Quasigroups and Related Systems **17** (2009), 135 – 148

A probabilistic model of error-detecting codes based on quasigroups

Verica Bakeva and Nataša Ilievska

Abstract. Error-detecting codes are used to detect errors when messages are transmitted through a noisy communication channel. We propose a new model of error-detecting codes based on quasigroups. In order to detect errors, we extend an input block $a_1a_2\dots a_n$ to a block $a_1a_2\dots a_nb_1b_2\dots b_n$, where $b_i = a_i * a_{r_{i+1}} * a_{r_{i+2}} * a_{r_{i+k-1}}$, $i = 1, 2, \dots, n$ where $*$ is a quasigroup operation and $r_j = \begin{cases} j, & j \leqslant n \\ j \mod n, & j > n \end{cases}$. We calculate an approximate formula which gives the probability that there will be errors which will not be detected in two special cases: for the set $A = \{0, 1\}$ and $k = 4$; and for the set $A = \{0, 1, 2, 3\}$ and $k = 2$. We find the optimal block length such that the probability of undetected errors is smaller than some previous given value ε. Also, we compare two considered codes and conclude that quasigroups of higher order give smaller probability of undetected errors. At the end of this paper we give a classification of quasigroups of order 4 according to goodness for proposed codes.

1. Introduction

We propose a new model of error-detecting codes based on quasigroup operations. Recall that a quasigroup $(Q, *)$ is a groupoid (i.e., algebra with one binary operation $*$ on the set Q) satisfying the law:

$$(\forall u, v \in Q)(\exists! x, y \in Q) \quad (x * u = v \ \& \ u * y = v) \tag{1}$$

In fact (1) says that the equations $x * u = v$, $u * y = v$ for each given $u, v \in Q$ and x, y unknown, have unique solutions.

In paper [1], using the image pattern authors gave classification of quasigroups of order 4 as fractal and non-fractal. In paper [2], the following definition of linear quasigroup is given. Let $(Q, *)$ be a quasigroup of order 2^n and let

2000 Mathematics Subject Classification: 68P30
Keywords: error-detecting codes, quasigroup, noisy channel, probability of undetected errors

$$f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$$

be its corresponding representation as vector valued Boolean function. If all f_i for $i = 1, 2, \ldots, n$ are linear polynomials, then this quasigroup is called linear quasigroup. Otherwise, if there exists function f_i for some $i = 1, 2, \ldots, n$ which is not linear, this quasigroup is called nonlinear quasigroup.

In papers [4] and [5], there are some design of codes based on quasigroups of order 2. Here, we define the code design based on quasigroups of arbitrary order (Section 2). In Section 3, we find the probability of undetected errors for the codes based on quasigroups of order 2 and $k = 4$ where k is number of symbols used in calculation of each redundancy symbol. On the same way, in Section 4, we give the probability of undetected errors for the codes based on quasigroups of order 4 and $k = 2$. We filter the 576 quasigroups of order 4 such that the probability of undetected errors does not depend of the input message. On that way, we obtain 160 quasigroups. In Section 5, we describe how to choose the block length n such that the probability of undetected errors is smaller than a given value ε. Also, we compare the maximums of the obtained probability functions of undetected errors for two considered codes and make some conclusions. In Section 6, we give a classification of obtained 160 quasigroups according to their goodness for our codes.

2. Designing of the codes

Let A be an arbitrary finite set called alphabet and $(A, *)$ be a given quasigroup. Let consider an input message

$$a_1 a_2 \ldots a_n a_{n+1} a_{n+2} \ldots a_{2n} a_{2n+1} \ldots, \quad (a_i \in A,\ i = 1, 2, \ldots)$$

which will be transmitted through a noisy channel. Since of the noise, the received message can be different of the sent one. Our goal is designing a code which will detect the errors during transmission such that the probability of undetected errors will be as small as possible. For that reason, we have to add some redundancy to the message, i.e., some control bits.

Let divide the input message to blocks with length n:

$$a_1 a_2 \ldots a_n, \quad a_{n+1} a_{n+2} \ldots a_{2n}, \ \ldots$$

We extend each block $a_1 a_2 \ldots a_n$ to a block $a_1 a_2 \ldots a_n b_1 b_2 \ldots b_n$ where

$$\begin{array}{lcl} b_1 & = & a_1 * a_2 * \cdots * a_k \\ b_2 & = & a_2 * a_3 * \cdots * a_{k+1} \\ \ldots & \ldots & \ldots\ldots\ldots\ldots\ldots \\ b_n & = & a_n * a_1 * \cdots * a_{k-1} \end{array} \tag{2}$$

where $k \leqslant n$.

