ON THE NONLINEAR CODES, OBTAINED FROM THE HAMMING CODE BY SWITCHINGS OF ijk-COMPONENTS, AS PARTIALLY ROBUST CODES

D.I. SIKERINA

Abstract. In the paper, the partially robustness of nonlinear codes, obtained from the Hamming code by the known switching method of ijk-components, is proven. Such codes have less undetectable (miscorrected) errors than traditional linear error-correcting codes of the same length, which is a great advantage for modern technologies when multiple and repeating errors are common. An error detection and correction algorithm for this construction is presented.

Keywords: the Hamming code, *ijk*-component, partially robust code, error detection, error correction.

1. Introduction

The reliability of memory is a decisive condition for present-day digital devices, and research of reliable methods of storing large amounts of information on board of the spacecraft makes a lot of sense. In case of the long-standing flash memories operation used in on-board spacecrafts' holding stations, properties of its semiconductor elements change. It is caused by repeated write/delete operations as well as the influence of space radiation and heavy cosmic particles. The aforesaid results in multiple bit errors, when the state of considerable number of memory cells changes ([1]). While using in flash memories on the board of the spacecraft, it is required for a code to have simple decoding algorithm, allowing to provide high decoding speed at low energy costs. In these situations different nonlinear code constructions can be used. Nonlinear robust and partially robust codes have been proposed in [2] as codes which provide equal protection against all the errors (including multiple bit errors – data corruption in several coordinate positions of a codeword). Such codes have fewer undetectable errors as well as errors that are miscorrected by all codewords, than classic linear codes, which do not guarantee error detection for multiple errors of multiplicity greater than the code distance.

Denote by $\mathbf{F}^n$ the n-dimensional vector space over the Galois field $GF(2)$ with the Hamming distance. Let $H^n \subset \mathbf{F}^n$ be the Hamming code – i.e. the linear binary perfect code of length $n = 2^s - 1$, where $s \in \{3, 4, 5, \ldots\}$. Following [3], represent the Hamming code as

$$H^n = \{(x, x + y, |x|) | x \in \mathbf{F}^{\frac{n-1}{2}}, y \in H^{\frac{n-1}{2}}\}. \tag{1}$$

Sikerina, D.I., On the nonlinear codes, obtained from the Hamming code by switchings of ijk-components, as partially robust codes.

The paper was prepared with the financial support of the Ministry of Science and Higher Education and of the Russian Federation, grant agreement No. FSRF-2020-0004. "Scientific basis for architectures and communication systems development of the onboard information and computer systems new generation in aviation, space systems and unmanned vehicles".

Only binary codes are considered in this paper. A code $D \subset \mathbf{F}^n$ of length n and size 2^k is *systematic*, if after deleting some $n-k$ columns of the code matrix all the 2^k remaining rows of length k are different. The Hamming code is systematic. Nonsystematic perfect codes also exist ([4]).

For any code $C \subset \mathbf{F}^n$ its *detection kernel* (also well-known as *kernel*, [2]) is the set of errors, masked by all codewords:

$$Ker_d(C) = \{e \in \mathbf{F}^n | e + c \in C, \forall c \in C\}.$$

If C is a linear code, then $Ker_d(C) = C$. The detection kernel of a code is its kernel in the usual sense ([5], [6]). The term *detection kernel* was introduced for consistency with another type of a code kernel. Let Alg_D be an error correcting algorithm for a code D, D_{er} be the set of errors which Alg_D attempts to correct, and $Alg_D(e,d)$ be the result of Alg_D when applied to the distorted codeword $e+d$. Then a *correction kernel* ([2]) is the set of errors outside D_{er}, which are miscorrected by all codewords:

$$Ker_c(D) = \{e \in \mathbf{F}^n | e \notin D_{er}, \forall d \in D\, \exists e' \in D_{er} : Alg_D(e,d) = Alg_D(e',d)\}.$$

A *conditionally detectable* (*conditionally miscorrected*) error is undetected (miscorrected) by not all of the codewords, but by some of them. There are no conditionally detectable (conditionally miscorrected) errors for linear codes. The set of conditionally detectable (conditionally miscorrected) errors of the code D we denote by $CDE(D)$ ($CME(D)$).

A code $D \subset \mathbf{F}^n$ is *robust* ([2]) if $Ker_d(D) = \{0\}$. The *error* $x \in \mathbf{F}^n$ *masking probability* is $Q_D(x) = \frac{|\{d \in D : d+x \in D\}|}{|D|}$. There are no undetectable errors for robust codes and $max_{(x \in \mathbf{F}^n \setminus \{0\})} Q_D(x) < 1$. In the general case, such codes have high coding and decoding complexity (as compared with linear codes). In some cases, an "intermediate" variant between linear and robust codes is considered. A code $D \subset \mathbf{F}^n$ of size 2^k is *partially robust* (see [2]) if it is systematic and $|Ker_d(D)| < 2^k$. The number of undetectable errors for such codes is greater than 0, but decreases by several orders of magnitude in comparison with linear perfect codes. Partially robust codes keep some structure of linear codes and can be used for the error correction, which is more interesting from the point of view of applications to memory as against robust codes. Such types of codes ensure a certain detection level for all the errors, what guarantees reliability of memory protected by partially robust codes. For any code D, its *error masking probability* is

$$Q_{mc}(D) = max_{(x \notin Ker_d(D))} Q_D(x).$$

Such characteristics as $|Ker_d|$, $|Ker_c|$ and Q_{mc} allow to compare codes efficient for multiple error detection and correction in flash memory (see [2]).

One method for constructing large class of nonlinear codes with different properties is a switching method. A code $D' = (D \setminus R) \cup R'$ is obtained by *switching* a set $R \subseteq D$ to R' in a code $D \subset \mathbf{F}^n$, if D' has the same parameters (i.e. the same length, size and the code distance) as D (see [7]). Such set R is called a *component* of D. If $R' = R + v_i$ for some $i \in \{1, 2, \ldots, n\}$, where $v_i = (0^{i-1}10^{n-i}) \in \mathbf{F}^n$, R is an i-component of D. Let $\alpha \subseteq \{1, 2, \ldots, n\}$. The set R is an α-component of D, if it is an i-component for any $i \in \alpha$ (see [8]). The first switching construction was presented by Vasil'ev ([3]).

The *nonlinearity of any function* $f : \mathbf{F}^s \to \{0,1\}$ can be measured with the help of its derivative $D_a f(x) = f(x+a) + f(x)$, where $a, x \in \mathbf{F}^s$. If $Pr(E)$ is a *probability*

of an event E occurrence, the *function f nonlinearity* is defined as

$$P_f = max_{a\in \mathbf{F}^s\setminus\{0\}} max_{b\in\{0,1\}} Pr(D_a f(x) = b).$$

The smaller values of P_f, the higher the corresponding nonlinearity of f.

It is proved in [2] that the Vasil'ev code V^{2s+1}, where $s \in \{3, 4, 5, \dots\}$, is partially robust, $|Ker_d(V^{2s+1})| = 2^s$, $Q_{mc}(V^{2s+1}) = P_f$. It is proved in [9] that a generalization of the well-known classical extended Mollard code to an arbitrary code length is partially robust, and for certain code parameters such generalization ensures better error protection than a generalization of Vasil'ev codes. This paper considers another well-known class of nonlinear codes, obtained from H^n by switching method of ijk-components [8], from the point of view of the concept of partially robustness, and properties of the kernels of the codes from [8].

2. The switching method of ijk-components

In [8], the method of ijk-components, letting us to do switchings of different i- and ijk-components of H^n, is adduced. It is proved in [8] that for any $i \in \{1, ..., n\}$, all the vectors $c \in H^n$, such that $weight(c) = 3, c_i = 1$, generate a vector subspace R_i – an i-component of H^n. Further, the weight of any vector $x \in \mathbf{F}^n$ we denote by $wt(x)$.

Perfect codes are closely associated with Steiner triple systems. A *Steiner triple system* of order n ($STS(n)$) is a family of 3-element subsets (triples) from $\{1, 2, ..., n\}$, such that every unordered pair of elements from $\{1, 2, ..., n\}$ appears in the only triple. It is well-known that for any perfect code $C \subset \mathbf{F}^n$, if $\mathbf{0}^n \in C$, then all the codewords $c \in C$, such that $wt(c) = 3$, form a $STS(n)$. If $STS(n)$ is a Steiner triple system, corresponding to H^n, then for every pair of coordinates $i, j \in \{1, 2, ...n\}$ there exists the only $k \in \{1, 2, ..., n\}$, such that $(i, j, k) \in STS(n)$ (by definition). If $c \in H^n$ is such a codeword that $wt(c) = 3, c_i = c_j = c_k = 1$, then a vector subspace R_{ijk} spanned by R_i and R_j is an $\{i, j, k\}$-component of H^n ([8]). A *neighbourhood* $K(M)$ of some set $M \subset F^n$ is a union of spheres, each of which has the Hamming radius equals to 1, and the center is some vector from M ([8]). The following theorems are true.

