Simulating the Error-Detecting Capability of the Error-Detecting Code

Natasha Ilievska
Faculty of Computer Science and Engineering, "Ss.Cyril and Methodius" University,
Skopje, Republic of Macedonia, Email: natasa.ilievska@finki.ukim.mk

***Abstract* - Using simulations, we analyze an error-detecting code from the aspect of the number of errors that the code surely detects. In order to conclude whether and how the order of the quasigroup used for coding affects the number of errors that the code surely detects, we use quasigroups of different orders for coding. Also, we code input blocks of different lengths in order to conclude whether the number of errors that the code surely detects depends on the length of the input block, i.e., the length of the code word.**

Keywords - error-detecting code; linear quasigroup; noise channel; binary symmetric channel; code word

I. Introduction

In this paper we consider an error-detecting code based on linear quasigroups ([1]). The probability of undetected errors for the analyzed code, i.e., the probability that there will be errors in the input block that the code will not detect is obtained in [1] and [2]. But, for every error-detecting code an important parameter is the maximum number of incorrectly transmitted bits to which the code detects the error for sure. In this paper, using simulations, we obtain this parameter. Namely, using simulations we obtain the number of code words that have j incorrectly transmitted bits and the number of code words that have j incorrectly transmitted bits, but the errors are not detected, where j runs from 1 to the length of the code words. Using these two values we calculate the percentage of detected incorrectly transmitted code words in which j bits are incorrectly transmitted, for every j from 1 to the length of the code word. We obtain these results for different values of the length of the code words and different values of the probability of bit-error in the binary symmetric channel. We consider the case when linear quasigroup of order 4 is used for coding, but also the case when linear quasigroup of order 8 is used for coding.

II. The Error-Detecting Code

Since the code is defined using linear quasigroups in what follows we give the definition of this algebraic structure.

Definition 1: Quasigroup is algebraic structure $(Q,*)$ such that

$$(\forall\, u, v\in Q)(\exists!\, x, y\in Q)(x*u=v\wedge u*y=v) \qquad (1)$$

Definition 2: The quasigroup $(Q,*)$ of order 2^q is linear if there are non-singular binary matrices A and B of order $q\times q$ and a binary matrix C of order $1\times q$, such that

$$(\forall x, y\in Q)\ x*y=z\Leftrightarrow \mathbf{z}=\mathbf{x}A+\mathbf{y}B+C \qquad (2)$$

where $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ are binary representations of x, y and z as vectors of order $1\times q$ and + is a binary addition.

When we say that $(Q,*)$ is a quasigroups of order 2^q, then we take $Q=\{0, 1, 2,\ldots, 2^q-1\}$.

Due to the Definition 2, linear quasigroups instead to be presented with the quasigroup operation * can be presented with a binary matrices A, B and C. We will do so in the future in this paper. Also, elements from the linear quasigroup Q of order 2^q will be presented as a binary vectors of length q.

Let the linear quasigroup Q of order 2^q is used for coding and let the input block be $a_1a_2\ldots a_n$, where $a_i\in Q$, $i=1, 2, \ldots, n$. Let A, B and C be the matrices that satisfy (2) and let $\mathbf{a}_i$ be the binary representation of the character a_i as a vector of length q, for $i=1, 2, \ldots, n$. The redundant characters are calculated using the following equation:

$$\mathbf{d}_i=\mathbf{a}_iA+\mathbf{a}_{i+1}B+C,\ i=1, 2, \ldots, n \qquad (3)$$

where all operations in indexes are modulo n and + is a binary addition.

Now, the extended block $\mathbf{a}_1\mathbf{a}_2\ldots\mathbf{a}_n\mathbf{d}_1\mathbf{d}_2\ldots\mathbf{d}_n$ is the code word that is transmitted through the binary symmetric channel. Since there are noises in the channel some of the characters may not be correctly transmitted. In order to check if there are errors in transmission, the receiver checks if the output block satisfies (3) for all $i\in\{1, 2, \ldots, n\}$. If for some i, (3) is not satisfied, the receiver concludes that there are errors in transmission and it asks the sender to send the block once again. Since the redundant characters are also transmitted through the channel, noises affect them also. Therefore, it is possible (3) to be satisfied for all $i\in\{1, 2, \ldots, n\}$ although some of the characters are incorrectly transmitted. This means that it is possible to have undetected errors in transmission. In this paper we will be focused on the maximum number of incorrectly transmitted bits in a code word to which the error will be detected for sure.

