The research focuses on an innovative error correction method that uses perfect binary arrays (PBAs), a powerful mathematical tool with unique properties that make it ideal for error correction. The research is aimed at studying the impact of uncorrelated mixed-type errors in the data exchange path, which allows using it in smart technologies with limited computing capabilities. The effectiveness of the approach is confirmed by simulation and comparison with other error correction methods. In order to further study the structural, cross-correlation and distance properties of orthogonal two-dimensional codes and the correcting capabilities of the proposed method, an information technology system for data transmission based on an equivalent class of perfect binary arrays has been developed. The proposed model evaluates the performance of the error correction code based on perfect binary arrays under various conditions, including correlated and uncorrelated interference and data exchange paths. A generator of PBA of equivalent classes has been built. An experimental evaluation of the correcting ability of the proposed two-dimensional codes was carried out by simulating various pre-code situations, including packet and random errors, for the cases of correlated and uncorrelated interference. Using a graphical interface, users will be able to enter the number and type of errors, determine whether they are random or packet errors, manually or automatically, move errors through the data packet, and view intermediate results. Thus, the complex nature of this study can be positioned as a promising approach and a reliable choice in the field of error correction

Keywords: error correction information coding, error detection, perfect binary arrays

UDC 681.32:007.5
DOI: 10.15587/1729-4061.2023.285540

DEVELOPMENT OF AN ERROR CORRECTION METHOD USING PERFECT BINARY ARRAYS

Pierre Murr
PhD, Assistant professor
Department of Computer Engineering
International University of Science and Technology in Kuwait
Mohamad Bin Qasim str., Ardiya Government Area, Kuwait, 70454
Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor, Head of Department*
E-mail: Serhii.Yevseiev@gmail.com
Stanislav Milevskyi
PhD, Associate Professor *
Marharyta Melnyk
PhD, Associate Professor
Department of Cyber Security and Information Protection
Private Institution "University of Science, Entrepreneurship and Technologies"
Mykoly Shpaka str., 3, Kyiv, Ukraine, 03113
Vitaliy Katsalap
PhD, Associate Professor**
Yurii Pribyliev
Doctor of Technical Sciences, Associate Professor**
Khazail Rzayev
PhD, Associate Professor
Department of Computer Technology and Cybersecurity
Azerbaijan Technical University
G. Javid ave., 25, Baku, Azerbaijan AZ 1073
Andrii Bryla
PhD, Associate Professor
Department of Systems Analysis and Optimization***
Oleksandr Shpak
PhD, Associate Professor
Department of Software System***
Pavlo Fedorka
Postgraduate Student
Department of Software System***
*Department of Cyber Security
National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
**Department of Information Technologies Employment and Information Security
The National Defence University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotskyi ave., 28, Kyiv, Ukraine, 03049
***Uzhhorod National University
Narodna sq., 3, Uzhhorod, Ukraine, 88000

Received date 11.05.2023
Accepted date 24.07.2023
Published date 30.08.2023

How to Cite: *Murr, P., Yevseiev, S., Milevskyi, S., Melnyk, M., Katsalap, V., Pribyliev, Y., Rzayev, K., Bryla, A., Shpak, O., Fedorka, P. (2023). Development of an errors correction method using perfect binary arrays. Eastern-European Journal of Enterprise Technologies, 4 (9 (124)), 45–53. doi: https://doi.org/10.15587/1729-4061.2023.285540*

1. Introduction

The reliability of information transmission in modern digital communication systems is a serious problem. Interference from various sources can distort the transmitted signal, which will lead to errors in the received data. To solve this problem, error correction codes are used to detect and correct errors in the signal. However, existing error correc-

tion methods have limitations in terms of their effectiveness and reliability.

Information processes are impossible without information transfer via data exchange paths. It is during the transmission of information that there is a threat of destruction of the transmitted information due to natural and artificial interference, which is inevitably present in data exchange paths. Error correction codes are often used to combat interference [1]. In addition, the transmitted information can be hacked by an attacker who can intercept, change or forge the information [2].

Error correction is the most important component of modern digital communication systems, ensuring that transmitted data remains reliable and accurate even in conditions of noise, interference and other sources of distortion. In this paper, we consider the problem of error correction during signal transmission, including related problems, methods used to solve these problems, and practical implications for modern communication systems.

The problem of correcting errors during data transmission can be presented as follows: we want to send a digital signal from the sender to the recipient over a communication channel, but we know that this channel is not ideal and can introduce errors to the signal. The goal is to develop a method that can detect and correct these errors so that the receiver can recover the original signal as accurately as possible. Error correction problems arise from the fact that errors can arise in various ways, including random noise, interference from other signals, and channel distortions such as fading or multipath. To detect and correct errors, it is necessary to develop methods that are reliable enough to handle these different types of errors and efficient enough to be implemented in real-time communication systems.

To protect the transmitted information from modification and falsification, various methods of error correction coding are commonly used [3]. However, to practically implement the detection and correction of various types of errors in smart technologies with limited computing resources, a new approach is needed that will meet the requirements for reliability, efficiency, and energy capacity.

2. Literature review and problem statement

Since the invention of Hamming codes in 1950, error correction methods have advanced significantly. In [4–6], the authors cover the main designs and constructions of codes from the geometric, algebraic, and graph-theoretic points of view, decoding algorithms. Turbo codes [7, 8] low-density parity check codes [9] provide excellent error correction efficiency, but require significant computational costs when working with other encoding and decoding algorithms.

In addition to computational complexity, error correction algorithms may introduce additional processing time [10], which may affect system latency, especially in real-time transmission applications. Finding a compromise between error correction capabilities and processing speed is critical. Hardware limitations create additional problems that must be taken into account when designing and implementing such systems [11], including limited memory, power consumption limitations, and availability of hardware resources.