Lemma 1. *([8]) A set $M \subset C$ is an i-component of a perfect code C for some $i \in \{1, 2, \dots, n\}$ if and only if $K(M) = K(M + v_i)$, where $v_i = (0^{i-1}10^{n-i}) \in \mathbf{F}^n$.*

Let $N_1 = 2^{\frac{n-3}{4}}$, $N_2 = 2^{\frac{n+5}{4} - log_2(n+1)}$.

Theorem 1. *([8]) Each Hamming code of length n can be presented as a union of disjoint ijk-components R^t_{ijk}, $t \in \{1, ..., N_2\}$, $i, j, k \in \{1, \dots, n\}$. Each of them can be represented as a union of disjoint i-components R^{pt}_i, $p \in \{1, ..., N_1\}$, $t \in \{1, ..., N_2\}$ (the same is also true for elements j and k):*

$$H^n = \bigcup_{t=1}^{N_2} R^t_{ijk} = \bigcup_{t=1}^{N_2} \bigcup_{p=1}^{N_1} R^{pt}_i.$$

Theorem 2. *([8]) If π is a cyclic permutation of integers $i, j, k \in \{1, 2, ...n\}$, $\nu : \{1, 2, ..., N_2\} \to \{i, j, k\}, \lambda : \{1, 2, ..., N_2\} \times \{1, 2, ..., N_1\} \to \{0, 1\}$ and $\mu : \{1, 2, ..., N_2\} \to \{0, 1\}$ are some functions, R^p_l is a l-component of H^n, $p \in \{1, ..., N_1\}$,*

$l \in \{i, j, k\}$, then one obtains a perfect code

$$C_{\lambda,\nu,\mu} = \bigcup_{t=1}^{N_2}(\bigcup_{p=1}^{N_1}(R^p_{\nu(t)} + \lambda(t,p) \cdot v_{\nu(t)}) + \mu(t) \cdot v_{\pi(\nu(t))}).$$

Taking into account (1),

$$H^{\frac{n-1}{2}} = \{(z, z+y, |z|) | z \in \mathbf{F}^{\frac{n-3}{4}}, y \in H^{\frac{n-3}{4}}\}. \tag{2}$$

Lemma 2. *The set $R = \{(x, x+(z,z,|z|), |x|) | x \in \mathbf{F}^{\frac{n-1}{2}}, z \in \mathbf{F}^{\frac{n-3}{4}}\}$ is a $\{\frac{n-1}{2}, n-1, n\}$-component of H^n.*

Proof. It is easy to prove that the set

$$R = \{(x, x+(z,z,|z|), |x|) | x \in \mathbf{F}^{\frac{n-1}{2}}, z \in \mathbf{F}^{\frac{n-3}{4}}\}$$

is a $(n-1)$-component and a n-component of H^n by straightly using the result of Lemma 1. Let us define the third element k of the triple $(k, n-1, n)$. A codeword from H^n, corresponding to the triple $(k, n-1, n)$, looks like

$$(x, x+t, |x|) = (0^{k-1}10^{n-k-2}11), x \in \mathbf{F}^{\frac{n-1}{2}}, t \in H^{\frac{n-1}{2}}.$$

Therefore, $|x| = 1$ and $wt(x) = 1$. If $t \neq \mathbf{0}^{\frac{n-1}{2}}$, the fact that $wt(x) = 1$ and $wt(x, x+t, |x|) = 3$ implies that $x+t = (\mathbf{0}^{\frac{n-1}{2}-1}1)$. Therefore, $wt(t) = 2$ – that is not even possible, as $t \in H^{\frac{n-1}{2}}$, $\mathbf{0}^{\frac{n-1}{2}} \in H^{\frac{n-1}{2}}$. It means that $t = \mathbf{0}^{\frac{n-1}{2}}$, $x = (\mathbf{0}^{\frac{n-1}{2}-1}1)$, $k = \frac{n-1}{2}$. The fact that $R \subset H^n$ is a $(\frac{n-1}{2})$-component of H^n can be also easily proven using the result of Lemma 1. Hence, R is a $\{\frac{n-1}{2}, n-1, n\}$-component of H^n and $R = R_{\frac{n-1}{2},n-1,n}$. □

Lemma 3. *The set $\{((x', x', g), (x', x', g) + (z, z, |z|), |g|) | x', z \in \mathbf{F}^{\frac{n-3}{4}}, g \in \{0, 1\}\}$ is a $(n-1)$-component $R_{n-1} \subset H^n$.*

Proof. To find $(n-1)$-components within $R_{\frac{n-1}{2},n-1,n} \subset H^n$, consider the set of $c \in H^n$, such that $wt(c) = 3, c_{n-1} = 1$. Due to (1) and (2), for any $c \in H^n$:

$$c = (x, x+(z, z+y, |z|), |x|), x = (x_1, \ldots, x_{\frac{n-1}{2}}) \in \mathbf{F}^{\frac{n-1}{2}}, z \in \mathbf{F}^{\frac{n-3}{4}}, y \in H^{\frac{n-3}{4}}.$$

Therefore, $wt(x) \leq 3$ and $|z| + x_{\frac{n-1}{2}} = 1$.

1) If $|z| = 1$, $x = \mathbf{0}^{\frac{n-1}{2}}$, there exist $\frac{n-3}{4}$ appropriate $c \in H^n$:

$$y = \mathbf{0}^{\frac{n-3}{4}}, z = (\mathbf{0}^{i-1}1\mathbf{0}^{\frac{n-3}{4}-i}), i \in \{1, 2, \ldots, \frac{n-3}{4}\}.$$

2) If $|z| = 1$, $wt(x) = 2$, there exist $\frac{n-3}{4}$ appropriate $c \in H^n$:

$$y = \mathbf{0}^{\frac{n-3}{4}}, z = (\mathbf{0}^{i-1}1\mathbf{0}^{\frac{n-3}{4}-i}), x = \mathbf{0}^{i-1}1\mathbf{0}^{\frac{n-7}{4}}1\mathbf{0}^{\frac{n+1}{4}-i}, i \in \{1, 2, \ldots, \frac{n-3}{4}\}.$$

3) If $|z| = 0$, $x_{\frac{n-1}{2}} = 1$, there exists the only appropriate $c \in H^n$:

$$x = \mathbf{0}^{\frac{n-1}{2}-1}1, y = \mathbf{0}^{\frac{n-3}{4}}, z = \mathbf{0}^{\frac{n-3}{4}}.$$

Hence, there exist exactly $\frac{n-1}{2}$ codewords $c \in H^n$, such that $wt(c) = 3, c_{n-1} = 1$:

$$h_1^i = (\mathbf{0}^{i-1}1\mathbf{0}^{\frac{n-3}{4}-1}1\mathbf{0}^{\frac{n-1}{2}-i-1}0, \mathbf{0}^{\frac{n-1}{2}-1}1, 0), i \in \{1, \ldots, \frac{n-3}{4}\},$$
$$h_2^i = (\mathbf{0}^{\frac{n-1}{2}}, \mathbf{0}^{i-1}1\mathbf{0}^{\frac{n-3}{4}-1}1\mathbf{0}^{\frac{n-1}{2}-i-1}1, 0), i \in \{1, \ldots, \frac{n-3}{4}\},$$
$$h_3 = (\mathbf{0}^{\frac{n-1}{2}-1}1, \mathbf{0}^{\frac{n-1}{2}-1}1, 1).$$

Therefore, a vector subspace of size $2^{\frac{n-1}{2}}$, spanned by h_1^i, h_2^i and h_3, where $i \in$ $\in \{1, \ldots, \frac{n-3}{4}\}$, is of the form:

$$\{\textstyle\sum_{i=1}^{\frac{n-3}{4}} \alpha_i h_1^i + \sum_{i=1}^{\frac{n-3}{4}} \beta_i h_2^i + \gamma h_3 | \alpha_i, \beta_i, \gamma \in \{0,1\}\} =$$
$$= \{((\alpha_1, \alpha_2, \ldots, \alpha_{\frac{n-3}{4}}, \alpha_1, \alpha_2, \ldots, \alpha_{\frac{n-3}{4}}, \gamma), (\beta_1, \beta_2, \ldots, \beta_{\frac{n-3}{4}}, \beta_1, \beta_2, \ldots, \beta_{\frac{n-3}{4}},$$
$$\textstyle\sum_{i=1}^{\frac{n-3}{4}} \alpha_i + \sum_{i=1}^{\frac{n-3}{4}} \beta_i + \gamma), \gamma) | \alpha_i, \beta_i, \gamma \in \{0,1\}\} =$$
$$= \{((x', x', g), (x', x', g) + (z, z, |z|), |g|) | x', z \in \mathbf{F}^{\frac{n-3}{4}}, g \in \{0,1\}\} = R_{n-1}.$$

□

Turning over all the distinct $x'' \in \mathbf{F}^{\frac{n-3}{4}}$, one obtains cosets R_{n-1} within

$$R_{\frac{n-1}{2},n-1,n} = \{((x', x' + x'', g), (x', x' + x'', g) + (z, z, |z|), |x''| + |g|)|$$
$$|x', x'', z \in \mathbf{F}^{\frac{n-3}{4}}, g \in \{0,1\}\}.$$

