S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 18, №2, стр. 1506–1516 (2021) УДК 519.1
DOI 10.33048/semi.2021.18.113 MSC 68P30

ERROR-TOLERANT ZZW-CONSTRUCTION

YU.V. KOSOLAPOV, F.S. PEVNEV

Abstract. In 2008 Zhang, Zhang, and Wang proposed a steganographic construction that is close to upper bound of efficiency. However this system and many other are fragile to errors in the stegocontainer. Such errors can occur for example during the image processing. In this paper the ZZW-construction is modified for extracting data if errors and erasures occur in stegocontainer. It is shown that the correction is possible when linear codes in projective metrics (such as Vandermonde metric and phase rotating metric) are used. The efficiency of proposed construction is better than one for the well-known efficient combinatorial stegosystem.

Keywords: combinatorial steganography, projective metrics, Vandermonde metric, linear code, ZZW-construction.

1. Introduction

1.1. **Actuality.** Steganographic methods are used to hide the fact of data transmission unlike cryptography aims to hide the content of transmitted data. One can embed information into an image, audio, video or other file with slight modification and then transmit this file via the public channel. In this way a *container* is a bit sequence obtained from the carrier signal with some deterministic way, e.g. the sequence of the least significant bits of a signal, and a *stegocontainer* is a container with embedded message.

However, stegosystems are not usually resistant to errors occurred in the stegocontainer. If one or more errors occur then the extracted message can differ a lot from the embedded one (see [1]). This problem has a great actuality. For example, images are very widespread containers and these images can be modified or recompressed during the upload to social networks.

Kosolapov, Yu.V, Pevnev, F.S., Error-tolerant ZZW-construction.
© 2021 Kosolapov Yu.V., Pevnev F.S.
Received December, 21, 2020, published December, 2, 2021.

If we say about combinatorial steganography the quality of the embedding method is measured with *embedding efficiency* $e = L/T$ and *embedding rate* $\alpha = L/n$, where $L(\leqslant n)$ is the bit-length of embedding message and T is average count of *embedding changes* (see [2]). In [3] authors obtained the upper bound of embedding efficiency with respect to a given embedding rate

$$e(\alpha) \leqslant \frac{\alpha}{h_2^{-1}(\alpha)},\ 0 \leqslant \alpha \leqslant 1, \tag{1}$$

where $-h_2(x) = x\log_2 x + (1-x)\log_2(1-x)$. In [2] authors proposed a construction with embedding efficiency close to the upper bound (1). This stegosystem is usually called ZZW-construction by the first letters of its authors. However this construction is not resistant to errors and erasures in a stegocontainer. In this paper we modify ZZW-construction to make data extraction possible when errors and erasures occur in a stegocontainer. The modified construction is based on codes in projective metrics such as Vandermonde metric and phase rotating metric.

1.2. **Related work.** Note that correction errors in a stegocontainer is a well-known problem. In [3] authors proved that in combinatorial steganography this problem is equivalent to designing a centered error-correcting code (see [4]) and proposed a construction based on Hamming codes and Reed–Solomon codes.

In [5] the scheme based on cyclic codes was described. These codes are also used for preliminary encoding data so the error correction in the stegocontainer becomes possible. The embedding efficiency is not greater than 1.72. The optimality of construction is not discussed.

The paper [6] is devoted to embedding information into JPEG images with error correction. The method is based on the Hamming $[7, 4, 3]_2$ code and Repeat-Accumulate codes. The decoder for this construction is described in the great part of the paper. Other codes and containers are not discussed in this paper.

A construction based on matrix embedding with trellis-codes was proposed in [7]. It is also shown that trellis-codes lead to increase the errors count in the extracted data even if the noise in the channel is low. So authors think that trellis-codes are not suitable for the noisy channels and should be avoided. If it is impossible to avoid such codes authors provide a method for decreasing the number of errors in the extracted data.

1.3. **Organization.** The rest of the paper is organized as follows. In Section 2.1 we recall necessary information about codes in projective metrics and prove the sufficient conditions for correction up to $l - k$ errors in Vandermonde metric with a linear $[l, k]_q$ code. In Section 3 this result is used to correct erasures and errors in a stegocontainer. ZZW-construction and its underlying methods such as matrix embedding and writing on wet paper are discussed in Section 2.2. Section 4 is devoted to results and discussion. Section 5 concludes the paper.

