{a, \ldots, a}_{n-3}, b, a, a)$, …, $(b, \underbrace{a, \ldots, a}_{n-1})$.*

Proof. Correctness of the lemma immediately follows from the structure of words given in its statement. △

Corollary 2. *Consider q^2 orbits with generators of the form $(\underbrace{a, \ldots, a}_{n-1}, b)$, where $a, b \in \mathbb{F}_q$ and the equality $a = b$ is allowed. Let V denote the number of words in these orbits that belong to an $(n, M, 2)_q^{\mathrm{PF}}$ code C. Then $V \le nq$.*

Proof. Apply Lemma 3. △

Corollary 3. *For the maximum possible cardinality of an $(n, M, d)_q^{\mathrm{PF}}$ code with distance $d \ge 2$, we have*

$$M_q^{\mathrm{PF}}(n, d) \le \binom{q + n - 1}{n} - q(q - n), \quad d \ge 2. \tag{10}$$

Proof. Apply Corollaries 1 and 2. △

3.3. RF Orbits, RF Subsets, and RF Vectors

Consider an orbit with generator $(a_1, a_2, \ldots, a_n)$. If all components a_i are distinct and $\sum\limits_{i=1}^{n} a_i = s \in \mathbb{F}_q$, then the orbit is called an $(n, s)_q^{\mathrm{RF}}$*-orbit*, or just an *RF orbit* (repetition free). We also denote it by O_{RF}. According to Section 3.1, regardless of s, the structure of an $(n, s)_q^{\mathrm{RF}}$-orbit is of the form

$$V_0 = q - n, \qquad V_1 = n, \qquad V_2 = V_3 = \ldots = V_n = 0. \tag{11}$$

Given q and n, the total number of RF orbits and the length of each RF orbit are, respectively,

$$N_{O_{RF}} = \binom{q}{n}, \qquad |O_{RF}| = n!. \tag{12}$$

Lemma 4. *All words of an $(n, M, d)_q^{\mathrm{PRF}}$ code belong to RF orbits of the group S_n. Furthermore, a PRF code can contain at most one word from each RF orbit.*

Lemmas 2 and 4 are fundamental for constructing PF and PRF codes.

Corollary 4. *For any distance d, for the maximum possible cardinality of an $(n, M, d)_q^{\mathrm{PRF}}$ code we have*

$$M_q^{\mathrm{PRF}}(n, d) \le \binom{q}{n}.$$

Proof. Apply Lemma 4 and relations (12). △

We call an n-subset of the field $\mathbb{F}_q$ composed of distinct elements an *RF subset.* An RF subset with the sum of all elements equal to s is called an $(n,s)_q^{\mathrm{RF}}$-*subset.* Such a subset is of the form

$$\{a_1,a_2,\ldots,a_n\}\subset\mathbb{F}_q,\qquad \sum_{i=1}^{n}a_i=s,\qquad a_i\neq a_j\quad\text{for}\quad i\neq j.$$

Let $N_{n,q}^{(s)}$ denote the total number of $(n,s)_q^{\mathrm{RF}}$-subsets.

Any ordering of elements of an $(n,s)_q^{\mathrm{RF}}$-subset results in an $(n,s)_q^{\mathrm{RF}}$-vector, which can be treated as a generator of an $(n,s)_q^{\mathrm{RF}}$-orbit. Thus, there exists a one-to-one correspondence between $(n,s)_q^{\mathrm{RF}}$-subsets and $(n,s)_q^{\mathrm{RF}}$-orbits. Therefore, the values $N_{n,q}^{(s)}$ play an important role in constructing and analyzing PF and PRF codes. Let $\mathbb{F}_q=\{e_0,e_1,\ldots,e_{q-1}\}$. Then

$$\sum_{i=0}^{q-1}N_{n,q}^{(e_i)}=\binom{q}{n}. \tag{13}$$

3.4. Codes $(n,M,2)_{2^m}^{\mathrm{PF}}$ and $(n,M,2)_{2^m}^{\mathrm{PRF}}$ as Subcodes of an $[n,n-1,2]_{2^m}$ RS Code

Throughout what follows, we consider $(n,M,2)_{2^m}^{\mathrm{PF}}$ and $(n,M,2)_{2^m}^{\mathrm{PRF}}$ codes over $\mathbb{F}_{2^m}$ with distance $d=2$. We denote elements of $\mathbb{F}_{2^m}$ by numbers, so that

$$\mathbb{F}_{2^m}=\{0,1,\ldots,2^{m-1}\}. \tag{14}$$

Here, the binary m-digit representation of a number coincides with the vector representation of the corresponding element over some basis. Since here we use addition of elements only, the choice of a basis is insignificant.

In the Appendix we obtain some helpful expressions for $N_{n,2^m}^{(s)}$, which come from the weight spectra of a Hamming code and its cosets.

We introduce the following notation:

$A_{w,2^m}$ is the number of weight-w codewords of the $[2^m-1,2^m-1-m,3]_2$ Hamming code with m parity checks;

$\overline{A}_{w,2^m}$ is the number of weight-w words in a coset of the $[2^m-1,2^m-1-m,3]_2$ Hamming code.

All codewords of an $[n,n-1,2]_{2^m}$ RS code can be obtained by appending a parity check to an $(n-1)$-dimensional information vector. Hence, we get the following result.

Lemma 5. *Consider an $[n,n-1,2]_{2^m}$ RS code and its cosets.*

(i) *The code contains all $(n,0)_{2^m}$-vectors and only these vectors. The group S_n partitions the code into disjoint $(n,0)_{2^m}$-orbits.*

(ii) *Let a coset have a nonzero syndrome $s\in\mathbb{F}_{2^m}$. Then this coset contains all $(n,s)_{2^m}$-vector and only these vectors. The group S_n partitions the coset into disjoint $(n,s)_{2^m}$-orbits.*

We call an orbit embedded in an RS code a *code orbit.* An RF orbit embedded in a code will be called a *code RF orbit.*

Lemmas 2–5 imply the following theorem.

Theorem 1. *Consider an $[n,n-1,2]_{2^m}$ RS code.*

(i) *A maximal PF subcode contains one and only one word from each code orbit regardless of its structure. The maximum cardinality $\overline{M}_{2^m}^{\mathrm{PF}}(n,2)$ equals the total number of code orbits.*

(ii) *A maximal PRF subcode contains one and only one word from each code RF orbit. The maximum cardinality $\overline{M}_{2^m}^{\mathrm{PRF}}(n,2)$ equals the total number of code RF orbits.*