In [12], it is noted that error correction codes introduce delays during encoding and decoding, and superfast codes are proposed to correct several adjacent errors. However, methods of minimizing such delays have not yet been sufficiently developed.

Perfect algebraic constructions, such as perfect binary arrays (PBAs) and bent sequences, have been widely studied in recent years. Sokolov [13] investigated the relationship between classes of perfect algebraic constructions, in particular perfect binary arrays, and bend sequences. Bent sequences, also known as truth tables of bent functions, form the basic class of perfect algebraic constructions and have found numerous applications in cryptography and coding theory.

In [13], the algebraic normal form of curved sequences of length n=16, which generate perfect binary arrays of order N=4, is presented. This gives insight into the properties and structure of perfect binary arrays, which are important in various applications. In addition, Sokolov determined the exact number of perfect binary arrays in the full set of curved sequences of length n=64, which contributed to a better understanding of the power of this class of perfect algebraic constructions.

Due to their unique properties, perfect binary arrays have found application in various fields, including coding theory [14], signal processing, and cryptography [15]. PBAs were also used in error correction codes, which have been widely studied in the literature [3, 16]. In addition to these methods, studies were conducted on the use of PBA-based codes in network and wireless communication systems [17].

Although there have been several studies on the use of PBAs in error correction codes, there is still room for further exploration of their potential. This study proposes a new method that uses PBA to create optimized error correction codes for more reliable error correction in data transmission and storage systems, and this method is expected to give several advantages. First, this method can be adapted to different types of errors encountered in real scenarios. This adaptability can significantly increase the reliability of data transmission, especially in environments subject to various sources of errors. Second, the optimization process facilitated by PBA can lead to the creation of error correction codes that provide increased efficiency and lower computational complexity. This can result in faster error detection and correction, reduced data transfer latency, and improved overall system performance.

3. The aim and objectives of the study

The aim of the study is to develop a method of error correction coding based on perfect binary arrays, which ensures sufficient redundancy to detect and correct errors.

To achieve the aim, the following objectives should be accomplished:

– to develop a mathematical apparatus of an error correction code based on perfect binary arrays;

– to develop a software package for implementing the performance evaluation model for the error correction code.

4. Research materials and methods

4. 1. Research object and hypothesis

The object of the research is the noise immunity of the data exchange path.

The research hypothesis is that by developing and implementing broadband orthogonal coding information technologies based on PBA, it is possible to achieve sufficient redundancy to detect and correct errors, thereby ensuring the reliability of information transmission over data exchange paths.

The following assumptions were made:

– mathematical structural properties of perfect binary arrays and their ideal autocorrelation functions are an interesting topic for studying their corrective capabilities;

– perfect binary arrays can be efficiently generated and classified for any length. In turn, the creation of an equivalent class is based on a simple rotation of lines and columns, which makes encoding and decoding very simple and fast;

– the large volume of the full PBA code allows increasing the level of noise immunity of the data exchange path, but at the same time, there is a problem of synchronization between the encoder and the decoder.

In order to evaluate the performance of the proposed method, a simulation was carried out to compare its accuracy and efficiency with other modern error correction methods. A model has also been developed to evaluate the performance of the error correction code based on PBA under the influence of correlated and uncorrelated interference of data exchange paths.

The simulation was carried out using Microsoft Visual C#. The simulation setup included a communication channel with different levels of interference, and the performance of the proposed method was compared with other existing error correction methods in these conditions.

The model was developed using a combination of analytical and simulation methods, using mathematical models to analyze the properties of the PBA-based code and its performance under various types of interference. Simulation-based methods were also used to verify analytical models and evaluate the performance of the error correction code in real conditions.

4. 2. Perfect binary arrays

Perfect binary arrays [18, 19] are two-dimensional arrays of size $N_1 \times N_2$:

$$H(N_1, N_2) = \|h_{i,j}\|, \tag{1}$$

$h_{i,j} \in \{+1, -1\}$ – PBA elements;
$i = \overline{0, N_1 - 1}$ – number of lines;
$j = \overline{0, N_2 - 1}$ – number of columns;
that have an ideal two-dimensional periodic autocorrelation function (TPACF):

$$R(N_1, N_2) = \|r_{m,n}\| = \begin{cases} N_1 \times N_2, & \text{when } m = n = 0; \\ 0, & \text{when } m \neq n. \end{cases} \tag{2}$$

Elements of TPACF (2) are calculated by the formula:

$$r_{m,n} = \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} h_{i,j} h_{i+m,\, j+n}. \tag{3}$$

Each PBA (1) of order N (size $N \times N$) – $\boldsymbol{H}^{(0)}(N) = h_{i,j}^{(0)}$, which we will call a reference (generating) array, generates a class of equivalent PBAs – E(N) class [20], by the operations of cyclic rotate of lines and (or) columns, the total number of generated arrays is:

$$\Psi^{E(N)} = N^2. \tag{4}$$

For example, a PBA class – $\boldsymbol{H}^{(E)}(N) = h_{i,j}^{(E)}$ can be obtained from a reference PBA by performing the operation of cyclic rotation of lines (L_{k1}) of the reference PBA by k_1 lines down and the operation of cyclic rotate of columns (Q_{k2}) of the reference PBA by k_2 columns to the right [21]:

$$H^{E(N)} = L_{k_1} H^{(0)}(N) Q_{k_2} \tag{5}$$

or

$$H(N_1, N_2) = \|h_{i,j}\|. \tag{6}$$

For example, for the reference PBA:

$$H^{(0)}(6) = \begin{bmatrix} + & + & + & + & + & - \\ + & - & + & + & - & + \\ - & + & - & + & - & - \\ + & + & - & - & + & + \\ - & + & - & + & - & - \\ - & + & + & + & + & - \end{bmatrix}. \tag{7}$$

Generates equivalent class PBA total $\Psi^{E(6)}$=36.