At first, each letter from the extended block $a_1a_2 \ldots a_nb_1b_2 \ldots b_n$ will be presented in 2-base system. After that the obtained binary block will be transmitted through the binary symmetrical channel with probability of bit error p $(0 < p < 0.5)$ (Figure 1)

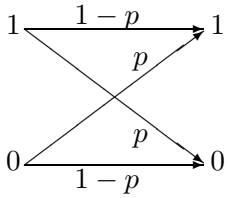

Figure 1: Binary symmetrical channel

The rate of this code is 1/2. Because of the noises in the channel, some of the characters may not be correctly transmitted. Let a_i be transmitted as a'_i, b_i as b'_i, $i \in \{1, 2, \ldots, n\}$. If the character transmission is correct than a'_i will have the same value as a_i. Otherwise, a'_i will not be the same as a_i. So, the output message is $a'_1a'_2 \ldots a'_nb'_1b'_2 \ldots b'_n$. To check if there are any errors during transmission, the receiver of the message checks if

$$\begin{array}{lcl} b'_1 & = & a'_1 * a'_2 * \cdots * a'_k \\ b'_2 & = & a'_2 * a'_3 * \cdots * a'_{k+1} \\ \ldots & \ldots & \ldots\ldots\ldots\ldots\ldots \\ b'_n & = & a'_n * a'_1 * \cdots * a'_{k-1} \end{array}$$

If any of these equalities are not satisfied, the receiver concludes that some errors occured during the block transmission and it asks from the sender to send that block once again. But, some equality can be satisfied although some characters in that equality are incorrectly transmitted. In that case, incorrect transmission (error in transmission) will not be detected. We will consider two special cases of the proposed code. For the first one, we choose $A = \{0, 1\}$ and $k = 4$ and for the second one, $A = \{0, 1, 2, 3\}$ and $k = 2$. Our goal is finding approximately the probability of undetected errors and make that probability as small as possible. In the both codes, each redundant

symbol b_i, defined in (2), includes the same number of bits, i.e., 4 bits from the input message, so it is reasonably to compare the obtained probabilities of undetected errors.

3. An error-detecting code based on quasigroup of order 2 and k=4

Let consider the binary set $A = \{0, 1\}$. There are only two quasigroup operations on the set A, and here we took $(A, *)$ to be defined by the table

$*$	0	1
0	0	1
1	1	0

Denote that same results will be obtained if another quasigroup is used.

Each block $a_1a_2 \dots a_n$ $(a_i \in A)$ is extended to a block

$$a_1a_2 \dots a_nb_1b_2 \dots b_n,$$

where $b_i = a_i * a_{r_{i+1}} * a_{r_{i+2}} * a_{r_{i+3}}$. Here

$$r_j = \begin{cases} j, & j \leqslant n \\ j(\mathrm{mod}\, n), & j > n \end{cases}$$

for $j = i + 1, i + 2, i + 3$.

Let introduce the following notation:

$$g(x_1, x_2, \dots, x_n) = x_1 * x_2 * \cdots * x_n,$$

where $x_i \in \{0, 1\}$, $i = 1, 2, \dots, n$. In order to determine the probability of undetected errors, we need the following proposition which proof is obvious.

Proposition 1. *If odd number of $x_1, x_2, \dots, x_n$ $(x_i \in \{0, 1\})$ change their values then $g(x_1, x_2, \dots, x_n)$ will change its value, too. If even number of $x_1, x_2, \dots, x_n$ change their values then the value of $g(x_1, x_2, \dots, x_n)$ will be unchanged.* □

Using the previous proposition and some combinatorics the following theorem can be proved.

Theorem 1. *Let $f_2(n,p)$ be the probability function of undetected errors in a transmitted block with length n through the binary symmetric channel where p is the probability of incorrect transmission of a bit. Then $f_2(n,p)$ is given by the following formulas:*

$$
\begin{aligned}
f_2(4,p) &= 6p^2(1-p)^6 + p^4(1-p)^4 + 4p^5(1-p)^3 + 4p^7(1-p)\\
f_2(5,p) &= 10p^4(1-p)^6 + 16p^5(1-p)^5 + 5p^8(1-p)^2\\
f_2(6,p) &= 2p^3(1-p)^9 + 6p^4(1-p)^8 + 18p^5(1-p)^7\\
&\quad +16p^6(1-p)^6 + 6p^7(1-p)^5 + 9p^8(1-p)^4 + O(p^9)\\
f_2(7,p) &= 7p^4(1-p)^{10} + 21p^5(1-p)^9 + 21p^6(1-p)^8 + 29p^7(1-p)^7\\
&\quad +28p^8(1-p)^6 + O(p^9)\\
f_2(8,p) &= 14p^4(1-p)^{12} + 8p^5(1-p)^{11} + 24p^6(1-p)^{10} + 56p^7(1-p)^9\\
&\quad +49p^8(1-p)^8 + O(p^9)\\
f_2(9,p) &= 9p^4(1-p)^{14} + 9p^5(1-p)^{13} + 36p^6(1-p)^{12} + 81p^7(1-p)^{11}\\
&\quad +63p^8(1-p)^{10} + O(p^9)\\
f_2(10,p) &= 10p^4(1-p)^{16} + 12p^5(1-p)^{15} + 20p^6(1-p)^{14} + 100p^7(1-p)^{13}\\
&\quad +120p^8(1-p)^{12} + O(p^9)\\
f_2(11,p) &= 11p^4(1-p)^{18} + 11p^5(1-p)^{17} + 22p^6(1-p)^{16} + 99p^7(1-p)^{15}\\
&\quad +132p^8(1-p)^{14} + O(p^9)\\
f_2(12,p) &= 12p^4(1-p)^{20} + 12p^5(1-p)^{19} + 30p^6(1-p)^{18} + 72p^7(1-p)^{17}\\
&\quad +162p^8(1-p)^{16} + O(p^9)\\
f_2(13,p) &= 13p^4(1-p)^{22} + 13p^5(1-p)^{21} + 26p^6(1-p)^{20} + 78p^7(1-p)^{19}\\
&\quad +182p^8(1-p)^{18} + O(p^9)\\
f_2(n,p) &= np^4(1-p)^{2n-4} + np^5(1-p)^{2n-5} + 2np^6(1-p)^{2n-6}\\
&\quad +6np^7(1-p)^{2n-7} + Ap^8(1-p)^{2n-8} + Bp^{n/2}(1-p)^{3n/2} + O(p^9),\\
&\qquad\qquad \textit{for } n \geqslant 14,
\end{aligned}
$$