Taking all the distinct $y \in H^{\frac{n-3}{4}}$, one obtains cosets $R_{\frac{n-1}{2},n-1,n}$ within

$$H^n = \{((x', x' + x'', g), (x', x' + x'', g) + (z, z + y, |z|), |x''| + |g|)|$$
$$|x', x'', z \in \mathbf{F}^{\frac{n-3}{4}}, y \in H^{\frac{n-3}{4}}, g \in \{0,1\}\}.$$

If we switch cosets $(\frac{n-1}{2})$-component $R_{\frac{n-1}{2},n-1,n}$ in H^n accordingly to $\mu : H^{\frac{n-3}{4}} \to \{0,1\}$ and cosets $(n-1)$-component R_{n-1} in $R_{\frac{n-1}{2},n-1,n}$ accordingly to $\lambda : \mathbf{F}^{\frac{n-3}{4}} \times H^{\frac{n-3}{4}} \to \{0,1\}$, we obtain the perfect code (by Theorem 2):

$$\{((x', x' + x'', g + \mu(y)), (x', x' + x'', g) + (z, z + y, |z| + \lambda(x'', y)), |x''| + |g|)|$$

$$|x', x'', z \in \mathbf{F}^{\frac{n-3}{4}}, y \in H^{\frac{n-3}{4}}, g \in \{0,1\}\}. \tag{3}$$

For any functions $\mu : H^{\frac{n-3}{4}} \to \{0,1\}$ and $\lambda : \mathbf{F}^{\frac{n-3}{4}} \times H^{\frac{n-3}{4}} \to \{0,1\}$, the codes

$$C_{\mu,\lambda}^{\frac{n-1}{2},n-1} = \{((x', x' + x'', g + \mu(y)), (x', x' + x'', g) + (z, z + y, |z| +$$
$$+\lambda(x'', y)), |x''| + |g|)|x', x'', z \in \mathbf{F}^{\frac{n-3}{4}}, y \in H^{\frac{n-3}{4}}, g \in \{0,1\}\},$$

$$C_{\mu,\lambda}^{n-1,n} = \{(x, x + (z, z + y, |z| + \mu(y)), |x| + \lambda(z, y))|$$
$$|x \in \mathbf{F}^{\frac{n-1}{2}}, z \in \mathbf{F}^{\frac{n-3}{4}}, y \in H^{\frac{n-3}{4}}\}$$

and

$$C_{\mu,\lambda}^{\frac{n-1}{2},n} = \{(x + (\mathbf{0}, \mu(y)), x + (z, z + y, |z|), |x| + \lambda(z, y))|$$
$$|x \in \mathbf{F}^{\frac{n-1}{2}}, \mathbf{0} \in \mathbf{F}^{\frac{n-1}{2}-1}, z \in \mathbf{F}^{\frac{n-3}{4}}, y \in H^{\frac{n-3}{4}}\}$$

are perfect ones.

Further we consider only $C_{\mu,\lambda}^{\frac{n-1}{2},n-1}$. Let $D = C_{\mu,\lambda}^{\frac{n-1}{2},n-1}$.

Let M_H be the code matrix of $H^{\frac{n-3}{4}}$, M_D be the code matrix of D, $L_1 = \frac{n+5}{4} - log_2(n+1)$, $L_2 = \frac{n+1}{2} - log_2(n+1)$. Further, for the sake of convenience, by $log(n)$ we always mean $log_2(n)$. Remember that the size of the systematic code $H^{\frac{n-3}{4}}$ of length $\frac{n-3}{4}$ equals to 2^{L_1}.

Lemma 4. *The code D is systematic.*

Proof. The first $\frac{n-3}{2}$ columns of M_D form all the $2^{\frac{n-3}{2}}$ different rows of length $\frac{n-3}{2}$, each of which repeats 2^{L_2+1} times. As $H^{\frac{n-3}{4}}$ is systematic code, one can delete

$log(n+1)-2$ columns at some numbers $i_1,\dots,i_{log(n+1)-2}$ from M_H to obtain all the 2^{L_1} different reduced rows $y_1,\dots,y_{2^{L_1}}$ of length L_1.

Delete from M_D the $(\frac{n-1}{2})$-th , $(i_1+\frac{n-1}{2})$-th, …, $(i_{log(n+1)-2}+\frac{n-1}{2})$-th, $(n-1)$-th columns, and consider the reduced codewords of D of the form

$$\{(x', x'+x'', x'+z, (\hat{x'}+\hat{x''}+\hat{z})+\hat{y}, |x''|+|g|)\},$$

where $x', x'', z \in \mathbf{F}^{\frac{n-3}{4}}, \hat{y} \in \{y_1,\dots,y_{2^{L_1}}\}, g \in \{0,1\}\}$, and $\hat{x'}, \hat{x''}, \hat{z} \in \mathbf{F}^{L_1}$ are obtained from $x', x'', z \in \mathbf{F}^{\frac{n-3}{4}}$ by deleting i_1-th, …, $i_{log(n+1)-2}$-th coordinates correspondingly. Let

$$a = (x'_1, x'_1+x''_1, x'_1+z_1, (\hat{x'_1}+\hat{x''_1}+\hat{z_1})+\hat{y_1}, |x''_1|+|g_1|)$$

and

$$b = (x'_2, x'_2+x''_2, x'_2+z_2, (\hat{x'_2}+\hat{x''_2}+\hat{z_2})+\hat{y_2}, |x''_2|+|g_2|)$$

be two reduced codewords. If $x'_1 \neq x'_2$ or $x''_1 \neq x''_2$, then $a \neq b$. If $x'_1 = x'_2$ and $x''_1 = x''_2$, then $a = b \iff$

$$\begin{cases} x'_1+z_1 = x'_2+z_2 \\ (\hat{x'_1}+\hat{x''_1}+\hat{z_1})+\hat{y_1} = (\hat{x'_2}+\hat{x''_2}+\hat{z_2})+\hat{y_2} \\ |x''_1|+|g_1| = |x''_2|+|g_2| \end{cases} \iff \begin{cases} z_1 = z_2 \\ \hat{y_1} = \hat{y_2} \\ g_1 = g_2 \end{cases}. \tag{4}$$

Therefore, $a = b$ if and only if the corresponding vectors x'_1 and x'_2, x''_1 and x''_2, z_1 and z_2, $\hat{y_1}$ and $\hat{y_2}$, g_1 and g_2 coincide. But the same $\hat{y_1}$ and $\hat{y_2}$ cannot correspond to different vectors from $H^{\frac{n-3}{4}}$ – otherwise, after deleting $log(n+1)-2$ columns from M_H there would be less than 2^{L_1} different rows of length L_1. That cannot be true, as $H^{\frac{n-3}{4}}$ is systematic. Therefore, $\hat{y_1} = \hat{y_2}$ if and only if the two initial codewords from $H^{\frac{n-3}{4}}$ coincide. As all the rows from M_H are distinct, one obtains distinct rows of length $n-log(n+1)$ after deleting $log(n+1)$ columns from M_D. The number of these distinct rows equals to $2^{\frac{n-3}{2}} \cdot 2^{\frac{n-3}{4}} \cdot 2^{\frac{n+5}{4}-log(n+1)} \cdot 2^1 = 2^{n-log(n+1)}$. Therefore, D is systematic. □

Let the codeword

$$c = ((x', x'+x'', g+\mu(y)), (x', x'+x'', g)+(z, z+y, |z|+\lambda(x'', y)), |x''|+|g|) \in D,$$

for some $x', x'', z \in \mathbf{F}^{\frac{n-3}{4}}, y \in H^{\frac{n-3}{4}}, g \in \{0,1\}$, is transmitted over a communication channel, $e = (e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}, e_3)$ is an occurred error, $e_{11}, e_{12}, e_{21}, e_{22} \in \mathbf{F}^{\frac{n-3}{4}}$, $e_{13}, e_{23}, e_3 \in \mathbf{F}^1$. Let H_{small} and H_{large} be canonical-form parity-check matrices of $H^{\frac{n-3}{4}}$ and $H^{\frac{n-1}{2}}$ from (2) respectively.