4. 3. Cross-correlation function of two PBA

The two-dimensional periodic cross-correlation function (TPCCF) [18, 22]:

$$B(N) = \|b_{m,n}\|. \tag{8}$$

Equation (8) is the correlation between two equivalent PBA classes – class $\boldsymbol{H}^{(0)}(N) = h_{i,j}^{(0)}$ and $\boldsymbol{H}^{(E)}(N) = h_{i,j}^{(E)}$ of dimension , the elements of TPCCF are calculated:

$$b_{m,n} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} h_{i,j}^{(0)} h_{i+m,j+n}^{(E)}, \tag{9}$$

where $i = \overline{0, N-1}$, $j = \overline{0, N-1}$ and $m = \overline{0, N-1}$, $n = \overline{0, N-1}$.

The TPACF for the $\boldsymbol{R}^{(0)}(N) = r_{i,j}^{(0)}$ reference PBA, rotated k_1 lines down and k_2 columns to the right. The TPCCF of arbitrary two arrays from the same class has one side peak value equal to , the spatial coordinates of this peak are uniquely determined by the values of the cyclic rotates of the lines and (or) columns of the $H^{(E)}(N)$ array relative to the reference $H^{(0)}(N)$:

$$B(N) = \|b_{m,n}\| = \|r_{i+k_1, j+k_2}^{(0)}\|. \tag{10}$$

$i+k_1$ and $j+k_2$ are reduced by *mod N*.

By using (6) and (9), the results are:

$$b_{m,n} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} h_{i,j}^{(0)} h_{i+m,j+n}^{(E)} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} h_{i,j}^{(0)} h_{i+m+k_1, j+n+k_2}^{(0)} = r_{i+k_1, j+k_2}^{(0)}. \tag{11}$$

Fig. 1 shows some examples of two-dimensional periodic cross-correlation functions where clearly it is clearly seen that the spatial coordinates of this peak move depending on the cyclic rotate.

Thus, it is possible to present any PBA equivalent to the class, which is built on the basis of the reference one as follows:

$$H^E(N) = L_{k_1} H^{(0)}(N) Q_{k_2}. \tag{12}$$

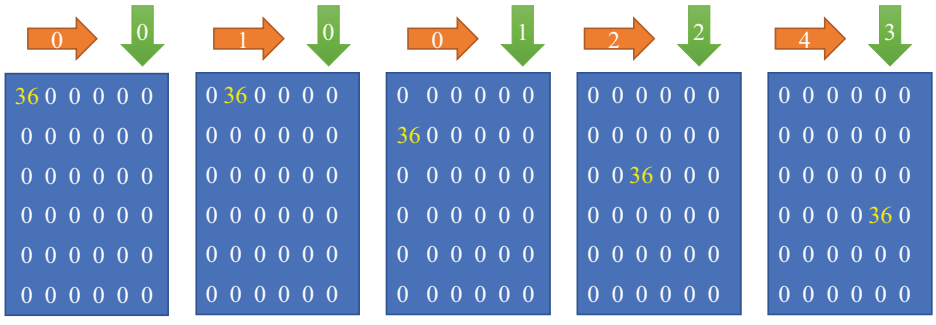

Fig. 1. Examples of two-dimensional periodic cross-correlation functions

From the analysis of relations (9) and (12), it follows that each TPCCF of arbitrary two arrays from the same $E(N)$ class has one side peak equal to N^2, the spatial coordinates of this peak are uniquely determined by the values of the cyclic rotates of the lines and (or) columns of this $H^{(E)}(N)$ relative to the reference $H^{(0)}(N)$. Consequently, it is advisable to use PBA of the $E(N)$ class at least to transmit N^2 messages in single-channel synchronous communication systems with noise-like two-dimensional cyclic signals [21].

5. Development of an error correction method based on perfect binary arrays

5. 1. Development of a mathematical apparatus for an error correction code based on perfect binary arrays

The proposed error correction method using PBA includes the following steps:

– encoding: the transmitted information is first encoded using a linear code built from the reference PBA. This encoding ensures that the transmitted information has sufficient redundancy to detect and correct errors;

– transmission: encoded information is transmitted over a communication channel subject to various types of interference;

– decoding: at the receiver side, the received information is decoded using a decoding algorithm that uses the properties of the PBA-based code. This decoding algorithm is designed to detect and correct errors that may have occurred during transmission;

– error correction: finally, any errors found are corrected using the error correction properties of the PBA-based code.

The principle of information modulation on the basis of cyclic rotations of the PBA equivalent to the $E(N)$ class is shown in Fig. 2. Based on this principle, a mathematical apparatus of the error correction method is proposed, which ensures the guaranteed reliability of information transmission by controlling the parameters of the correcting abilities of the code.