III. The Error-Detecting Capability

We will consider the case when linear quasigroup of order 4 is used for coding and the case when linear quasigroup of order 8 is used for coding. Also, we will consider several values for the length of the code words and several values for the probability of bit-error p in the binary symmetric channel. From the obtained results we will conclude whether and how the order of the quasigroup and the length of the code words affect the number of errors that the code surely. First, we will explain the simulation process.

A. The simulation process

In this subsection we will give short description on the process of simulation. For given n and j, the percentage of detected incorrectly transmitted code words of length n bits with j incorrectly transmitted bits, transmitted through a binary symmetric channel with a probability of bit-error p is obtained in the following way:

We use quasigroup Q of order 2^q for coding. First, we generate a long input message, for example around 2000000 characters from the alphabet Q. Then, this message is separated into blocks with length $n/(2q)$ and each block is coded separately. The length of the generated input message is chosen so that it is divisible by $n/(2q)$. After that, this coded message, which contains all the coded blocks, is turned into binary form. Since the rate of the code is ½, each coded block, i.e., each code word will have $2n/(2q)=n/q$ characters from the quasigroup Q. The binary representation of each character from the quasigroup Q contains q bits, from where follows that the code words have length $q \cdot n/q=n$ bits. We generate the noise in the binary symmetric channel, which is a binary string with length equal to the length of the coded input message turned into binary form. The noise string is generated such that the probability of occurrence of 1 in this string is p. The positions in the noise string to which there is 1 are the positions on the coded input message in a binary form that are incorrectly transmitted. The output message is calculated with simply adding per modulo 2 the coded input message in a binary form and the noise string. Now, from the noise string, for every $j \in \{1, 2, \ldots, n\}$, we count the number of incorrectly transmitted code words with j incorrectly transmitted bits and using the output message we obtain the number of incorrectly transmitted code words with j incorrectly transmitted bits in which the error is not detected. The percentage of undetected incorrectly transmitted code words with j incorrectly transmitted bits is calculated by simply dividing this two numbers and multiplying the result by 100%. To obtain the percentage of detected incorrectly transmitted code words with j incorrectly transmitted, we subtract this percentage from 100%.

The accuracy of the simulation procedure depends on the length of the generated input message. A larger length of the message implies greater accuracy. Since the goal is to obtain the number of errors that the code surely detects, in order to have higher accuracy, we need to have large number of incorrectly transmitted code words with small number of incorrectly transmitted bits. For that reason, first we chose the probability of bit-error p in the channel to have small value (i.e., 0.05, 0.07 and 0.09) and we generated messages with length of approximately 2000000 characters from the quasigroup since in this case the obtained results from the simulation showed that the number of incorrectly transmitted blocks whit j incorrectly transmitted bits mostly is of order 10^4, for small values of j. On the other hand, the number of such code words in which the error is not detected mostly is of order 10^0 and sometimes 10^1. This means that the precision in the quotient of the number of undetected incorrectly transmitted code words with j incorrectly transmitted bits and the number of incorrectly transmitted code words with j incorrectly transmitted bits mostly is of order 10^{-4}, i.e., up to the fourth decimal and sometimes is 10^{-3}, i.e., up to the third decimal. Therefore, when the number of incorrectly transmitted bits j is small number, the precision of the percentage of detected incorrectly transmitted code words with j incorrectly transmitted bits mostly is up to the second decimal and in some rare cases up to the first decimal. When the quasigroup of order 4 is used for coding, we are interested to see what happens when there are more incorrectly transmitted bits in a code word. For that reason, to obtain the same accuracy as previously, we need to obtain larger number of incorrectly transmitted code words with more incorrectly transmitted bits. Therefore, we chose larger values of the probability of bit-error p in the channel (i.e., 0.15 and 0.2), which ensures sufficient accuracy of the results.

The focus of the paper is in the number of errors that the code surely detects, which means that for every j we are interested whether the code detects all incorrectly transmitted code words with j incorrectly transmitted bits or some of them pass undetected. This means that we are interested only whether the percentage of detected incorrectly transmitted code words with a given number of incorrectly transmitted bits is 100% or it is not 100%. For all above, the obtained accuracy is more than sufficient.