2. Preliminaries

2.1. **Projective metrics.** To decode a vector $\mathbf{z} = (z_1, ..., z_n)$ one can usually find a codeword $\mathbf{c} = (c_1, ..., c_n)$ such that $\mathbf{c}$ is the closest to $\mathbf{z}$ in some metric. Perhaps, the most frequently used metric is the Hamming metric $\rho_H(\mathbf{c}, \mathbf{z}) = |\{i\colon c_i \neq z_i\}|$. Note that the Hamming metric is a special case of projective metric (see [8]). To define a projective metric suppose $\mathbb{F}_q^n$ is a linear space and $\mathcal{F} = (\mathbf{f}_i)_{i=1}^N$ is $n \times N$

matrix, where $n \leqslant N$ and the set of columns $\mathbf{f}_i$ contains a basis for $\mathbb{F}_q^n$. The *$\mathcal{F}$-norm* $\mathcal{N}_{\mathcal{F}}(\mathbf{x})$ of a vector $\mathbf{x}(\in \mathbb{F}_q^n)$ is corresponded to $\mathcal{F}$ and is defined as

$$\mathcal{N}_{\mathcal{F}}(\mathbf{x}) = \min_{\substack{\mathbf{a}\in\mathbb{F}_q^N: \\ \mathcal{F}\mathbf{a}=\mathbf{x}}} \mathcal{N}_H(\mathbf{a}),$$

where

$$\mathcal{N}_H(\mathbf{a}) = \mathrm{wt}(\mathbf{a}) = \rho_H(\mathbf{a}, \mathbf{0})$$

is also called *the Hamming weight* (or *weight*) of the vector $\mathbf{a}$. In other words, since $\mathbf{x}$ can be considered as a linear combinations of vectors $\mathbf{f}_i$ by some different ways we see that the $\mathcal{F}$-norm of a vector $\mathbf{x}$ is equal to the least number of vectors $\mathbf{f}_i$ in such linear combination. A vector is called an *elementary error* if its $\mathcal{F}$-norm is equal to 1, so vectors $\mathbf{f}_i$ are elementary errors. The *$\mathcal{F}$-distance* for vectors $\mathbf{a}$ and $\mathbf{b}$ is defined as $\mathcal{N}_{\mathcal{F}}(\mathbf{a} - \mathbf{b})$.

It is worth noting that the projective metric corresponds to the distance in some Cayley graph on the set of all vectors with the set of generators consists of all columns of the matrix $\mathcal{F}$ and all collinear vectors to them (see [9]). Cayley graphs are related to some classical problems in pure mathematics and many practical problems in various fields of science (see survey [10]). Particularly Cayley graphs are used in steganography to construct efficient stegosystems without active warden assumption [11].

The Hamming metric corresponds to an identity $n \times n$ matrix I_n. Let us consider *phase rotation invariant code*s as an example of codes in non-Hamming projective metric (see [12]). This metric is called *phase rotating metric* (PR-metric) and corresponds to the matrix $\mathcal{F} = [I_n|\mathbf{1}^T]$, where $\mathbf{1}^T$ is a transposed all-one vector of the length n. Thus the elementary errors set for PR-metric include the similar set for the Hamming metric and the all-one vector in addition. These codes can be simply designed basing on usual codes in the Hamming metric. In fact, the next proposition can be proved (see [12]).

Proposition 1. *Suppose the $[n, k, d]_2$ code in the Hamming metric contains the all-one vector; then there exists a $[n-1, k-1]_2$ code with minimum PR-distance equal to d.*

Another important special case of projective metric is *Vandermonde metric* (see [13]). Let $\mathcal{F}$ be a Vandermonde matrix over $\mathbb{F}_q$:

$$\mathcal{F} = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \alpha_1 u_1 & \alpha_2 u_2 & \dots & \alpha_m u_m \\ \alpha_1 u_1^2 & \alpha_2 u_2^2 & \dots & \alpha_m u_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1 u_1^{l-1} & \alpha_2 u_2^{l-1} & \dots & \alpha_m u_m^{l-1} \end{pmatrix}, \tag{2}$$

where $l \leqslant m$, $\alpha_i \neq 0$, $u_i \neq u_j$. The generator matrix of an error correcting code in this metric is a transposed Vandermonde matrix over $\mathbb{F}_q$:

$$G^T = \begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_k \\ \beta_1 v_1 & \beta_2 v_2 & \dots & \beta_k v_k \\ \beta_1 v_1^2 & \beta_2 v_2^2 & \dots & \beta_k v_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1 v_1^{l-1} & \beta_2 v_2^{l-1} & \dots & \beta_k v_k^{l-1} \end{pmatrix}, \tag{3}$$

where $k < l$, $\beta_i \neq 0$, $v_i \neq v_j$, $v_i \neq u_j$. It is clear that

$$k + m \leqslant q. \tag{4}$$

The code spanned by the rows of matrix G is $[l, k]_q$ code and is able to correct errors of weight $\lfloor (l-k)/2 \rfloor$ in Vandermonde metric. It takes polynomial time to reduce decoding of such codes to decoding of generalized Reed–Solomon codes (see [13]).