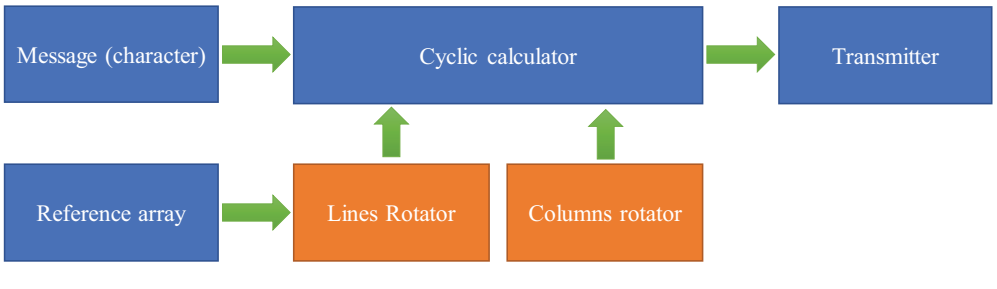

Fig. 2. Principle of information modulation based on cyclic rotations of perfect binary arrays

Suppose that the message consists of discrete characters, each of which is selected from some finite set – the alphabet:

$$A=\{a_0,a_1,\ldots,a_{q-1}\}, \tag{13}$$

the alphabet consisting of q different characters. To transmit each character $\boldsymbol{a}_i$, where i is the character number in the alphabet, the modulator will use one reference PBA of the $E(N)$ class.

The cyclic calculator device operates in modular arithmetic and accordingly calculates the parameters k_1 and k_2 by the number of the transmitted character of expression (13), for the transmitted PBA as follows:

$$k_1=\operatorname{int}(i/N). \tag{14}$$

$$k_2=\operatorname{mod}N. \tag{15}$$

It is obvious that the choice of dimension N for the PBA of the $E(N)$ class must consider that $N^2\geq q$.

The lines rotator L_{k1} produces a cyclic rotate of the reference PBA $H^{(0)}(N)$ by k_1 (14) lines down – $L_{k1}H^{(0)}(N)$. The columns rotator Q_{k2} produces a cyclic rotate of the reference PBA $H^{(0)}(N)$ by k_2 (15) columns to the right. The results of the two rotations are $L_{k1}H^{(0)}(N)Q_{k2}$.

The demodulator is built on the basis of expression (9) and consists of one two- dimensional filter matched to the reference PBA $H^{(0)}(N)$ with a block for determining the most likely coordinates ($k_{1'}$ and $k_{2'}$) of the peak of the TPCCF between the reference and received PBAs, while the number of the most likely transmitted character is determined as follows:

$$i'=k_1'\times N+k_2'. \tag{16}$$

The recipient of the messages does not know which PBA of the equivalent $E(N)$ class was set as basic (reference). In the case of receiving a single PBA, it is impossible to determine what parameters of the cyclic rotate of lines (k_1) and columns (k_2) were and, accordingly, it is impossible to determine under what number the character was transmitted.

The class of two-dimensional correcting $E(N)$ codes. The correcting properties of $E(N)$ codes are much better compared to the corresponding BCH codes of

maximum length, in terms of correcting packet (correlated) errors, while uncorrelated errors are corrected the same way.

B_m – all nonzero (peaks) of the TPACF and TPCCF (equal to N^2in the absence of noise and interference) and we consider that the coordinates of their location carry information about the transmitted message (16). In other words, we will carry out information modulation by cyclic rotates of the reference array.

Let the ensemble of messages $A=\{\alpha_j\}$, $j=\overline{0,N^2-1}$.

From the consideration of the correlation properties of the TPACF and TPCCF, the $E(N)$ code follows, which is the decoder of the $E(N)$ code (Fig. 2). Thus, at $j=N^2$, the code can be built on the basis of one two-dimensional correlator scheme. A two-dimensional matched filter with a carrier of the $H^{(0)}(N)$ array and a coordinate search scheme (k_1 and k_2) of the main lobe (peak) B_m, where the coordinates refer to the upper left corner of the TPCCF.

By construction, orthogonal $E(N)$ codes are equidistant codes, and their code distance (dist) in the Hamming metric is determined by the relation:

$$d=\min\left\{dist\left(E_i(N)\right),\left(E_k(N)\right)\right\}=N^2/2, \qquad (19)$$

where $i,k=\overline{1,N^2}$, $i\neq k$.

The construction-code distance d (19) is equal to the number of element-by-element discrepancies (differences) of arbitrary two code words of a two-dimensional $E(N)$ code.

Thus, based on the corrective abilities of $E(N)$ codes built on the basis of PBA, under the influence of correlated and uncorrelated interference of data exchange paths, a mathematical apparatus is proposed that uses error correction based on perfect binary arrays, which provides a guaranteed level of information transmission reliability.

5. 2. Development of a software package for implementing the performance evaluation model for the error correction code

To implement the proposed performance evaluation model of the proposed error correction coding method, a graphical interface has been developed, shown in Fig. 3.

The model is universal and allows research on the use of codes for transmitting information built on the basis of PBAs of orders $N=2^2=4$, $N=3\times2^1=6$, $N=2^3=8$, $N=3\times2^2=12$ and $N=2^4=16$.

The corresponding PBA $H^{(0)}(N)$, of a given order N, which is used as a reference, is read from the file and fed to the modulator. At the second input of the modulator, the number of the character (message) is fed, which is entered from the keyboard.

Information modulation is carried out using cyclic rotates of PBA according to the algorithm developed in the subsection (Information modulation using equivalent PBA). The screen displays the reference PBA $H^{(0)}(N)$ and the PBA obtained as a result of cyclic rotates $L_{k1}H^{(0)}(N)Q_{k2}$ (Fig. 4) and TPCCF between the reference PBA and the cyclically rotated one.

Packet and random errors can be entered into the data exchange path (Fig. 5, 6). For packet errors, the program user can change the length of the error packet, and the packet itself can move the code "left" and "right". To speed up the study, an automatic movement of the error packet "to the right" along the code is provided. Due to the inertia of the model and graphic display, the user can view the intermediate results of the model when the error packet moves in automatic mode.

The software allows users to enter any number of random errors into the model. It is possible to randomly change a certain number of elements «+1» and elements «–1» of the code separately (Fig. 7). The program also allows manual error correction (input) in the data exchange path (Fig. 8).