Theorem 3. *Let $\lambda : \mathbf{F}^{\frac{n-3}{4}} \times H^{\frac{n-3}{4}} \to \{0,1\}$ and $\mu : H^{\frac{n-3}{4}} \to \{0,1\}$ be some nonlinear functions with $P_\lambda < 1$ and $P_\mu < 1$. The code D is partially robust, $|Ker_d(D)| = 2^{\frac{n-1}{2}}$, $Q_{mc}(D) \leq P_\lambda$.*

Proof. An error e is masked if and only if a distorted codeword

$$c' = ((x', x'+x'', g+\mu(y))+(e_{11}, e_{12}, e_{13}), (x', x'+x'', g)+(z, z+y, |z|+\lambda(x'', y))+$$
$$+(e_{21}, e_{22}, e_{23}), |x''|+|g|+e_3),$$

obtained at the output of the communication channel, coincides with some

$$\tilde{c} = ((\tilde{x}', \tilde{x}'+\tilde{x}'', \tilde{g}+\mu(\tilde{y})), (\tilde{x}', \tilde{x}'+\tilde{x}'', \tilde{g})+(\tilde{z}, \tilde{z}+\tilde{y}, |\tilde{z}|+\lambda(\tilde{x}'', \tilde{y})), |\tilde{x}''|+|\tilde{g}|) \in D.$$

Taking into account the definition of the parity-check matrix, the following correlations are true:

$$\begin{cases} \tilde{x}' = x' + e_{11}, \tilde{x}'' = x'' + e_{11} + e_{12}, \tilde{z} = z + e_{11} + e_{21} \\ \tilde{y} = y + e_{11} + e_{12} + e_{21} + e_{22} \\ \tilde{g} = g + |e_{11}| + |e_{12}| + e_3 \\ \mu(\tilde{y}) = \mu(y) + |e_{11}| + |e_{12}| + e_{13} + e_3 \\ \lambda(\tilde{x}'', \tilde{y}) = \lambda(x'', y) + |e_{12}| + |e_{21}| + e_{23} + e_3 \end{cases} \iff \tag{5}$$

$$\iff \begin{cases} H_{small}(e_{11} + e_{12} + e_{21} + e_{22})^T = \mathbf{0}^{L_1} \\ H_{large}(e_{11} + e_{21}, e_{12} + e_{22}, |e_{11}| + |e_{21}|)^T = \mathbf{0}^{L_2} \\ \mu(\tilde{y}) = \mu(y) + |e_{11}| + |e_{12}| + e_{13} + e_3 \\ \lambda(\tilde{x}'', \tilde{y}) = \lambda(x'', y) + |e_{12}| + |e_{21}| + e_{23} + e_3 \end{cases}. \tag{6}$$

I. An error e is always masked by D if and only if

$$\begin{cases} e_{11} = e_{12} \\ e_{21} = e_{22} \\ e_3 = e_{13} \\ e_{23} = |e_{12}| + |e_{21}| + e_{13}. \end{cases} \tag{7}$$

The number of such errors depends on the number of different vectors $e_{11}, e_{21} \in \mathbf{F}^{\frac{n-3}{4}}$, $e_{13} \in \mathbf{F}^1$ and is equal to $2^{\frac{n-3}{4}} \cdot 2 \cdot 2^{\frac{n-3}{4}} = 2^{\frac{n-1}{2}}$.

II. An error e is conditionally detectable in the following cases:

1) Conditionally detectable errors, which masking probabilities depend on the nonlinearity of λ, can be obtained if and only if

$$\begin{cases} e_{11} + e_{12} + e_{21} + e_{22} = \mathbf{0}^{\frac{n-3}{4}} \\ e_3 = |e_{11}| + |e_{12}| + e_{13} \\ e_{12} \neq e_{11} \end{cases}. \tag{8}$$

Thus,

$$\lambda(\tilde{x}'', \tilde{y}) = \lambda(x'', y) + |e_{12}| + |e_{21}| + e_{23} + e_3 \iff$$
$$\lambda(x'' + e_{11} + e_{12}, y) + \lambda(x'', y) = |e_{12}| + |e_{21}| + e_{23} + e_3 \iff$$
$$Pr(\lambda(x'' + e_{11} + e_{12}, y) + \lambda(x'', y) = |e_{12}| + |e_{21}| + e_{23} + e_3) \leq P_\lambda.$$

Any error of such type is masked by D with a probability $\leq P_\lambda$. The number of such errors depends on the number of different vectors $e_{11}, e_{21} \in \mathbf{F}^{\frac{n-3}{4}}$, $e_{13}, e_{23} \in \mathbf{F}^1$, $e_{12} \in \mathbf{F}^{\frac{n-3}{4}} \backslash \{e_{11}\}$ and is equal to $2^{\frac{n-3}{4}} \cdot (\frac{2^{\frac{n-3}{4}}}{2} - 1) \cdot 2 \cdot 2^{\frac{n-3}{4}} \cdot 2 = 2^{\frac{n+1}{2}} \cdot (2^{\frac{n-7}{4}} - 1)$.

2) Conditionally detectable errors, which masking probabilities depend on the nonlinearity of λ and μ, can be obtained if and only if

$$e_{11} + e_{12} + e_{21} + e_{22} \in H^{\frac{n-3}{4}} \backslash \mathbf{0}^{\frac{n-3}{4}}. \tag{9}$$

Thus,

$$\mu(\tilde{y}) = \mu(y) + |e_{11}| + |e_{12}| + e_{13} + e_3 \iff$$
$$Pr(\mu(y + e_{11} + e_{12} + e_{21} + e_{22}) + \mu(y) = |e_{11}| + |e_{12}| + e_{13} + e_3) \leq P_\mu,$$

and

$$\lambda(\tilde{x}'', \tilde{y}) = \lambda(x'', y) + |e_{12}| + |e_{21}| + e_{23} + e_3 \iff$$

$Pr(\lambda(x''+e_{11}+e_{12}, y+e_{11}+e_{12}+e_{21}+e_{22})+\lambda(z,y) = |e_{12}|+|e_{21}|+e_{23}+e_3) \leq P_\lambda$. Any error from this class is masked by D with a probability $\leq P_\mu \cdot P_\lambda$. The number of these errors is equal to $2^{\frac{n-3}{4}} \cdot 2^{\frac{n-3}{4}} \cdot 2 \cdot 2^{\frac{n-3}{4}} \cdot (\frac{2^{\frac{n-3}{4}}}{\frac{n-3}{4}+1} - 1) \cdot 2 \cdot 2 = 2^{\frac{n+5}{4}} \cdot 2^{\frac{n-1}{2}} \cdot (\frac{2^{\frac{n+5}{4}}}{n+1} - 1)$.

Therefore, $|CDE(D)| = 2^{n+2-log(n+1)} - 2^{\frac{3n-1}{4}} - 2^{\frac{n+1}{2}}$. Any conditionally detected error is masked by D with a probability less than or equal to $max\{P_\lambda, P_\mu \cdot P_\lambda\} = P_\lambda$. In the worst case, an error is masked by $P_\lambda \times |D|$ codewords, and $Q_{mc}(D) = P_\lambda$.

There are $2^{\frac{n-1}{2}}$ errors masked by all the codewords from D. As D is systematic and $|Ker_d(D)| = 2^{\frac{n-1}{2}} < 2^{n-log(n+1)} = |D|$, the code D is partially robust. □

3. Memory protection architecture of the code $\bar{C}_{\mu,\lambda}^{\frac{n-1}{2},n-1}$

Let $\bar{D}$ be an extended code of length $n+1$, obtained from $D = C_{\mu,\lambda}^{\frac{n-1}{2},n-1}$ by parity checking. Codewords from $\bar{D}$ are of the form $c = (c_1^1, c_1^2, c_1^3, c_2^1, c_2^2, c_2^3, c_3, c_4)$, where

$$c_1^1 = x' \in \mathbf{F}^{\frac{n-3}{4}},\ \ c_1^2 = x' + x'' \in \mathbf{F}^{\frac{n-3}{4}},\ \ c_1^3 = g + \mu(y) \in \mathbf{F}^1,$$

$$c_2^1 = x' + z \in \mathbf{F}^{\frac{n-3}{4}},\ \ c_2^2 = x' + x'' + z + y \in \mathbf{F}^{\frac{n-3}{4}},\ \ c_2^3 = g + |z| + \lambda(x'', y) \in \mathbf{F}^1,$$

$$c_3 = |x''| + |g| \in \mathbf{F}^1,\ \ c_4 = |x''| + |g| + |y| + |z| + \mu(y) + \lambda(x'', y) \in \mathbf{F}^1,$$

$x', x'', z \in \mathbf{F}^{\frac{n-3}{4}}, y \in H^{\frac{n-3}{4}}, g \in \{0,1\}$, $\mu : H^{\frac{n-3}{4}} \to \{0,1\}$ and $\lambda : \mathbf{F}^{\frac{n-3}{4}} \times H^{\frac{n-3}{4}} \to \{0,1\}$ are nonlinear functions. Assume that decoder received a word $\tilde{c}$. Let us try to correct an error, if any. The word $\tilde{c}$ can be "split" into parts accordingly to the construction of the code $\bar{D}$: $\tilde{c} = (\tilde{c}_1^1, \tilde{c}_1^2, \tilde{c}_1^3, \tilde{c}_2^1, \tilde{c}_2^2, \tilde{c}_2^3, \tilde{c}_3, \tilde{c}_4)$. Let $e = (e_1^1, e_1^2, e_1^3, e_2^1, e_2^2, e_2^3, e_3, e_4) \in \mathbf{F}^{n+1}$ be the error vector: $c = \tilde{c} + e$ (using the maximum likelihood principle).