Table 1. Some code orbits of an $[n, n-1, 2]_{2^m}$ RS code, $n \le 2^m$

Orbit	Nonzero components of the orbit structure	Orbit generator (a, b, c, d, e, f are different elements of $\mathbb{F}_{2^m}$)	Number of orbits N_{O_j}	Orbit length $\lvert O_j \rvert$
$O_1 = O_{RF}$	$V_0 = 2^m - n$, $V_1 = n$	$(a_1, a_2, \ldots, a_n)$, $a_1 + a_2 + \ldots + a_n = 0$, $a_i \ne a_j$ for $i \ne j$	$N_{n,2^m}^{(0)} =$ $A_{n-1,2^m} + A_{n,2^m}$	$n!$
O_2	$V_0 = 2^m - 1$, $V_n = 1$	$(\underbrace{a, \ldots, a}_{n})$, $n = 2p$	2^m	1
O_3	$V_0 = 2^m - 2$, $V_p = 2$	$(\underbrace{a, \ldots, a}_{p}, \underbrace{b, \ldots, b}_{p})$, p even	$\binom{2^m}{2}$	$\binom{n}{p}$
O_4	$V_0 = 2^m - p$, $V_2 = p$	$(a_1, a_1, a_2, a_2, \ldots, a_p, a_p)$	$\binom{2^m}{p}$	$2^{-p} n!$
O_5	$V_0 = 2^m - 4$, $V_1 = 3$, $V_{n-3} = 1$	$(\underbrace{a, \ldots, a}_{n-3}, b, c, d)$, $a + b + c + d = 0$, $n = 2p$	$2^m \cdot \frac{1}{3} \binom{2^m - 1}{2}$	$\frac{n!}{(n-3)!}$
O_6	$V_0 = 2^m - 5$, $V_1 = 4$, $V_{n-4} = 1$	$(\underbrace{a, \ldots, a}_{n-4}, b, c, d, e)$, $b+c+d+e = 0$, $n = 2p \ge 6$	$2^m \frac{1}{2^m - 3} \binom{2^m - 1}{4}$	$\frac{n!}{(n-4)!}$
O_7	$V_0 = 2^m - 4$, $V_1 = 2$, $V_{p-1} = 2$	$(\underbrace{a, \ldots, a}_{p-1}, \underbrace{b, \ldots, b}_{p-1}, c, d)$, p even, $a + b + c + d = 0$	$\binom{2^m}{2} (2^{m-1} - 1)$	$\frac{n!}{(p-1)!\,(p-1)!}$
O_8	$V_0 = 2^m - 6$, $V_1 = 4$, $V_{p-2} = 2$	$(\underbrace{a, \ldots, a}_{p-2}, \underbrace{b, \ldots, b}_{p-2}, c, d, e, f)$, p even, $c + d + e + f = 0$, $n \ge 8$	$\binom{2^m}{2} \Bigl(2^{m-1} - 1$ $+ \frac{1}{3} \binom{2^m - 1}{2}$ $\times (2^{m-2} - 2)\Bigr)$	$\frac{n!}{(p-2)!\,(p-2)!}$
O_9	$V_0 = 2^m - 5$, $V_1 = 3$, $V_{p-1} = 1$, $V_{p-2} = 1$	$(\underbrace{a, \ldots, a}_{p-1}, \underbrace{b, \ldots, b}_{p-2}, c, d, e)$, p even, $a + c + d + e = 0$, $n \ge 8$	$\binom{2^m}{3} (2^m - 4)$	$\frac{n!}{(p-1)!\,(p-2)!}$
O_{8+t}	$V_0 = 2^m - p + t - 1$, $V_2 = p - t$, $V_{2t} = 1$	$(\underbrace{b, \ldots, b}_{2t}, a_1, a_1, \ldots$ $\ldots, a_{p-t}, a_{p-t})$, $n = 2p$, $t = 2, 3, \ldots, p-1$	$\binom{2^m}{p-t} (2^m - p + t)$	$\frac{1}{(2t)!} 2^{t-p} n!$

Lemma 6. *An* $[n, n-1, 2]_{2^m}$ *RS code with* $n \le 2^m$, $m \ge 3$, *contains the code orbits presented in Table* 1, *where* O_1 *is an RF orbit.*

Proof. Lengths of all orbits in Table 1 are computed using equation (8).

The structure of the RF orbit O_1 is of the form (11) regardless of whether it is a code orbit or not. Similarly, for a generator of an RF orbit it is necessary that $a_i \ne a_j$ for $i \ne j$. Finally, equality $a_1 + \ldots + a_n = 0$ for a generator of a *code* RF orbit must hold due to Lemma 5 (i). Properties of a generator and the definition of $N_{n,q}^{(s)}$ imply $N_{O_1} = N_{n,2^m}^{(0)}$. Then we use formula (21) from the Appendix.

For the orbits O_2–O_9 and O_{8+t} we use Lemma 5 (i). Taking properties of the field $\mathbb{F}_{2^m}$ into account, all generators of the orbits O_2–O_9 and O_{8+t} have zero sum of elements. The structure of an orbit is determined by the form of its generator. The number of orbits O_2, O_3, O_4, and O_{8+t} is determined by (7), since there are no constraints on the generators. For the orbits O_5 and O_6, an element a can be chosen in 2^m ways. Then we use Lemma 13 (ii), see the Appendix. For the orbits O_7 and O_8, a pair a, b can be chosen in $\binom{2^m}{2}$ ways. Then we use Lemma 13 (iii). Finally, for the orbit O_9, a pair a, b can be chosen in $2^m(2^m - 1)$ ways, since a and b are not interchangeable. Then we use Lemma 13 (iii) again. △

Theorem 2. *A maximal PRF subcode of an* $[n, n-1, 2]_{2^m}$ *RS code has cardinality*

$$\overline{M}_{2^m}^{\mathrm{PRF}}(n,2) = N_{n,2^m}^{(0)} = A_{n-1,2^m} + A_{n,2^m}. \tag{15}$$

Moreover, all words of a maximal PRF subcode can be obtained from words of weights $n-1$ *and* n *of the binary* $[2^m-1, 2^m-1-m, 3]_2$ *Hamming code.*

Proof. According to Theorem 1 (ii), a maximal PRF subcode contains exactly one word from each code RF orbit. Then we use Lemma 6 and the orbit O_1 from Table 1.

Let us arrange (in any order) the $(n,0)_{2^m}^{\mathrm{RF}}$-subsets specified in Lemma 10 (i), constructed from words of weights $n-1$ and n of the binary $[2^m-1, 2^m-1-m, 3]_2$ Hamming code. As a result, we obtain $(n,0)_{2^m}^{\mathrm{RF}}$-vectors, which can be regarded as words of a maximal PRF code. △

Corollary 5. *For* $n \in \{2^m-2,\ 2^m-1,\ 2^m\}$, *a maximal PRF subcode of an* $[n, n-1, 2]_{2^m}$ *RS code has cardinality*

$$\overline{M}_{2^m}^{\mathrm{PRF}}(2^m,2) = \overline{M}_{2^m}^{\mathrm{PRF}}(2^m-1,2) = 1, \qquad \overline{M}_{2^m}^{\mathrm{PRF}}(2^m-2,2) = 0.$$

Proof. Apply Theorem 2 and Lemma 11; see the Appendix. △

A PF or PRF code is constructed if structures and generators of all orbits that compose the code are defined.

It follows from Lemma 6 and Theorem 2 that *the task of constructing a maximum PRF subcode of an* $[n, n-1, 2]_{2^m}$ *RS code is solved*, and a precise value of the maximum cardinality $\overline{M}_{2^m}^{\mathrm{PRF}}(n,2)$ is obtained.

Taking into account Lemma 6 and Theorems 1 and 2, a maximal PF subcode of an $[n, n-1, 2]_{2^m}$ RS code can be constructed in the following way.

Algorithm A. Constructing a maximal PF subcode of an $[n, n-1, 2]_{2^m}$ RS code.

1. In Table 1 select orbits O_j appearing in an RS code with the given n. The set of indices of these orbit is denoted by J_n (RF orbits O_1 are always present). Compute the total number M of the selected code orbits and the number Σ of words in them:

$$M = \sum_{j \in J_n} N_{O_j}, \qquad \Sigma = \sum_{j \in J_n} N_{O_j} |O_j|.$$

2. Check the equality

$$\Sigma = 2^{m(n-1)}. \tag{16}$$

If (16) holds, exit the algorithm, letting

$$\overline{M}_{2^m}^{\mathrm{PF}}(n,2) = M.$$

If (16) does not hold, go to Step 3.

3. Based on the technique used for constructing Table 1 and on the proof of Lemma 6, find an admissible (for the given parameters) structure of an orbit O_{new} that was not used at previous steps. Find the length $|O_{\mathrm{new}}|$ of this orbit and the number $N_{O_{\mathrm{new}}}$ of such orbits. Correct $\Sigma = \Sigma + N_{O_{\mathrm{new}}}|O_{\mathrm{new}}|$ and $M = M + N_{O_{\mathrm{new}}}$. Go to Step 2.

Note that when relation (16) holds, the selected orbits contain the whole RS code. In this case, a maximal PF subcode is constructed, and its cardinality $\overline{M}_{2^m}^{\mathrm{PF}}(n,2)$ equals the total number of code orbits M.

Efficiency of Algorithm A is illustrated in Section 4.1, where interesting examples of constructing maximal PF subcodes of an $[n,n-1,2]_8$ RS code are given. In these examples, Step 3 was not used.

3.5. Codes $(n,M,2)_{2^m}^{\mathrm{PF}}$ and $(n,M,2)_{2^m}^{\mathrm{PRF}}$ as Subsets of the Space $\mathbb{F}_{2^m}^n$

In the general case, where we are not limited by subcodes of RS codes, the following algorithms are useful.

Algorithm B. Constructing a PRF code as a union of PRF codes derived from an RS code and its cosets.

Let $n \ge 4$. The desired $(n,M,2)_{2^m}^{\mathrm{PRF}}$ code is denoted by $\mathcal{C}$.

