Quasigroups and Related Systems **22** (2014), 223 – 246

Proving the probability of undetected errors for an error-detecting code based on quasigroups

Nataša Ilievska

Abstract. In one previous paper, we proposed a new model of error-detecting codes based on quasigroups on the following way. Each input block $a_1a_2\dots a_n$ is extended to a block $a_1a_2\dots a_nb_1b_2\dots b_n$ where $b_i = a_i * a_{r_{i+1}} * a_{r_{i+2}} * a_{r_{i+k-1}}$, $i \in \{1,2,\dots,n\}$, $*$ is a quasigroup operation and $r_j = \begin{cases} j, & j \leqslant n \\ j \mod n, & j > n \end{cases}$. We have already derived approximate formula for the probability of undetected errors when quasigroups of order 4 are used for coding and $k = 2$. In this paper, we derive approximate formula for the probability of undetected errors when also quasigroups of order 4 are used for coding, but $k = 3$. We find the optimal block length such that the probability of undetected errors is smaller than some previously given value ε and give classification of quasigroups of order 4 according to goodness for the code when $k = 3$. Also, we compare these two considered codes and conclude that the best set of quasigroups for coding for both codes contains only linear fractal quasigroups and the code with $k = 3$ gives much smaller probability of undetected errors. At the end, we compare the code considered in this paper with well-known error-detecting codes: CRC, Hamming and Reed-Muller.

1. Introduction

Messages can be corrupted due to two main reasons:

1) human factor
2) noises in the communication channels (or storage failure when message is stored in a memory).

The first type of errors occurs when a human incorrectly enters the message. In [5] and [21] are given the most frequent errors due to human factor. Since, there are only a few types of errors that are more frequent, this type of errors can be detected by adding one check digit on the message (check character system). On the other side, second type of errors appears due to noises in the channel during the transmission of the message (under the influence of weather conditions, hardware failure and etc.). This type of errors is more general, i.e. there are more possibilities for a message to be incorrectly transmitted. For this reason, more

2010 Mathematics Subject Classification: 68P30
Keywords: error-detecting codes, quasigroup, probability of undetected errors, noisy channel, binary symmetric channel

redundant characters should be added on the message in order to detect second type of errors.

Quasigroups are nice algebraic structures that can be used in order to detect errors in messages. There are several defined and well investigated check character systems based on quasigroups ([9] – [6], [17] – [20]). On the other side, there are not much error-detecting codes based on quasigroups intended for errors of the second type. There are some code designs based on quasigroups of order 2 ([15], [16]) and a general model based on quasigroups of arbitrary order ([4]). The model defined in [4] adds redundant characters as much as the message length. In this paper we will continue to analyze the model by examining other special case.

2. A model of error-detecting code

Binary symmetric channel is a channel, in which inputs and outputs are 0 and 1 (Figure 1). There are noises in the channel, because of which 0 can be transmitted in to 1 and vice versa with probability p$<1/2$. Because of these, the output message may not be same as the input one. So, we need a mechanism to discover is the correct message received. For this reason, on the input message we concatenate characters, defined by the code, which will help us to discover if the message is correctly transmitted or not.

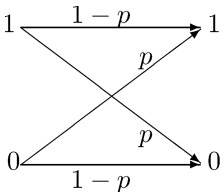

Figure 1: Binary symmetric channel

In [4] we have defined a model of error-detecting code with rate 1/2 in the following way. Let A be an arbitrary finite set called alphabet and $(A, *)$ be a given quasigroup. First, the input message

$$a_1a_2\dots a_na_{n+1}a_{n+2}\dots a_{2n}a_{2n+1}\dots, \quad (a_i \in A,\ i = 1, 2, \dots)$$

is divided in to blocks with length n:

$$a_1a_2\dots a_n,\ \ a_{n+1}a_{n+2}\dots a_{2n}, \dots$$

and each block $a_1a_2\dots a_n$ is coded separately, i.e. is extended to a block $a_1a_2\dots a_nb_1b_2\dots b_n$ where

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

where $k \leqslant n$.

After that, each character from the extended block $a_1a_2 \dots a_nb_1b_2 \dots b_n$ is presented in 2-base system and obtained binary block is transmitted through the binary symmetric channel with probability of bit error p $(0 < p < 0.5)$.

Since there are 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, $i \in \{1, 2, \dots, n\}$. If a_i is correctly transmitted than $a'_i = a_i$. Otherwise, a'_i will not be equal to a_i. The same holds for b_i and b'_i. So, the output message is $a'_1a'_2 \dots a'_nb'_1b'_2 \dots b'_n$. To check if there are any errors in transmission, the receiver of the message checks if

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

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 of the characters in that equality are not correctly transmitted. In that case, incorrect transmission (errors in transmission) will not be detected. Clearly, it is good the probability of undetected errors to be as small as posible.

In [4] is considered the case when $A = \{0, 1, 2, 3\}$ and $k = 2$. Now, in this paper we consider the case when also $A = \{0, 1, 2, 3\}$, but $k = 3$. After calculating the approximate formula for the probability of undetected errors and determining the best class of quasigroups for this code, we will compere it with the code over the set $A = \{0, 1, 2, 3\}$ and $k = 2$.

3. The probability of undetected errors for the error-detecting code based on quasigroups of order 4 and k=3

Let consider the set $A = \{0, 1, 2, 3\}$ and let $*$ be an arbitrary quasigroup operation on A. According to (1), 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

$$\begin{array}{lcl} b_1 & = & a_1 * a_2 * a_3 \\ b_2 & = & a_2 * a_3 * a_4 \\ \dots & \dots & \dots\dots\dots\dots\dots\dots \\ b_{n-2} & = & a_{n-2} * a_{n-1} * a_n \\ b_{n-1} & = & a_{n-1} * a_n * a_1 \\ b_n & = & a_n * a_1 * a_2 \end{array} \tag{2}$$

The extended message is transmitted through the binary symmetric channel. We want to calculate the probability that there will be errors which will not be de-

tected. There are 576 quasigroups of order 4. 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 probability is independent from the distribution of the input message. After filtering, from the 576 quasigroups of order 4, only 160 quasigroups remained. All of them are fractal quasigroups ([10]). For the filtered 160 quasigroups, we derived a formula for calculating the probability function of undetected errors. It is given by the next theorem. But, first we need the following definition.

Definition 1. *Distance* between the characters a_i and a_j in the block $a_1a_2...a_n$ is the minimum of the numbers $((i-j)\ mod\ n)$ and $((j-i)\ mod\ n)$, where $(m\ mod\ n)$ is the smallest natural number which is congruent with m modulo n.

Theorem 1. *Let $f_3(n,p)$ 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:*

$$
\begin{aligned}
f_3(3,p) &= 3v_1v_0^2 + 3r_{23}v_0 + r_{33}\\
f_3(4,p) &= 4v_1v_0^4 + 4v_2v_0^2 + 2s_{24}v_0^2 + 4r_{34}v_0 + O(p^7)\\
f_3(5,p) &= 5v_1v_0^6 + 5v_2v_0^4 + 5c_1v_0^3 + 5v_3v_0^2 + 5s_{35}v_0^2 + O(p^7)\\
f_3(6,p) &= 6v_1v_0^8 + 6v_2v_0^6 + 6c_1v_0^5 + 3v_1^2v_0^4 + 6v_3v_0^4 + 6c_2v_0^3 + 6c_2'v_0^3\\
&\quad +2s_{36}v_0^3 + O(p^7)\\
f_3(7,p) &= 7v_1v_0^{10} + 7v_2v_0^8 + 7c_1v_0^7 + 7v_1^2v_0^6 + 7v_3v_0^6 + 7c_2v_0^5 + 7c_2'v_0^5 + 7v_2v_1v_0^4\\
&\quad +7c_3v_0^4 + O(p^7)\\
f_3(8,p) &= 8v_1v_0^{12} + 8v_2v_0^{10} + 8c_1v_0^9 + 12v_1^2v_0^8 + 8v_3v_0^8 + 8c_2v_0^7 + 8c_2'v_0^7\\
&\quad +16v_2v_1v_0^6 + 8c_3v_0^6 + 8c_1v_1v_0^5 + O(p^7)\\
f_3(n,p) &= nv_1v_0^{2n-4} + nv_2v_0^{2n-6} + nc_1v_0^{2n-7} + \frac{n(n-5)}{2}v_1^2v_0^{2n-8} + nv_3v_0^{2n-8}\\
&\quad +nc_2v_0^{2n-9} + nc_2'v_0^{2n-9} + n(n-6)v_2v_1v_0^{2n-10} + nc_3v_0^{2n-10}\\
&\quad +n(n-7)c_1v_1v_0^{2n-11} + \frac{n(n^2-15n+56)}{6}v_1^3v_0^{2n-12} + O(p^7),\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \textit{for } n \geqslant 9.
\end{aligned}
$$