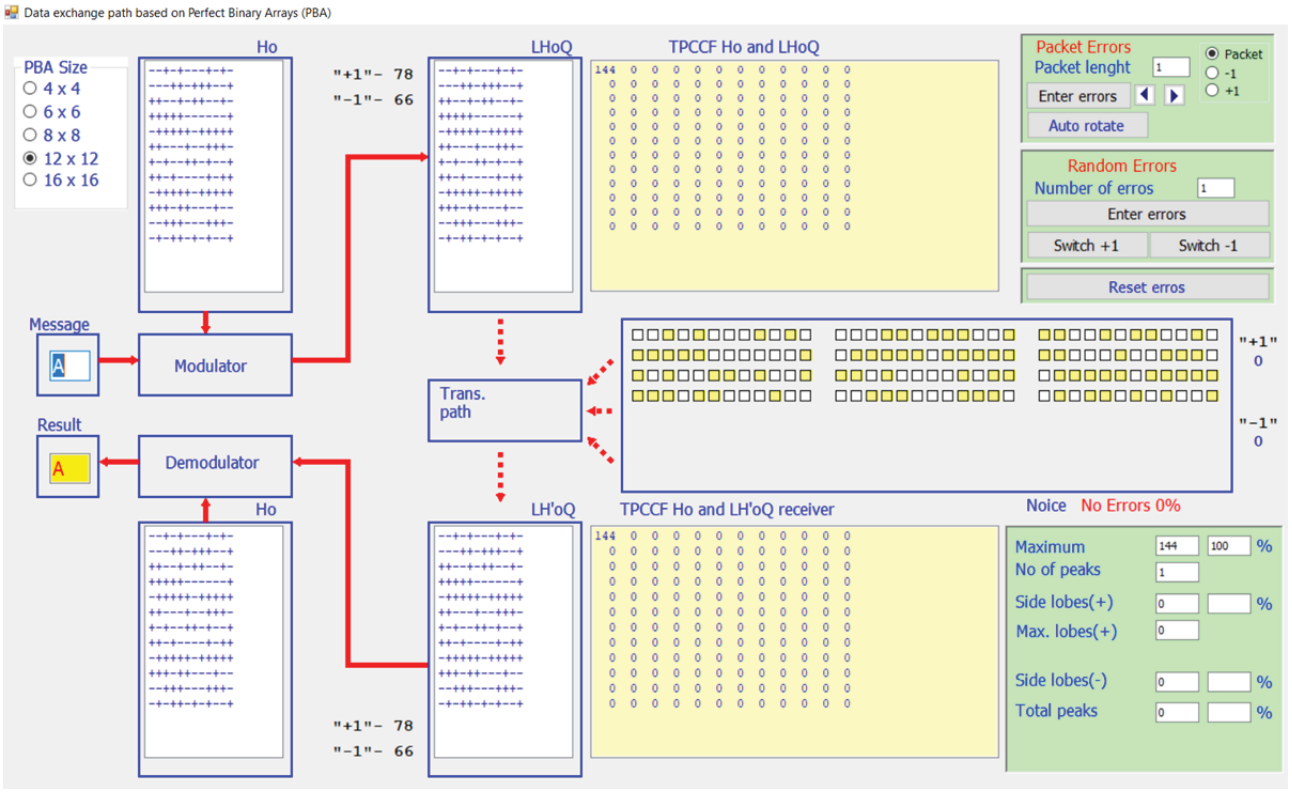

Fig. 3. GUI for the "Data exchange path based on Perfect Binary Arrays" model

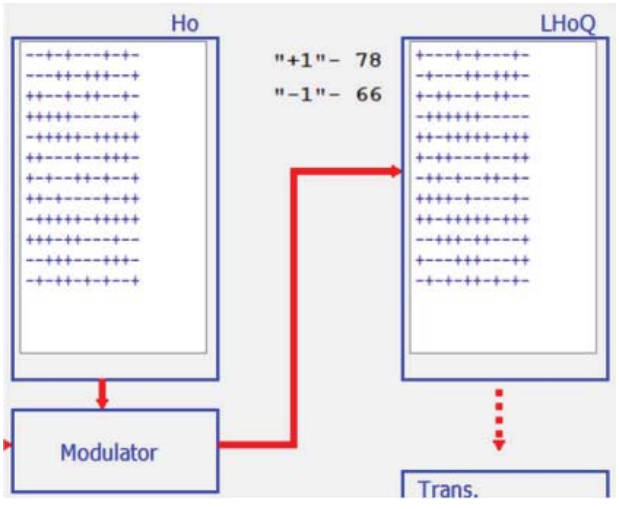

Fig. 4. Cyclic rotation of our PBA

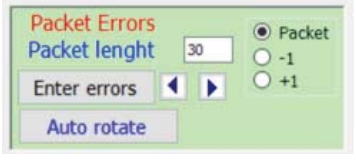

Fig. 5. Packet and random error adder

Fig. 6. Errored bits

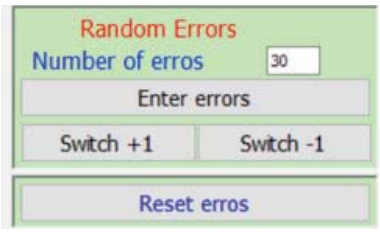

Fig. 7. Random error bit adder

The two-dimensional matched filter calculates a two-dimensional periodic cross-correlation function (TPCCF) between the reference code built on the basis of $H^{(0)}(N)$ and the error code received from the data exchange path (Fig. 9).