where

$$
A = \begin{cases} \dfrac{(n+9)n}{2}, & n = 15, 17, 19, \ldots \\ \dfrac{(n+8)n}{2}, & n = 14, 16, 18, \ldots \end{cases}
\qquad
B = \begin{cases} 0, & n \text{ odd} \\ 2, & n \text{ even, but } 4 \dagger n \\ 6, & 4 | n \end{cases}
$$

□

The remainder $O(p^9)$ denotes that the coefficients are exactly determined in terms which contain p^i, $i < 9$. To obtain exactly the probability of undetected errors, i.e., to obtain exactly $O(p^9)$, one has to make much complicated combinatorial calculations. In the Figure 2, we can see that

for small values of n, all functions have maximum in $p = 0,5$. When the block length n increases, the maximum becomes smaller, it goes to the left and the sequence of maximums converges to 0.

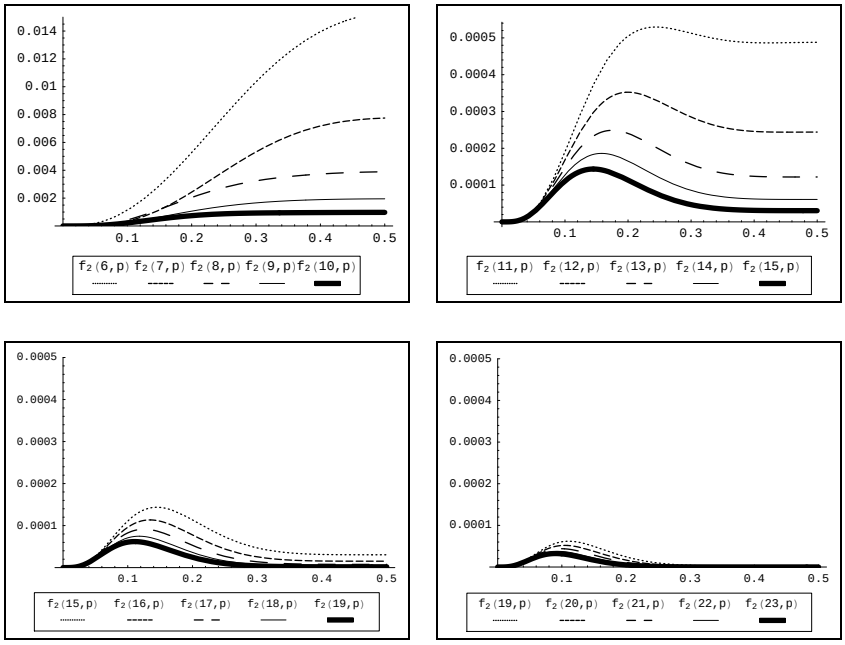

Figure 2: The probability functions of undetected errors

4. An error-detecting code based on quasigroup of order 4 and k=2

Let consider the set $A = \{0, 1, 2, 3\}$ and let $*$ be an arbitrary quasigroup operation on A. According to (2), we extend each block $a_1a_2 \dots a_n$ $(a_i \in A)$ to a block $a_1a_2 \dots a_nb_1b_2 \dots b_n$, where $b_i = a_i * a_{(i \mod n)+1}$, $i = 1, 2, \dots, n$. The extended message is transmitted through the binary symmetrical channel again. As previous, we want to calculate the probability that there will be errors which will not be detected. There are 576 quasigroups of order 4. We find that for some quasigroups, the probability of undetected errors depends on the distribution of letters in the input message. So, we filtered the quasigroups such that this formula is independent from the distribution

of the input message. After filtering, from the 576 quasigroups of order 4, only 160 quasigroups remain. All of them are fractal quasigroups, but not all fractal quasigroups are in these 160 quasigroups ([1]). For the filtered 160 quasigroups, we obtained a formula for calculating the probability function of undetected errors. It is given by the following theorem which proof is done in [3].