In the formulas, we use the following notations:
v_k - the probability of undetected errors when exactly k consecutive characters of the initial message $a_1a_2\dots a_n$ are incorrectly transmitted (the characters $a_i, a_{i+1}, \dots,$
a_{i+k-1} are incorrectly transmitted, but a_{i-2}, a_{i-1}, a_{i+k} and a_{i+k+1} are correctly transmitted), $k = 1, 2, 3$;
v_0 - the probability of correct transmission of a character;
c_1 - the probability of undetected errors when exactly the two characters: a_i and a_{i+2} of the initial message $a_1a_2\dots a_n$ are incorrectly transmitted
c_2 - the probability of undetected errors when exactly the three characters: a_i, a_{i+1} and a_{i+3} of the initial message $a_1a_2\dots a_n$ are incorrectly transmitted

c_2' - the probability of undetected errors when exactly the three characters: a_i, a_{i+2} and a_{i+3} of the initial message $a_1a_2 \dots a_n$ are incorrectly transmitted
c_3 - the probability of undetected errors when exactly the three characters: a_i, a_{i+2} and a_{i+4} of the initial message $a_1a_2 \dots a_n$ are incorrectly transmitted
r_{ij} - the probability of undetected errors in a block with length j if exactly i consecutive characters are incorrectly transmitted, $i = 2, 3, j = 3, 4$;
s_{24} - the probability of undetected errors in a block with length 4 - $a_1a_2a_3a_4$ when exactly the two nonconsecutive characters - a_i and a_{i+2} are incorrectly transmitted;
s_{35} - the probability of undetected errors in a block with length 5 - $a_1a_2a_3a_4a_5$ when exactly the three characters - a_i, a_{i+1} and a_{i+3} are incorrectly transmitted;
s_{36} - the probability of undetected errors in a block with length 6 - $a_1a_2a_3a_4a_5a_6$ when exactly the three characters - a_i, a_{i+2} and a_{i+4} are incorrectly transmitted.
All operations on the indexes are per modulo n, but for shorter record it is not denoted in the formulas.

Proof. Since each character of the alphabet $A = \{0, 1, 2, 3\}$ can be presented by two bits, it is clear that $v_0 = (1-p)^2$. Let denote the following random events:
A: errors occur in not more than 3 characters of the initial message $a_1a_2...a_n$ and errors are not detected;
A_k: errors occur in exactly k characters of the initial message and errors are not detected, k=1,2,3.
Then we have that

$$A = A_1 + A_2 + A_3 \tag{3}$$

Let calculate $P(A_1)$. The initial message has n characters and each of them can be incorrectly transmitted. There are n choices for choosing a character a_i which is incorrectly transmitted. The error will not be detected if the characters b_{i-2}, b_{i-1} and b_i are transmitted such that the equalities $b'_{i-2} = a'_{i-2} * a'_{i-1} * a'_i$, $b'_{i-1} = a'_{i-1} * a'_i * a'_{i+1}$ and $b'_i = a'_i * a'_{i+1} * a'_{i+2}$ are satisfied. The rest $2n-4$ characters are correctly transmitted, so

$$P(A_1) = nv_1v_0^{2n-4}, \text{ for } n \geqslant 3 \tag{4}$$

For calculating the probability $P(A_2)$, we denote the random events:
B_1: two consecutive characters a_i and a_{i+1} of the initial message $a_1a_2...a_n$ are incorrectly transmitted and the errors are not detected;
B_2: two characters on distance two, i.e. characters a_i and a_{i+2} of the initial message $a_1a_2...a_n$ are incorrectly transmitted and the errors are not detected;
B_3: two characters on distance greater than two of the initial message $a_1a_2...a_n$ are incorrectly transmitted and the errors are not detected;
Then

$$A_2 = B_1 + B_2 + B_3 \tag{5}$$

There are n choices for two consecutive characters a_i and a_{i+1} which are incorrectly transmitted. The error will not be detected if the characters b_{i-2}, b_{i-1}, b_i and b_{i+1} are transmitted such that the equalities $b'_{i-2} = a'_{i-2} * a'_{i-1} * a'_i$, $b'_{i-1} = a'_{i-1} * a'_i * a'_{i+1}$, $b'_i = a'_i * a'_{i+1} * a'_{i+2}$ and $b'_{i+1} = a'_{i+1} * a'_{i+2} * a'_{i+3}$ are satisfied. The rest $2n-6$ characters are correctly transmitted, so we have that

$$P(B_1) = \begin{cases} nv_2v_0^{2n-6}, & n \geqslant 4 \\ 3r_{23}v_0, & n = 3 \end{cases} \tag{6}$$

There are also n choices for two characters on distance two, a_i and a_{i+2} which are incorrectly transmitted. The error will not be detected if the characters b_{i-2}, b_{i-1}, b_i, b_{i+1} and b_{i+2} are transmitted such that the equalities $b'_{i-2} = a'_{i-2} * a'_{i-1} * a'_i$, $b'_{i-1} = a'_{i-1} * a'_i * a'_{i+1}$, $b'_i = a'_i * a'_{i+1} * a'_{i+2}$, $b'_{i+1} = a'_{i+1} * a'_{i+2} * a'_{i+3}$ and $b'_{i+2} = a'_{i+2} * a'_{i+3} * a'_{i+4}$ are satisfied. The rest $2n-7$ characters are correctly transmitted, so we have that

$$P(B_2) = \begin{cases} nc_1v_0^{2n-7}, & n \geqslant 5 \\ 2s_{24}v_0^2, & n = 4 \end{cases} \tag{7}$$

The number of two characters on distance greater than two is $\frac{C_n^1 \cdot C_{n-5}^1}{2} = \frac{n(n-5)}{2}$, for $n \geqslant 6$. If a_q and a_w are the two characters on distance greater than two that are incorrectly transmitted and we denote this two random events:
Q: a_q is incorrectly transmitted and error is not detected;
W: a_w is incorrectly transmitted and error is not detected;
than, since Q and W are independent events, the probability of undetected error in this two characters is v_1^2. For the error to remain undetected, the redundant characters b_{q-2}, b_{q-1}, b_q, b_{w-2}, b_{w-1} and b_w must be transferred such that corresponding equations are satisfied. The rest $2n-8$ characters are correctly transmitted. Hence,

$$P(B_3) = \frac{n(n-5)}{2} v_1^2 v_0^{2n-8}, \text{ for } n \geqslant 6 \tag{8}$$

By replacing of (6), (7) and (8) in (5), we obtain the probability of A_2. For calculating the probability $P(A_3)$, we introduce the following random events:
C_1: three consecutive characters a_i, a_{i+1} and a_{i+2} of the initial message $a_1a_2...a_n$ are incorrectly transmitted and the errors are not detected;
C_2: three characters, such that the distance between first and second character is one, and the distance between second and third character is two, i.e. a_i, a_{i+1} and a_{i+3} of the initial message are incorrectly transmitted and the errors are not detected;
C_2': three characters, such that the distance between first and second character is two, and the distance between second and third character is one, i.e. a_i, a_{i+2} and a_{i+3} of the initial message are incorrectly transmitted and the errors are not detected;

C_3: two consecutive characters and one on distance greater than two from the both consecutive characters of the initial message are incorrectly transmitted and the errors are not detected;
C_4: three characters, such that the distance between first and second character is two, and the distance between second and third character is also two, i.e. a_i, a_{i+2} and a_{i+4} of the initial message are incorrectly transmitted and the errors are not detected;
C_5: two characters, which are on distance two, and one character on distance greater than two from the both of them of the initial message are incorrectly transmitted and the errors are not detected;
C_6: three characters such that each two of them are on distance greater than two of the initial message are incorrectly transmitted and the errors are not detected;
These six events cover all possible choices of three characters that can be incorrectly transferred. Therefore, since events are disjoint,

$$A_3 = C_1 + C_2 + C_2' + C_3 + C_4 + C_5 + C_6 \tag{9}$$

As previously, we find that:

$$P(C_1) = \begin{cases} n \cdot v_3 \cdot v_0^{2n-8}, & n \geqslant 5 \\ 4r_{34}v_0, & n = 4 \\ r_{33}, & n = 3 \end{cases} \tag{10}$$

$$P(C_2) = \begin{cases} n \cdot c_2 \cdot v_0^{2n-9}, & n \geqslant 6 \\ 5s_{35}v_0^2, & n = 5 \end{cases} \tag{11}$$

$$P(C_2') = n \cdot c_2' \cdot v_0^{2n-9}, \text{ for } n \geqslant 6 \tag{12}$$

For $n = 5$ event C_2' coincide with the event C_2, due to which it does not appear in the final formula.