B. Linear quasigroup of order 4 is used for coding

In what follows, we will represent the linear quasigroups used for coding by their binary matrices that satisfy (2). The matrices will be presented as a list of lists, i.e., the matrix is a list in which the first list is the first row, the second list is the second row of the matrix etc.

We use the following linear quasigroup of order 4 for coding:

$$A=\{\{0, 1\}, \{1, 1\}\}, B=\{\{1, 1\}, \{1, 0\}\}, C=\{\{0, 0\}\} \quad (4)$$

First, in the next example we will illustrate the coding, transmitting and simulation procedure when for coding is used the linear quasigroup given in (4)

Example 1: Let for coding be used the linear quasigroup given in (4). In practice the generated input message is long a few million characters, but for this example we will take small input message with length 15 characters from the quasigroup Q and the code words will have length n=20 bits. Let the input message be 230122100132131. First, we divide the input message into blocks of length $n/(2q)=20/(2\cdot 2)=5$ characters and we code each block separately. The first block is $a_1a_2a_3a_4a_5=23012$, which turned into binary form is $\boldsymbol{a_1a_2a_3a_4a_5}=1011000110$. Now, using (3) we code this block:

$$\boldsymbol{d_1}=\boldsymbol{a_1}A+\boldsymbol{a_2}B+C=[1\ 0]A+[1\ 1]B+C=[0\ 0]$$
$$\boldsymbol{d_2}=\boldsymbol{a_2}A+\boldsymbol{a_3}B+C=[1\ 1]A+[0\ 0]B+C=[1\ 0]$$
$$\boldsymbol{d_3}=\boldsymbol{a_3}A+\boldsymbol{a_4}B+C=[0\ 0]A+[0\ 1]B+C=[1\ 0]$$
$$\boldsymbol{d_4}=\boldsymbol{a_4}A+\boldsymbol{a_5}B+C=[0\ 1]A+[1\ 0]B+C=[0\ 0]$$
$$\boldsymbol{d_5}=\boldsymbol{a_5}A+\boldsymbol{a_1}B+C=[1\ 0]A+[1\ 0]B+C=[1\ 0]$$

The coded block, i.e., the code word is $cw_1=\boldsymbol{a_1a_2a_3a_4a_5d_1d_2d_3d_4d_5}=10110001100010100010$. In a same manner we code the other two blocks 21001 and

32131 whit what we obtain the code words cw_2=1001000 0011111001000 and cw_3=1110011101011110001O respectively. The coded input message is obtained by concatenation of the three codewords: $cw_1cw_2cw_3$=10110 0011000101000101001000001111100100011100111010 111100010. Now, the noise, which is a binary string with length equal to the length of coded input message $cw_1cw_2cw_3$, is generated. To generate this string, we need the probability of bit-error in the binary symmetric channel. Let say that it is p=0.1. The noise string is a string in which on each position the probability of occurrence of 1 is p, while the probability of occurrence of 0 is 1-p. In order to generate such string, for each position a random number in the interval (0, 1) is generated. If this number is smaller than p, the element on that position is 1, otherwise it is 0. Let the generated noise string be: ns=001011000000100000000001000000 10000000000000000000000000000. The output message is calculated as a sum modulo 2 of the coded input message and the noise string, i.e., the output message is ou=$cw_1cw_2cw_3$+ns=1011000110001010001010 0100000111110010001110011101011110001O+0010110 0000010000000000010000001000000000000000000000 0000000=1001110110000010001010000000101110010 001110011101011110001O. This is the message that the receiver receives. The message contains three blocks: 10011101100000100010, 10000000010111001000 and 11100111010111100010. From the noise string, we can see which code words are incorrectly transmitted and how many bits are incorrectly transmitted. Namely, first 20 bits represent the errors in the first code word, etc. If there is 1 on some position the corresponding bit from the code word is incorrectly transmitted, otherwise it is correctly transmitted. Therefore, if there is at least one 1 in the noise string, the code word is incorrectly transmitted. In this way we conclude that the first and the second code words are incorrectly transmitted, while the third code word is correctly transmitted. Since in the noise string for the first code word there are four 1's, we conclude that there are four incorrectly transmitted bits in the first code word. In a same manner we conclude that there are two incorrectly bits in the second code word. For each incorrectly transmitted code word, in order to check whether the code will detect the errors in transmission, we check whether the output block satisfies (3). The output block that corresponds to the first code word is 10011101100000100010. If the code word is correctly transmitted, the first 10 bits are the information bits, while the last 10 bits are the redundant bits. Now, we check whether the last 10 bits 0000100010 are the redundant bits for the first 10 bits 1001110110:

$$\boldsymbol{a_1}'A+\boldsymbol{a_2}'B+C=[1\ 0]A+[0\ 1]B+C=[1\ 1]\neq[0\ 0]=\boldsymbol{d_1}'$$

We see that (3) is not satisfied for i=1, which means that the code will detect the error in transmission of the first code word. In the same way we conclude that the code will detect errors in transmission of the second code word.

But, if the noise string is 00101100001100100000000 0000000000000000000000000000000000000, then there is one code word with six incorrectly transmitted bits (the first code word), while the other two code words are correctly transmitted (the output is 100111011011100000 101001000001111100100011100111010111100010). Now, we can check that the code will not detect the error in transmission. Namely, the output block for the first code word is $\boldsymbol{a_1}'\boldsymbol{a_2}'\boldsymbol{a_3}'\boldsymbol{a_4}'\boldsymbol{a_5}'\boldsymbol{d_1}'\boldsymbol{d_2}'\boldsymbol{d_3}'\boldsymbol{d_4}'\boldsymbol{d_5}'$=10011101101 110000010. We check whether (3) is satisfied:

$$\boldsymbol{a_1}'A+\boldsymbol{a_2}'B+C=[1\ 0]A+[0\ 1]B+C=[1\ 1]=\boldsymbol{d_1}'$$
$$\boldsymbol{a_2}'A+\boldsymbol{a_3}'B+C=[0\ 1]A+[1\ 1]B+C=[1\ 0]=\boldsymbol{d_2}'$$
$$\boldsymbol{a_3}'A+\boldsymbol{a_4}'B+C=[1\ 1]A+[0\ 1]B+C=[0\ 0]=\boldsymbol{d_3}'$$
$$\boldsymbol{a_4}'A+\boldsymbol{a_5}'B+C=[0\ 1]A+[1\ 0]B+C=[0\ 0]=\boldsymbol{d_4}'$$
$$\boldsymbol{a_5}'A+\boldsymbol{a_1}'B+C=[1\ 0]A+[1\ 0]B+C=[1\ 0]=\boldsymbol{d_5}'$$

We see that (3) is satisfied for all $i\in\{1, 2, 3, 4, 5\}$, which means that the code will not detect the error in transmission in the first code word.

Since we want to obtain the maximum number of incorrectly transmitted bits to which the code detects the error for sure, first we want to have large number of incorrectly transmitted code words with small number of incorrectly transmitted bits. For that reason, we choose small values for the probability of bit-error. We made simulations for three different values of the probability of bit-error in the binary symmetric channel, i.e., p=0.05, p=0.07 and p=0.09. When the information block has length m characters from the quasigroup, then the coded block has length $2m$. Since every character from the quasigroup of order 4 is represented with 2 bits, follows that the code words have length $4m$, $m\geq2$. We coded input blocks of length $4m$ characters, where $2\leq m\leq16$, which means that the code words have length n from 8 bits to 64 bits with step 4 bits, i.e., $n\in\{4m|\ 2\leq m\leq16\}$.
The obtained results when the values of the probability of bit-error p is 0.05, 0.07 and 0.09 are given in Table I, Table II and Table III, respectively. In the tables are given the percentages of detected incorrectly transmitted code words of length n bits when j bits are incorrectly transmitted, $j\in\{1, 2, \ldots, n\}$. As we can see, the code surely detects up to 3 incorrectly transmitted bits, regardless of the length of the code word. Also, we can notice that for j=4, the percentage of detected errors increases when the length of the code words increases. For these small values of the probability of bit-error p, the number of code words with larger number of incorrectly transmitted bits is small and the code detects all such incorrectly transmitted code words. Therefore, the percentages of detected incorrectly transmitted code words with larger number of incorrectly transmitted bits in Table I, Table II and Table III are 100%. The empty fields in the tables indicates that there are no incorrectly transmitted code words with the corresponding length and number of incorrectly transmitted bits.