Let us show that the correction ability of codes in Vandermonde metric can be improved if an additional information about error's structure is given. The *error locator* of an error vector $\mathbf{e} \in \mathbb{F}_q^l$ is the vector $\mathbf{e}_{loc} \in \mathbb{F}_2^m$ such that

$$\exists \mathbf{a} \colon \operatorname{supp}(\mathbf{a}) \subseteq \operatorname{supp}(\mathbf{e}_{loc}), \quad \mathcal{F}\mathbf{a}^T = \mathbf{e}^T, \tag{5}$$

where $\operatorname{supp}(\mathbf{x}) = \{i : x_i \neq 0\}$.

Lemma 1. *Suppose C is an $[l, k]_q$ code in Vandermonde metric with corresponded matrix of the form* (2)*, the generator matrix of code C has the form* (3)*,*

$$\mathbf{z} = \mathbf{c} + \mathbf{e},\ \mathbf{c} \in C, \tag{6}$$

$\mathbf{e}_{loc}$ is error locator of $\mathbf{e}$, $\mathcal{N}_H(\mathbf{e}_{loc}) = t \leqslant l - k$. Then the error $\mathbf{e}$ can be found in polynomial time.

Proof. Firstly let us construct a matrix G_{ext}

$$G_{ext}^T = (G^T | \mathbf{f}_{i_1} \mathbf{f}_{i_2} \dots \mathbf{f}_{i_t}), \quad \{i_1, \dots, i_t\} = \operatorname{supp}(\mathbf{e}_{loc}). \tag{7}$$

To decode $\mathbf{z}^T$ we need to solve the system of equations

$$G_{ext}^T \widetilde{\mathbf{m}}^T = \mathbf{z}^T$$

for the vector $\widetilde{\mathbf{m}}$. On the one hand this system has a solution because the $\mathbf{z}$ is a linear combination of columns of matrix G_{ext}^T. On the other hand there exists only one solution of the system because $\operatorname{rank}(G_{ext}^T) = k + t \leqslant l$. The first k coordinates of $\widetilde{\mathbf{m}}$ are equal to information vector $\mathbf{m}$ corresponding to codeword $\mathbf{c}$. To complete the proof let us note that $\mathbf{e} = \mathbf{z} - \mathbf{m}G$. □

Using (5), we obviously have $\mathcal{N}_{\mathcal{F}}(\mathbf{e}) \leqslant \mathcal{N}_H(\mathbf{e}_{loc})$. Combining this inequality with Lemma 1 we can conclude that it is able to correct up to $l-k$ errors in Vandermonde metric in some special cases if the error locator is given. A more general lemma can be proved.

Lemma 2. *Suppose C is an $[l, k]_q$ code in Vandermonde metric with corresponding matrix of the form* (2)*, the generator matrix of code C has the form* (3)*, the error vector $\mathbf{e}$ in* (6) *is the sum of two vectors $\mathbf{e}^1$ and $\mathbf{e}^2$ such that*

$$\operatorname{supp}(\mathbf{e}_{loc}^1) \cap \operatorname{supp}(\mathbf{e}_{loc}^2) = \emptyset,$$

$\mathcal{N}_H(\mathbf{e}_{loc}^1) = v$, $\mathcal{N}_H(\mathbf{e}_{loc}^2) = t$, $v + 2t \leqslant l - k$, $m - v \geqslant l$, and $\mathbf{e}_{loc}^1$ is given. Then the error $\mathbf{e}$ can be found in polynomial time.

Proof. Firstly let us construct a matrix

$$\mathcal{F}_{ext} = (\mathbf{f}_{j_1} \mathbf{f}_{j_2} \dots \mathbf{f}_{j_{m-v}}),$$

where $\{j_1, \dots, j_{m-v}\} = \{1, ..., n\} \setminus \operatorname{supp}(\mathbf{e}_{loc}^1)$. In [13], authors prove that $[l, (k+v)]_q$ code C_{ext} spanned by the columns of matrix (7), where $\mathbf{e}_{loc} = \mathbf{e}_{loc}^1$, is able to correct

no more than $\lfloor (l-(k+v))/2 \rfloor$ errors in $\mathcal{F}_{ext}$-metric in polynomial time. Any $\mathbf{z}$ from (6) can be considered as a sum

$$\mathbf{z} = \mathbf{c} + \mathbf{e}^1 + \mathbf{e}^2 = \tilde{\mathbf{c}} + \mathbf{e}^2,$$

where $\tilde{\mathbf{c}} \in C_{ext}$, and $\mathbf{e}^2$ is error vector. Since

$$\mathcal{N}_{\mathcal{F}_{ext}}(\mathbf{e}^2) \leqslant \mathcal{N}_H(\mathbf{e}^2_{loc}) = t \leqslant \left\lfloor \frac{l-(k+v)}{2} \right\rfloor,$$

it follows that $\tilde{\mathbf{c}}$ can be efficiently obtained. The first k coordinates of $\widetilde{\mathbf{m}}$ corresponding to codeword $\tilde{\mathbf{c}} (\in C_{ext})$ are equal to information vector $\mathbf{m}$. To complete the proof let us note that $\mathbf{e} = \mathbf{z} - \mathbf{m}G$. □