1. Based on Lemma 12 (see the Appendix), construct $(n,N_{n,2^m}^{(s)},2)_{2^m}^{\mathrm{PRF}}$ codes with sum of elements equal to s for all $s=0,1,\ldots,2^m-1$. Arrange elements of $\mathbb{F}_{2^m}$ in some order. An example of such arrangement is given in (14). Rearrange all words with $s \neq 0$ in descending order of elements, and words with $s=0$, in ascending order. We call the obtained PRF codes $\mathcal{C}_s$-codes.
2. Compose the code $\mathcal{C}=\mathcal{C}_0 \cup \mathcal{C}_1$. By the construction, this code has distance 2. Set $s'=2$.
3. Obtain a code $\mathcal{C}_{s'}^*$ by permuting every word of the code $\mathcal{C}_{s'}$ in one and the same way. Examples of such permutations include cyclic shifts and swapping some (fixed for a given s') pairs of elements. By using the trial and error method, find operations that provide distance 2 in the combined code $\mathcal{C} \cup \mathcal{C}_{s'}^*$. Set $\mathcal{C}=\mathcal{C}\cup\mathcal{C}_{s'}^*$. If no such operations exist, the code $\mathcal{C}$ is not changed.
4. If $s'=2^m-1$, exit the algorithm. Otherwise, set $s'=s'+1$ and go to Step 3.

The efficiency of Algorithm B is illustrated in Section 4.2, where we construct a practically interesting maximal $(4,M,2)_8^{\mathrm{PRF}}$ code with cardinality $M=\binom{8}{4}$ (see Example 1). In this example, all permutations providing distance 2 in the combined code $\mathcal{C}\cup\mathcal{C}_{s'}^*$ are found for each s'.

The following greedy algorithm is also helpful.

Algorithm C. Constructing a PF or PRF code with a “good” distance spectrum.

Denote the desired $(n,M,2)_{2^m}^{\mathrm{PF}}$ or $(n,M,2)_{2^m}^{\mathrm{PRF}}$ code by $\mathcal{V}$.

1. If a PF code is constructed, find all orbits of the group S_n in the space $\mathbb{F}_{2^m}^n$ (this can be done by enumerating all combinations of 2^m things n at a time with repetitions). If a PRF code is constructed, find all RF orbits of the group S_n in the space $\mathbb{F}_{2^m}^n$ (this can be done by enumerating all combinations of 2^m things n at a time without repetitions). Let $O_1,O_2,\ldots,O_{M_0}$ denote the constructed orbits, where $M_0=\binom{2^m+n-1}{n}$ for a PF code and $M_0=\binom{2^m}{n}$ for a PRF code. Let $O_i=\{c_{i,1},c_{i,2},\ldots,c_{i,|O_i|}\}$, where $c_{i,j}$ is an n-dimensional vector from the orbit O_i.
2. Arbitrarily choose a vector $c_{1,j}$ in the orbit O_1 and set
$$\mathcal{V}=\{v_1\},\qquad v_1=c_{1,j},\qquad M=1,\qquad i=2.$$
3. For *each* vector $c_{i,j}$ in an orbit O_i compute the spectrum of distances between $c_{i,j}$ and all words of the code $\mathcal{V}=\{v_1,v_2,\ldots,v_M\}$ constructed at previous steps:
$$\operatorname{spec}(c_{i,j},\mathcal{V})=(s_1,s_2,\ldots,s_n),\quad s_u=|\{k:\ v_k\in\mathcal{V},\ d(c_{i,j},v_k)=u\}|,$$
where $d(c,v)$ is the Hamming distance between c and v.

4. If there is no spectrum $\operatorname{spec}(c_{i,j}, \mathcal{V})$ such that $s_1 = 0$, set $i = i + 1$ and go to Step 6 (in this case the generator of the orbit O_i is not included in the code $\mathcal{V}$). If a spectrum with $s_1 = 0$ exists, go to Step 5.
5. Select all vectors $c_{i,j}$ whose distance spectrum satisfies $s_1 = 0$. From them, select a vector with the smallest s_2. If there are several such vectors, select the one with the smallest s_3, and so on, up to s_n. If there are still several vectors left, choose one at random. Denote the chosen vector by $c_{i,t}$. Set
$$M = M + 1, \qquad v_M = c_{i,t}, \qquad \mathcal{V} = \mathcal{V} \cup \{v_M\}, \qquad i = i + 1.$$
Go to Step 6.
6. If $i > M_0$, exit the algorithm. Otherwise, go to Step 3.

Performance of Algorithm C is illustrated in Section 4.2, where we construct a $(4, 70, 2)_8^{\mathrm{PRF}}$ code in Example 2 with better distance spectrum than that in Example 1. In this example for every orbit there exists a vector $c_{i,j}$ whose spectrum has $s_1 = 0$. That is why the code $\mathcal{V}$ is maximal.

Basically, an $(n, M, 2)_{2^m}^{\mathrm{PF}}$ code can have larger cardinality than an $(n, M, 2)_{2^m}^{\mathrm{PRF}}$ code, since constraints on PF are looser. For constructing a PF code as a subset of the space $\mathbb{F}_{2^m}^n$, we can take a PRF code obtained by algorithm B or C as a basis. Then we can append generators of orbits with repetitions that preserve code distance 2.

Efficiency of this technique is shown in Section 4.2, where we build a $(4, M, 2)_8^{\mathrm{PF}}$ code with cardinality 114, while the maximum cardinality of a $(4, M, 2)_8^{\mathrm{PRF}}$ code is 70.

4. EXAMPLES OF $(n, M, 2)_8^{\mathrm{PF}}$ AND $(n, M, 2)_8^{\mathrm{PRF}}$ CODE CONSTRUCTIONS

In this section we assume $n = 4$ or $n = 8$ and $m = 3$.

4.1. Codes $(n, M, 2)_8^{\mathrm{PF}}$ and $(n, M, 2)_8^{\mathrm{PRF}}$ as Subcodes of an $[n, n-1, 2]_8$ RS Code

In Theorems 3 and 4 we use algorithm A (see Section 3.4).

Theorem 3. (i) *Consider the orbits O_1, O_2, and O_3 given in Table* 1. *The symmetric group S_4 partitions the $[4, 3, 2]_8$ RS code into* 50 *separate $(4, 0)_8$-orbits*: 14 *RF orbits O_1*, 8 *orbits O_2, and* 28 *orbits O_3 with $p = 2$.*

(ii) *A maximal PF subcode of the $[4, 3, 2]_8$ RS code consists of* 50 *words*; *i.e.*,
$$\overline{M}_8^{\mathrm{PF}}(4, 2) = 50.$$

(iii) *A maximal PRF subcode of the $[4, 3, 2]_8$ RS code contains $N_{4,8}^{(0)} = \frac{1}{4}\binom{8}{3}$ words*:
$$\overline{M}_8^{\mathrm{PRF}}(4, 2) = 14.$$

Proof. In (i) and (ii) we use algorithm A.

(i) The numbers and lengths of orbits are indicated in Table 1. We set $J_4 = \{1, 2, 3\}$. For $N_{4,8}^{(0)}$ we use Lemma 13 (i). Taking the lengths of the orbits stated in Table 1 into account, we deduce that 50 orbits contain $\Sigma = \sum\limits_{j=1}^{3} N_{O_j}|O_j| = 8^3$ codewords, i.e., the entire $[4, 3, 2]_8$ RS code.

(ii) According to Theorem 1 (i), a maximal PF subcode contains precisely one word from each code orbit regardless of its structure.

(iii) This follows from Theorem 2 and Lemma 13 (i). △

Theorem 4. (i) *Consider the orbits* O_1–O_9 *and* O_{8+t} *defined in Table* 1. *The symmetric group* S_8 *partitions the* $[8,7,2]_8$ *RS code into* 835 $(8,0)_8$*-orbits: one RF orbit* O_1, 8 *orbits* O_2, 28 *orbits* O_3, 70 *orbits* O_4, 56 *orbits* O_5, 56 *orbits* O_6, 84 *orbits* O_7, 84 *orbits* O_8, 224 *orbits* O_9, 168 *orbits* O_{8+2}, *and* 56 *orbits* O_{8+3}. *Here for all orbits with parameter* p *we set* $p=4$.

(ii) *A maximal PF subcode of the* $[8,7,2]_8$ *RS code contains* 835 *words*; *i.e.*,

$$\overline{M}_8^{\rm PF}(8,2)=835.$$

(iii) *A maximal PRF subcode of the* $[8,7,2]_8$ *RS code contains one word and is also a maximal* $(8,M,2)_8^{\rm PRF}$ *code*; *i.e.*,

$$\overline{M}_8^{\rm PRF}(8,2)=M_8^{\rm PRF}(8,2)=1.$$

Proof. In (i) and (ii) we use algorithm A.