Theorem 2. *Let $f_4(n,p)$ be the probability of undetected errors in a transmitted block with length n through the binary symmetric channel where p is the probability of incorrect transmission of a bit. If one of the filtered 160 quasigroups is used for designing the code, then the probability of undetected errors is given by the following formulas:*

$$\begin{aligned}
f_4(2,p) &= 2v_0v_1 + r_2\\
f_4(3,p) &= 3v_0^3v_1 + 3v_0v_2 + r_3\\
f_4(4,p) &= 4v_0^5v_1 + 4v_0^3v_2 + 2v_0^2v_1^2 + 4v_0v_3 + r_4\\
f_4(n,p) &= nv_1v_0^{2n-3} + nv_2v_0^{2n-5} + \frac{n(n-3)}{2}v_1^2v_0^{2n-6} + nv_3v_0^{2n-7}\\
&\quad + n(n-4)v_2v_1v_0^{2n-8} + \frac{n(n-4)(n-5)}{6}v_1^3v_0^{2n-9} + nv_4v_0^{2n-9}\\
&\quad + n(n-5)v_3v_1v_0^{2n-10} + \frac{n(n-5)}{2}v_2^2v_0^{2n-10}\\
&\quad + \frac{n(n-5)(n-6)}{2}v_2v_1^2v_0^{2n-11} + \frac{n(n-5)(n-6)(n-7)}{24}v_1^4v_0^{2n-12},
\end{aligned}$$

for $n \geqslant 5$. In the formulas, we use the following notations:
v_k - the probability of undetected errors when exactly k consecutive characters of the initial message $a_1a_2\ldots a_n$ are incorrectly transmitted (the characters $a_i, a_{i+1}, \ldots, a_{i+k-1}$ are incorrectly transmitted, but a_{i-1} and a_{i+k} are correctly transmitted), $k = 1,2,3,4$;
v_0 - the probability of correct transmission of a character;
r_k - the probability of undetected errors in a block with length k if all k characters are incorrectly transmitted, $k = 2,3,4$. □

Now, using the Theorem 2 and formulas for the probabilities v_k, functions $f_4(n,p)$ can be determined for all 160 fractal quasigroups. These 160 quasigroups do not define 160 different functions for the probability of undetected errors, but only 7. These functions are given in Section 6 (Figure 5) where using these functions, we give a classification of the quasigroups of order 4 according to goodness for our codes.

The quasigroups which give the smallest probability of undetected errors are the best for code design. For these quasigroups, using some combina-

torics we calculate the following expressions for v_i and r_j.

$$
\begin{aligned}
v_0 &= (1-p)^2 \\
v_1 &= 3(1-p)^2p^4 \\
v_2 &= (1-p)^2p^4(9p^4-16p^3+12p^2-4p+1) \\
v_3 &= (1-p)^2p^6(3p^2-4p+2)(9p^4-20p^3+18p^2-8p+2) \\
v_4 &= (1-p)^2p^8(81p^8-432p^7+1060p^6-1548p^5+1475p^4-944p^3+400p^2 \\
&\quad -104p+13) \\
r_2 &= p^4(9p^4-32p^3+48p^2-32p+8) \\
r_3 &= p^4(27p^8-144p^7+348p^6-484p^5+429p^4-252p^3+98p^2-24p+3) \\
r_4 &= p^6(81p^{10}-576p^9+1904p^8-3792p^7+5012p^6-4576p^5+2928p^4-1312p^3 \\
&\quad +404p^2-80p+8)
\end{aligned}
$$

Now, the probability of undetected errors is determined by the following formulas:

$$
\begin{aligned}
f_{4,1}(2,p) &= p^4(15p^4-56p^3+84p^2-56p+14) \\
f_{4,1}(3,p) &= p^4(63p^8-372p^7+990p^6-1540p^5+1545p^4-1032p^3+452p^2 \\
&\quad -120p+15) \\
f_{4,1}(4,p) &= p^4(255p^{12}-2032p^{11}+7560p^{10}-17360p^9+27556p^8-32112p^7 \\
&\quad +28440p^6-19440p^5+10206p^4-4000p^3+1104p^2-192p+16) \\
f_{4,1}(n,p) &= np^4(1-p)^{2(2n-8)}\times \\
&\quad \times\Big[4-48p+274p^2-980p^3+(8n+2431)p^4-8(8n+547)p^5 \\
&\quad +2(130n+2853)p^6-4(166n+1259)p^7+(9n^2+1078n+2297)p^8 \\
&\quad -4(9n^2+270n-139)p^9+(81n^2+371n-890)p^{10} \\
&\quad -2(45n^2-165n+194)p^{11}+(3/8)(9n^3-42n^2+75n-34)p^{12}\Big] \\
&\quad +O(p^7), \qquad \text{for } n \geqslant 5.
\end{aligned}
$$

The function $f_{4,1}(n,p)$ without the remainder $O(p^7)$ gives the probability that at most 4 characters of the input message are incorrectly transmitted and the errors are not detected. As previous, to obtain the probability of undetected errors exactly, one has to calculate the probability that more than 4 characters are incorrectly transmitted and the errors are not detected, which is much complicated combinatorial problem. The shape of the probability functions of undetected errors is similar as in the previous case. When the block length n increases the maximum of these functions becomes smaller, it goes to the left and the sequence of maximums converges to 0 (Figure 3).