2.2. **ZZW-construction.** To begin with let us briefly describe the embedding method called *writing on wet paper* (see [14]) so far as this method is used in ZZW-construction. Suppose $\mathbf{c}$ is an empty container and $\mathbf{m}$ is the message to be embedded. Some coordinates of the container are forbidden to be changed. These coordinates are called "wet" and others are called "dry". We also assume that the receiver can not differ "wet" and "dry" coordinates but have to extract the message anyway. In coding theory such "wet paper" channel is called as *memory with defective cells* (see [15]).

Let ω be the set of "dry" coordinates for the container $\mathbf{c}$. We denote the stego-container with embedded message by $\mathbf{z}$. The sender and receiver must choose the same $l \times m$ matrix D ($l \leqslant m$) and then the extracting rule is

$$D\mathbf{z}^T = \mathbf{m}^T. \tag{8}$$

Let $\mathbf{v} = \mathbf{z} - \mathbf{c}$, then $D(\mathbf{c}+\mathbf{v})^T = \mathbf{m}^T$ and

$$D\mathbf{v}^T = \mathbf{m}^T - D\mathbf{c}^T = \widetilde{\mathbf{m}}^T.$$

Suppose $\mathbf{v}_\omega$ is the vector containing the coordinates of the vector $\mathbf{v}$ belonging to ω and $\mathbf{v}_{\bar{\omega}}$ is the vector containing other coordinates of the vector $\mathbf{v}$. Then

$$D\mathbf{v}^T = D_\omega \mathbf{v}_\omega^T + D_{\bar{\omega}} \mathbf{v}_{\bar{\omega}}^T,$$

where D_ω is the matrix containing the columns of the matrix D corresponding to ω. Since $\mathbf{v}_{\bar{\omega}} = \mathbf{0}$ then

$$D_\omega \mathbf{v}_\omega^T = \widetilde{\mathbf{m}}^T. \tag{9}$$

To embed the message one should solve (9) for $\mathbf{v}_\omega$, when D, ω, and $\widetilde{\mathbf{m}}$ are given. Let us remark that it is a challenge to choose the same matrix D for the sender and receiver when multiple data transmission occurred. In [14] authors propose to generate a pseudo-random matrix using a shared secret key. The next problem is to transmit the length of the embedded message since this length depends on solvability of (9) and may differ from one transmission to another. As follows from [14] to fix this problem one can take $L_0 = \lceil \log_2 M \rceil$ coordinates in the beginning of the message to put the information about the length into them, where M is the greatest length of the message and is usually equal to the container's length. Consider that the receiver can generate the matrix D row-by-row. Then he or she generates the first L_0 rows of the matrix D, extracts the length by multiplying this submatrix by the received vector, generates all other rows of D, and finally extracts the whole message. The channel has negligible decrease of capacity and the same asymptotic efficiency.

To describe ZZW-construction (see [2]) let an empty container $X(\in \mathbb{F}_2^n, n = m2^r)$ be a matrix

$$\begin{bmatrix} x_{1,1} & x_{2,1} & \dots & x_{m,1} \\ x_{1,2} & x_{2,2} & \dots & x_{m,2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,2^r-1} & x_{2,2^r-1} & \dots & x_{m,2^r-1} \\ x_{1,2^r} & x_{2,2^r} & \dots & x_{m,2^r} \end{bmatrix} = \begin{bmatrix} \mathbf{x}_1^T & \mathbf{x}_2^T & \dots & \mathbf{x}_m^T \\ x_{1,2^r} & x_{2,2^r} & \dots & x_{m,2^r} \end{bmatrix}. \tag{10}$$

It is proposed to form two stegochannels for any container of the form (10). First of those channels is called *the sum channel*. The sum channel is a vector $\mathbf{y} = (y_1, \dots, y_m)$, $y_i = \oplus_{j=1}^{2^r} x_{i,j}$ for every $i = 1, ..., m$. To embed the message $\mathbf{m}_1 = (m_{1,1}, \dots, m_{1,m})$ into $\mathbf{y}$ it is necessary to flip any (but only one) bit in the i-th column of the matrix of the form (10) if $m_{1,i} \neq y_i$ and do nothing otherwise. Let us denote by τ the set of coordinates needed to be changed for embedding,

$$\tau = \{i \in \{1, \dots, m\} \colon m_{1,i} \neq y_i\}, \quad |\tau| = \mu. \tag{11}$$

It is possible to embed the message into a random container with changing $m/2$ bits in average.