(i) The numbers and lengths of orbits are given in Table 1. We set $J_8=\{1,2,\dots,11\}$. For $N_{8,8}^{(0)}$ we use (29); see the Appendix. Taking into account the orbit lengths from Table 1, we find that 835 orbits contain $\Sigma=\sum\limits_{j=1}^{11}N_{O_j}|O_j|=8^7$ codewords, i.e., the entire $[8,7,2]_8$ RS code.

(ii) According to Theorem 1 (i), a maximal PF subcode contains one word from each code orbit regardless of its structure.

(iii) Use Corollaries 4 and 5. △

4.2. Codes $(n,M,2)_8^{\rm PF}$ *and* $(n,M,2)_8^{\rm PRF}$ *as Subsets of the Space* $\mathbb{F}_8^n$

Maximal $(4,70,2)_8^{\rm PRF}$ code

Example 1. To construct a maximal $(4,70,2)_8^{\rm PRF}$ code, we use algorithm B (see Section 3.5).

By Lemma 13 (i) we have $N_{4,8}^{(0)}=14$. By Corollary 6 and Lemma 14 (see the Appendix), we have $N_{4,8}^{(s)}=8$ for all $s\neq0$.

The codes $\mathcal{C}_0$ and $\mathcal{C}_1$ have the following form:

$$\mathcal{C}_0=\{0123,0145,0167,0246,0257,0347,0356,1247,1256,1346,1357,2345,2367,4567\},$$
$$\mathcal{C}_1=\{7530,7521,7431,7420,6531,6520,6430,6421\}.$$

The codes $\mathcal{C}_{s'}^*$ have the following form:

$$\begin{aligned}
\mathcal{C}_2^*&=\{7261,7360,7342,7140,6352,6150,5241,5340\},\\
\mathcal{C}_3^*&=\{7136,7026,7235,7015,6234,6014,5024,5134\},\\
\mathcal{C}_4^*&=\{6507,6417,5427,2107,5436,3106,3205,3214\},\\
\mathcal{C}_5^*&=\{1765,0764,3754,0731,2654,0621,1532,0432\},\\
\mathcal{C}_6^*&=\{5276,4376,4075,2073,4165,2163,1052,1043\},\\
\mathcal{C}_7^*&=\{6735,6724,5714,3712,5604,3602,3501,2401\}.
\end{aligned}$$

To obtain the codes $\mathcal{C}_{s'}^*$ from $\mathcal{C}_{s'}$, we used the following permutations:

$s'=2$ → swap the 2nd and 3rd elements,
$s'=3$ → swap the 2nd and 4th elements,
$s'=4$ → cyclic left shift by one position,
$s'=5$ → cyclic right shift by one position,
$s'=6$ → cyclic right shift by two positions,
$s'=7$ → swap the 1st and 2nd elements, then swap the 3rd and 4th elements.

Table 2. Some orbits of the group S_4 in the space $\mathbb{F}_8^4$

Orbit	Nonzero components of the orbit structure	Orbit generator	Number of orbits	Orbit length
$O_{aaab}^{(s)}$	$V_0 = 6$, $V_1 = 1$, $V_3 = 1$	(a, a, a, b), $a + b = s$, $s \neq 0$	8	4
$O_{aabb}^{(\delta)}$	$V_0 = 6$, $V_2 = 1$	(a, a, b, b), $a + b = \delta$, $\delta \neq 0$	4	6

The distance of 2 for the combined code $\mathcal{C} \cup \mathcal{C}_{s'}^*$ in each iteration of Step 3 of Algorithm B with $s' = 2, 3, \ldots, 7$ was checked on a computer.

The desired $(4, M, 2)_8^{\mathrm{PRF}}$ code is of the form $\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \bigcup\limits_{s'=2}^{7} \mathcal{C}_{s'}^*$. Its cardinality is $M = 14 + 7 \cdot 8 = 70$.

Example 2. Another instance of a $(4, 70, 2)_8^{\mathrm{PRF}}$ code, code $\mathcal{V}$, was obtained on a computer by using Algorithm C (see Section 3.5):

$$\begin{aligned}\mathcal{V} = \{&3210, 4102, 5021, 2601, 1720, 0314, 1053, 0136, 1307, 0541, 6140, 4017, 1065, 7510,\\ &6701, 2430, 5203, 0623, 3072, 0452, 2046, 7204, 0265, 2570, 7026, 4350, 6034, 3407,\\ &5630, 0375, 0763, 4506, 7405, 0647, 5760, 3124, 1532, 6312, 2173, 4251, 1246, 2714,\\ &6125, 2157, 7162, 5413, 3461, 7341, 3615, 5371, 1673, 1564, 4715, 1476, 7651, 4523,\\ &6243, 3742, 5326, 5237, 2367, 5642, 4275, 6427, 2756, 3654, 3547, 4736, 7635, 6574\}.\end{aligned}$$

Let $D = \{d_1, d_2, \ldots, d_n\}$ denote the distance spectrum of an (n, M, d) code, where d_i is the number of occurrences of distance i between codewords. Obviously, $d_i = 0$ for $i < d$.

Theorem 5. *Codes* $(4, 70, 2)_8^{\mathrm{PRF}}$ *given in Examples* 1 *and* 2 *are maximal PRF codes*; *i.e.*,

$$M_8^{\mathrm{PRF}}(4, 2) = 70.$$

Distance spectra of these code are as follows: $D = \{0, 234, 712, 1469\}$ *for Example* 1 *and* $D = \{0, 95, 900, 1420\}$ *for Example* 2.

Proof. According to Corollary 4, these codes $\mathcal{C}$ have the maximum cardinality. Distance spectra were computed directly. △

Code $(4, 114, 2)_8^{\mathrm{PF}}$

Lemma 7. *In the space* $\mathbb{F}_8^4$ *there exist orbits of the group* S_4 *mentioned in Table* 2.

Proof. Lengths of the orbits result from (8). An element a for an orbit $O_{aaab}^{(s)}$ can be chosen arbitrarily. Thus, there are eight such orbits. Given any nonzero δ in the field $\mathbb{F}_8$, there are four different pairs of elements a, b for which $a + b = \delta$. Hence, there are four orbits $O_{aabb}^{(\delta)}$. △

Lemma 8. *Given any nonzero* $s \in \mathbb{F}_8$, *the distance between any two words of the set* $\bigcup\limits_{a=0}^{7} O_{aaab}^{(s)}$ *is at least* 2.

Proof. The set $\bigcup\limits_{a=0}^{7} O_{aaab}^{(s)}$ is embedded in a coset of a $[4, 3, 2]_8$ RS code with generator $(0, 0, 0, s)$. △

Lemma 9. *For any set of nonzero elements* $\delta_j \in \mathbb{F}_8$, *the distance between any two words of the set* $\bigcup\limits_{j}\bigcup\limits_{i} O_{a_i a_i b_i b_i}^{(\delta_j)}$ *is at least* 2.

Proof. The set $\bigcup\limits_{j}\bigcup\limits_{i} O_{a_i a_i b_i b_i}^{(\delta_j)}$ is embedded in a $[4, 3, 2]_8$ RS code. △

Construction D. Write the nonzero elements of $\mathbb{F}_8$ as follows: $\{s_1, s_2, s_3, s_4, \delta_1, \delta_2, \delta_3\}$. Let $\mathcal{C}$ be a set of cardinality 70 obtained in Example 1. We construct four sets T_j of cardinality 8:

$$T_1 = \bigcup_{a_i=0}^{7} b_{1,i}a_ia_ia_i, \qquad T_2 = \bigcup_{a_i=0}^{7} a_ib_{2,i}a_ia_i, \qquad T_3 = \bigcup_{a_i=0}^{7} a_ia_ib_{3,i}a_i, \qquad T_4 = \bigcup_{a_i=0}^{7} a_ia_ia_ib_{4,i},$$
$$b_{j,i} = a_i + s_j, \quad j = 1,2,3,4, \quad i = 0,1,\ldots,7.$$

For every nonzero element δ_k, we write four elements $\{a_{k,1}, a_{k,2}, a_{k,3}, a_{k,4}\}$ of the field for which $a_{k,u} \neq a_{k,v} + \delta_k$ if $u \neq v$. Then we construct three sets D_k of cardinality 4:

$$D_k = \bigcup_{h=1}^{4} a_{k,h}a_{k,h}b_{k,h}b_{k,h}, \quad b_{k,h} = a_{k,h} + \delta_k, \quad k = 1,2,3.$$

We will construct a $(4,114,2)_8$ code $\mathcal{U}$ in the following way:

$$\mathcal{U} = \mathcal{C} \cup \bigcup_{j=1}^{4} T_j \cup \bigcup_{k=1}^{3} D_k.$$

Theorem 6. (i) *The code $\mathcal{U}$ of Construction D is a $(4,114,2)_8^{\mathrm{PF}}$ code.*

(ii) *We have the estimate*

$$M_8^{\mathrm{PF}}(4,2) \geq 114. \tag{17}$$

Proof. The code cardinality of 114 directly follows from the construction. The PF property is based on Lemma 2. From Theorem 5 and Lemmas 8 and 9 we obtain the minimum distance of 2 inside the following subsets of the code: $\mathcal{C}$, T_j, and $\bigcup\limits_{k=1}^{3} D_k$.