$$P(C_3) = n(n-6) \cdot v_2 \cdot v_1 \cdot v_0^{2n-10}, \text{ for } n \geqslant 7 \tag{13}$$

$$P(C_4) = \begin{cases} n \cdot c_3 \cdot v_0^{2n-10}, & n \geqslant 7 \\ 2s_{36}v_0^3, & n = 6 \end{cases} \tag{14}$$

$$P(C_5) = n(n-7) \cdot c_1 \cdot v_1 \cdot v_0^{2n-11}, \text{ for } n \geqslant 8 \tag{15}$$

$$\begin{aligned} P(C_6) &= (C_n^3 - 4 * C_n^1 - C_n^1 C_{n-6}^1 - C_n^1 C_{n-7}^1) \cdot v_1^3 \cdot v_0^{2n-12} \\ &= (\tfrac{n(n^2-15n+56)}{6}) v_1^3 \cdot v_0^{2n-12}, \text{ for } n \geqslant 9 \end{aligned} \tag{16}$$

Now, we obtain the formula for $f_3(n,p)$ by simply using (3) - (16) and a fact that the probability of undetected errors if more than 3 characters are incorrectly transmitted is of order $O(p^7)$.

In the most of the previous formulas, some special cases are separated. The reason is that the incorrectly transmitted characters of the initial message act on different redundant characters and thus the corresponding probabilities of undetected errors are different. For example, let consider the case when two consecutive

characters, say a_1 and a_2, of the initial message are incorrectly transmitted. If the initial message has length greater than 3, than redundant character b_2 is affected only by character a_2. But, if the initial message has length exactly 3, than b_2 is affected not only by a_2, but also by a_1. For this reason the probability of undetected errors if exactly two consecutive characters a_i and a_{i+1} of the initial message $a_2a_2\dots a_n$ are incorrectly transmitted has different values when $n=3$ and $n>3$. Because of this, in the formula for $P(B_1)$, the case for $n=3$ is given as a special case and we introduce notation r_{23} instead of v_2 (since r_{23} is not equal to v_2 for $n=3$). For the same reasons are introduced new notations in all other special cases. □

Note that the formula for the probability of undetected errors in Theorem 1 is valid for quasigroups of arbitrary order for which the probability of undetected errors does not depend on the distribution of the characters in the input message.

For each qausigroup, probabilities $v_k, c_1, c_2, c_2', c_3, r_{ij}, s_{24}, s_{35}, s_{36}$ can be easily calculated using some combinatorics and the formula for total probability. Replacing them in Theorem 1, we can obtain functions $f_3(n,p)$ for all 160 remained fractal quasigroups. After calculating functions $f_3(n,p)$ for all 160 quasigroups, we concluded that these 160 quasigroups do not define 160 different functions for the probability of undetected errors, but only 17. Using these functions, we give a classification of the quasigroups of order 4 according to goodness for our codes. The classification is given in the next section. The quasigroups which give the smallest probability of undetected errors are the best for code design.

Let $f_{3,i}(n,p)$ be the probability of undetected errors for the quasigroups in the i-th set in the classification. For shorter record, we give these formulas without the remainder $O(p^7)$, which practically represent the probability that at most 3 characters of the input message are incorrectly transmitted and the errors are not detected. To obtain exact probability of undetected errors, one should add $O(p^7)$ to these probabilities. Since for small values of p, $O(p^7)$ is inconsiderably small, in the future we will work with $f_{3,i}(n,p)$ without the remainder $O(p^7)$. The probabilities of undetected errors are determined by the following formulas:

$$
\begin{aligned}
f_{3,1}(3,p) &= p^3(1-p)^3(p^6-9p^5+36p^4-52p^3+42p^2-18p+4)\\
f_{3,1}(4,p) &= 2p^4(1-p)^4(-p^8+4p^7+12p^6-32p^5+22p^4+2p^3-6p^2+1)\\
f_{3,1}(5,p) &= 5p^5(1-p)^6(-p^9+2p^8-6p^7+56p^6-162p^5+236p^4-201p^3+103p^2-30p+4)\\
f_{3,1}(6,p) &= p^5(1-p)^9(11p^{10}-21p^9+15p^8-201p^7+894p^6-1752p^5+1968p^4-1380p^3\\
&\quad +606p^2-154p+18)\\
f_{3,1}(7,p) &= 7p^5(1-p)^{13}(3p^{10}-5p^9-3p^8-23p^7+157p^6-319p^5+354p^4-242p^3+104p^2\\
&\quad -26p+3)\\
f_{3,1}(8,p) &= 4p^5(1-p)^{16}(-9p^{11}+24p^{10}+2p^9-4p^8-297p^7+918p^6-1338p^5+1192p^4\\
&\quad -692p^3+260p^2-58p+6)\\
f_{3,1}(n,p) &= \frac{1}{6}np^5(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[18-210p+1146p^2-3810p^3+8508p^4+6(4n-2239)p^5-6(25n-2593)p^6\\
&\quad +3(139n-4583)p^7-(612n-9420)p^8+(471n-4629)p^9+8(n^2-33n+206)p^{10}\\
&\quad -3(4n^2-47n+175)p^{11}+6(n^2-8n+21)p^{12}-(n^2-6n+11)p^{13}\Big],\quad \text{for } n\geqslant 9.
\end{aligned}
\tag{17}
$$