To see what happens when the number of code words with larger number of incorrectly transmitted bits is greater, we increase the probability of bit-error in the binary symmetric channel. In Table IV and Table V are given the percentages of detected errors when the probability of bit-error p is 0.15 and 0.2. Since in these cases the probability of bit-error is higher, there are more incorrectly transmitted bits. From the tables we can see that the code detects errors in transmission whenever odd number of bits are incorrectly transmitted. For given j, increasing the length of the code words n generally results with increased percentage of detected incorrectly transmitted code words with j incorrectly transmitted bits.

TABLE I. PERCENTAGES OF DETECTED INCORRECTLY TRANSMITTED CODE WORDS OF LENGTH N BITS WITH J INCORRECTLY TRANSMITTED BITS WHEN LINEAR QUASIGROUP OF ORDER 4 IS USED FOR CODING AND THE PROBABILITY OF BIT-ERROR IS P=0.05

	j									
n	1	2	3	4	5	6	7	8	9	10
8	100%	100%	100%	75,3463%	100%					
12	100%	100%	100%	97,4871%	100%	100%				
16	100%	100%	100%	99,1865%	100%	100%	100%			
20	100%	100%	100%	99,5680%	100%	100%	100%	100%		
24	100%	100%	100%	99,8111%	100%	100%	100%	100%		
28	100%	100%	100%	99,8957%	100%	100%	100%	100%		
32	100%	100%	100%	99,8478%	100%	100%	100%	100%	100%	100%
36	100%	100%	100%	99,9360%	100%	100%	100%	100%	100%	100%
40	100%	100%	100%	99,9544%	100%	100%	100%	100%	100%	100%
44	100%	100%	100%	99,9689%	100%	100%	100%	100%	100%	100%
48	100%	100%	100%	99,9762%	100%	100%	100%	100%	100%	100%
52	100%	100%	100%	99,9909%	100%	100%	100%	100%	100%	100%
56	100%	100%	100%	99,9689%	100%	100%	100%	100%	100%	100%
60	100%	100%	100%	99,9912%	100%	100%	100%	100%	100%	100%
64	100%	100%	100%	99,9781%	100%	100%	100%	100%	100%	100%

TABLE II. PERCENTAGES OF DETECTED INCORRECTLY TRANSMITTED CODE WORDS OF LENGTH N BITS WITH J INCORRECTLY TRANSMITTED BITS WHEN LINEAR QUASIGROUP OF ORDER 4 IS USED FOR CODING AND THE PROBABILITY OF BIT-ERROR IS P=0.07

	j									
n	1	2	3	4	5	6	7	8	9	10
8	100%	100%	100%	80,2281%	100%	100%				
12	100%	100%	100%	96,5970%	100%	98,2143%	100%			
16	100%	100%	100%	99,1708%	100%	100%	100%	100%		
20	100%	100%	100%	99,5536%	100%	99,6785%	100%	100%	100%	
24	100%	100%	100%	99,8296%	100%	99,8612%	100%	100%	100%	100%
28	100%	100%	100%	99,9014%	100%	100%	100%	100%	100%	100%
32	100%	100%	100%	99,9138%	100%	100%	100%	100%	100%	100%
36	100%	100%	100%	99,9080%	100%	100%	100%	100%	100%	100%
40	100%	100%	100%	99,9813%	100%	100%	100%	100%	100%	100%
44	100%	100%	100%	99,9723%	100%	99,9893%	100%	100%	100%	100%
48	100%	100%	100%	99,9844%	100%	100%	100%	100%	100%	100%
52	100%	100%	100%	99,9806%	100%	100%	100%	100%	100%	100%
56	100%	100%	100%	99,9932%	100%	100%	100%	100%	100%	100%
60	100%	100%	100%	99,9926%	100%	100%	100%	100%	100%	100%
64	100%	100%	100%	99,9899%	100%	100%	100%	100%	100%	100%