The minimum distance of 2 between the subsets directly follows from their structure. In particular, since each word of the subset $\mathcal{C}$ contains no repeated elements, and words of T_j and D_k contain only two different elements, the distance between $\mathcal{C}$ and T_j and between $\mathcal{C}$ and D_k is at least 2. The distance between words of different subsets T_j, e.g., between words $b_{1,i}a_ia_ia_i$ and $a_ib_{2,i}a_ia_i$, is also at least 2, even if the elements a_i coincide. Finally, since $s_j \neq \delta_k$, $s_j, \delta_k \neq 0$, $b_{1,i} = a_i + s_1$, and $b_{k,h} = a_{k,h} + \delta_k$, the distance between words of the subsets T_j and D_k, e.g., $b_{1,i}a_ia_ia_i$ and $a_{k,h}a_{k,h}b_{k,h}b_{k,h}$, is at least 2. Indeed, if $b_{k,h} = a_i$, then $a_{k,h} \neq a_i$ and $a_{k,h} = b_{k,h} + \delta_k \neq a_i + s_1 = b_{1,i}$.

Existence of this code implies estimate (17). △

5. PRF CODE WITH SIGN MANIPULATION

Now we introduce one more coded modulation scheme, which is a modification of the proposed PRF codes.

Let $\boldsymbol{h}_{i_1}$ and $\boldsymbol{h}_{i_2}$ denote distinct columns of an Hadamard matrix. Then we have the following:

- The columns $\boldsymbol{h}_{i_1}$ and $-\boldsymbol{h}_{i_2}$ are orthogonal, and the squared Euclidean distance between them is

$$d_E^2(\boldsymbol{h}_{i_1}, -\boldsymbol{h}_{i_2}) = \frac{L}{2} \cdot 2^2 + \frac{L}{2} \cdot 0^2 = 2L.$$

- The columns $\boldsymbol{h}_{i_1}$ and $-\boldsymbol{h}_{i_1}$ are not orthogonal, $\boldsymbol{h}_{i_1}^T \times -\boldsymbol{h}_{i_1} = -L$, and the squared Euclidean distance between them is $d_E^2(\boldsymbol{h}_{i_1}, -\boldsymbol{h}_{i_1}) = L \cdot 2^2 = 4L$.

Choose some PRF code $\mathcal{S}$, whose words are composed of columns of an Hadamard matrix (see Section 3 for construction algorithms). Let the transmitted information be represented by a natural number $a \leq |\mathcal{S}|$ and a vector $\boldsymbol{b} = (b_1, \ldots, b_{N_T})$, $b_i = \pm 1$. Let us describe the encoding procedure.

Choose a word $\boldsymbol{S}_a \in \mathcal{S}$. The encoding result is the matrix

$$\overline{\boldsymbol{S}}_{\boldsymbol{ab}} = \boldsymbol{S}_a \mathrm{diag}(b_1, \ldots, b_{N_T}).$$

We call the code $\overline{\mathcal{S}}$ whose words are matrices $\overline{\boldsymbol{S}}_{\boldsymbol{ab}}$ a PRF code with sign manipulation. This code satisfies constraint (3), which can be proved analogously to the proof of Lemma 1. Here the matrix $\frac{1}{L}\boldsymbol{H}^T\overline{\boldsymbol{S}}_{\boldsymbol{ab}}$ is composed of elements $0, 1, -1$ and contains exactly one nonzero element in each column.

Formally, the rate of a PRF code with sign manipulation can be greater than 1. The cardinality of the code $\overline{\mathcal{S}}$ is 2^{N_T} times as large as the cardinality of the original PRF code.

Note that if we change the decodability constraint (3) into a stricter one that secures the transmission if $\exists j : \ a_j \neq 0$, then codes with rates above 1 cannot exist. This can easily be proved by regarding this state of the channel as a usual SISO (single input, single output) channel.

Constructing PF codes with sign manipulation is also possible, but this is more complicated due to impossibility of independent change of signs of identical columns.

6. DECODING

We use the maximum likelihood decoding technique. First, we compute the values of the likelihood function at all possible codewords $\boldsymbol{S}$. Then we apply the map $\mathcal{L}$ and compute the likelihood function for all codewords $\boldsymbol{c}$. Thus we get a soft decoder.

Let us construct the likelihood function:

$$\mathbf{P}(s_i^t \,|\, \alpha_{ij}, r_j^t) = \frac{\mathbf{P}(s_i^t \,|\, \alpha_{ij})}{\mathbf{P}(r_j^t \,|\, \alpha_{ij})}\, \mathbf{P}(r_j^t \,|\, \alpha_{ij}, s_i^t) = \mathrm{const} \cdot \mathbf{P}\left(\eta_j^t = r_j^t - \sum_{i=0}^{N_T} \alpha_{ij} s_i^t\right).$$

The probability density function is

$$p(s_i^t \,|\, \alpha_{ij}, r_j^t) = \mathrm{const} \cdot \exp\left(\frac{\left|r_j^t - \sum\limits_{i=0}^{N_T} \alpha_{ij} s_i^t\right|^2}{2\sigma^2}\right) = \mathrm{const} \cdot \exp\left(\frac{f(s_i^t \,|\, \alpha_{ij}, r_j^t)}{2\sigma^2}\right),$$
$$f(s_i^t \,|\, \alpha_{ij}, r_j^t) = \sum_{j=0}^{N_R} \sum_{t=0}^{L} \left| r_j^t - \sum_{i=0}^{N_T} \alpha_{ij} s_i^t \right|^2. \tag{18}$$

As we have shown above, all columns of a PRF code are orthogonal; i.e., $\sum\limits_{t=1}^{L} s_i^t s_j^t = L\delta_{ij}$, where δ_{ij} is the Kronecker operator. Therefore, we can use the approach described in [3] and rewrite (18) in the following form:

$$f(s_i^t \,|\, \alpha_{ij}, r_j^t) = \sum_{i=0}^{N_T} \sum_{t=0}^{L} \left(\left| s_i^t - \sum_{j=0}^{N_R} \alpha_{ij}^* r_j^t \right|^2 + \left(-1 + \sum_{j=0}^{N_T} |\alpha_{ij}|^2\right) |s_i^t|^2 \right) + \mathrm{const}.$$

Since s_i^t are elements of an Hadamard matrix, we have $|s_i^t| = 1$. The expression in the inner brackets does not depend on s_i^t, and the likelihood function takes the form

$$f(s_i^t \,|\, \alpha_{ij}, r_j^t) = \sum_{i=0}^{N_T} \sum_{t=0}^{L} \left| s_i^t - \sum_{j=0}^{N_R} \alpha_{ij}^* r_j^t \right|^2 + \mathrm{const}, \tag{19}$$

where x^* is the complex conjugation operator.

Having applied the map $\mathcal{L}(s_i^t)$, we obtain the likelihood value $f(\boldsymbol{c})$ for all elements of $\mathbb{F}_L^{N_T}$. Moreover, for a PRF code we can compute the likelihood for any particular element of $\mathbb{F}_L$, i.e., for each symbol of the codeword. This allows us to use efficient decoding methods developed for q-ary symmetric channels that dot not take into account specific peculiarities of the data transmission. Here we can use iterative error-correction algorithms, but we do not consider them in this paper.

In the case of PRF codes with sign manipulation, the above procedure changes only a little. Equation (19) takes the form

$$f(s_i^t, b_i \,|\, \alpha_{ij}, r_j^t) = \sum_{i=0}^{N_T} \sum_{t=0}^{L} \left| s_i^t b_i - \sum_{j=0}^{N_R} \alpha_{ij}^* r_j^t \right|^2 + \text{const.} \tag{20}$$

7. ESTIMATION OF THE ERROR-CORRECTION CAPABILITY BY SIMULATION

To estimate the error-correction capability of the proposed coded modulation, we developed a simulation model in MATLAB Simulink.