$$
\begin{aligned}
f_{3,2}(3,p) &= p^4(1-p)^3(p^5-9p^4+36p^3-20p^2-6p-6)\\
f_{3,2}(4,p) &= 2p^5(1-p)^5(p^6-3p^5+41p^4-87p^3+93p^2-51p+12)\\
f_{3,2}(5,p) &= 5p^5(1-p)^7(p^8-p^7+13p^6-43p^5+77p^4-81p^3+51p^2-18p+3)\\
f_{3,2}(6,p) &= p^5(1-p)^9(11p^{10}-21p^9+39p^8-305p^7+1116p^6-2052p^5+2210p^4-1488p^3\\
&\quad +630p^2-156p+18)\\
f_{3,2}(7,p) &= 7p^5(1-p)^{13}(3p^{10}-5p^9-3p^8-31p^7+181p^6-349p^5+374p^4-249p^3+105p^2\\
&\quad -26p+3)\\
f_{3,2}(8,p) &= 4p^5(1-p)^{15}(9p^{12}-33p^{11}+14p^{10}+14p^9+355p^8-1383p^7+2464p^6-2684p^5\\
&\quad +1954p^4-970p^3+320p^2-64p+6)\\
f_{3,2}(n,p) &= \frac{1}{6}np^5(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[18-210p+1152p^2-3870p^3+8772p^4+6(4n-2351)p^5-6(25n-2774)p^6\\
&\qquad +3(143n-4991)p^7-(678n-10638)p^8+(597n-5799)p^9+8(n^2-45n+296)p^{10}\\
&\qquad -3(4n^2-55n+231)p^{11}+6(n^2-8n+21)p^{12}-(n^2-6n+11)p^{13}\Big],\quad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,3}(3,p) &= p^3(-p^9+12p^8-18p^7-20p^6+93p^5-120p^4+75p^3-21p^2+1)\\
f_{3,3}(4,p) &= 2p^4(1-p)^5(p^7-19p^6+61p^5-83p^4+58p^3-16p^2-2p+2)\\
f_{3,3}(5,p) &= 5p^5(1-p)^8(-p^7+16p^6-45p^5+82p^4-87p^3+58p^2-22p+4)\\
f_{3,3}(6,p) &= p^5(1-p)^{10}(-11p^9+154p^8-461p^7+784p^6-1040p^5+1138p^4-888p^3+450p^2\\
&\quad -132p+18)\\
f_{3,3}(7,p) &= 7p^5(1-p)^{12}(-3p^{11}+40p^{10}-146p^9+276p^8-376p^7+478p^6-553p^5+492p^4\\
&\quad -302p^3+120p^2-28p+3)\\
f_{3,3}(8,p) &= 4p^5(1-p)^{15}(9p^{12}-113p^{11}+430p^{10}-862p^9+1247p^8-1633p^7+2024p^6\\
&\quad -2082p^5+1588p^4-844p^3+296p^2-62p+6)\\
f_{3,3}(n,p) &= \frac{1}{6}np^5(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[18-204p+1074p^2-3420p^3+7296p^4+6(4n-1867)p^5-6(23n-2237)p^6\\
&\qquad +3(113n-4561)p^7-36(11n-328)p^8+9(13n-807)p^9+4(2n^2+27n+625)p^{10}\\
&\qquad -3(4n^2+25n+87)p^{11}+6(n^2-3)p^{12}-(n^2-6n+11)p^{13}\Big],\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,4}(3,p) &= p^3(-p^9+12p^8-18p^7-20p^6+93p^5-120p^4+75p^3-21p^2+1)\\
f_{3,4}(4,p) &= 2p^3(1-p)^4(-p^9+20p^8-76p^7+164p^6-224p^5+212p^4-141p^3+62p^2-16p+2)\\
f_{3,4}(5,p) &= 5p^5(1-p)^7(p^8-17p^7+61p^6-103p^5+109p^4-83p^3+47p^2-17p+3)\\
f_{3,4}(6,p) &= p^5(1-p)^9(11p^{10}-165p^9+663p^8-1397p^7+2076p^6-2388p^5+2108p^4-1350p^3\\
&\quad +582p^2-150p+18)\\
f_{3,4}(7,p) &= 7p^5(1-p)^{11}(3p^{12}-43p^{11}+202p^{10}-526p^9+960p^8-1356p^7+1525p^6-1347p^5\\
&\quad +906p^4-445p^3+150p^2-31p+3)\\
f_{3,4}(8,p) &= 4p^5(1-p)^{15}(9p^{12}-113p^{11}+478p^{10}-1142p^9+1979p^8-2723p^7+3042p^6\\
&\quad -2690p^5+1812p^4-890p^3+300p^2-62p+6)\\
f_{3,4}(n,p) &= \frac{1}{6}np^5(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[18-204p+1086p^2-3570p^3+8106p^4+6(2n-2267)p^5-12(3n-1457)p^6\\
&\qquad -3(3n+5741)p^7+6(35n+2071)p^8-3(149n+1929)p^9+4(2n^2+93n+343)p^{10}\\
&\qquad -3(4n^2+41n+7)p^{11}+6(n^2-3)p^{12}-(n^2-6n+11)p^{13}\Big],\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,5}(3,p) &= p^4(63p^8-327p^7+990p^6-1540p^5+1545p^4-1032p^3+452p^2-120p+15)\\
f_{3,5}(4,p) &= 2p^4(1-p)^6(87p^6-230p^5+307p^4-240p^3+120p^2-36p+6)\\
f_{3,5}(5,p) &= 5p^4(1-p)^6(75p^{10}-394p^9+973p^8-1464p^7+1498p^6-1092p^5+574p^4-216p^3\\
&\quad +57p^2-10p+1)\\
f_{3,5}(6,p) &= p^4(1-p)^{10}(693p^{10}-2886p^9+5967p^8-7940p^7+7471p^6-5186p^5+2731p^4\\
&\quad -1088p^3+316p^2-60p+6)\\
f_{3,5}(7,p) &= 7p^4(1-p)^{12}(165p^{12}-880p^{11}+2320p^{10}-3976p^9+4894p^8-4548p^7+3286p^6\\
&\quad -1872p^5+840p^4-290p^3+73p^2-12p+1)\\
f_{3,5}(8,p) &= 4p^4(1-p)^{16}(447p^{12}-2096p^{11}+5160p^{10}-8448p^9+10108p^8-9236p^7+6614p^6\\
&\quad -3752p^5+1681p^4-580p^3+146p^2-24p+2)\\
f_{3,5}(n,p) &= \frac{1}{6}np^4(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[6-84p+588p^2-2688p^3+3(n+2979)p^4-6(5n+3807)p^5+3(59n+15327)p^6\\
&\qquad -696(n+105)p^7+(n^2+1911n+90236)p^8-6(n^2+623n+13902)p^9\\
&\qquad +3(7n^2+1727n+17900)p^{10}-4(11n^2+1239n+5032)p^{11}\\
&\qquad +3(21n^2+994n+503)p^{12}-6(9n^2+150n-281)p^{13}+9(3n^2-6n+5)p^{14}\Big],\\
&\qquad\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,6}(3,p) &= 3p^4(1-p)^2(21p^6-82p^5+145p^4-144p^3+86p^2-30p+5)\\
f_{3,6}(4,p) &= 2p^4(1-p)^6(87p^6-230p^5+315p^4-264p^3+146p^2-48p+8)\\
f_{3,6}(5,p) &= 5p^4(1-p)^8(75p^8-244p^7+402p^6-400p^5+266p^4-122p^3+39p^2-8p+1)\\
f_{3,6}(6,p) &= 3p^4(1-p)^8(231p^{12}-1424p^{11}+4152p^{10}-7616p^9+9892p^8-9628p^7+7202p^6\\
&\quad -4168p^5+1853p^4-620p^3+150p^2-24p+2)\\
f_{3,6}(7,p) &= 7p^4(1-p)^{12}(165p^{12}-880p^{11}+2336p^{10}-4024p^9+5042p^8-4828p^7+3594p^6\\
&\quad -2080p^5+926p^4-310p^3+75p^2-12p+1)\\
f_{3,6}(8,p) &= 4p^4(1-p)^{14}(447p^{14}-2990p^{13}+9855p^{12}-21064p^{11}+32714p^{10}-39160p^9\\
&\quad +37228p^8-28424p^7+17419p^6-8494p^5+3243p^4-944p^3+200p^2-28p+2)\\
f_{3,6}(n,p) &= \frac{1}{6}np^4(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[6-84p+600p^2-2832p^3+3(n+3235)p^4-6(5n+4207)p^5+3(59n+16947)p^6\\
&\qquad -24(29n+3321)p^7+(n^2+1917n+96284)p^8-6(n^2+629n+14484)p^9\\
&\qquad +3(7n^2+1757n+18210)p^{10}-4(11n^2+1269n+4942)p^{11}\\
&\qquad +3(21n^2+1018n+367)p^{12}-6(9n^2+150n-281)p^{13}+9(3n^2-6n+5)p^{14}\Big],\\
&\qquad\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,7}(3,p) &= p^4(63p^8-371p^2+990p^6-1540p^5+1545p^4-1032p^3+452p^2-120p+15)\\
f_{3,7}(4,p) &= 2p^4(1-p)^6(87p^6-230p^5+315p^4-232p^3+98p^2-24p+4)\\
f_{3,7}(5,p) &= 5p^4(1-p)^8(75p^8-244p^7+402p^6-408p^5+278p^4-128p^3+40p^2-8p+1)\\
f_{3,7}(6,p) &= 3p^4(1-p)^{10}(231p^{10}-962p^9+1997p^8-2692p^7+2591p^6-1842p^5+979p^4\\
&\quad -384p^3+108p^2-20p+2)\\
f_{3,7}(7,p) &= 7p^4(1-p)^{12}(165p^{12}-880p^{11}+2336p^{10}-4040p^9+5082p^8-4872p^7+3620p^6\\
&\quad -2088p^5+927p^4-310p^3+75p^2-12p+1)\\
f_{3,7}(8,p) &= 4p^4(1-p)^{14}(447p^{14}-2990p^{13}+9855p^{12}-21096p^{11}+32858p^{10}-39440p^9\\
&\quad +37536p^8-28632p^7+17505p^6-8514p^5+3245p^4-944p^3+200p^2-28p+2)\\
f_{3,7}(n,p) &= \frac{1}{6}np^4(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[6-84p+600p^2-2832p^3+3(n+3237)p^4-6(5n+4217)p^5+3(59n+17033)p^6\\
&\qquad -24(29n+3347)p^7+(n^2+1917n+97208)p^8-6(n^2+629n+14624)p^9\\
&\qquad +21(n^2+251n+2622)p^{10}-4(11n^2+1269n+4966)p^{11}\\
&\qquad +3(21n^2+1018n+367)p^{12}-6(9n^2+150n-281)p^{13}+9(3n^2-6n+5)p^{14}\Big],\\
&\qquad\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,8}(3,p) &= 3p^4(1-p)^2(21p^6-82p^5+145p^4-144p^3+86p^2-30p+5)\\
f_{3,8}(4,p) &= 2p^4(1-p)^4(87p^8-404p^7+850p^6-1048p^5+842p^4-460p^3+170p^2-40p\\
&\quad +5)\\
f_{3,8}(5,p) &= 5p^4(1-p)^8(75p^8-244p^7+410p^6-424p^5+292p^4-134p^3+41p^2-8p+1)\\
f_{3,8}(6,p) &= p^4(1-p)^{10}(693p^{10}-2886p^9+6111p^8-8308p^7+8099p^6-5866p^5+3143p^4\\
&\quad -1216p^3+332p^2-60p+6)\\
f_{3,8}(7,p) &= 7p^4(1-p)^{12}(165p^{12}-880p^{11}+2368p^{10}-4152p^9+5274p^8-5092p^7+3806p^6\\
&\quad -2200p^5+971p^4-320p^3+76p^2-12p+1)\\
f_{3,8}(8,p) &= 4p^4(1-p)^{16}(447p^{12}-2096p^{11}+5304p^{10}-8880p^9+10928p^8-10348p^7\\
&\quad +7658p^6-4408p^5+1943p^4-640p^3+152p^2-24p+2)\\
f_{3,8}(n,p) &= \frac{1}{6}np^4(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[6-84p+606p^2-2904p^3+3(n+3367)p^4-6(5n+4427)p^5+63(3n+853)p^6\\
&\quad -72(11n+1165)p^7+(n^2+2247n+99806)p^8-6(n^2+735n+14598)p^9\\
&\quad +21(n^2+285n+2512)p^{10}-4(11n^2+1371n+4516)p^{11}\\
&\quad +3(21n^2+1042n+263)p^{12}-6(9n^2+150n-281)p^{13}+9(3n^2-6n+5)p^{14}\Big],\\
&\qquad\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,9}(3,p) &= p^3(-p^9+12p^8-18p^7-20p^6+93p^5-120p^4+75p^3-21p^2+1)\\
f_{3,9}(4,p) &= 2p^4(1-p)^5(p^7-19p^6+61p^5-83p^4+58p^3-16p^2-2p+2)\\
f_{3,9}(5,p) &= 5p^4(1-p)^7(p^9-17p^8+61p^7-79p^6+33p^5+27p^4-42p^3+24p^2-7p+1)\\
f_{3,9}(6,p) &= p^4(1-p)^{10}(-11p^{10}+154p^9-557p^8+832p^7-536p^6-50p^5+408p^4-372p^3\\
&\quad +180p^2-48p+6)\\
f_{3,9}(7,p) &= 7p^4(1-p)^{12}(-3p^{12}+40p^{11}-178p^{10}+404p^9-520p^8+358p^7-31p^6-198p^5\\
&\quad +221p^4-130p^3+47p^2-10p+1)\\
f_{3,9}(8,p) &= 4p^4(1-p)^{15}(9p^{13}-113p^{12}+526p^{11}-1326p^{10}+2039p^9-1909p^8+860p^7\\
&\quad +308p^6-834p^5+702p^4-354p^3+114p^2-22p+2)\\
f_{3,9}(n,p) &= \frac{1}{6}np^4(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[6-72p+408p^2-1404p^3+3168p^4+12(n-392)p^5-6(15n-691)p^6\\
&\quad +36(9n-26)p^7-3(235n+889)p^8+12(86n+299)p^9-3(353n+541)p^{10}\\
&\quad +(8n^2+636n-44)p^{11}-3(4n^2+57n-73)p^{12}+6(n^2-3)p^{13}\\