To form the second channel the appropriately modified vectors $\mathbf{x}_1$,...,$\mathbf{x}_m$ are multiplied by the parity-check matrix for the $[2^r - 1, 2^r - r - 1, 3]_2$ Hamming code. As a result we get the set of syndromes for appropriately modified vectors $\mathbf{x}_1$,...,$\mathbf{x}_m$. Since the covering radius for any Hamming code is equal to one then for any vector $\mathbf{s}_i(\in \mathbb{F}_2^r)$ there exists a vector $\mathbf{e}_i$ such that $H(\mathbf{x}_i + \mathbf{e}_i)^T = \mathbf{s}_i^T$ and $\mathrm{wt}(\mathbf{e}_i) \leqslant 1$. In other words it is possible to get any syndrome with changing no more than one bit of vector $\mathbf{x}_i$. This fact can be used for embedding a message $\mathbf{m}_2$ into the second channel using writing on wet paper. The second channel is further called *the vector channel*. A container in this channel is a sequence of bits of syndromes $\mathbf{s}_i$. If the syndrome corresponds to the set τ (see (11)) then the bits of this syndrome are "dry" (and the syndrome is called "dry"). Bits of other syndromes are "wet" (and the syndromes are called "wet"). Finally, if $\mathbf{x}_i$ corresponds to τ and has the exact syndrome (so $\mathbf{x}_i$ can not be changed) the bit $x_{i,2^r}$ should be flipped. Thus $\mathbf{m}_1$ and $\mathbf{m}_2$ can be embedded into any container of the form (10).

The parameters of ZZW depend on the method of embedding information into the sum channel (see [2]). There is also some indeterminacy in the capacity of the vector channel since the count of "dry" positions depends on the sum channel. Nevertheless it is possible to embed $m + \frac{rm}{2}$ bits in average into the container of length $n = m2^r$ with changing $m/2$ bits in average.

3. Modified ZZW-construction

3.1. **Single error correction.** Let us point out that ZZW-construction can not recover the message if errors occur in the stegocontainer. Suppose there is only one corrupted bit in a stegocontainer of the form (10). It leads to one error in the sum channel. One can use $[m, k_1]_2$ code C_{sum} to fix this error. Note that the length of the message embedding to the sum channel decreases to k_1. Consider what a single bit error in the vector channel leads to. Suppose there is a mapping of the linear space $\mathbb{F}_2^r$ to the finite field $\mathbb{F}_{2^r}$ then a stegocontainer in the vector channel can be

considered as a vector $\mathbf{z} = (z_1, \ldots, z_m)$ over the field $\mathbb{F}_{2^r}$. Let us also assume the $l \times m$ matrix D from (8) consists of elements from $\mathbb{F}_{2^r}$ and $l \leqslant m$. A single bit error in the stegocontainer of the form (10) can lead to corruption of one coordinate of the vector $\mathbf{z}$. Thus the corrupted stegocontainer in the vector channel is denoted as $\tilde{\mathbf{z}} = \mathbf{z} + \mathbf{e}$, where $\mathrm{wt}(\mathbf{e}) \leqslant 1$. If we combine this with the rule (8) we obtain

$$D\tilde{\mathbf{z}}^T = D(\mathbf{z} + \mathbf{e})^T = \mathbf{m}_2^T + \lambda \mathbf{d},$$

where $\mathbf{d}$ is a column of the matrix D. Since $0 \leqslant \mathrm{wt}(\mathbf{d}) \leqslant l$ then it is quite hard to use error-correcting codes in the Hamming metric. On the other hand this error can be corrected if the vector $\mathbf{m}_2$ is a codeword of suitable $[l, k]_{2^r}$ code C_{vec} in the projective metric corresponding to matrix D. This code should be able to correct elementary errors (in other words these errors are columns of the matrix D being multiplied by scalar value and the D-norm of any those errors is equal to one).

Let us restrict ZZW-construction to use code C_{vec} in the projective metric. Assume D is a Vandermonde matrix over $\mathbb{F}_{2^r}$ (see (2)). Then there exists a suitable code C_{vec} spanned by the columns of matrix (3). The error locator for a single bit error is obtained by decoding of code C_{sum} in the sum channel. Since $v = 1$ and $t = 0$ according to Lemma 2 so we get $k = l - 1$. Note that if $|\tau| = \mu \geqslant l$ and D is $l \times m$ Vandermonde matrix then $\mathrm{rank}(D_\tau) = l$ so there exists a solution of (9) for an arbitrary right part. Hence it is possible to embed lr bits with writing on wet paper when there are at least l "dry" syndromes. Thus it is possible to embed $kr = (l-1)r$ bits (and $rm/2 - r$ bits in average since $\mu = m/2$ in average and $l = \mu$) into the vector channel. Since

$$k + m = l - 1 + m \leqslant 2m - 1 \leqslant 2^r$$

it is enough to put $2m - 1 \leqslant 2^r$ to fit the restriction (4). So $m \leqslant 2^{r-1}$.