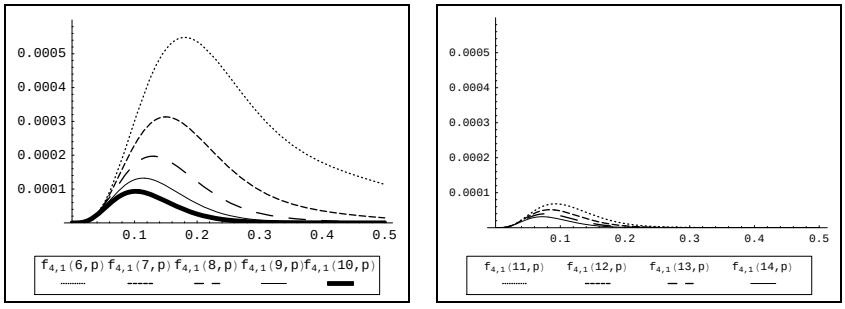

Figure 3: The probability functions of undetected errors

5. Controlling of undetected errors and comparing of the previous two codes

We want to control the probability of undetected errors, actually to make that probability smaller than some previous given value ε. So, we can find for which values of n the maximum of the function $f(n,p)$ ($f(n,p)$ can be $f_2(n,p)$ or $f_{4,1}(n,p)$) is smaller then ε. Since the sequence of maximums of the functions $f(n,p)$ is strictly decreasing and converges to 0 when $n \to \infty$, there will be $n_0 \in \mathbb{N}$, such that the maximum of the function $f(n,p)$ will be smaller than ε, for all $n \geqslant n_0$ and the maximum of the function $f(n,p)$ will be greater than ε, for all $n < n_0$. We choose $n = n_0$ (see Figure 4).

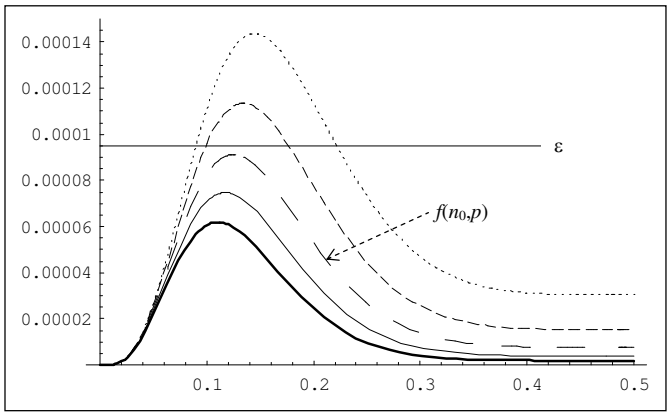

Figure 4: Choosing of n_0

Now, we separate the message in blocks with length n and we code every block individually. From all values of n which satisfies the condition $f(n,p) < \varepsilon$, we choose the smallest one since in this case we have fastest transmission. Namely, if the receiver detects errors in the received block, it asks for repeated transmission, so it is better the block length to be as small as possible.

In the Table 1, we give the maximums of the probability functions of undetected errors for the first and the second proposed code. From this table, we can conclude that the maximums of the functions of undetected errors are smaller when the quasigroups of order 4 are used. It suggest that using the quasigroup of order 4 we obtain better and more efficiently codes.

n	Quasigroups of order 2	Quasigroups of order 4
10	9.75609×10^{-4}	9.35406×10^{-5}
11	5.29529×10^{-4}	6.82458×10^{-5}
12	3.52349×10^{-4}	5.14707×10^{-5}
13	2.48784×10^{-4}	3.97896×10^{-5}
14	1.86131×10^{-4}	3.14013×10^{-5}
15	1.43616×10^{-4}	2.52198×10^{-5}
16	1.13480×10^{-4}	2.05631×10^{-5}
17	9.13489×10^{-5}	1.69878×10^{-5}
18	7.47017×10^{-5}	1.41968×10^{-5}
19	6.19084×10^{-5}	1.19860×10^{-5}
20	5.19030×10^{-5}	1.02120×10^{-5}
21	4.39585×10^{-5}	8.77182×10^{-6}
22	3.75666×10^{-5}	7.59050×10^{-6}
23	3.23631×10^{-5}	6.61231×10^{-6}
24	2.80827×10^{-5}	5.79537×10^{-6}
25	2.45283×10^{-5}	5.10775×10^{-6}
26	2.15517×10^{-5}	4.52483×10^{-6}

Table 1: The maximums of the probability functions

6. Classification of quasigroups of order 4 according to goodness for proposed codes

As we mentioned in Section 4 we filtered 576 quasigroups of order 4 such that the probability of undetected errors does not depend on the distribution of letters in the input messages. After filtering only 160 quasigroups remain

and they give 7 different functions of probability of undetected errors. The best of these functions is $f_{4,1}(n,p)$ given in Section 4. Others are given with the following formulas.