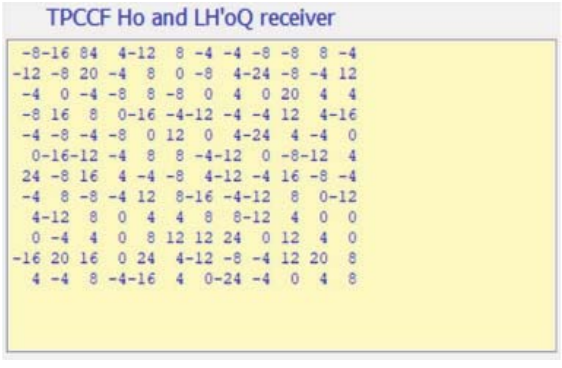

Fig. 9. TPCCF between the received PBA and initial PBA

The model calculates the level of the main peak and its percentage compared to the theoretical main peak, the number of main peaks, i.e., the number of maximum peaks with the same amplitude. The number of positive and negative side peaks, the total number of side peaks of the TPCCF are calculated separately, and the level of maximum positive and negative side peaks is shown in Fig. 10.

The model determines the coordinates of the main peak and, using the maximum likelihood method, decides on the transferred letter (Fig. 11, 12). If it is impossible to correctly determine the transmitted character, a question mark is displayed instead.

Thus, the developed model allows us not only to investigate the operation of a tunable two-dimensional matched filter, but also to study the effect of various errors in the data exchange path on the reliability of receiving communication.

Fig. 10. Error effect on TPCCF

Fig. 8. Errored bits

Thus, the proposed software package provides experimental research and allows practical implementation for the required level of reliability.

The results of the study of the corrective ability of the two-dimensional code under the action of packet errors of length t_n=18 are

presented in Table 1. The bold type in this table marks the numbers of the most critical positions of the beginning of the packet, at which the ratio B_m/B_{max}.

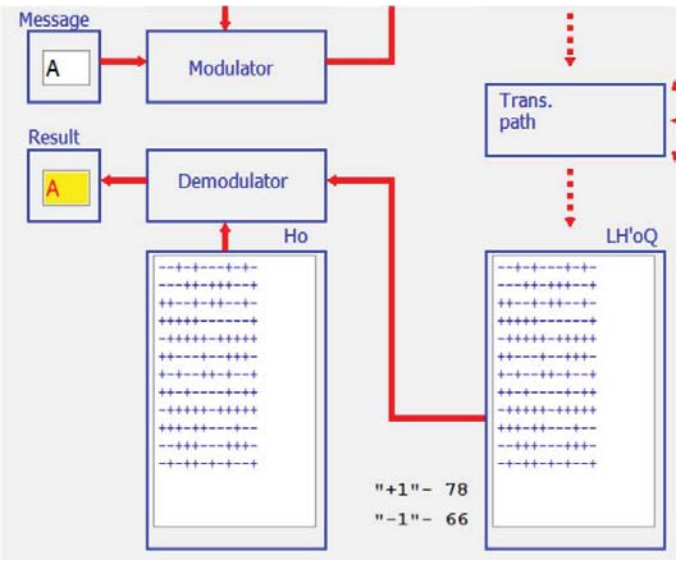

Fig. 11. Example of receiving the letter «A»

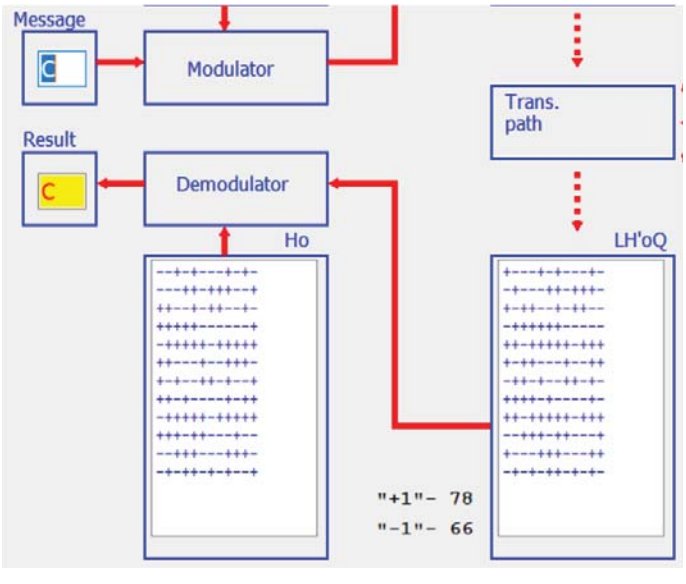

Fig. 12. Another example using the character «C»

Table 1

Operating principle of a two-dimensional decoder — a correlation type code under the action of packet errors

Packet number	B_m/B_{max}							
1–8	28/16	28/20	28/20	28/20	28/20	28/24	28/20	28/20
9–16	28/20	28/20	28/16	28/16	28/16	28/16	28/12	28/16
17–24	28/16	28/16	28/16	28/16	28/16	28/16	28/16	28/16
25–32	28/20	28/20	28/20	28/20	28/20	28/20	28/24	28/24
33–40	28/20	28/20	28/20	28/24	28/24	28/20	28/20	28/20
41–48	28/20	28/20	28/20	28/20	28/16	28/20	28/24	28/24
49–56	28/20	28/16	28/16	28/16	28/16	28/16	28/16	28/12
57–64	28/12	28/12	28/12	28/12	28/16	28/16	28/12	28/16

Indeed, if the size of the error packet is increased by one, then at critical positions the ratio of the main peak to the maximum TPCCF peak becomes equal to one: B_m/B_{max}, i.e., there will be uncertainty in the decoder operation. From the analysis of Table 2, it is easy to see that the $E(8)$ code also corrects a significant portion of the larger packet error length $t_n>18$.