Note that the receiver must obtain l to generate matrix D and extract information. The method proposed in [14] and described above is useless since the bits carrying the length of the message can be corrupted. One possible solution of this problem is to choose fixed value l. Let us use the following technique. If $\mu(= |\tau|)$ is quite small then we flip all bits of vector $\mathbf{y}$. This leads to double flipping of bits from τ and single flipping of other bits. Hence the set τ is changed and $\tau_{new} = \{1, ..., m\} \setminus \tau$, $|\tau_{new}| = m - \mu$. It is clear that

$$\max\{|\tau|, |\tau_{new}|\} = \max\{\mu, m - \mu\} \geqslant \lceil m/2 \rceil .$$

Thus it becomes possible to fix $l = \lceil m/2 \rceil$ though the count of "dry" syndromes can be larger in fact. To use this technique we need to restrict the code C_{sum}. Since the all-bit inversion can occur then phase rotation invariant codes are suitable if these codes are able to correct up to two errors: the first one is an error in stegocontainer and the second is an all-bit inversion. Surely the $[m, k_1]_2$ code C_{sum} for the sum channel must be shared between the sender and receiver. Since $l = \lceil m/2 \rceil$ and $k = l - 1$ then matrices D and G can be generated in advance.

The embedding process contains two steps. The message is preliminary split into two parts. In the first step one part of the message is encoded into the codeword $\mathbf{m}_1 (\in C_{\mathrm{sum}})$ and is embedded into the sum channel $\mathbf{y}$. The set τ of "dry" coordinates is also defined in this step. In the second step another part of the message is encoded with the $(\lceil m/2 \rceil - 1) \times \lceil m/2 \rceil$ matrix G of the form (3) and is embedded into the vector channel with writing on wet paper using the $\lceil m/2 \rceil \times m$ matrix $D = \mathcal{F}$

(see (2)). If y_i is flipped but $\mathbf{x}_i$ is forbidden for changing then $x_{i,2^r}$ should be flipped.

The extracting process also contains two steps. In the first step one part of the message is extracted from the sum channel and decoded with the C_{sum} decoder. If any single error occurred then it is corrected and the error locator is obtained. In the second step another part of the message is extracted from the vector channel using the rule (8) and is decoded with the C_{vec} decoder. If any single error occurred then it is corrected using the error locator obtained on the first step.

Thus the count of bits possible for embedding into a container of the form (10) is equal to $L = O(m) + (\lceil m/2 \rceil - 1)r$. Using the Stirling's approximation we get the number of embedding changes

$$T = \sum_{i=0}^{\lceil m/2 \rceil - 1} \frac{(m-i)C_m^i}{2^m} + \sum_{i=\lceil m/2 \rceil}^{m} \frac{iC_m^i}{2^m} = \frac{m}{2}\left(1 + \frac{C_{m-1}^{\lfloor (m-1)/2 \rfloor}}{2^{m-1}}\right) \approx \frac{m}{2}\left(1 + \sqrt{\frac{2}{\pi m}}\right). \tag{12}$$

The embedding efficiency is equal to

$$e = \frac{L_i}{T} \approx \frac{O(m) + (\lceil m/2 \rceil - 1)r}{m/2 + \sqrt{(m/2\pi)}}.$$

3.2. **Correction of multiple errors.** The construction described above can be generalized to correct up to t errors.

Theorem 1. *Suppose C is $[m+1, k_1+1, 2(t+1)+1]_2$ code containing the all-one vector and there exists an efficient decoder for this code. Then there exists a polynomial-time algorithm of embedding $k_1 + (\lceil m/2 \rceil - t)r$ bits into a container of the form* (10) *and t or less errors in the stegocontainer can be corrected.*

Proof. As it follows from Proposition 1 the phase rotation invariant $[m, k_1, 2(t+1)+1]_2$ code C_{sum} can be designed based on the code C. The decoder of C_{sum} is simply obtained from the decoder of C (see [13]). The $[l,k]_{2^r}$ code C_{vec} in the Vandermonde metric can be also designed, where $k = l - t$, $l \leqslant m$. This means that ZZW-construction can be modified in the way described above using C_{sum} and C_{vec}. This modified construction allows to embed $k_1 + (\lceil m/2 \rceil - t)r$ bits into a container of the form (10).