$$
\begin{aligned}
f_{4,2}(2,p) &= (1-p)^2p^2(3p^2-4p+2)(5p^2-2p+1)\\
f_{4,2}(3,p) &= 3(1-p)^4p^4(21p^4-40p^3+44p^2-24p+6)\\
f_{4,2}(4,p) &= (1-p)^4p^4(255p^8-1012p^7+1982p^6-2468p^5+2145p^4-1320p^3+556p^2\\
&\quad -144p+18)\\
f_{4,2}(n,p) &= np^4(1-p)^{2(2n-8)}\times\\
&\quad \times\Big[4-48p+275p^2-990p^3+(8n+2475)p^4-8(8n+561)p^5\\
&\qquad +2(130n+2943)p^6-4(166n+1305)p^7+(9n^2+1078n+2409)p^8\\
&\qquad -4(9n^2+270n-131)p^9+(81n^2+371n-890)p^{10}\\
&\qquad -2(45n^2-165n+194)p^{11}+(3/8)(9n^3-42n^2+75n-34)p^{12}\Big]\\
&\quad +O(p^7), \qquad \text{for } n\geqslant 5.
\end{aligned}
$$

$$
\begin{aligned}
f_{4,3}(2,p) &= p^2(-p^6+8p^5-12p^4+8p^3-p^2-2p+1)\\
f_{4,3}(3,p) &= p^3(-p^9+12p^8-66p^7+220p^6-411p^5+456p^4-312p^3+132p^2-33p+4)\\
f_{4,3}(4,p) &= p^3(-p^{13}+16p^{12}-120p^{11}+560p^{10}-1628p^9+3216p^8-4568p^7+4800p^6\\
&\quad -3765p^5+2188p^4-918p^3+264p^2-47p+4)\\
f_{4,3}(n,p) &= (1/24)np^3(1-p)^{2(2n-10)}\times\\
&\quad \times\Big[24-384p+2952p^2+12(n-1203)p^3-48(3n-1045)p^4+48(18n-2731)p^5\\
&\quad +4(n^2-837n+66488)p^6-8(4n^2-1158n+53327)p^7\\
&\quad +4(37n^2-4845n+136880)p^8+(n^3-446n^2+31259n-566302)p^9\\
&\quad -4(n^3-226n^2+9701n-118268)p^{10}+2(5n^3-658n^2+18469n-159020)p^{11}\\
&\quad -4(4n^3-347n^2+6665n-42412)p^{12}+(19n^3-1078n^2+14453n-69890)p^{13}\\
&\quad -4(4n^3-149n^2+1433n-5314)p^{14}+2(5n^3-116n^2+817n-2302)p^{15}\\
&\quad -4(n^3-14n^2+71n-154)p^{16}+(n^3-10n^2+35n-50)p^{17}\Big]\\
&\quad +O(p^7), \qquad \text{for } n\geqslant 5.
\end{aligned}
$$

$$
\begin{aligned}
f_{4,4}(2,p) &= (1-p)^2p^3(-p^3+6p^2-7p+4)\\
f_{4,4}(3,p) &= (1-p)^3p^3(p^6-9p^5+36p^4-44p^3+30p^2-12p+3)\\
f_{4,4}(4,p) &= (1-p)^4p^3(-p^9+12p^8-66p^7+220p^6-399p^5+440p^4-300p^3+128p^2-32p+4)\\
f_{4,4}(n,p) &= (1/24)np^3(1-p)^{2(2n-10)}\times\\
&\quad \times\Big[24-384p+2976p^2+12(n-1229)p^3-144(n-361)p^4+24(37n-5729)p^5\\
&\quad +4(n^2-891n+70274)p^6-4(8n^2-2535n+113035)p^7\\
&\quad +8(20n^2-2709n+72514)p^8+(n^3-530n^2+35747n-601066)p^9\\
&\quad -4(n^3-289n^2+11342n-126548)p^{10}+2(5n^3-880n^2+21883n-172004)p^{11}\\
&\quad -16(n^3-119n^2+1979n-11494)p^{12}+(19n^3-1474n^2+17129n-74834)p^{13}\\
&\quad -4(4n^3-197n^2+1721n-5698)p^{14}+10(n^3-28n^2+197n-518)p^{15}\\
&\quad -4(n^3-14n^2+71n-154)p^{16}+(n^3-10n^2+35n-50)p^{17}\Big]\\
&\quad +O(p^7), \qquad \text{for } n\geqslant 5.
\end{aligned}
$$

$$
\begin{aligned}
f_{4,5}(2,p) &= (1-p)p^2(p^5+9p^4-19p^3+17p^2-8p+2)\\
f_{4,5}(3,p) &= (1-p)^3p^3(p^6-9p^5+36p^4-60p^3+54p^2-24p+5)\\
f_{4,5}(4,p) &= (1-p)^2p^3(-p^{11}+14p^{10}+37p^9-276p^8+567p^7-526p^6+125p^5+216p^4-252p^3\\
&\quad +128p^2-34p+4)
\end{aligned}
$$