TABLE III. PERCENTAGES OF DETECTED INCORRECTLY TRANSMITTED CODE WORDS OF LENGTH N BITS WITH J INCORRECTLY TRANSMITTED BITS WHEN LINEAR QUASIGROUP OF ORDER 4 IS USED FOR CODING AND THE PROBABILITY OF BIT-ERROR IS P=0.09

	j									
n	1	2	3	4	5	6	7	8	9	10
8	100%	100%	100%	78,5852%	100%	100%				
12	100%	100%	100%	96,7768%	100%	97,9275%	100%	100%		
16	100%	100%	100%	99,1552%	100%	99,4166%	100%	100%	100%	
20	100%	100%	100%	99,6004%	100%	100%	100%	100%	100%	100%
24	100%	100%	100%	99,7429%	100%	99,9766%	100%	100%	100%	100%
28	100%	100%	100%	99,8510%	100%	99,986%	100%	100%	100%	100%
32	100%	100%	100%	99,8777%	100%	99,9903%	100%	100%	100%	100%
36	100%	100%	100%	99,9429%	100%	100%	100%	100%	100%	100%
40	100%	100%	100%	99,9629%	100%	100%	100%	100%	100%	100%
44	100%	100%	100%	99,9681%	100%	100%	100%	100%	100%	100%
48	100%	100%	100%	99,9764%	100%	100%	100%	100%	100%	100%
52	100%	100%	100%	99,9799%	100%	99,9953%	100%	100%	100%	100%
56	100%	100%	100%	99,9885%	100%	100%	100%	99,9888%	100%	100%
60	100%	100%	100%	99,9865%	100%	100%	100%	99,9907%	100%	100%
64	100%	100%	100%	99,9946%	100%	100%	100%	100%	100%	100%

TABLE IV. PERCENTAGES OF DETECTED INCORRECTLY TRANSMITTED CODE WORDS OF LENGTH N BITS WITH J INCORRECTLY TRANSMITTED BITS WHEN LINEAR QUASIGROUP OF ORDER 4 IS USED FOR CODING AND THE PROBABILITY OF BIT-ERROR IS P=0.15

	j									
n	1	2	3	4	5	6	7	8	9	10
8	100%	100%	100%	79,6357%	100%	100%	100%			
12	100%	100%	100%	97,0214%	100%	96,4126%	100%	95,3488%	100%	
16	100%	100%	100%	99,5851%	100%	99,3124%	100%	99,3464%	100%	100%
20	100%	100%	100%	99,6125%	100%	99,8402%	100%	99,8948%	100%	98,9583%
24	100%	100%	100%	99,7836%	100%	99,9415%	100%	99,9788%	100%	100%
28	100%	100%	100%	99,8367%	100%	99,9854%	100%	100%	100%	99,9208%
32	100%	100%	100%	99,9084%	100%	99,9920%	100%	99,9850%	100%	100%
36	100%	100%	100%	99,9491%	100%	99,9973%	100%	100%	100%	100%
40	100%	100%	100%	99,9593%	100%	100%	100%	99,9953%	100%	100%
44	100%	100%	100%	99,9842%	100%	100%	100%	100%	100%	100%
48	100%	100%	100%	99,9846%	100%	100%	100%	100%	100%	100%

TABLE V. PERCENTAGES OF DETECTED INCORRECTLY TRANSMITTED CODE WORDS OF LENGTH N BITS WITH J INCORRECTLY TRANSMITTED BITS WHEN LINEAR QUASIGROUP OF ORDER 4 IS USED FOR CODING AND THE PROBABILITY OF BIT-ERROR IS P=0.2

	j											
n	1	2	3	4	5	6	7	8	9	10	11	12
8	100%	100%	100%	80,1485%	100%	100%	100%					
12	100%	100%	100%	96,9511%	100%	96,3782%	100%	98,0226%	100%	100%		
16	100%	100%	100%	99,1185%	100%	99,3189%	100%	98,7104%	100%	96,4912%	100%	100%
20	100%	100%	100%	99,6090%	100%	99,8510%	100%	99,8310%	100%	100%	100%	100%
24	100%	100%	100%	99,7872%	100%	99,9282%	100%	99,9268%	100%	100%	100%	100%
28	100%	100%	100%	99,8308%	100%	99,9921%	100%	99,9884%	100%	99,9857%	100%	99,9047%
32	100%	100%	100%	99,9044%	100%	99,9887%	100%	99,9937%	100%	100%	100%	100%
36	100%	100%	100%	99,9331%	100%	100%	100%	100%	100%	100%	100%	100%
40	100%	100%	100%	99,9790%	100%	100%	100%	99,9968%	100%	100%	100%	100%
44	100%	100%	100%	99,9840%	100%	99,9942%	100%	100%	100%	100%	100%	100%
48	100%	100%	100%	99,9980%	100%	99,9911%	100%	100%	100%	100%	100%	100%