Define a syndrome $S = (S_1, S_2, S_3, S_4, S_5)$ for locating and correcting errors, where $S_1 \in \mathbf{F}^{L_2}, S_2 \in \mathbf{F}^{L_1}, S_3, S_4, S_5 \in \mathbf{F}^1$:

$$S_1 = H_{large}(\tilde{c}_1^1+\tilde{c}_2^1, \tilde{c}_1^2+\tilde{c}_2^2, \tilde{c}_1^3+\tilde{c}_2^3+\mu(\tilde{c}_1^1+\tilde{c}_2^1+\tilde{c}_1^2+\tilde{c}_2^2)+\lambda(\tilde{c}_1^1+\tilde{c}_1^2, \tilde{c}_1^1+\tilde{c}_2^1+\tilde{c}_1^2+\tilde{c}_2^2))^T,$$

$$S_2 = H_{small}(\tilde{c}_1^1 + \tilde{c}_2^1 + \tilde{c}_1^2 + \tilde{c}_2^2)^T,$$

$$S_3 = |\tilde{c}_1^1| + |\tilde{c}_1^2| + \tilde{c}_1^3 + \tilde{c}_3 + \mu(\tilde{c}_1^1 + \tilde{c}_2^1 + \tilde{c}_1^2 + \tilde{c}_2^2),$$

$$S_4 = |\tilde{c}_2^1| + |\tilde{c}_1^2| + \tilde{c}_2^3 + \tilde{c}_3 + \lambda(\tilde{c}_1^1 + \tilde{c}_1^2, \tilde{c}_1^1 + \tilde{c}_2^1 + \tilde{c}_1^2 + \tilde{c}_2^2),$$

$$S_5 = |\tilde{c}_1^1| + |\tilde{c}_1^2| + |\tilde{c}_1^3| + |\tilde{c}_2^1| + |\tilde{c}_2^2| + |\tilde{c}_2^3| + |\tilde{c}_3| + |\tilde{c}_4|.$$

The purpose of the following algorithm is to declare single and multiple errors, and to correct single errors.

Let h_j^{large} be the j-th column of H_{large}, where $j \in \{1, \ldots, \frac{n-1}{2}\}$, h_i^{small} be the i-th column of H_{small}, $u_i = (0^{i-1}, 1, 0^{\frac{n-3}{4}-i}) \in \mathbf{F}^{\frac{n-3}{4}}$, where $i \in \{1, ..., \frac{n-3}{4}\}$.

Algorithm for detecting/correcting errors

(1) Compute the syndrome $S = (S_1, S_2, S_3, S_4, S_5)$ for $\tilde{c}$.
(2) If $S = \mathbf{0}$, no error is detected. Otherwise, there exists an error which is detected.
(3) If $S_5 = 0$ and at least one of $S_1, S_2, S_3, S_4 \neq 0$, then an error of even multiplicity is detected. Data will go without any correction.
(4) If $S_1 = \mathbf{0}$, $S_2 = \mathbf{0}$, $S_3 = S_4 = 0$, $S_5 = 1$, flip the $(n+1)$-th bit of $\tilde{c}$ and recalculate S. If $S = \mathbf{0}$, then a single error $e = (\mathbf{0}^n, 1)$ in the $(n+1)$-th bit of $\tilde{c}$ is detected and successfully corrected.

(5) If $S_1 = \mathbf{0}$, $S_2 = \mathbf{0}$, $S_3 = S_4 = S_5 = 1$, flip the n-th bit of $\tilde{c}$ and recalculate S. If $S = \mathbf{0}$, then a single error $e = (\mathbf{0}^{n-1}, 1, 0)$ in the n-th bit of $\tilde{c}$ is detected and successfully corrected.

(6) If $S_1 = h^{large}_{\frac{n-1}{2}}$, $S_2 = \mathbf{0}$, $S_3 = 1$, $S_4 = 0$, $S_5 = 1$, flip the $(\frac{n-1}{2})$-th bit of $\tilde{c}$ and recalculate S. If $S = \mathbf{0}$, then a single error $e = (\mathbf{0}^{\frac{n-1}{2}-1}, 1, \mathbf{0}^{\frac{n+3}{2}})$ in the $(\frac{n-1}{2})$-th bit of $\tilde{c}$ is detected and successfully corrected.

(7) If $S_1 = h^{large}_{\frac{n-1}{2}}$, $S_2 = \mathbf{0}$, $S_3 = 0$, $S_4 = 1$, $S_5 = 1$, flip the $(n-1)$-th bit of $\tilde{c}$ and recalculate S. If $S = \mathbf{0}$, then a single error $e = (\mathbf{0}^{n-2}, 1, \mathbf{0}^2)$ in the $(n-1)$-th bit of $\tilde{c}$ is detected and successfully corrected.

(8) If $S_2 = h^{small}_i$, $S_5 = 1$, for $i \in \{1, ..., \frac{n-3}{4}\}$, then either a single bit error occurs to one of the $\{1, ..., \frac{n-1}{2} - 1, \frac{n-1}{2} + 1, ..., n-2\}$ bits of c or an error of odd multiplicity is detected. Calculate $y = \tilde{c}^1_1 + \tilde{c}^1_2 + \tilde{c}^2_1 + \tilde{c}^2_2 + u_i$, $\mu(y) + \mu(y + u_i)$, $x'' = \tilde{c}^1_1 + \tilde{c}^2_1 + u_i$, $\lambda(x'', y)$, $\lambda(x'' + u_i, y + u_i)$.

  (a) If $S_1 = h^{large}_i + h^{large}_{\frac{n-1}{2}} \cdot (\mu(y) + \mu(y+u_i) + \lambda(x'', y) + \lambda(x''+u_i, y+u_i))$, $S_3 = 1 + \mu(y) + \mu(y + u_i)$, $S_4 = \lambda(x'', y) + \lambda(x'' + u_i, y + u_i)$, flip the i-th bit of $\tilde{c}$ and recalculate S. If $S = \mathbf{0}$, then a single bit error $e = (\mathbf{0}^{i-1}, 1, \mathbf{0}^{n-i+1})$ is detected and successfully corrected.

  (b) If $S_1 = h^{large}_{i+\frac{n-3}{4}} + h^{large}_{\frac{n-1}{2}} \cdot (\mu(y) + \mu(y+u_i) + \lambda(x'', y) + \lambda(x''+u_i, y+u_i))$, $S_3 = 1 + \mu(y) + \mu(y + u_i)$, $S_4 = \lambda(x'', y) + \lambda(x'' + u_i, y + u_i) + 1$, flip the $(i + \frac{n-3}{4})$-th bit of $\tilde{c}$ and recalculate S. If $S = \mathbf{0}$, a single error $e = (\mathbf{0}^{i+\frac{n-3}{4}-1}, 1, \mathbf{0}^{\frac{3n+7}{4}-i})$ is detected and successfully corrected.

  (c) If $S_1 = h^{large}_i + h^{large}_{\frac{n-1}{2}} \cdot (\mu(y) + \mu(y+u_i) + \lambda(x'', y) + \lambda(x''+u_i, y+u_i))$, $S_3 = \mu(y) + \mu(y + u_i)$, $S_4 = \lambda(x'', y) + \lambda(x'' + u_i, y + u_i) + 1$, flip the $(i + \frac{n-1}{2})$-th bit of $\tilde{c}$ and recalculate S. If $S = \mathbf{0}$, then a single error $e = (\mathbf{0}^{i+\frac{n-1}{2}-1}, 1, \mathbf{0}^{\frac{n+3}{2}-i})$ is detected and successfully corrected.

  (d) If $S_1 = h^{large}_{i+\frac{n-3}{4}} + h^{large}_{\frac{n-1}{2}} \cdot (\mu(y) + \mu(y+u_i) + \lambda(x'', y) + \lambda(x''+u_i, y+u_i))$, $S_3 = \mu(y) + \mu(y + u_i)$, $S_4 = \lambda(x'', y) + \lambda(x'' + u_i, y + u_i)$, flip the $(i + \frac{3n-5}{4})$-th bit of $\tilde{c}$ and recalculate S. If $S = \mathbf{0}$, then a single error $e = (\mathbf{0}^{i+\frac{3n-5}{4}-1}, 1, \mathbf{0}^{\frac{n+9}{4}-i})$ is detected and successfully corrected.

(9) In the other cases, an error of odd multiplicity greater than or equal to 3 is detected and no correction will be attempted.

If $c \in \bar{D}$, $\tilde{c} = (\tilde{c}^1_1, \tilde{c}^2_1, \tilde{c}^3_1, \tilde{c}^1_2, \tilde{c}^2_2, \tilde{c}^3_2, \tilde{c}_3, \tilde{c}_4)$ is the vector received by decoder, $e = (e_1, e_2, e_3, e_4) = c + \tilde{c}$ is an error vector, where $e_1 = (e^1_1, e^2_1, e^3_1), e_2 = (e^1_2, e^2_2, e^3_2)$, then:

$$S_1 = H_{large}(e_1 + e_2 + (\mathbf{0}^{\frac{n-1}{2}-1}, \lambda(x'' + e^1_1 + e^2_1, y + e^1_1 + e^1_2 + e^2_1 + e^2_2) + \lambda(x'', y) + \\ + \mu(e^1_1 + e^1_2 + e^2_1 + e^2_2 + y) + \mu(y)))^T,$$

$$S_2 = H_{small}(e^1_1 + e^1_2 + e^2_1 + e^2_2)^T, \tag{10}$$

$$S_3 = |e^1_1| + |e^2_1| + e^3_1 + e_3 + \mu(e^1_1 + e^1_2 + e^2_1 + e^2_2 + y) + \mu(y),$$

$$S_4 = |e^1_2| + |e^2_1| + e^3_2 + e_3 + \lambda(x'' + e^1_1 + e^2_1, y + e^1_1 + e^1_2 + e^2_1 + e^2_2) + \ + \lambda(x'', y),$$

$$S_5 = |e_1| + |e_2| + |e_3| + |e_4|.$$

For clarity, further we will represent the syndrome S depending on its structure $S = (S_1, S_2, S_3, S_4, S_5)$ (for example, if $S = \mathbf{0}$, write it as $S = (\mathbf{0}^{L_2}, \mathbf{0}^{L_1}, 0, 0, 0)$).