$$
\begin{aligned}
f_{4,5}(n,p) &= (1/24)np^3(1-p)^{2(2n-10)}\times \\
&\times\Big[24-330p+2544p^2+12(n-933)p^3-24(5n-1424)p^4+12(47n-6355)p^5 \\
&+4(n^2-411n+31844)p^6-4(5n^2-849n+39922)p^7 \\
&+4(7n^2-1431n+37058)p^8+(n^3+82n^2+8855n-100714)p^9 \\
&-4(n^3+116n^2+3131n-14012)p^{10}+2(5n^3+518n^2+7177n-20420)p^{11} \\
&-4(4n^3+361n^2+2777n-9916)p^{12}+(19n^3+1334n^2+4385n-28466)p^{13} \\
&-4(4n^3+205n^2-133n-2602)p^{14}+2(5n^3+148n^2-647n-286)p^{15} \\
&-4(n^3+10n^2-97n+134)p^{16}+(n^3-10n^2+35n-50)p^{17}\Big] \\
&+O(p^7), \qquad \text{for } n\geqslant 5.
\end{aligned}
$$

$$
\begin{aligned}
f_{4,6}(2,p) &= (1-p)^2p^2(-p^4+6p^3-3p^2+1) \\
f_{4,6}(3,p) &= (1-p)^3p^3(p^6-9p^5+36p^4-52p^3+42p^2-18p+4) \\
f_{4,6}(4,p) &= (1-p)^4p^3(-p^9+12p^8-66p^7+220p^6-319p^5+280p^4-180p^3+88p^2 \\
&\quad -27p+4) \\
f_{4,6}(n,p) &= (1/24)np^3(1-p)^{2(2n-10)}\times \\
&\times\Big[24-360p+2592p^2+12(n-995)p^3-120(n-329)p^4+12(51n-8297)p^5 \\
&+4(n^2-537n+49598)p^6-20(n^2-285n+15938)p^7 \\
&+4(13n^2-2955n+104282)p^8+(n^3-110n^2+19199n-445066)p^9 \\
&-4(n^3-52n^2+6047n-96152)p^{10}+2(5n^3-178n^2+11749n-133004)p^{11} \\
&-4(4n^3-119n^2+4349n-36172)p^{12}+(19n^3-490n^2+9761n-60338)p^{13} \\
&-4(4n^3-89n^2+1013n-4594)p^{14}+2(5n^3-92n^2+649n-2014)p^{15} \\
&-4(n^3-14n^2+71n-154)p^{16}+(n^3-10n^2+35n-50)p^{17}\Big] \\
&+O(p^7), \qquad \text{for } n\geqslant 5.
\end{aligned}
$$

$$
\begin{aligned}
f_{4,7}(2,p) &= (1-p)^2p^2(1+p)(-p^3+7p^2-6p+2) \\
f_{4,7}(3,p) &= (1-p)^4p^3(4-p)(p^4-4p^3+12p^2-8p+2) \\
f_{4,7}(4,p) &= (1-p)^4p^3(-p^3+6p^2-7p+4)(p^6-6p^5+23p^4-36p^3+30p^2-12p+2) \\
f_{4,7}(n,p) &= (1/24)np^3(1-p)^{2(2n-12)}\times \\
&\times\Big[48-960p+9168p^2+24(2n-2319)p^3-48(16n-5021)p^4 \\
&+48(122n-16489)p^5+16(2n^2-1785n+127894)p^6 \\
&-24(16n^2-4188n+178017)p^7+48(42n^2-5635n+152925)p^8 \\
&+4(4n^3-1492n^2+142127n-2630189)p^9 \\
&-48(4n^3-224n^2+19395n-263790)p^{10} \\
&+48(22n^3-263n^2+24382n-265501)p^{11} \\
&-8(436n^3-1819n^2+139409n-1320164)p^{12} \\
&+144(53n^3-208n^2+5721n-49048)p^{13} \\
&-48(240n^3-1285n^2+11191n-79021)p^{14} \\
&+4(3030n^3-21073n^2+94395n-427394)p^{15} \\
&-24(366n^3-3035n^2+11013n-29366)p^{16} \\
&+12(354n^3-3268n^2+11509n-21701)p^{17} \\
&-8(163n^3-1588n^2+5591n-8906)p^{18}+12(20n^3-199n^2+699n-1030)p^{19} \\
&-24(n^3-10n^2+35n-50)p^{20}+(n^3-10n^2+35n-50)p^{21}\Big] \\
&+O(p^7), \qquad \text{for } n\geqslant 5.
\end{aligned}
$$

The plots of the previous functions for $n = 7$ are given on the Figure 5. We can see that the function $f_{4,1}(n,p)$ is the best one, it gives the smallest probability of undetected errors. But the function $f_{4,2}(n,p)$ is very closed to the $f_{4,1}(n,p)$. Their plots almost overlap each other. Using functions

$f_{4,i}(n,p)$ for $i = 1,\ldots,7$ we can classify remaining 160 quasigroups in 7 sets.