C. Linear quasigroup of order 8 is used for coding

We use the following linear quasigroup of order 8:

$$A=\{\{1, 0, 1\}, \{0, 1, 1\}, \{1, 1, 1\}\},$$
$$B=\{\{0, 1, 1\}, \{1, 1, 1\}, \{1, 0, 1\}\}, \quad (5)$$
$$C=\{\{0, 0, 0\}\}$$

Again, we make simulations for values of the probability of bit-error p=0.05, 0.07 and 0.09. When we use quasigroups of order 8, the code words have length that is multiple of 6. We obtained the percentage of detected incorrectly transmitted code words for code words of length n from 12 bits to 66 bits with step 6 bits, i.e. $n\in\{6m|\ 2\leq m\leq 11\}$. The obtained results are given in Table VI, Table VII and Table VIII. From the tables can be seen that for code words of length 12 and 18 bits, the code surely detects up to 2 incorrectly bits, while for code words od length greater than 18 bits, the code surely detects up to 3 incorrectly bits. As in the case when quasigroup of order 4 is used for coding, when the length of the code word increases, the percentage of detected incorrectly transmitted code words with j incorrectly transmitted bits generally increases, too. Due to the small number of incorrectly transmitted code words with more than 4 incorrectly transmitted bits, this property is not so obvious when p=0.05, but when p=0.09 it becomes obvious.

TABLE VI. PERCENTAGES OF DETECTED INCORRECTLY TRANSMITTED CODE WORDS OF LENGTH N BITS WITH J INCORRECTLY TRANSMITTED BITS WHEN LINEAR QUASIGROUP OF ORDER 8 IS USED FOR CODING AND THE PROBABILITY OF BIT-ERROR IS P=0.05

	j									
n	1	2	3	4	5	6	7	8	9	10
12	100%	100%	98,1302%	98,5625%	99,4792%	100%	100%			
18	100%	100%	99,5710%	99,9352%	99,8875%	100%	100%			
24	100%	100%	100%	99,9751%	100%	100%	100%	100%		
30	100%	100%	100%	99,9775%	100%	100%	100%	100%	100%	100%
36	100%	100%	100%	99,9828%	100%	100%	100%	100%	100%	100%
42	100%	100%	100%	99,9929%	100%	100%	100%	100%	100%	100%
48	100%	100%	100%	99,9968%	99,9931%	100%	100%	100%	100%	100%
54	100%	100%	100%	99,997%	99,9942%	100%	100%	100%	100%	100%
60	100%	100%	100%	99,9942%	100%	100%	100%	100%	100%	100%
66	100%	100%	100%	99,9971%	100%	100%	100%	100%	100%	100%

TABLE VII. PERCENTAGES OF DETECTED INCORRECTLY TRANSMITTED CODE WORDS OF LENGTH N BITS WITH J INCORRECTLY TRANSMITTED BITS WHEN LINEAR QUASIGROUP OF ORDER 8 IS USED FOR CODING AND THE PROBABILITY OF BIT-ERROR IS P=0.07

	j									
n	1	2	3	4	5	6	7	8	9	10
12	100%	100%	98,2049%	98,8929%	98,5149%	98,7342%	100%			
18	100%	100%	99,6278%	99,8986%	99,8930%	99,8358%	100%	100%	100%	
24	100%	100%	100%	99,9564%	99,8890%	100%	99,7506%	100%	100%	100%
30	100%	100%	100%	99,9723%	99,9743%	100%	100%	100%	100%	100%
36	100%	100%	100%	99,9846%	99,9908%	100%	100%	100%	100%	100%
42	100%	100%	100%	99,9979%	100%	100%	100%	100%	100%	100%
48	100%	100%	100%	99,9958%	100%	100%	100%	100%	100%	100%
54	100%	100%	100%	99,9933%	100%	100%	100%	100%	100%	100%
60	100%	100%	100%	99,9976%	100%	100%	100%	100%	100%	100%
66	100%	100%	100%	99,9972%	100%	100%	100%	100%	100%	100%