Lemma 5. *If $S = (\mathbf{0}^{L_2}, \mathbf{0}^{L_1}, 0, 0, 1)$, there exist $2^{\frac{n-1}{2}} - 1$ error vectors meeting the syndrom which are miscorrected by $\bar{D}$. The only error $e = (\mathbf{0}^n, 1)$ is corrected, $2^{\frac{n+1}{2}} \cdot (2^{\frac{n-3}{4}} - 1)$ errors are miscorrected with a probability not more than P_λ, and $2^{\frac{n+1}{2}} \cdot 2^{\frac{n-3}{4}} \cdot (\frac{2^{\frac{n-3}{4}}}{\frac{n+1}{4}} - 1)$ errors are miscorrected by algorithm with a probability less than or equal to $P_\mu \cdot P_\lambda$.*

Proof. Let $S = (\mathbf{0}^{L_2}, \mathbf{0}^{L_1}, 0, 0, 1)$.

a) If $e_1^1 = e_1^2$ and $e_1^1 + e_2^1 + e_1^2 + e_2^2 = \mathbf{0}^{\frac{n-3}{4}}$, then $e_2^1 = e_2^2$ and (10) $\iff$

$$(11) \qquad \begin{cases} e_2^3 = |e_1^1| + |e_2^1| + e_3 \\ H_{small}(\mathbf{0}^{\frac{n-3}{4}})^T = \mathbf{0}^{L_1} \\ e_1^3 = e_3 \\ |e_1^2| = |e_1^1| \\ e_4 = |e_1| + |e_2| + |e_3| + 1. \end{cases}$$

The number of these errors is equal to $2^{\frac{n-3}{4}} \cdot 1 \cdot 2 \cdot 2^{\frac{n-3}{4}} \cdot 1 \cdot 1 \cdot 1 \cdot 1 = 2^{\frac{n-1}{2}}$. The error $(\mathbf{0}^n, 1)$ is corrected by algorithm. The other $2^{\frac{n-1}{2}} - 1$ errors are miscorrected.

b) If $e_1^2 \neq e_1^1$, $e_1^1 + e_2^1 + e_1^2 + e_2^2 = \mathbf{0}^{\frac{n-3}{4}}$, then $e_2^2 = e_1^1 + e_2^1 + e_1^2$. Therefore, the system of equations (10) $\iff$

$$(12) \qquad \begin{cases} H_{large}(e_1^1 + e_2^1, e_1^1 + e_2^1, e_1^3 + e_2^3 + |e_2^1| + |e_1^1| + |e_2^2| + e_2^3 + e_3)^T = \mathbf{0}^{L_2} \\ H_{small}(\mathbf{0}^{\frac{n-3}{4}})^T = \mathbf{0}^{L_1} \\ e_3 = |e_1^1| + |e_1^2| + e_1^3 \\ |e_2^1| + |e_1^2| + e_2^3 + e_3 + \lambda(x'' + e_1^1 + e_1^2, y) + \lambda(x'', y) = 0 \\ e_4 = |e_1| + |e_2| + |e_3| + 1. \end{cases}$$

We obtain that

$$H_{large}(e_1^1 + e_2^1, e_1^1 + e_2^1, e_1^3 + e_2^3 + |e_2^1| + |e_1^1| + |e_2^2| + e_2^3 + e_3)^T = \mathbf{0}^{L_2} \iff \mathbf{0}^{\frac{n-3}{4}} \in H^{\frac{n-3}{4}}$$

– this condition is always true in this case. These errors are conditionally miscorrected. Their miscorrection probabilities depend on the nonlinearity of λ, and their number is equal to $2^{\frac{n+1}{2}} \cdot (2^{\frac{n-3}{4}} - 1)$. Repeating the arguments from Theorem 3,

$$|e_2^1| + |e_1^2| + e_2^3 + e_3 + \lambda(x'' + e_1^1 + e_1^2, y) + \lambda(x'', y) = 0 \iff$$

$$Pr(\lambda(x'' + e_1^1 + e_1^2, y) + \lambda(x'', y) = |e_2^1| + |e_1^2| + e_2^3 + e_3) \leq P_\lambda.$$

An error from this class is miscorrected by algorithm with a probability not more than P_λ.

c) If $e_1^1 + e_2^1 + e_1^2 + e_2^2 \neq 0$, then (10) $\iff$

$$(13) \qquad \begin{cases} H_{large}(e_1^1 + e_2^1, e_1^2 + e_2^2, e_1^3 + e_2^3 + |e_2^1| + |e_1^2| + e_2^3 + e_3 + |e_1^1| + |e_1^2| + e_1^3 + \\ \quad + e_3)^T = \mathbf{0}^{L_2} \\ e_2^2 \in e_1^1 + e_2^1 + e_1^2 + H^{\frac{n-3}{4}} \backslash \{\mathbf{0}^{\frac{n-3}{4}}\} \\ |e_1^1| + |e_1^2| + e_1^3 + e_3 + \mu(e_1^1 + e_2^1 + e_1^2 + e_2^2 + y) + \mu(y) = 0 \\ |e_2^1| + |e_1^2| + e_2^3 + e_3 + \lambda(x'' + e_1^1 + e_1^2, y + e_1^1 + e_2^1 + e_1^2 + e_2^2) + \\ \quad + \lambda(x'', y) = 0 \\ e_4 = |e_1| + |e_2| + |e_3| + 1. \end{cases}$$

As

$$H_{large}(e_1^1+e_2^1, e_1^2+e_2^2, e_1^3+e_2^3+|e_2^1|+|e_1^2|+e_2^3+e_3+|e_1^1|+|e_1^2|+e_1^3+e_3)^T = \mathbf{0}^{L_2} \iff$$

$$e_1^1 + e_2^1 + e_1^2 + e_2^2 \in H^{\frac{n-3}{4}},$$

this condition is always true in this case. Errors from this class are conditionally miscorrected. Their miscorrection probabilities depend on the nonlinearity of λ and μ. The number of errors is equal to $2^{\frac{n-3}{4}} \cdot 2^{\frac{n-3}{4}} \cdot 2 \cdot 2^{\frac{n-3}{4}} \cdot (\frac{2^{\frac{n-3}{4}}}{\frac{n+1}{4}} - 1) \cdot 2 \cdot 2 \cdot 1 = 2^{\frac{n+1}{2}} \cdot 2^{\frac{n-3}{4}} \cdot (\frac{2^{\frac{n-3}{4}}}{\frac{n+1}{4}} - 1)$.

As above,

$$\mu(e_1^1 + e_2^1 + e_1^2 + e_2^2 + y) + \mu(y) + |e_1^1| + |e_1^2| + e_1^3 + e_3 = 0 \iff$$

$$Pr(\mu(e_1^1 + e_2^1 + e_1^2 + e_2^2 + y) + \mu(y) = |e_1^1| + |e_1^2| + e_1^3 + e_3) \leq P_\mu,$$

and

$$\lambda(x'' + e_1^1 + e_1^2, y + e_1^1 + e_2^1 + e_1^2 + e_2^2) + \lambda(x'', y) + |e_2^1| + |e_1^2| + e_2^3 + e_3 = 0 \iff$$

$$Pr(\lambda(x'' + e_1^1 + e_1^2, y + e_1^1 + e_2^1 + e_1^2 + e_2^2) + \lambda(x'', y) = |e_2^1| + |e_1^2| + e_2^3 + e_3) \leq P_\lambda.$$

An error from this class is miscorrected with a probability not more than $P_\mu \cdot P_\lambda$. □

Remember that h_i^{small} is the i-th column of the matrix H_{small}, $i \in \{1, \ldots, \frac{n-3}{4}\}$, and h_j^{large} is the j-th column of the matrix H_{large}, $j \in \{1, \ldots, \frac{n-1}{2}\}$.

Lemma 6. *If* $S = (h_i^{large} + h_{\frac{n-1}{2}}^{large} \cdot (\lambda(x''+u_i, y+u_i) + \lambda(x'', y) + \mu(u_i+y) + \mu(y)), h_i^{small}, 1+\mu(u_i+y)+\mu(y), \lambda(x''+u_i, y+u_i)+\lambda(x'', y), 1)$, *for some* $i \in \{1, \ldots, \frac{n-3}{4}\}$, *there exist* $\frac{n-3}{4}$ *error vectors of the form* $e = (\mathbf{0}^{\frac{n-3}{4}+i-1}, 1, \mathbf{0}^{\frac{3n+7}{4}-i})$ *meeting the syndrome, which are corrected by the algorithm,* $\frac{n-3}{4} \cdot (2^{\frac{n+1}{4}} - 1)$ *errors are miscorrected and* $\frac{n-3}{4} \cdot 2^{\frac{n+5}{4}} \cdot (2^{\frac{n-3}{4}} - 1)$ *errors are conditionally miscorrected by* $\bar{D}$ *with a probability not more than* P_λ.