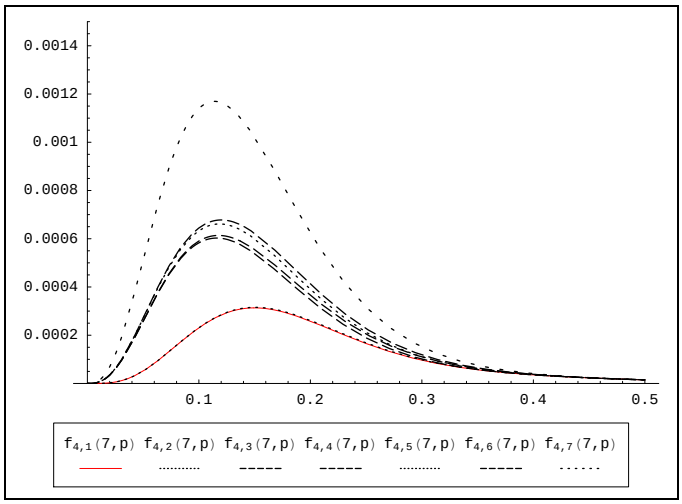

Figure 5: Seven different functions of probability of undetected errors

Each quasigroup is presented by a number according to lexicographic ordering of the set of quasigroups of order 4. Namely, each quasigroup is presented as a string of 16 letters that is a concatenation of the rows of the corresponding Latin square. Then lexicographic ordering of that strings is applied, assuming that the letters are already ordered. The obtained sets of quasigroups are ordered such that the quasigroups from the first set give the smallest, and the quasigroups from the last set give the biggest probability of undetected errors.

Set 1: 46, 92, 111, 127, 160, 213, 222, 274, 303, 355, 364, 417, 450, 466, 485, 531
Set 2: 43, 93, 101, 133, 157, 196, 235, 275, 302, 342, 381, 420, 444, 476, 484, 534
Set 3: 40, 80, 116, 138, 166, 206, 228, 269, 308, 349, 371, 411, 439, 461, 497, 537
Set 4: 14, 21, 37, 54, 71, 77, 100, 132, 163, 179, 192, 197, 234, 243, 253, 272, 305, 324, 334, 343, 380, 385, 398, 414, 445, 477, 500, 506, 523, 540, 556, 563
Set 5: 27, 83, 113, 139, 146, 203, 229, 285, 292, 348, 374, 431, 438, 464, 494, 550
Set 6: 4, 24, 26, 60, 70, 82, 110, 126, 147, 169, 182, 212, 223, 252, 262, 284, 293, 315, 325, 354, 365, 395, 408, 430, 451, 467, 495, 507, 517, 551, 553, 573

Set 7 can be presented as union of two subsets:

Subset $7'$: 1, 11, 51, 57, 172, 189, 246, 259, 318, 331, 388, 405, 520, 526, 566, 576
Subset $7''$: 7, 9, 49, 63, 174, 185, 242, 263, 314, 335, 392, 403, 514, 528, 568, 570

Repeat that all of these 160 quasigroups are fractal. The sets 1-6 contain

only linear fractal quasigroups. The set 7 contains two subsets such that the subset $7'$ contains linear fractal quasigroups too, but the subset $7''$ contains 16 nonlinear fractal quasigroups with nonlinear part $x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4$ (see [2]). Also, one can check that there is not quasigroup in Set 1 which is a group.

7. Conclusion

In this paper we compare two special cases of these codes: the first one with the binary set $A = \{0, 1\}$ and $k = 4$ and the second one with the set $A = \{0, 1, 2, 3\}$ and $k = 2$. In the both codes, each control bit includes 4 bits from the input message and the rates of the both codes are the same, so the comparing of two codes are reasonable. From this comparing we can conclude that the obtained results are much better when we use quasigroups of order 4. Also, in this paper we give a classification of quasigroups of order 4 according to goodness for proposed codes. Our next step is to develop some other codes based on quasigroups of order 4 or 2^k for $k \geqslant 3$, which give smaller probability of undetected errors.

Acknowledgment. We are particularly grateful to Professor Smile Markovski for the valuable ideas and suggestions while working of this paper.

References

[1] **V. Dimitrova, S. Markovski**, *Classification of quasigroups by image patterns*, Proc. Fifth International Confer. Informatics and Information Technology, Bitola, Republic of Macedonia (2007), 152 – 160.

[2] **D. Gligoroski, V. Dimitrova, S. Markovski**, *Quasigroups as Boolean functons, their equation systems and Gröbner bases*, short-note for RISC Book Series, Springer, "Groebner, Coding, and Cryptography", Ed. T.Mora, L.Perret, S.Sakata, M.Sala, and C.Traverso (2009), 415-420.

[3] **N. Ilievska, V. Bakeva**, *A Model of error-detecting codes based on quasigroups of order 4*, Proc. Sixth International Confer. Informatics and Information Technology, Bitola, Republic of Macedonia (2008), 7 – 11.

[4] **S. Markovski, V. Bakeva**, *On Error-detecting codes based on quasigroup operation*, Proc. Fourth International Confer. Informatics and Information Technology, Bitola, Republic of Macedonia (2003), 400 – 405.

[5] **S. Markovski, V. Bakeva**, *Error-detecting codes with cyclically defined redundancy*, Proc. Third Congress of Math. of Macedonia (2005), 485 – 492.

Received September 2, 2009

Institute of Informatics, Faculty of Natural Sciences and Mathematics, P.O.Box 162, Skopje, Republic of Macedonia

E-mail: {verica,natasha}@ii.edu.mk