&\quad -(n^2-6n+11)p^{14}\Big],\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,10}(3,p) &= p^3(1-p)^3(p^6-9p^5+36p^4-52p^3+42p^2-18p+1)\\
f_{3,10}(4,p) &= 2p^4(1-p)^5(p^7-11p^6+33p^5-41p^4+25p^3-3p^2-4p-2)\\
f_{3,10}(5,p) &= 5p^4(1-p)^7(p^9-5p^8+25p^7-24p^6-17p^5+54p^4-50p^3+25p^2-7p+1)\\
f_{3,10}(6,p) &= p^4(1-p)^9(11p^{11}-21p^{10}+183p^9-641p^8+900p^7-420p^6-385p^5+741p^4\\
&\quad -546p^3+228p^2-54p+6)\\
f_{3,10}(7,p) &= 7p^4(1-p)^{11}(3p^{13}-3p^{12}+34p^{11}-188p^{10}+432p^9-502p^8+227p^7+188p^6\\
&\quad -405p^5+344p^4-176p^3+57p^2-11p+1)\\
f_{3,10}(8,p) &= 4p^4(1-p)^{15}(9p^{13}+7p^{12}+70p^{11}-400p^{10}+879p^9-993p^8+435p^7+389p^6\\
&\quad -815p^5+689p^4-352p^3+114p^2-22p+2)\\
f_{3,10}(n,p) &= \frac{1}{6}np^4(1-p)^{4n-21}\times\\
&\quad \times\Big[6-90p+642p^2-2844p^3+3(n+2863)p^4-3(9n+6089)p^5+3(39n+8993)p^6\\
&\quad -3(105n+8279)p^7+(n^2+543n+6242)p^8-6(n^2+85n-3289)p^9\\
&\quad +3(5n^2-4n-11513)p^{10}-(17n^2-630n-30101)p^{11}\\
&\quad +3(n^2-203n-5622)p^{12}+6(2n^2+7n+1256)p^{13}-(8n^2-222n+3286)p^{14}\\
&\quad -3(n^2+17n-296)p^{15}+3(n^2-14n+19)p^{16}+(n^2-6n+11)p^{17}\Big],\quad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,11}(3,p) &= p^2(1-p)^3(p^7-9p^6+36p^5-36p^4+6p^3+18p^2-13p+3)\\
f_{3,11}(4,p) &= 2p^4(1-p)^5(p^7-3p^6-7p^5+25p^4-23p^3+13p^2-6p+2)\\
f_{3,11}(5,p) &= 5p^4(1-p)^8(-p^8-13p^6+54p^5-55p^4+20p^3+3p^2-4p+1)\\
f_{3,11}(6,p) &= p^4(1-p)^9(11p^{11}-21p^{10}+87p^9-497p^8+1248p^7-1512p^6+884p^5-78p^4\\
&\quad -234p^3+162p^2-48p+6)\\
f_{3,11}(7,p) &= 7p^4(1-p)^{12}(-3p^{12}+8p^{11}-18p^{10}+100p^9-312p^8+497p^7-425p^6+169p^5\\
&\quad +25p^4-66p^3+35p^2-9p+1)\\
f_{3,11}(8,p) &= 4p^4(1-p)^{15}(9p^{13}-33p^{12}+62p^{11}-242p^{10}+855p^9-1675p^8+1894p^7\\
&\quad -1210p^6+292p^5+182p^4-202p^3+88p^2-20p+2)\\
f_{3,11}(n,p) &= \frac{1}{6}np^4(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[6-66p+324p^2-870p^3+1152p^4+6(2n+39)p^5-6(13n+647)p^6\\
&\quad +6(37n+1256)p^7-3(111n+2681)p^8+30(9n+181)p^9-3(37n+801)p^{10}\\
&\quad +8(n^2-9n+122)p^{11}-3(4n^2-39n+151)p^{12}+6(n^2-8n+21)p^{13}\\
&\quad -(n^2-6n+11)p^{14}\Big],\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,12}(3,p) &= p^3(1-p)^3(p^6-9p^5+36p^4-52p^3+42p^2-18p+4)\\
f_{3,12}(4,p) &= 2p^3(1-p)^5(p^8-11p^7+57p^6-105p^5+103p^4-69p^3+36p^2-12p+2)\\
f_{3,12}(5,p) &= 5p^4(1-p)^8(-p^8+4p^7+3p^6-5p^5+10p^4-14p^3+12p^2-5p+1)\\
f_{3,12}(6,p) &= p^4(1-p)^9(11p^{11}-21p^{10}+63p^9-209p^8+438p^7-462p^6+137p^5+225p^4\\
&\quad -300p^3+168p^2-48p+6)\\
f_{3,12}(7,p) &= 7p^4(1-p)^{11}(3p^{13}-3p^{12}+18p^{11}-92p^{10}+252p^9-402p^8+371p^7-144p^6\\
&\quad -87p^5+164p^4-114p^3+45p^2-10p+1)\\
f_{3,12}(8,p) &= 4p^4(1-p)^{13}(9p^{15}-11p^{14}+41p^{13}-261p^{12}+943p^{11}-2057p^{10}+2890p^9\\
&\quad -2562p^8+1110p^7+410p^6-1065p^5+875p^4-428p^3+132p^2-24p+2)\\
f_{3,12}(n,p) &= \tfrac{1}{6}np^4(1-p)^{4n-21}\times\\
&\quad \times\Big[6-84p+546p^2-2148p^3+3(n+1855)p^4-9(3n+1057)p^5+3(37n+3119)p^6\\
&\quad -15(17n+19)p^7+(n^2+297n-15556)p^8-6(n^2-2n-4610)p^9\\
&\quad +3(5n^2-194n-9167)p^{10}-(17n^2-834n-18257)p^{11}\\
&\quad +3(n^2-145n-3108)p^{12}+6(2n^2-20n+785)p^{13}-(8n^2-222n+2326)p^{14}\\
&\quad -3(n^2+9n-208)p^{15}+3(n^2-14n+19)p^{16}+(n^2-6n+11)p^{17}\Big],\ \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,13}(3,p) &= p^4(63p^8-372p^7+990p^6-1540p^5+1545p^4-1032p^3+452p^2-120p+15)\\
f_{3,13}(4,p) &= 2p^4(1-p)^6(87p^6-230p^5+299p^4-232p^3+118p^2-36p+6)\\
f_{3,13}(5,p) &= 5p^4(1-p)^8(75p^8-244p^7+406p^6-428p^5+319p^4-172p^3+66p^2-16p+2)\\
f_{3,13}(6,p) &= p^4(1-p)^8(693p^{12}-4272p^{11}+12624p^{10}-23864p^9+32414p^8-33456p^7\\
&\quad +26952p^6-17088p^5+8448p^4-3160p^3+844p^2-144p+12)\\
f_{3,13}(7,p) &= 7p^4(1-p)^{12}(165p^{12}-880p^{11}+2424p^{10}-4352p^9+5680p^8-5680p^7+4472p^6\\
&\quad -2800p^5+1382p^4-520p^3+140p^2-24p+2)\\
f_{3,13}(8,p) &= 4p^4(1-p)^{12}(447p^{16}-3884p^{15}+16650p^{14}-46164p^{13}+92333p^{12}-141352p^{11}\\
&\quad +171868p^{10}-169984p^9+138720p^8-93952p^7+52626p^6-24112p^5+8804p^4\\
&\quad -2464p^3+496p^2-64p+4)\\
f_{3,13}(n,p) &= \tfrac{1}{6}np^4(1-p)^{2(2n-12)}\times\\
&\quad \times\Big[12-240p+2328p^2-14544p^3+12(n+5466)p^4-192(n+1182)p^5+\\
&\quad 72(21n+8677)p^6-48(161n+29145)p^7+4(2n^2+7092n+644923)p^8\\
&\quad -48(2n^2+1632n+82023)p^9+12(44n^2+13889n+414219)p^{10}\\
&\quad -8(220n^2+34623n+645521)p^{11}+(3972n^2+362433n+4369143)p^{12}\\
&\quad -24(268n^2+15603n+123157)p^{13}+12(644n^2+25363n+129025)p^{14}\\
&\quad -24(292n^2+7999n+24589)p^{15}+6(801n^2+15223n+23388)p^{16}\\
&\quad -8(307n^2+3873n+1064)p^{17}+12(75n^2+550n-483)p^{18}\\
&\quad -24(9n^2+24n-59)p^{19}+9(3n^2-6n+5)p^{20}\Big],\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,14}(3,p) &= p^2(63p^{10}-372p^9+1038p^8-1780p^7+2085p^6-1752p^5+1076p^4-480p^3\\
&\quad +150p^2-30p+3)\\
f_{3,14}(4,p) &= 2p^4(1-p)^6(87p^6-230p^5+303p^4-244p^3+131p^2-42p+7)\\
f_{3,14}(5,p) &= 2p^4(1-p)^8(75p^8-244p^7+410p^6-448p^5+360p^4-216p^3+92p^2-24p+3)\\
f_{3,14}(6,p) &= p^4(1-p)^8(693p^{12}-4272p^{11}+12576p^{10}-23560p^9+31810p^8-32976p^7\\
&\quad +26928p^6-17304p^5+8595p^4-3200p^3+848p^2-144p+12)\\
f_{3,14}(7,p) &= 7p^4(1-p)^{12}(165p^{12}-880p^{11}+2368p^{10}-4200p^9+5490p^8-5576p^7+4492p^6\\
&\quad -2864p^5+1420p^4-530p^3+141p^2-24p+2)\\
f_{3,14}(8,p) &= 4p^4(1-p)^{16}(447p^{12}-2096p^{11}+5304p^{10}-9024p^9+11464p^8-11416p^7\\
&\quad +9084p^6-5752p^5+2843p^4-1060p^3+282p^2-48p+4)\\
f_{3,14}(n,p) &= \tfrac{1}{6}np^4(1-p)^{2(2n-9)}\times\\
&\quad \times\Big[12-168p+1146p^2-5016p^3+3(3n+5221)p^4-18(5n+2043)p^5\\
&\quad +(453n+66669)p^6-24(61n+3929)p^7+(n^2+3321n+103508)p^8\\
&\quad -6(n^2+913n+14316)p^9+3(7n^2+2195n+16808)p^{10}\\
&\quad -4(11n^2+1407n+4336)p^{11}+3(21n^2+1042n+263)p^{12}\\
&\quad -6(9n^2+150n-281)p^{13}+9(3n^2-6n+5)p^{14}\Big],\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,15}(3,p) &= p^2(-p^{10}-84p^9+462p^8-1140p^7+1665p^6-1590p^5+1042p^4-447p^3\\
&\quad +150p^2-30p+3)\\
f_{3,15}(4,p) &= 2p^4(1-p)^6(-p^6-22p^5+85p^4-122p^3+96p^2-38p+7)\\
f_{3,15}(5,p) &= 5p^4(1-p)^8(-p^8+4p^7+43p^6-141p^5+204p^4-166p^3+82p^2-23p+3)\\
f_{3,15}(6,p) &= p^4(1-p)^8(-11p^{12}+128p^{11}+180p^{10}-2576p^9+7811p^8-13248p^7\\
&\quad +14857p^6-11716p^5+6651p^4-2714p^3+770p^2-138p+12)\\
f_{3,15}(7,p) &= 7p^4(1-p)^{11}(3p^{13}-35p^{12}+2p^{11}+500p^{10}-1836p^9+3616p^8-4722p^7\\
&\quad +4405p^6-3028p^5+1545p^4-577p^3+151p^2-25p+2)\\
f_{3,15}(8,p) &= 4p^4(1-p)^{13}(9p^{15}-107p^{14}+225p^{13}+883p^{12}-5883p^{11}+16161p^{10}\\
&\quad -28356p^9+35580p^8-33482p^7+24144p^6-13419p^5+5703p^4-1808p^3\\
&\quad +406p^2-58p+4)\\
f_{3,15}(n,p) &= \tfrac{1}{6}np^4(1-p)^{4n-21}\times\\
&\quad \times\Big[12-198p+1578p^2-8034p^3+3(3n+9701)p^4-3(35n+26353)p^5\\
&\quad +3(193n+55141)p^6-3(655n+89949)p^7+(n^2+4503n+343976)p^8\\
&\quad -6(n^2+1204n+56803)p^9+3(5n^2+2712n+86437)p^{10}\\
&\quad -(17n^2+6228n+148771)p^{11}+3(n^2+961n+21058)p^{12}\\
&\quad +6(2n^2-61n-3352)p^{13}-(8n^2+522n-5666)p^{14}-3(n^2-143n+632)p^{15}\\
&\quad +3(n^2-46n+179)p^{16}+(n^2-6n+11)p^{17}\Big],\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,16}(3,p) &= p^2(-p^{10}-84p^9+462p^8-1140p^7+1665p^6-1590p^5+1042p^4-447p^3+150p^2\\
&\quad -30p+3)\\
f_{3,16}(4,p) &= 2p^4(1-p)^6(-p^6-22p^5+81p^4-118p^3+95p^2-38p+7)\\
f_{3,16}(5,p) &= 5p^4(1-p)^6(-p^{10}+6p^9+26p^8-191p^7+487p^6-689p^5+610p^4-352p^3+131p^2\\
&\quad -29p+3)\\
f_{3,16}(6,p) &= p^4(1-p)^{10}(-11p^{10}+106p^9+331p^8-1860p^7+3654p^6-4122p^5+3047p^4\\
&\quad -1540p^3+530p^2-114p+12)\\
f_{3,16}(7,p) &= 7p^4(1-p)^{11}(3p^{13}-35p^{12}+18p^{11}+468p^{10}-1824p^9+3640p^8-4760p^7+4430p^6\\
&\quad -3036p^5+1546p^4-577p^3+151p^2-25p+2)\\
f_{3,16}(8,p) &= 4p^4(1-p)^{15}(9p^{13}-89p^{12}+78p^{11}+976p^{10}-3839p^9+7535p^8-9707p^7+8945p^6\\
&\quad -6095p^5+3095p^4-1154p^3+302p^2-50p+4)\\
f_{3,16}(n,p) &= \tfrac{1}{6}np^4(1-p)^{4n-21}\times\\
&\quad \times\Big[12-198p+1578p^2-8034p^3+3(3n+9703)p^4-3(35n+26377)p^5\\
&\quad +3(195n+55253)p^6-3(677n+90175)p^7+(n^2+4809n+343998)p^8\\
&\quad -6(n^2+1333n+56320)p^9+3(5n^2+3092n+84259)p^{10}\\
&\quad -(17n^2+7158n+141769)p^{11}+3(n^2+1057n+19826)p^{12}\\
&\quad +6(2n^2-40n-3263)p^{13}-(8n^2+642n-5930)p^{14}-3(n^2-151n+656)p^{15}\\
&\quad +3(n^2-46n+179)p^{16}+(n^2-6n+11)p^{17}\Big],\qquad \text{for } n\geqslant 9.
\end{aligned}
$$