A channel was defined by equation (1). The signal-to-noise ratio varied from 0 to 30 dB with step 1. The maximum likelihood decoding was utilized. We used $N_T = 4$ transmitting antennas and $N_R = 1, 2, 4$ receiving antennas. The code length was $L = 8$. We tested two codes: a PF code of cardinality 256 and a PRF code of cardinality 64. They are subcodes of codes obtained by the greedy algorithm (Algorithm C): respectively, of a PF code of cardinality 281 and PRF code of cardinality 70 (see Example 2 in Section 4.2). The rates of the PF code of cardinality 256 and PRF code of cardinality 64 are 1 and 0.75, respectively. Simulation halted after reaching 1000 erroneous bits or 1 000 000 code bits, whichever happens the first.

The obtained results are plotted in the figures below.

To simplify the analysis, we introduce the concept of effective diversity order. Recall that the diversity order in a MIMO communication system is $N_R N_T$. The error-correction capability in a MIMO communication system without coding that performs the maximum likelihood demodulation is said to be optimal for a given diversity order. Codes that reach the optimal error-correction capability are called optimal. If the error-correction capability of a code is equal to that of an optimal code of diversity order D, we say that the effective diversity order of this code is D.

In Fig. 1, solid lines denote theoretical curves for optimal STBC (space-time block) codes given in [3]. Their diversity orders are $1, 2, 4, 8, 16$, from top to bottom. Stars denote simulation results for PRF codes. From top to bottom: $N_R = 1, 2, 4$ and, respectively, the diversity order is $4, 8, 16$.

Let us estimate the effective diversity order of the PRF codes using the plot: for $N_R = 1$ and $N_R = 2$ the effective diversity order of the PRF code is half the optimal. But for $N_R = 4$, the PRF code is optimal. Thus, we may conclude that the error-correction capability of the PRF codes strongly depends on the number of receiving antennas and is in some cases optimal. The rate of the PRF codes is below 1. The advantage of the PRF codes is existence of a construction algorithm for any given L and N_T.

In Fig. 2, stars denote simulation results for a PRF code, and triangles, for a PF code. From top to bottom: $N_R = 1, 2, 4$. The plot shows that the error-correction capability of the PRF code is better than that of the PF code, but as the number of receiving antennas increases, this difference becomes smaller.

The notation in Fig. 3 is the same as in the preceding plots. The effective diversity order of the PF code is half the optimal. For $N_R = 4$, it becomes a little greater. Thus, the error-correction capability of the PF code is lower than the optimal, but the code has fast construction algorithms for arbitrary values of L and N_T.

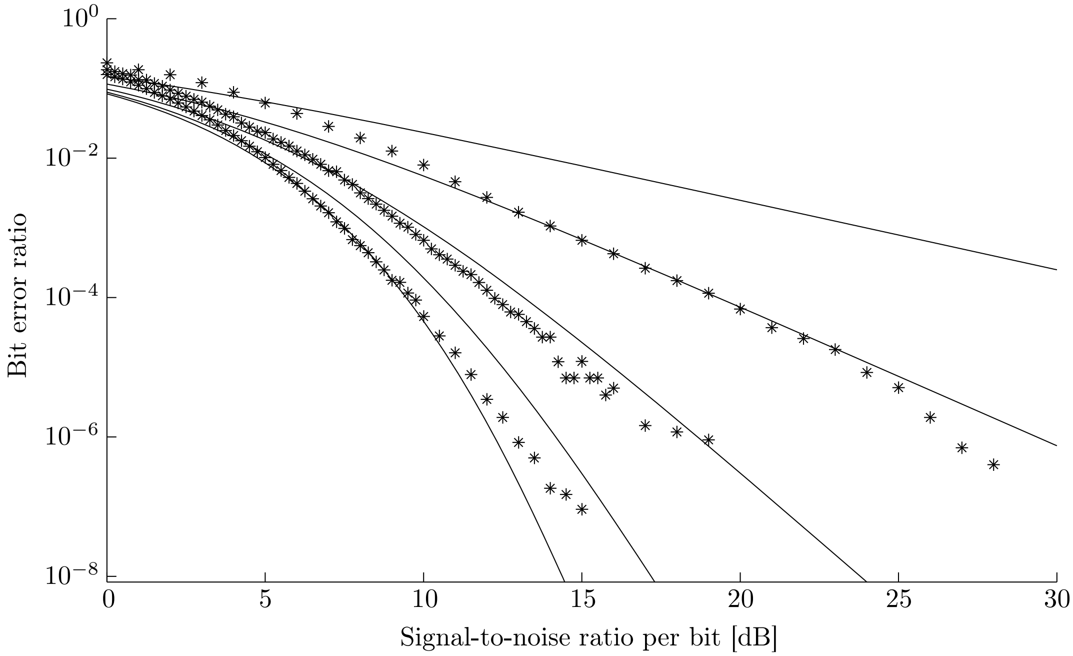

Fig. 1. Simulation results: comparison of PRF and optimal codes.

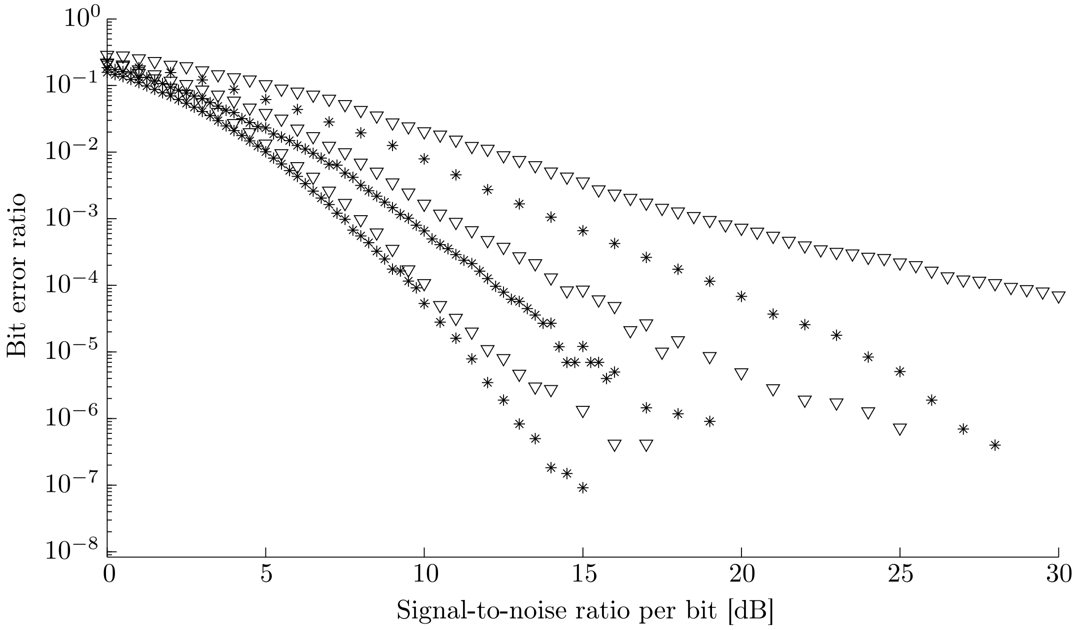

Fig. 2. Simulation results: comparison of PF and PRF codes.

Figure 4 shows a change in the error-correction capability of the PRF code when using sign manipulation in the case of $L = 8$ and $N_R = 4$. Stars denote simulation result for the PRF code, and circles, for the PRF code with sign manipulation. The theoretical curve corresponds to the diversity order of 16. The initial PRF code is constructed by Algorithm C and has the rate of 3/4. Adding sign manipulation increases the code rate up to 5/4. Existence of codes with rates above 1 is possible because of using several transmitting antennas and due to constraint (3). The error-correction capability decreases with increasing code rate, and in the presented case the loss amounts to 1 dB only. For other channel parameters, the loss was found to be higher: from 2 to 4 dB.