By t_1 denote the count of stegocontainer columns such that odd number of errors occurred in each such column. By t_2 denote the count of stegocontainer columns such that even non-zero number of errors occurred in each such column. It is clear that $2t_2 + t_1 \leqslant t = l - k$. This leads to t_1 errors in the sum channel. Since the code C_{sum} is able to correct $t+1 \geqslant t_1+1$ errors, one can extract the message from the sum channel and obtain the partial error locator $\mathbf{e}^1_{loc}$ in the vector channel ($\mathcal{N}_H(\mathbf{e}^1_{loc}) = t_1$). The error $\mathbf{e}^2$ in the vector channel occurs on account of stegocontainer columns with even number of errors. To apply Lemma 2 the condition $m - t_1 \geqslant l$ must be satisfied. Since $t_1 \leqslant t < l = \left\lceil \frac{m}{2} \right\rceil$ then $t_1 \leqslant \left\lfloor \frac{m}{2} \right\rfloor = m - \left\lceil \frac{m}{2} \right\rceil = m - l$. Thus the application of Lemma 2 yields a polynomial-time correction up to t errors. □

It is obviously that the number of the embedding changes does not change (see (12)). The count of bits possible for embedding is

$$L = \alpha m + (\lceil m/2 \rceil - t)r, \tag{13}$$

where α is information rate of the C_{sum}. Thus the embedding efficiency is equal to

$$e = \frac{L}{T} \approx \frac{\alpha m + (\lceil m/2 \rceil - t)r}{m/2 + \sqrt{(m/2\pi)}}. \tag{14}$$

The similar theorem can be proved for the case of errors and erasures.

Theorem 2. *Suppose the minimum PR-distance of a phase rotation invariant code C_{sum} satisfies the inequality $d_{\text{PR}} \geqslant 2t+v+3$ and parameters of an $[l,k]_{2^r}$ code C_{vec} satisfies the equality $k = l - (t+v)$. Then there exists a polynomial-time algorithm of correcting up to t errors and v erasures in a container of the form* (10).

Proof. Suppose v_1 is the count of stegocontainer columns with at list one erasures, t_1 is the count of stegocontainer columns such that odd number of errors and no erasures occurred in each such column, and t_2 is the count of stegocontainer columns such that even non-zero number of errors and no erasures occurred in each such column. It is clear that $2t_2 + t_1 + v_1 \leqslant t + v = l - k$. This leads to t_1 errors and v_1 erasures in the sum channel. Since $v_1 + 2(t_1 + 1) \leqslant v + 2t + 2 \leqslant d_{\text{PR}} - 1$ and phase rotation can occur then it is able to extract the message from the sum channel and to obtain the partial error locator $\mathbf{e}^1_{loc}$ in the vector channel ($\mathcal{N}_H(\mathbf{e}^1_{loc}) = v_1 + t_1$). The error $\mathbf{e}^2$ in the vector channel occurs on account of stegocontainer columns with even number of errors and no erasures. To apply Lemma 2 the condition $m - l \geqslant t_1 + v_1$ must be satisfied. Indeed as

$$t_1 + v_1 \leqslant t + v = l - k < l = \left\lceil \frac{m}{2} \right\rceil$$

0 then

$$t_1 + v_1 \leqslant \left\lfloor \frac{m}{2} \right\rfloor = m - \left\lceil \frac{m}{2} \right\rceil = m - l.$$

Thus the application of Lemma 2 yields a polynomial-time correction up to t errors and v erasures. □

4. Results and discussion

Let us provide the results of computation for $t = 2$. For the modified ZZW-construction we suppose base code for the sum channel as Reed–Muller code with minimal distance equal to 8, so this code is able to correct up to three errors and $t = 2$. For example, the base $[16, 5, 8]_2$ Reed–Muller code is used to design $[15, 4]_2$ code C_{sum}. The stegosystem parameters calculated by (12), (13), (14) are listed in Table 1. To compare with we use the stegosystem proposed in [3] since this one is close to our modification. The parameters of stegocontainer and efficiency for this system are listed in Table 2.

It is shown that modified ZZW stegosystem is more efficient than stegosystem proposed in [3] for some parameters of stegocontainer (see and compare values in the last row of each table). An actual problem is to design codes of large dimension containing the all-one vector because these codes can be basic for phase rotation invariant codes used in the sum channel. This codes are called *self-complementary* (see [16] for details). Particulary these codes meet the Grey–Rankin bound and can be either linear or not. In fact these code are related to Hadamard matrices and SDP designs (designs with the symmetric difference property).