$$
\begin{aligned}
f_{3,17}(3,p) &= p^2(63p^{10}-372p^9+1086p^8-2020p^7+2625p^6-2472p^5+1700p^4-840p^3\\
&\quad +285p^2-60p+6)\\
f_{3,17}(4,p) &= 2p^4(1-p)^8(87p^4-56p^3+84p^2-56p+14)\\
f_{3,17}(5,p) &= 5p^4(1-p)^8(75p^8-244p^7+422p^6-524p^5+507p^4-360p^3+172p^2-48p+6)\\
f_{3,17}(6,p) &= p^4(1-p)^8(693p^{12}-4272p^{11}+12864p^{10}-25256p^9+36506p^8-41232p^7\\
&\quad +37080p^6-26304p^5+14352p^4-5800p^3+1636p^2-288p+24)\\
f_{3,17}(7,p) &= 7p^4(1-p)^{12}(165p^{12}-880p^{11}+2488p^{10}-4672p^9+6528p^8-7152p^7+6264p^6\\
&\quad -43686p^5+2370p^4-960p^3+272p^2-48p+4)\\
f_{3,17}(8,p) &= 4p^4(1-p)^{12}(447p^{16}-3884p^{15}+16826p^{14}-47684p^{13}+98681p^{12}-158360p^{11}\\
&\quad +204452p^{10}-217056p^9+191468p^8-140432p^7+84936p^6-41632p^5+16088p^4\\
&\quad -4704p^3+976p^2-128p+8)\\
f_{3,17}(n,p) &= \tfrac{1}{6}np^4(1-p)^{2(4n-12)}\times\\
&\quad \times\Big[24-480p+4608p^2-28244p^3+36(n+3432)p^4-576(n+712)p^5\\
&\quad +24(181n+44525)p^6-48(427n+46523)p^7+4(2n^2+16929n+948511)p^8\\
&\quad -48(2n^2+3461n+110115)p^9+12(44n^2+26097n+505445)p^{10}\\
&\quad -8(220n^2+57891n+717095)p^{11}+(3972n^2+543921n+4449999)p^{12}\\
&\quad -24(268n^2+21251n+116269)p^{13}+12(644n^2+31747n+114193)p^{14}\\
&\quad -24(292n^2+9327n+20493)p^{15}+6(801n^2+16765n+17794)p^{16}\\
&\quad -8(307n^2+4083n+218)p^{17}+12(75n^2+562n-535)p^{18}\\
&\quad -24(9n^2+24n-59)p^{19}+9(3n^2-6n+5)p^{20}\Big], \qquad \text{for } n\geqslant 9.
\end{aligned}
$$