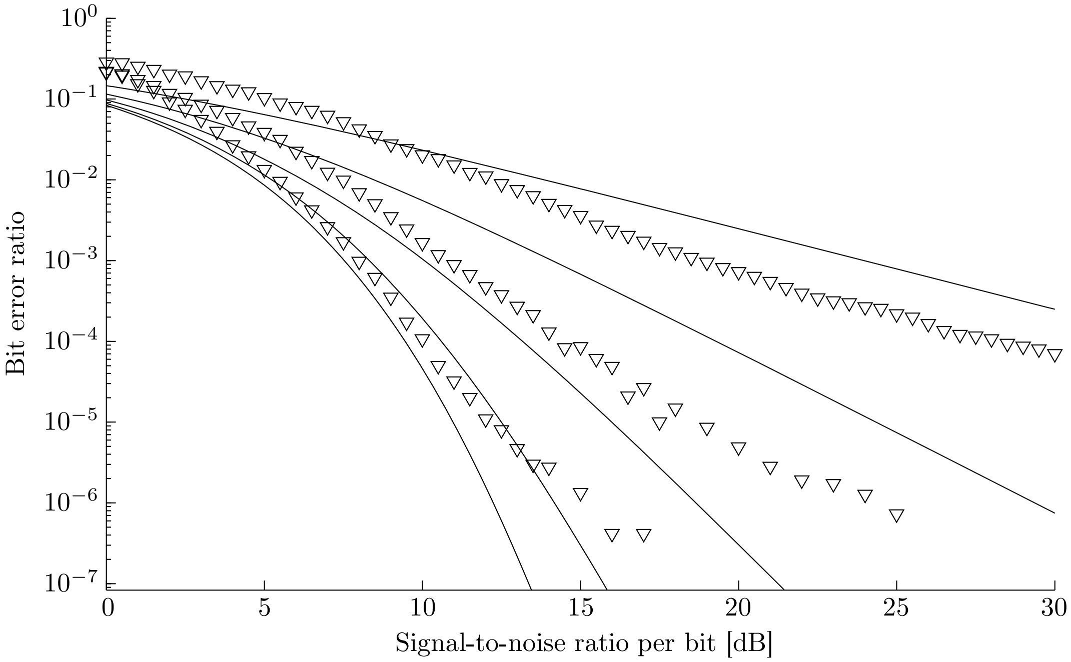

Fig. 3. Simulation results: comparison of PF and optimal codes.

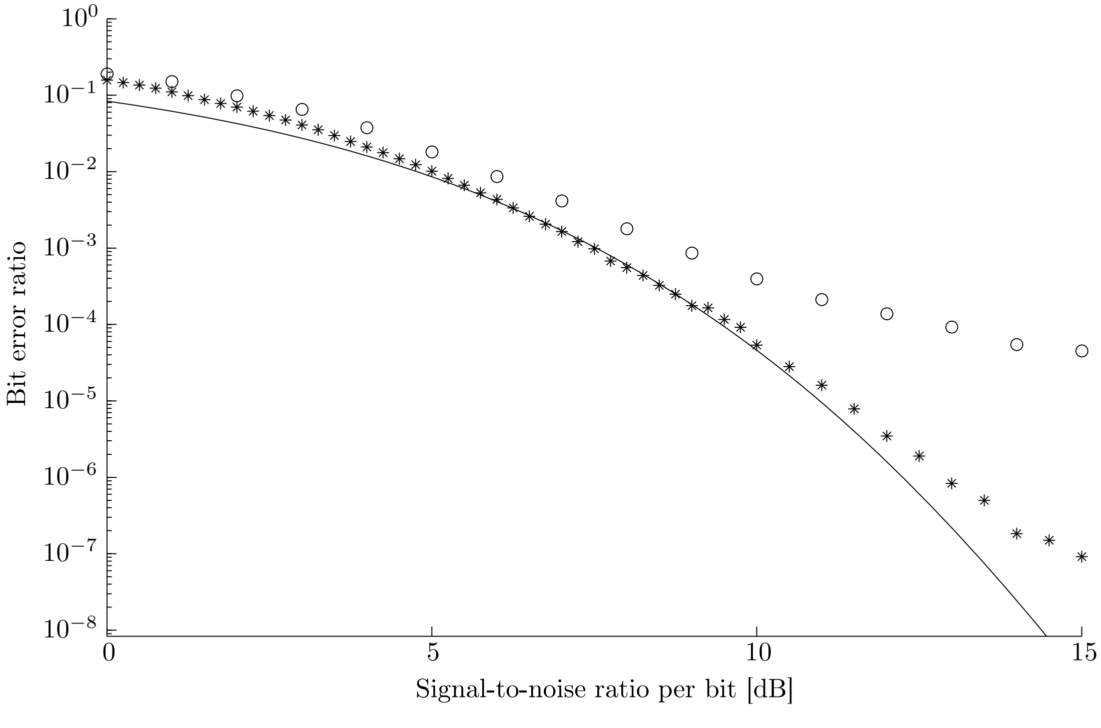

Fig. 4. Estimation of the error-correction capability of a PRF code with sign manipulation.

8. CONCLUSION

In this paper we proposed new coded modulation, which uses a system of orthogonal vectors to pass to codes in the space $\mathbb{F}_L^{N_T}$. We stated a decodability constraint and proposed a PRF code satisfying this constraint. Then we built a mathematical model for PF and PRF codes. With its aid, we obtained some estimates for the cardinality of the codes and proposed construction algorithms for them. We built PF and PRF codes of relatively high (in several cases, maximum) cardinality.

In the Simulink environment, we conducted simulation for the proposed coded modulation scheme in a Rayleigh channel which is quasi-stationary during transmission of one block, with a receiver having exact knowledge on the channel state. The results showed the advantage of the PRF codes over the PF codes, as well as high error-correction capability in the case of sufficiently many receiving antennas.

APPENDIX

Subsets of the field $\mathbb{F}_{2^m}$ with a fixed sum of elements. We use the notation of Sections 3.1 and 3.3. The field $\mathbb{F}_{2^m}$ is represented in the form (14).

Lemma 10. *Consider the* $[2^m-1, 2^m-1-m, 3]_2$ *Hamming code.*

(i) *To each codeword of weight w, the following two RF subsets of the field $\mathbb{F}_{2^m}$ correspond: a $(w,0)^{\mathrm{RF}}_{2^m}$-subset consisting of nonzero elements and a $(w+1,0)^{\mathrm{RF}}_{2^m}$-subset containing the zero element. There is a one-to-one correspondence between sets of all codewords of weights w and $w-1$ and all $(w,0)^{\mathrm{RF}}_{2^m}$-subsets.*

(ii) *Consider a coset of the code with a syndrome $s \neq 0$. To each word of weight w of the coset, the following two RF subsets of $\mathbb{F}_{2^m}$ correspond: a $(w,s)^{\mathrm{RF}}_{2^m}$-subset consisting of nonzero elements and a $(w+1,s)^{\mathrm{RF}}_{2^m}$-subset containing the zero element. There is a one-to-one correspondence between sets of all words of weights w and $w-1$ in the coset and all $(w,s)^{\mathrm{RF}}_{2^m}$-subsets.*

Proof. The parity-check matrix of the code consists of all different *nonzero* binary m-position *columns*, which can be treated as *elements* of the field $\mathbb{F}_{2^m}$ according to (14). The zero column (not contained in the matrix) corresponds to the zero element of $\mathbb{F}_{2^m}$.

(i) Every codeword of weight w corresponds to a set of w different nonzero columns whose sum is the zero column. One can add the zero column to the w-set to obtain a set of $w+1$ different columns with zero sum.

(ii) Consider a coset of the code with a nonzero m-position syndrome column, which can be treated as a nonzero element s of $\mathbb{F}_{2^m}$. Every word of weight w of the coset corresponds to a set of w different nonzero columns whose sum is s. One can add the zero column to the w-set to obtain a set of $w+1$ different columns with sum s.

By the construction, the correspondence between words and column sets specified in (i) and (ii) is one-to-one. △

Corollary 6. *Let* $3 \le w \le 2^m-1$.