Proof. For any $i \in \{1, \ldots, \frac{n-3}{4}\}$:

1) If $e_1^1 + e_2^1 + e_1^2 + e_2^2 = \mathbf{0}^{\frac{n-3}{4}}$, then $S_2 = H_{small}(\mathbf{0}^{\frac{n-3}{4}})^T = \mathbf{0}^{L_1} \neq h_i^{small}$, for any $i \in \{1, \ldots, \frac{n-3}{4}\}$ (by definition of H_{small}). Therefore, here we obtain an empty set of appropriate errors.

2) If $e_1^1 + e_2^1 + e_1^2 + e_2^2 \neq \mathbf{0}^{\frac{n-3}{4}}$, then the system of equations (10) $\iff$

$$\begin{cases} H_{large}(e_1 + e_2 + (\mathbf{0}^{\frac{n-3}{2}}, \lambda(x'' + e_1^1 + e_1^2, y + u_i) + \lambda(x'', y) + \mu(y + u_i) + \\ \quad +\mu(y)))^T = h_i^{large} + h_{\frac{n-1}{2}}^{large} \cdot (\lambda(x'' + u_i, y + u_i) + \lambda(x'', y) + \\ \quad +\mu(u_i + y) + \mu(y)) \\ e_1^1 + e_2^1 + e_1^2 + e_2^2 = u_i \\ e_3 = 1 + |e_1^1| + |e_1^2| + e_1^3 \\ e_2^3 = 1 + |e_1^1| + |e_2^1| + e_1^3 + \lambda(x'' + e_1^1 + e_1^2, y + u_i) + \\ \quad +\lambda(x'' + u_i, y + u_i) \\ e_4 = 1 + |e_1| + |e_2| + |e_3|. \end{cases} \tag{14}$$

a) If $e_1^1+e_1^2=u_i$, then $e_2^1+e_2^2=\mathbf{0}^{\frac{n-3}{4}}$, then (14) $\Longleftrightarrow$

$$(15)\quad \begin{cases} H_{large}(e_1+e_2)^T+h^{large}_{\frac{n-1}{2}}\cdot(\lambda(x''+u_i,y+u_i)+\lambda(x'',y)+\mu(y+u_i)+ \\ \quad +\mu(y))=h_i^{large}+h^{large}_{\frac{n-1}{2}}\cdot(\lambda(x''+u_i,y+u_i)+\lambda(x'',y)+\mu(u_i+y)+ \\ \quad +\mu(y)) \\ e_2^1+e_2^2=\mathbf{0}^{\frac{n-3}{4}}, e_1^2=e_1^1+u_i \\ e_3=e_1^3 \\ e_2^3=1+|e_1^1|+|e_2^1|+e_1^3 \\ e_4=1+|e_1|+|e_2|+|e_3|. \end{cases}$$

As

$$H_{large}(e_1+e_2)^T+h^{large}_{\frac{n-1}{2}}\cdot(\lambda(x''+u_i,y+u_i)+\lambda(x'',y)+\mu(y+u_i)+\mu(y))=$$
$$=h_i^{large}+h^{large}_{\frac{n-1}{2}}\cdot(\lambda(x''+u_i,y+u_i)+\lambda(x'',y)+\mu(u_i+y)+\mu(y))\Longleftrightarrow$$
$$H_{large}(e_1+e_2)^T=h_i^{large}\Longleftrightarrow e_1+e_2=(0^{i-1}10^{\frac{n-3}{2}-i}),$$

then (15) $\Longleftrightarrow$

$$(16)\quad \begin{cases} e_2^1=e_1^1+u_i \\ e_2^2=e_1^2, e_1^2=e_1^1+u_i \\ e_3=e_1^3 \\ e_2^3=e_1^3 \\ e_4=1+|e_1|+|e_2|+|e_3|. \end{cases}$$

The number of these errors is equal to $\frac{n-3}{4}\cdot 2^{\frac{n-3}{4}}\cdot 1\cdot 2\cdot 1\cdot 1\cdot 1\cdot 1\cdot 1=\frac{n-3}{4}\cdot 2^{\frac{n+1}{4}}$. There exist $\frac{n-3}{4}$ errors between them of the form $e=(\mathbf{0}^{i-1},1,\mathbf{0}^{n-i})$, which are corrected by the algorithm ($i\in\{1,\dots,\frac{n-3}{4}\}$). The other errors are miscorrected.

b) If $e_1^1+e_1^2\neq u_i$, then (14) $\Longleftrightarrow$

$$(17)\quad \begin{cases} H_{large}(e_1+e_2)^T+H_{large}((\mathbf{0}^{\frac{n-3}{2}},\lambda(x''+e_1^1+e_1^2,y+u_i)+\lambda(x'',y)+ \\ \quad +\mu(y+u_i)+\mu(y)))^T=h_i^{large}+h^{large}_{\frac{n-1}{2}}\cdot(\lambda(x''+u_i,y+u_i)+ \\ \quad +\lambda(x'',y)+\mu(u_i+y)+\mu(y)) \\ e_2^2=u_i+e_1^1+e_2^1+e_1^2 \\ e_3=1+|e_1^1|+|e_1^2|+e_1^3 \\ e_2^3=1+|e_1^1|+|e_2^1|+e_1^3+\lambda(x''+e_1^1+e_1^2,y+u_i)+ \\ \quad +\lambda(x''+u_i,y+u_i) \\ e_4=1+|e_1|+|e_2|+|e_3|. \end{cases}$$

Therefore,

$$H_{large}(e_1+e_2)^T+H_{large}((\mathbf{0}^{\frac{n-3}{2}},\lambda(x''+e_1^1+e_1^2,y+u_i)+\lambda(x'',y)+\mu(y+u_i)+\mu(y)))^T=$$
$$=h_i^{large}+h^{large}_{\frac{n-1}{2}}\cdot(\lambda(x''+u_i,y+u_i)+\lambda(x'',y)+\mu(u_i+y)+\mu(y))\Longleftrightarrow$$
$$H_{large}(e_1^2+e_2^2,e_1^2+e_2^2,e_1^3+e_2^3)^T=h^{large}_{\frac{n-1}{2}}\cdot(\lambda(x''+e_1^1+e_1^2,y+u_i)+\lambda(x''+u_i,y+u_i)).$$

The last correlation is true if and only if

$$e_1^2=e_2^2,\quad e_1^3+e_2^3=\lambda(x''+e_1^1+e_1^2,y+u_i)+\lambda(x''+u_i,y+u_i).$$

These are conditionally miscorrected errors, which miscorrection probability depends on the nonlinearity of λ. Their number is equal to $\frac{n-3}{4} \cdot 2^{\frac{n+5}{4}} \cdot (2^{\frac{n-3}{4}} - 1)$. Also,

$$e_2^3 = 1 + |e_1^1| + |e_2^1| + e_1^3 + \lambda(x'' + e_1^1 + e_1^2, y + u_i) + \lambda(x'' + u_i, y + u_i) \iff$$
$$\lambda(x'' + e_1^1 + e_1^2, y + u_i) + \lambda(x'' + u_i, y + u_i) = e_1^3 + e_2^3 \iff$$
$$Pr(\lambda(x'' + e_1^1 + e_1^2, y + u_i) + \lambda(x'' + u_i, y + u_i) = e_1^3 + e_2^3) \le P_\lambda.$$

An error from this class is miscorrected by algorithm with a probability less than or equal to P_λ. □

Theorem 4. *Let $\bar{D}$ be an extended code of length $n+1$, constructed by the switching method of ijk-components from H^n using nonlinear functions $\lambda : \mathbf{F}^{\frac{n-3}{4}} \times H^{\frac{n-3}{4}} \to \{0,1\}$ and $\mu : H^{\frac{n-3}{4}} \to \{0,1\}$, with $P_\lambda < 1$ and $P_\mu < 1$. The code $\bar{D}$ is partially robust with $|Ker_d(\bar{D}| = 2^{\frac{n-1}{2}}$. The number of errors miscorrected by all codewords is $|Ker_c(\bar{D})| = 2^{\frac{n+1}{4}} \cdot (2^{\frac{n+5}{4}} + n - 3) - n - 1$. Also, $|CME(\bar{D})| = 2^{n+3-log(n+1)} + 2^{\frac{n+1}{2}} \cdot (n-7) + 2^{\frac{n+5}{4}} \cdot (n-3)$. The conditionally miscorrected errors miscorrection probability is less than or equal to P_λ.*

Proof. The fact that $\bar{D}$ is partially robust code with $|Ker_d(\bar{D})| = 2^{\frac{n-1}{2}}$ follows from Theorem 3.