TABLE VIII. PERCENTAGES OF DETECTED INCORRECTLY TRANSMITTED CODE WORDS OF LENGTH N BITS WITH J INCORRECTLY TRANSMITTED BITS WHEN LINEAR QUASIGROUP OF ORDER 8 IS USED FOR CODING AND THE PROBABILITY OF BIT-ERROR IS P=0.09

	j									
n	1	2	3	4	5	6	7	8	9	10
12	100%	100%	98,1008%	98,8065%	99,1677%	97,9381%	100%			
18	100%	100%	99,6734%	99,9135%	99,8203%	99,8158%	100%	100%	100%	100%
24	100%	100%	100%	99,9605%	99,9614%	100%	100%	100%	100%	100%
30	100%	100%	100%	99,9706%	99,9679%	100%	99,9782%	100%	100%	100%
36	100%	100%	100%	99,9904%	99,9950%	100%	100%	100%	100%	100%
42	100%	100%	100%	99,9932%	99,9977%	100%	100%	100%	100%	100%
48	100%	100%	100%	99,9980%	99,9977%	100%	100%	100%	100%	100%
54	100%	100%	100%	99,9952%	100%	100%	100%	100%	100%	100%
60	100%	100%	100%	99,9970%	100%	100%	100%	100%	100%	100%
66	100%	100%	100%	99,9967%	100%	100%	100%	100%	100%	100%

D. *Comparison of the error-detecting capability for quasigroups of order 4 and order 8*

In both cases, when the length of the code words is greater than 18 bits, the code surely detects up to 3 incorrectly transmitted bits. But, for shorter code words, i.e., a code words with length smaller than or equal to 18 bits, the code based on a linear quasigroup of order 4 detects for sure up to 3 incorrectly, while the code based on a linear quasigroup of order 8 detects for sure up to 2 incorrectly transmitted bits.

We can notice that in both cases, for a given number of incorrectly transmitted bits *j*, the percentage of detected incorrectly transmitted code words increases when the length of the code word increases. Also, for a same probability of bit-error in the binary symmetric channel and equal lengths of the code words, the quasigroup of order 8 gives greater percentage of detected incorrectly transmitted code words with *j* incorrectly transmitted bits, for all possible even values of *j*. For all odd values of *j*, the code based on linear quasigroup of order 4 detects all incorrectly transmitted code words with *j* incorrectly transmitted bits, while this is not a case when linear quasigroup of order 8 is used for coding.

IV. CONCLUSION

When the linear quasigroup of order 4 is used for coding, the analyzed code surely detects up to 3 incorrectly transmitted bits, regardless of the length of the code words. When the linear quasigroup of order 8 is used for coding, the code surely detects up to 2 incorrectly transmitted bits when code word has length 12 or 18 bits and up to 3 incorrectly transmitted bits when code word has length greater than 18 bits. Also, when linear quasigroup of order 4 is used for coding, the code detects the errors in transmission whenever odd number of bits are incorrectly transmitted.

ACKNOWLEDGMENT

This work was partially financed by the Faculty of Computer Science and Engineering at the “Ss.Cyril and Methodius” University.

REFERENCES

[1] V. Bakeva and N. Ilievska, “A probabilistic model of error-detecting codes based on quasigroups,” Quasigroups and Related Systems, vol. 17, no. 2, pp. 135-148, 2009.

[2] N. Ilievska and D. Gligoroski, “Quasigroup redundancy check codes for safety-critical systems,” Proc. of 11th Advanced Internetional Conference on Telecommunications IARIA, pp. 72-77, 2015.

[3] N. Ilievska and V. Bakeva, “A model of error-detecting codes based on quasigroups of order 4,” Proc. 6th Int. Conf. on Informatics and Information Technologies, R.Macedonia, pp. 7-11, 2008.

[4] W. W. Peterson and D. T. Brown, “Cyclic Codes for Error Detection,” in Proceedings of the IRE, vol. 49, no. 1, pp. 228-235, 1961.

[5] J.C. Knight, “Safety Critical Systems: Challenges and Directions,” in Proceedings of the 24th International Conference on Software Engineering, pp. 547-550, 2002.