3.1. Controlling the probability of undetected errors

The graphics of the above functions are given in Figure 2. Some functions are so close, that they practically overlapping.

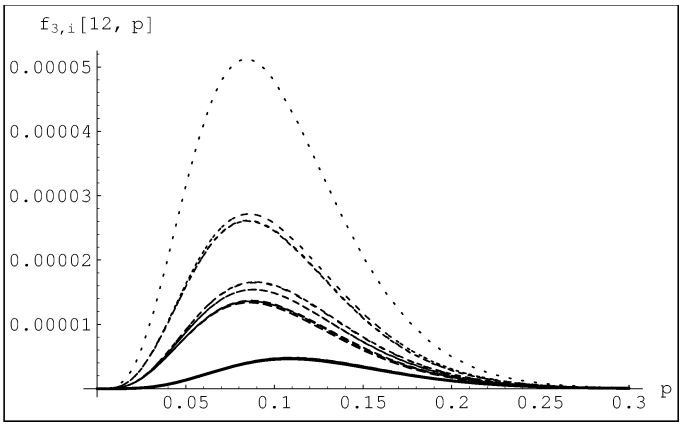

Figure 2: 17 different functions for the probability of undetected errors for $k=3$

As we can see, when the block length n increases, the maximum of these functions becomes smaller and the sequence of maximums converges to 0 (Figure 3). Using this property, we can control errors. Namely, if we want the probability of undetected errors to be smaller than some previous given value ε, we are searching for the smallest natural number n for which the maximum of the function $f_{3,i}(n,p)$

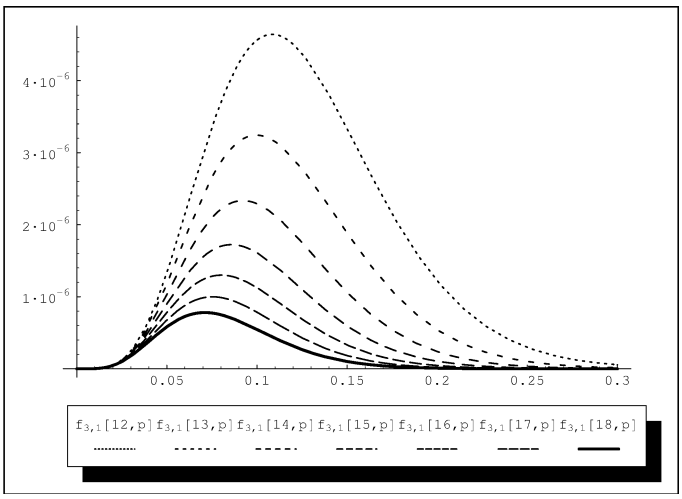

Figure 3: The best probability function for different values of block length n

is smaller then ε. Since the sequence of maximums of the functions $f_{3,i}(n,p)$ is strictly decreasing and converges to 0 when $n \to \infty$, there will be $n \in \mathbb{N}$, with this property. Now, we separate the message into blocks with length n and we code every block individually.

4. Classification of quasigroups of order 4 according to goodness for proposed codes for k=3

As we mentioned in previous section, we filtered the quasigroups of order 4 such that the probability of undetected errors does not depend on the distribution of the letters in the input messages. After filtration only 160 quasigroups remained. These 160 quasigroups are separated in 17 sets, such that quasigroups in a same set have same probability of undetected errors and quasigroups in different sets have different probability of undetected errors.

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.
Each quasigroup is presented by a number according to the lexicographic ordering of the set of quasigroups of order 4.