A multiple-bit error is miscorrected (or conditionally miscorrected) as a single-bit error if and only if one of the next cases is true:

1) $S = (\mathbf{0}^{L_2}, \mathbf{0}^{L_1}, 0, 0, 1)$;
2) $S = (\mathbf{0}^{L_2}, \mathbf{0}^{L_1}, 1, 1, 1)$;
3) $S = (h^{large}_{\frac{n-1}{2}}, \mathbf{0}^{L_1}, 1, 0, 1)$;
4) $S = (h^{large}_{\frac{n-1}{2}}, \mathbf{0}^{L_1)}, 0, 1, 1)$;

5a) $S = (h_i^{large} + h^{large}_{\frac{n-1}{2}} \cdot (\lambda(x'' + u_i, y + u_i) + \lambda(x'', y) + \mu(u_i + y) + \mu(y)), h_i^{small}, 1 + \mu(u_i + y) + \mu(y), \lambda(x'' + u_i, y + u_i) + \lambda(x'', y), 1)$, for some $i \in \{1, \ldots, \frac{n-3}{4}\}$;

5b) $S = (h^{large}_{i+\frac{n-3}{4}} + h^{large}_{\frac{n-1}{2}} \cdot (\lambda(x'' + u_i, y + u_i) + \lambda(x'', y) + \mu(y + u_i) + \mu(y)), h_i^{small}, 1 + \mu(u_i + y) + \mu(y), 1 + \lambda(x'' + u_i, y + u_i) + \lambda(x'', y), 1)$, for some $i \in \{1, \ldots, \frac{n-3}{4}\}$;

5c) $S = (h_i^{large} + h^{large}_{\frac{n-1}{2}} \cdot (\lambda(x'' + e_1^1 + e_1^2, y + e_1^1 + e_2^1 + e_1^2 + e_2^2) + \lambda(x'', y) + \mu(e_1^1 + e_2^1 + e_1^2 + e_2^2 + y) + \mu(y)), h_i^{small}, \mu(u_i + y) + \mu(y), 1 + \lambda(x'' + u_i, y + u_i) + \lambda(x'', y), 1)$, for some $i \in \{1, \ldots, \frac{n-3}{4}\}$;

5d) $S = (h^{large}_{i+\frac{n-3}{4}} + h^{large}_{\frac{n-1}{2}} \cdot (\lambda(x'' + e_1^1 + e_1^2, y + e_1^1 + e_2^1 + e_1^2 + e_2^2) + \lambda(x'', y) + \mu(e_1^1 + e_2^1 + e_1^2 + e_2^2 + y) + \mu(y)), h_i^{small}, \mu(u_i + y) + \mu(y), \lambda(x'' + u_i, y + u_i) + \lambda(x'', y), 1)$, for some $i \in \{1, \ldots, \frac{n-3}{4}\}$.

Similarly to Lemma 5, in each of the cases 1 – 4, there are $2^{\frac{n-1}{2}} - 1$ errors which are miscorrected by $\bar{D}$, the only error ($e = (\mathbf{0}^n, 1)$ in the case 1), $e = (\mathbf{0}^{n-1}, 1, 0)$ in 2), $e = (\mathbf{0}^{\frac{n-3}{2}}, 1, \mathbf{0}^{\frac{n+1}{2}})$ in 3), $e = (\mathbf{0}^{n-2}, 1, \mathbf{0}^2)$ in 4)) is corrected, $2^{\frac{n+1}{2}} \cdot (2^{\frac{n-3}{4}} - 1)$ errors are miscorrected with a probability less than or equal to P_λ, and $2^{\frac{n+1}{2}} \cdot 2^{\frac{n-3}{4}} \cdot (\frac{2^{\frac{n-3}{4}}}{2^{\frac{n+1}{4}}} - 1)$ errors are miscorrected by the algorithm with a probability less than or equal to $P_\mu \cdot P_\lambda \le P_\lambda$.

Similarly to Lemma 6, in each of the cases 5a) – 5d), there exist $\frac{n-3}{4}$ errors ($(\mathbf{0}^{\frac{n-3}{4}+i-1}, 1, \mathbf{0}^{\frac{3n+7}{4}-i})$ in 5a), $(\mathbf{0}^{\frac{n-3}{4}+i-1}, 1, \mathbf{0}^{\frac{3n+7}{4}-i})$ in 5b), $(\mathbf{0}^{\frac{n-1}{2}+i-1}, 1, \mathbf{0}^{\frac{n+3}{2}-i})$ in 5c), $(\mathbf{0}^{\frac{3n-5}{4}+i-1}, 1, \mathbf{0}^{\frac{n+9}{4}-i})$ in 5d), $i \in \{1, \ldots, \frac{n-3}{4}\}$), which are corrected by the

algorithm, $\frac{n-3}{4} \cdot (2^{\frac{n+1}{4}} - 1)$ errors are miscorrected and $\frac{n-3}{4} \cdot 2^{\frac{n+5}{4}} \cdot (2^{\frac{n-3}{4}} - 1)$ errors are conditionally miscorrected by $\bar{D}$ with a probability less than or equal to P_λ.

In the upshot, there exist $n+1$ errors, which are successfully corrected by $\bar{D}$, $|Ker_c(\bar{D})| = 2^{\frac{n+1}{4}} \cdot (2^{\frac{n+5}{4}} + n - 3) - n - 1$, $|CME(\bar{D})| = 2^{n+3-log(n+1)} + 2^{\frac{n+1}{2}} \cdot (n - 7) + 2^{\frac{n+5}{4}} \cdot (n-3)$. □

Remark. All the obtained results are true for the codes $\bar{C}_{\mu,\lambda}^{\frac{n-1}{2},n}$ and $\bar{C}_{\mu,\lambda}^{n-1,n}$, as well as for the other codes from Theorem 2.

4. Conclusion

An extended code, constructed by the switching method of ijk-components from H^n, is capable of correcting all the single errors and of detecting double and multiple bit errors. The numbers of undetectable and miscorrected errors for nonlinear codes, constructed by the switching method of ijk-components from H^n, are less than the corresponding numbers for the extended maximal linear code. Assuming that all the errors are equiprobable, the code $\bar{C}_{\mu,\lambda}^{\frac{n-1}{2},n-1}$, being partially robust, provides better memories protection than extended maximal linear codes in situations when a probability of multiple errors is high, while having the same order of encoding and decoding complexity. As distinct from linear codes, the nonlinear code $\bar{C}_{\mu,\lambda}^{\frac{n-1}{2},n-1}$ has conditionally detectable and conditionally miscorrected errors, so detection and correction of these errors depend on the message. This means that the codes from Theorem 2 also provide better memories protection against repeating errors.

For the extended Vasil'ev code $\bar{V}^n$, the number of detectable errors is $2^{\frac{n-1}{2}}$, $|CDE(\bar{V}^n)| = 2^{n+1-log(n+1)} - 2^{\frac{n+1}{2}}$ (see [2]), $|Ker_d(\bar{C}_{\mu,\lambda}^{\frac{n-1}{2},n-1})| = |Ker_d(\bar{V}^n)|$. At the same time, $|CDE(\bar{V}^n)| < |CDE(\bar{C}_{\mu,\lambda}^{\frac{n-1}{2},n-1})|$, for any length $n \geq 15$. The class of different codes, constructed by the switching method of ijk-components from H^n is wider than the class of Vasil'ev codes. So, using extended nonlinear codes, constructed by the switching method of ijk-components from H^n, may be advantageous.

The author is sincerely grateful to F.I.Solov'eva for valuable remarks and discussions, and to a reviewer for useful comments leading to improvements in the text.

References

[1] Wang Z., Karpovsky M.,Joshi A.J. *Nonlinear Multi-Error Correcting Codes for Reliable MLC NAND Flash Memories*, IEEE Trans. on VLSI, **20**:7 (2012), 1221-1234.

[2] Wang Z., Karpovsky M., Kulikowski K.J.*Replacing linear Hamming codes by robust nonlinear codes results in a reliability improvement of memories*, Proceedings of IEEE/IFIP International Conference on Dependable Systems and Networks, (2009), 514 - 523.

[3] Vasil'ev Yu.L.*On nongroup close-packed codes*, Problems of Cybernetics, **8** (1963), 337 – 339 (in Russian).

[4] Avgustinovich S. V., Solov'eva F. I.*On the nonsystematic perfect binary codes*, Problems of Inform. Transm., **32**:3 (1996) 47 – 50.

[5] Hergert F.*Algebraische Methoden fur Nichtlineare Codes*, Dissertation, Technische Hochschule Darmstadt, Germany, 1985.

[6] Avgustinovich S. V., Solov'eva F. I.*On the ranks and kernels problem for perfect codes*, Problems of Inform. Transm., **39**:4 (2003), 30 – 34.

[7] Solov'eva F. I.*Survey on perfect codes*, Mat. Vopr. Kibern., **18** (2013), 5 – 34.

[8] Avgustinovich S. V., Solov'eva F. I.*Construction of perfect binary codes by sequential translations of α-components*, Problems of Inform. Transm., **33**:3 (1997) 15 – 21.
[9] Kovalevskaya D.I.*Mollard Code as a Robust Nonlinear Code*, Problems of Inform. Transm., **54**:1 (2018), 34–47

Darya Igorevna Sikerina
State university of Aerospace Instrumentation,
Bolshaya Morskaya St., 67,
190000, Saint-Petersburg, Russia
Email address: dikovalevskaya@gmail.com