(i) *We have*

$$N^{(0)}_{w,2^m} = A_{w-1,2^m} + A_{w,2^m}. \tag{21}$$

(ii) *For $s \neq 0$, the value $N^{(s)}_{w,2^m}$ does not depend on s. We have*

$$N^{(s)}_{w,2^m} = \overline{A}_{w-1,2^m} + \overline{A}_{w,2^m}, \quad s \neq 0. \tag{22}$$

Proof. Relations (21) and (22) follow from Lemma 10. Note also that all cosets of a binary Hamming code have the same weight spectrum [10, Section 6.6]. △

To compute the values $N^{(s)}_{w,2^m}$ by formulas (21) and (22), the following known relations for the weight spectrum of the binary $[2^m-1, 2^m-1-m, 3]_2$ Hamming code and its coset [10] are useful:

$$A_{0,2^m} = A_{2^m-1,2^m} = 1, \qquad A_{1,2^m} = A_{2,2^m} = A_{2^m-3,2^m} = A_{2^m-2,2^m} = 0, \tag{23}$$

$$A_{3,2^m} = \frac{1}{3}\binom{2^m-1}{2}, \qquad A_{4,2^m} = \frac{2^m-4}{3\cdot 4}\binom{2^m-1}{2} = \frac{1}{2^m-3}\binom{2^m-1}{4}, \tag{24}$$

$$wA_{w,2^m} + A_{w-1,2^m} + (2^m - w + 1)A_{w-2,2^m} = \binom{2^m-1}{w-1}, \tag{25}$$

$$\overline{A}_{w,2^m} = \frac{1}{2^m-1}\left(\binom{2^m-1}{w} - A_{w,2^m}\right). \tag{26}$$

From (23)–(26) it follows that

$$\overline{A}_{0,2^m} = \overline{A}_{2^m-1,2^m} = 0, \qquad \overline{A}_{1,2^m} = \overline{A}_{2^m-2,2^m} = 1, \qquad \overline{A}_{2,2^m} = \overline{A}_{2^m-3,2^m} = 2^{m-1}-1, \tag{27}$$

$$\overline{A}_{3,2^m} = \frac{(2^m-4)(2^{m-1}-1)}{3}, \qquad \overline{A}_{4,2^m} = \frac{(2^{m-1}-1)(2^m-4)^2}{3\cdot 4}. \tag{28}$$

Lemma 11. *We have the following equalities*:

$$\begin{gathered} N^{(0)}_{1,2^m} = N^{(0)}_{2^m,2^m} = N^{(0)}_{2^m-1,2^m} = N^{(s)}_{1,2^m} = N^{(s)}_{2^m-1,2^m} = 1, \quad s \neq 0, \\ N^{(0)}_{2,2^m} = N^{(0)}_{2^m-2,2^m} = N^{(s)}_{2^m,2^m} = 0, \quad s \neq 0, \\ N^{(s)}_{2,2^m} = N^{(s)}_{2^m-2,2^m} = 2^{m-1}, \quad s \neq 0. \end{gathered} \tag{29}$$

Proof. Use relations (23) and (27) and the following facts: the sum of all elements of a filed is zero; the sum of two different elements of $\mathbb{F}_{2^m}$ is nonzero. △

Lemma 12. *Let $n \le 2^m$. For all $s = 0, 1, \dots, 2^m-1$, let all possible $(n,s)^{\mathrm{RF}}_{2^m}$-subsets of $\mathbb{F}_{2^m}$ be constructed by the methods of Lemma* 10. *Arrange each $(n,s)^{\mathrm{RF}}_{2^m}$-subset in an arbitrary order*, *transforming it into an $(n,s)^{\mathrm{RF}}_{2^m}$-vector of $\mathbb{F}^n_{2^m}$. Then for a fixed s, all the obtained $(n,s)^{\mathrm{RF}}_{2^m}$-vectors form an $(n, N^{(s)}_{n,2^m}, 2)^{\mathrm{PRF}}_{2^m}$ code embedded in either the $[n, n-1, 2]_{2^m}$ RS code* (*if* $s = 0$) *or a coset of this code with syndrome $s \neq 0$.*

Proof. Use Lemma 5. Note also that minimum distance of any coset of an $[n, n-1, 2]_{2^m}$ RS code is 2. △

Lemma 13. *Consider the field $\mathbb{F}_{2^m}$ and quadruples $\{a, b, c, d\}$ of different field elements with zero sum*, $a + b + c + d = 0$. *Then*

(i) *In total there are $N^{(0)}_{4,2^m}$ quadruples*, *where*

$$N^{(0)}_{4,2^m} = \frac{1}{4}\binom{2^m}{3}.$$

(ii) *Each element of the field $\mathbb{F}_{2^m}$ is contained in $\frac{1}{3}\binom{2^m-1}{2}$ quadruples and is not contained in $\frac{1}{2^m-3}\binom{2^m-1}{4}$ quadruples.*

(iii) *Each pair a, b of elements of the field is completely contained in $2^{m-1}-1$ quadruples and has no intersection with $\frac{1}{3}\binom{2^m-1}{2}(2^{m-2}-2) + 2^{m-1} - 1$ quadruples. Furthermore*, *there are $\frac{1}{6}(2^m-2)(2^m-4)$ quadruples that contain a but do not contain b.*

Proof. (i) This follows from (21) and (24).

(ii) Fix an element a. To obtain a quadruple with zero sum, only two of three elements b, c, d can be taken arbitrarily. The number of ways to choose is $\binom{2^m-1}{2}$. Furthermore, one and the same quadruple can be obtained in three ways. Thus, exactly $\frac{1}{3}\binom{2^m-1}{2}$ quadruples with zero sum contain the element a. The other $N^{(0)}_{4,2^m} - \frac{1}{3}\binom{2^m-1}{2}$ quadruples do not contain this element.

(iii) Fix elements a and b. Only one of two elements c, d can be taken arbitrarily to obtain a quadruple with zero sum. The number of ways to choose is $2^m - 2$. Here the same quadruple is obtained in two ways. Thus, exactly $2^{m-1} - 1$ quadruples with zero sum contain the pair a, b.

By the above, the element a is contained in $\frac{1}{3}\binom{2^m-1}{2}$ quadruples, $2^{m-1} - 1$ of which contain also the element b. Hence, there are $\frac{1}{3}\binom{2^m-1}{2} - (2^{m-1} - 1)$ quadruples that contain a but do not contain b.

The remaining situation (i.e., no intersection) takes place for

$$N^{(0)}_{4,2^m} - 2\left(\frac{1}{3}\binom{2^m-1}{2} - (2^{m-1} - 1)\right) - (2^{m-1} - 1)$$

quadruples. △

Lemma 14. *Consider the field $\mathbb{F}_{2^m}$ and quadruples $\{a, b, c, d\}$ of different field elements with a nonzero sum $a + b + c + d = s$. In total there are $N^{(s)}_{4,2^m}$ such quadruples, where*

$$N^{(s)}_{4,2^m} = \frac{2^m(2^{m-2} - 1)(2^{m-1} - 1)}{3}, \quad s \neq 0.$$

Proof. This follows from (22) and (28). △

The authors are grateful to a reviewer for helpful comments.

REFERENCES

1. Proakis, J.G., *Digital Communications*, New York: McGraw-Hill, 1995, 3rd ed. Translated under the title *Tsifrovaya svyaz'*, Moscow: Radio i Svyaz', 2000.
2. Alamouti, S.M,. A Simple Transmit Diversity Technique for Wireless Communications, *IEEE J. Select. Areas Commun.*, 1998, vol. 16, no. 8, pp. 1451–1458.
3. Tarokh, V., Jafarkhani, H., and Calderbank, A.R., Space-Time Block Codes from Orthogonal Designs, *IEEE Trans. Inform. Theory*, 1999, vol. 45, no. 5, pp. 1456–1467.
4. Gesbert, D., Shafi, M., Shiu, D., Smith, P.J., and Naguib, A., From Theory to Practice: An Overview of MIMO Space-Time Coded Wireless Systems, *IEEE J. Select. Areas Commun.*, 2003, vol. 21, no. 3, pp. 281–302.
5. Lusina, P.J., Algerbaic Designs of Space Time Codes, *PhD Thesis*, Ulm, Germany: Univ. of Ulm, 2003.
6. Jafarkhani, H., *Space-Time Coding: Theory and Practice*, Cambridge: Cambridge Univ. Press, 2005.
7. Kreschuk, A.A., Code Construction for MIMO Systems Based on a Subset of Rows of an Hadamard Matrix, in *Proc. Conf. of Young Scientists and Engineers on Information Technologies and Systems (ITaS'10), Gelendzhik, Russia, 2010*, Moscow: Inst. Probl. Peredachi Inf. Ross. Akad. Nauk, 2010, pp. 104–107.
8. Davydov, A.A., Zyablov, V.V., and Kalimullin, R.E., Subcodes of Reed–Solomon Code with Special Properties, in *Proc. 12th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2010), Novosibirsk, Russia, 2010*, pp. 116–122.
9. Davydov, A.A., Zyablov, V.V., and Kalimullin, R.E., Special Sequences as Subcodes of Reed-Solomon Codes, *Probl. Peredachi Inf.*, 2010, vol. 46, no. 4, pp. 56–82 [*Probl. Inf. Trans.* (Engl. Transl.), 2010, vol. 46, no. 4, pp. 321–345].
10. MacWilliams, F.J. and Sloane, N.J.A., *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977. Translated under the title *Teoriya kodov, ispravlyayushchikh oshibki*, Moscow: Svyaz', 1979.