For comparison, we note that the closest (63,6) BCH code of maximum length reliably corrects all error packets of size $t_n=15$ [23], while, as shown by the modeling of BCH codes with majority decoding, only part of the structures of larger packets ($t_n>15$) can be corrected.

The correcting ability of two-dimensional PBA-based codes is much higher, compared to the maximum length BCH codes of the same size, in terms of correcting packet (correlated) errors (Table 2), while uncorrelated errors are corrected the same way.

Table 2

Comparative analysis of the correcting ability of two-dimensional $E(N)$ codes based on PBA and BCH codes

$E(N)$ code	Code length $n=N^2$	16	36	64	144	256	576
	Maximum packet error length t_n	3	10	18	45	92	236
BCH code	Code length $n=2^k-1$	15	31	63	127	255	511
	Maximum packet error length $E(N)$	3	7	15	31	63	127

Analysis of the results of Tables 1, 2 confirms that the set of lengths of $E(N)$ codes ($N=2^k$, $N=3\,2^k$) also exceeds the set of lengths of BCH codes ($N=2^k-1$). With an increase in size N, the volumes of complete PBA classes grow significantly, which ensures the practical reliability of information by quickly changing the working ensembles of $E(N)$ codes of a given order.

6. Discussion of the results of developing an error correction coding method based on perfect binary arrays

The use of PBA allows developing a secure system that is equivalent to, and in some cases better than, other similar systems. This is achieved due to the structural properties of perfect binary arrays, including cross-correlation and distance properties of two-dimensional $E(N)$ codes.

A cyclic rotation of the lines and (or) columns of the reference array generates an equivalent class $E(N)$, which made it possible to build information modulation based on PBA. The cyclic calculator device operates in modular arithmetic and calculates the parameters k_1 and k_2 (14, 15) and, therefore, the size N for the PBA of the $E(N)$ class must be no less than $N^2\geq q$, the number of characters in the alphabet. A 6x6 PBA will be able to encode 36 different characters, for example, the English alphabet only – uppercase or lowercase letters (24 letters). An 8x8 PBA will be able to encode 64 different characters, for example, the English alphabet – uppercase and lowercase (52 letters), and additional 12 characters.

The work also showed the principle of operation and construction of a demodulator, which determines the maximum likelihood coordinates (k_1 and k_2) of the TPCCF peak between the reference and received PBA.

The development of smart technologies forms a new range of digital services, but at the same time, almost all "smart" areas refer to critical infrastructure facilities [24–27]. The formation of an infrastructure based on smart technologies is associated with the need to limit computing resources and energy consumption. Thanks to a simple and fast way to build a PBA and an equivalent class, the proposed method confirms the possibility of using it in smart chipsets, including microcontrollers with limited resources.

Using the graphical interface of the developed software package, users can conduct various studies of the proposed error correction method. Thus, form initial data: enter the number and type of errors, determine whether they are random or packet errors, manually or automatically, move the errors through the data packet and view intermediate results.

The presented results of studies of the proposed method of the correcting ability of two-dimensional $E(N)$ codes based on PBA codes in Table 2 confirm good code parameters. When using them, it is possible not only to correct errors, but also to provide the possibility of generating the required code with the given error correction parameters. The main limitations are reduced to the length of the input sequence, and, accordingly, the presented results provide efficiency in the transmission of short messages (highlighted in bold in Table 2), which can be formed in sensors, various elements of various types of signaling of cyber-physical systems and/or elements of critical infrastructure facilities. The findings indicate that $E(N)$ codes can be used as an efficient error correction mechanism for communication paths subject to both correlated and uncorrelated errors. In addition, PBA-based codes can be used to reduce packet errors and improve overall system reliability.

Thus, the proposed approach makes it possible to take into account the capabilities of an error correction code, the technical capabilities of the communication channel, which minimizes computing resources for practical implementation. The proposed method can be used in smart technologies with limited computing resources to ensure the required level of information transmission reliability. A promising direction is the practical use of the proposed method in wireless channels of "Smart House" cyber-physical systems. Future studies suggest evaluating the performance of these codes in the presence of more complex interference models such as channel fading and interference from other wireless devices. In addition, researchers can explore hybrid coding schemes that combine the strengths of different coding methods to achieve a higher level of error correction. Such a study could provide a better understanding of the capabilities and limitations of these codes in practical scenarios.

However, more research needs to be done on the use of the proposed approach to correcting errors in large (more than 1,000 characters) information grids, which will largely determine their further use in various-purpose information and communication systems.

7. Conclusions

1. The study presents the mathematical apparatus of the error correction coding method based on the corrective abilities of two-dimensional $E(N)$ codes in the presence of both correlated and uncorrelated noise in data exchange paths. It was found that two-dimensional $E(N)$ codes are able to correct errors with the same efficiency in both Euclidean and Hamming metrics. Moreover, $E(N)$ codes exhibit the same correcting capabilities as BCH codes in terms of correcting uncorrelated or random errors. The PBA-based two-dimensional code method offers significantly better correction capabilities than BCH codes of similar length to correct packet or correlated errors.

2. The proposed software package for implementing the method provides new opportunities for the potential application of PBA-based codes in microcontrollers. Combining their information protection capabilities with data correction, PBA-based codes can be used to develop fault-tolerant cyber-physical systems of critical infrastructure facilities.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The study was conducted without financial support.

Data availability

The manuscript has no associated data.