Таблица 1. Efficiency of modified ZZW for $t = 2$

m	15	31	63
r	5	6	7
stegocontainer length, n	480	1984	8064
$l = \lceil m/2 \rceil$	8	16	32
$k = l - t$	6	14	30
C_{sum} rate, α	4/15	5/31	6/63
embedded bits, L	34	99	251
average embedding changes, T	9.07	17.74	34.68
embedding efficiency, e	3.75	5.58	7.24

Таблица 2. Efficiency of stegosystem [3] for $t = 2$

m	15	31	63
r	5	6	7
stegocontainer length, n	465	1953	8001
embedded bits, L	55	162	413
average embedding changes, T	14.53	30.52	62.51
embedding efficiency, e	3.78	5.31	6.61

5. Conclusions

In this paper we have proposed a new technique for the code design of an error-tolerant modification of ZZW-construction. The efficiency of proposed construction is comparable with the efficiency of construction from [3] for some fixed parameters (see Tables 1, 2 for details). In despite of this we expect that the efficiency can be increased by using another codes in the sum channel. Designing of such codes is an open problem. Particulary there is an actual problem to design self-complementary codes of large dimension because these codes can be optimal for phase rotation invariant codes used in the sum channel.

Acknowledgments

The authors are grateful to the reviewer for valuable comments and useful advice on the direction of further research on the relationship between projective metrics and Cayley graphs.

References

[1] G. Pan, Y.J. Wu, Z.H. Wu, *A novel data hiding method for two-color images*, Lect. Notes Comput. Sci., **2229** (2001), 261–270. Zbl 1050.68552

[2] W. Zhang, X. Zhang, S. Wang, *Maximizing steganographic embedding efficiency by combining Hamming codes and wet paper codes*, Proc. 10th Int. Workshop Inf. Hiding, Lecture Notes in Computer Science, **5284** (2008), 60–71.

[3] F. Galand, G. Kabatiansky, *Information hiding by coverings*, Proceedings 2003 IEEE Information Theory Workshop, 2003, 151–154.

[4] L.A. Bassalygo, M.S. Pinsker, *Centered error-correcting codes*, Probl. Inf. Transm., **35**:1 (1999), 25–31. Zbl 1014.94029

[5] X. Zhang, S. Wang, *Stego-encoding with error correction capability*, IEICE Trans. Fundamentals, **E88-A**:12 (2005), 3663–3667.

[6] A. Sarkar, U. Madhow, B. Manjunath, *Matrix embedding With pseudorandom coefficient selection and error correction for robust and secure steganography*, IEEE Transactions on Information Forensics and Security, **5**:2 (2010), 225–239.

[7] C. Kin-Cleaves, A.D. Ker, *Adaptive steganography in the noisy channel with dual-syndrome trellis codes*, 2018 IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, Hong Kong, 2018, 1–7.

[8] E.M. Gabidulin, J. Simonis, *Metrics generated by families of subspaces*, IEEE Trans. Inf. Theory, **44**:3 (1998), 1336–1341. Zbl 0910.94025

[9] O. Ore, *Theory of Graphs*, American Mathematical Society, Colloquium Publications, **38**, (AMS), Providence, 1962. Zbl 0105.35401

[10] E.V. Konstantinova, *Some problems on Cayley graphs*, Linear Algebra Appl., **429**:11-12 (2008), 2754–2769. Zbl 1148.05037

[11] J.-L. Kim, J. Park, S. Choi, *Steganographic schemes from perfect codes on Cayley graphs*, Des. Codes Cryptography, **87**:10 (2019), 2361–2374. Zbl 1419.94070

[12] E.M. Gabidulin, M. Bossert, *Hard and soft decision decoding of phase rotation invariant block codes*, 1998 International Zurich Seminar on Broadband Communications. Accessing, Transmission, Networking. Proceedings (Cat. No. 98TH8277), Zurich, Switzerland, 1998, 249–251.

[13] E.M. Gabidulin, V.A. Obernikhin, *Codes in the Vandermonde F-metric and their application*, Probl. Inf. Transm., **39**:2 (2003), 159–169. Zbl 1162.94414

[14] J. Fridrich, M. Goljan, P. Lisonek, D. Soukal, *Writing on wet paper*, IEEE Trans. Signal Process., **53**:10 (2005), 3923–3935. Zbl 1370.94555

[15] A.V. Kuznetsov, B.S. Tsybakov, *Coding in a memory with defective cells*, Probl. Peredaci Inform., **10**:2 (1974), 52–60. Zbl 0311.94012

[16] G. McGuire, *Quasi-symmetric designs and codes meeting the Grey-Rankin bound*, J. Comb. Theory, Ser. A, **78**:2 (1997), 280–291. Zbl 0873.05011

Yuri Vladimirovich Kosolapov
Southern Federal Univercity,
105/42, Bol'shaya Sadovaya str.,
Rostov-on-Don, 344006, Russia
Email address: yvkosolapov@sfedu.ru

Fedor Sergeevich Pevnev
Southern Federal Univercity,
105/42, Bol'shaya Sadovaya str.,
Rostov-on-Don, 344006, Russia
Email address: pevnev@sfedu.ru