References

1. Lin, S., Costello, D. J. (2001). Error Control Coding. Prentice-Hall. URL: https://pg024ec.files.wordpress.com/2013/09/error-control-coding-by-shu-lin.pdf
2. Belim, S. V., Larionov, I. B. (2020). Noise proof coding based on orthogonal functions. Journal of Physics: Conference Series, 1441 (1), 012034. doi: https://doi.org/10.1088/1742-6596/1441/1/012034
3. Kumari, S., Gahalod, L., Changlani, S. (2022). Study of Different Types of Error Detection and Correction Code in Wireless Communication. International Journal of Scientific Research in Science, Engineering and Technology, 9 (3), 448–455. doi: https://doi.org/10.32628/ijsrset2293138
4. Patil, A., Darkunde, N. (2018). Algorithmic Approach for Error-Correcting Capability and Decoding of Linear Codes Arising from Algebraic Geometry. Lecture Notes in Networks and Systems, 509–517. doi: https://doi.org/10.1007/978-981-13-0586-3_51
5. Huffman, W. C., Pless, V. (2003). Fundamentals of error-correcting codes. Cambridge University Press. doi: https://doi.org/10.1017/cbo9780511807077

6. Moon, T. K. (2005). Error Correction Coding. John Wiley & Sons. doi: https://doi.org/10.1002/0471739219
7. Salija, P., Yamuna, B., Padmanabhan, T. R., Mishra, D. (2022). A Generic Reliability Based Direct Decoding Algorithm for Turbo Codes. Wireless Personal Communications, 125 (1), 785–801. doi: https://doi.org/10.1007/s11277-022-09577-2
8. Sholiyi, A.O. (2011). Irregular Block Turbo Codes for Communication Systems. Swansea University. URL: https://core.ac.uk/download/pdf/161881205.pdf
9. Venkatesh, D. Y., Mallikarjunaiah, K., Srikantaswamy, M. (2022). A Comprehensive Review of Low Density Parity Check Encoder Techniques. Ingénierie Des Systèmes d Information, 27 (1), 11–20. doi: https://doi.org/10.18280/isi.270102
10. Süzer, A. E., Oktal, H. (2023). A comparison analysis on forward error correction technology: a future perspective for GNSS. Aircraft Engineering and Aerospace Technology, 95 (8), 1311–1320. doi: https://doi.org/10.1108/aeat-10-2021-0319
11. Abdelkareem, A. E. (2022). Hardware considerations of a DSP based wireless coded receiver under limited resources. 2022 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE). doi: https://doi.org/10.1109/itss-ioe56359.2022.9990939
12. Saiz-Adalid, L.-J., Gracia-Moran, J., Gil-Tomas, D., Baraza-Calvo, J.-C., Gil-Vicente, P.-J. (2019). Ultrafast Codes for Multiple Adjacent Error Correction and Double Error Detection. IEEE Access, 7, 151131–151143. doi: https://doi.org/10.1109/access.2019.2947315
13. Sokolov, A. (2019). Interrelation Between the Class of Bent-Sequences and the Class of Perfect Binary Arrays. Computer Modeling and Intelligent Systems, 2353, 339–349. doi: https://doi.org/10.32782/cmis/2353-27
14. Jedwab, J., Li, S. (2022). Group rings and character sums: tricks of the trade. arXiv. doi: https://doi.org/10.48550/arXiv.2211.11986
15. Goresky, M., Klapper, A. (2012). Algebraic Shift Register Sequences. Cambridge University Press. doi: https://doi.org/10.1017/cbo9781139057448
16. Hedayat, A. S., Sloane, N. J. A., Stufken, J. (1999). Orthogonal Arrays. Springer Series in Statistics. Springer. doi: https://doi.org/10.1007/978-1-4612-1478-6
17. Yurish, S. (2019). Advances in Networks, Security and Communications: Reviews, Vol. 2. All Rights Reserved - Standard Copyright License, 145–188. URL: https://www.lulu.com/shop/sergey-yurish/advances-in-networks-security-and-communications-reviews-vol-2/paperback/product-1gqqegqz.html?page=1&pageSize=4
18. Jedwab, J., Mitchell, C., Piper, F., Wild, P. (1994). Perfect binary arrays and difference sets. Discrete Mathematics, 125 (1-3), 241–254. doi: https://doi.org/10.1016/0012-365x(94)90165-1
19. Wild, P. (1988). Infinite families of perfect binary arrays. Electronics Letters, 24 (14), 845. doi: https://doi.org/10.1049/el:19880575
20. Mazurkov, M., Chechel'nitskii, V. Y. (2003). The classes of equivalent and generative perfect binary arrays for cdma-technologies. Radioelectronics and Communications Systems, 46 (5), 40–46.
21. Bomer, L., Antweiler, M. (1990). Two-dimensional perfect binary arrays with 64 elements. IEEE Transactions on Information Theory, 36 (2), 411–414. doi: https://doi.org/10.1109/18.52492
22. Mazurkov, M. I., Chechel'nitskii, V. Ya., Murr, P. (2008). Information security method based on perfect binary arrays. Radioelectronics and Communications Systems, 51 (11), 612–614. doi: https://doi.org/10.3103/s0735272708110095
23. Pless, V., Huffman, W. C. (Eds.) (1998). Handbook of Coding Theory. Elsevier.
24. Dovgyi, S., Kopiika, O. (2022). Standard Model of System Architecture of Enterprise IT Infrastructure. Lecture Notes in Networks and Systems, 181–201. doi: https://doi.org/10.1007/978-3-031-16368-5_9
25. Dovgiy, S., Kopiika, O., Kozlov, O. (2021). Architectures for the Information Systems, Network Resources, and Network Services (short paper). Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II. Volume I. Co-located with International Conference on Problems of Infocommunications. Science and Technology (PICST 2021), 293–301. URL: https://ceur-ws.org/Vol-3187/short9.pdf
26. Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O. et al. (2022). Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies, 2 (9 (116)), 44–59. doi: https://doi.org/10.15587/1729-4061.2022.254545
27. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et. al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. doi: https://doi.org/10.15587/978-617-7319-57-2