Set 1: 43, 133, 157, 235, 342, 420, 444, 534
Set 2: 83, 113, 203, 285, 292, 374, 464, 494
Set 3: 40, 138, 166, 228, 349, 411, 439, 537
Set 4: 80, 116, 206, 269, 308, 371, 461, 497
Set 5: 92, 111, 213, 274, 303, 364, 466, 485
Set 6: 82, 110, 212, 284, 293, 365, 467, 495
Set 7: 77, 100, 197, 272, 305, 380, 477, 500
Set 8: 37, 60, 70, 132, 163, 234, 252, 262, 315, 325, 343, 414, 445, 507, 517, 540
Set 9: 46, 127, 160, 222, 355, 417, 450, 531
Set 10: 54, 71, 243, 253, 324, 334, 506, 523
Set 11: 14, 21, 179, 192, 385, 398, 556, 563
Set 12: 93, 101, 196, 275, 302, 381, 476, 484
Set 13: 49, 51, 57, 63, 174, 185, 246, 259, 318, 331, 392, 403, 514, 520, 526, 528
Set 14: 26, 126, 147, 223, 354, 430, 451, 551
Set 15: 27, 139, 146, 229, 348, 431, 438, 550
Set 16: 4, 24, 169, 182, 395, 408, 553, 573
Set 17: 1, 7, 9, 11, 172, 189, 242, 263, 314, 335, 388, 405, 566, 568, 570, 576

The probability of undetected errors for the quasigroups in the Set i is given with the function $f_{3,i}(n,p)$ from the previous section. All of these 160 quasigroups are fractal. The best for coding are quasigroups in the set 1. All quasigroups in set 1 are linear fractal quasigroups.

5. Comparison of the codes for $k = 2$ and $k = 3$

The code for $k = 2$ is considered in [4]. In that paper we concluded that probability of undetected errors for $k = 2$, depends on the distribution of the letters in the input message. After filtration 160 quasigroups remained. With simple comparison of the results from this paper with the results from the paper [4], we can conclude that the same 160 fractal quasigrups remained after filtration for both codes. But, in the case with $k = 2$, these 160 quasigroups give 7 different sets, such that quasigroups in the same set have same probability of undetected errors. An important fact is that the best sets of quasigroups for both codes contain only linear fractal quasigroups.

We will denote with $f_{2,1}(n,p)$ the probability of undetected errors for the best class of quasigroups for the code when $k = 2$. This function is derived in [4]. On Figure 5 in [4] we can see that second best function is very close to the $f_{2,1}(n,p)$. Their plots almost overlap each other. For this reason, we can assume that quasigroups from these two sets are equally good for coding.

The best set of quasigroups in the case when $k = 3$ is subset of the second best set of quasigroups for the code when $k = 2$. For the reasons explained above, we can assume that the best set of quasigroups for the code when $k = 3$ is subset from the best set of quasigroups for the code when $k = 2$.

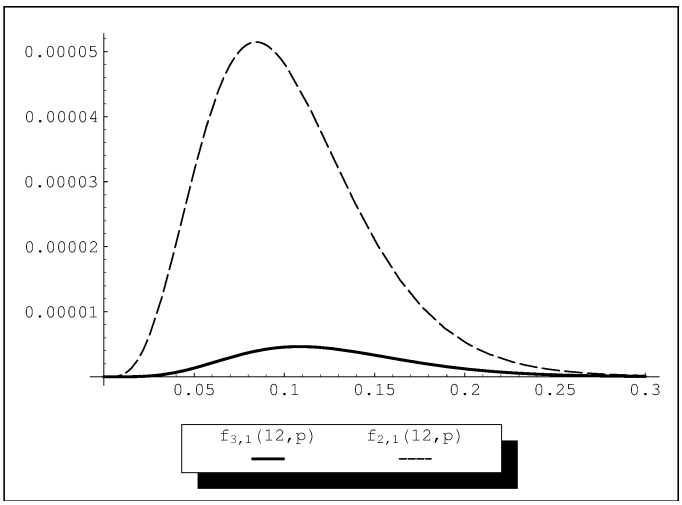

Figure 4: The best probability functions for both codes: $f_{2,1}(n,p)$ for the code with $k=2$ and $f_{3,1}(n,p)$ for the code with $k=3$

In Figure 4 are given functions for the best sets of quasigroups for both codes, i.e. $f_{2,1}(n,p)$ and $f_{3,1}(n,p)$. As we can see, probability of undetected errors for the code with $k=3$ is much smaller than for the code with $k=2$. In the Table 1, are given the maximums of the functions for the probability 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 around 10 times smaller for the code with $k=3$. Since, addition of one more character in the definition of each redundant character will slightly increase the coding time, but the probability of undetected errors is much smaller, we can conclude that the code with $k=3$ is better for coding.

6. Comparison with other codes

In this section we will compare the code considered in this paper ($k=3$) with other well-known error-detecting codes. Namely, we will compare the code with CRC, Humming and Reed-Muller codes. Since, it make most sense to compare codes with a same rate, we will do that whenever possible.

6.1 Comparison with CRC code

CRC is a standard in error-detection. It is most often used error-detecting code. Ability of the code to detect errors depends on the chosen polynomial for coding. We will consider several cases of polynomials, accepted as a standard for coding. Namely, we will consider CRC-12 (defined with the polynomial $g(x)=x^{12}+x^{11}+$

n	$k=2$	$k=3$
10	9.35406×10^{-5}	1.06987×10^{-5}
11	6.82458×10^{-5}	6.89244×10^{-6}
12	5.14707×10^{-5}	4.64338×10^{-6}
13	3.97896×10^{-5}	3.2436×10^{-6}
14	3.14013×10^{-5}	2.33481×10^{-6}
15	2.52198×10^{-5}	1.72369×10^{-6}
16	2.05631×10^{-5}	1.30035×10^{-6}
17	1.69878×10^{-5}	9.9951×10^{-7}
18	1.41968×10^{-5}	7.80948×10^{-7}
19	1.19860×10^{-5}	6.19047×10^{-7}
20	1.02120×10^{-5}	4.97045×10^{-7}
21	8.77182×10^{-6}	4.03692×10^{-7}
22	7.59050×10^{-6}	3.31277×10^{-7}
23	6.61231×10^{-6}	2.74405×10^{-7}
24	5.79537×10^{-6}	2.29236×10^{-7}
25	5.10775×10^{-6}	1.92994×10^{-7}
26	4.52483×10^{-6}	1.63643×10^{-7}

Table 1: The maximums of the probability functions for $k = 2$ and $k = 3$

x^3+x^2+x+1), CRC-ANSI (defined with the polynomial $g(x) = x^{16}+x^{15}+x^2+x+1$) and CRC-CCITT (defined with the polynomial $g(x) = x^{16}+x^{12}+x^5+1$). These are most commonly used CRC codes. Unlike the codes defined with the model in [4], CRC code adds constant number of redundant characters, regardless of the length of the information block. CRC-12 adds 12 bits, while CRC-ANSI and CRC-CCITT add 16 bits. There are numerous papers which investigated the probability of undetected errors of CRC codes. We will use results obtained in [22]. In Table 2 are given maximums of their probabilities of undetected errors for different values of the block length ([22]) and corresponding probability of undetected errors for our code. The block lengths are expressed in bits. Each character from the set $\{0, 1, 2, 3\}$ on which our code is defined can be presented with two bits. This means that, if the block length is n symbols from the set $\{0, 1, 2, 3\}$, than the block length of the binary representation is $2n$. For this reason, the value of the probability of undetected errors for block length n in Table 2 corresponds with the value of the probability of undetected errors for block length $n/2$ in Table 1.

As we can see from Table 2, our code has smaller probability of undetected errors than CRC-12 for all values of block length n which are greater than 10. For n greater than 12 our code has smaller probability of undetected errors than CRC-12 and CRC-ANSI. For n greater than 14 our code has smaller probability of undetected errors than all considered CRC codes. There is the most sense to compare codes with a same rate. Our code has rate 1/2. CRC-12 will have rate

n	$k=3$	CRC-12	CRC-ANSI	CRC-CCITT
6	1.53809×10^{-2}	$4.98239403 \times 10^{-4}$	$2.09564372 \times 10^{-4}$	$1.82571298 \times 10^{-4}$
8	3.04367×10^{-3}	$4.37709580 \times 10^{-4}$	$1.93778075 \times 10^{-4}$	$1.68755027 \times 10^{-4}$
10	5.8113×10^{-4}	$4.34696788 \times 10^{-4}$	$1.71779543 \times 10^{-4}$	$1.49835850 \times 10^{-4}$
12	1.46302×10^{-4}	$4.92904790 \times 10^{-4}$	$1.49497882 \times 10^{-4}$	$1.31108736 \times 10^{-4}$
14	6.13344×10^{-5}	$5.22761450 \times 10^{-4}$	$1.37334592 \times 10^{-4}$	$1.14947191 \times 10^{-4}$
16	3.11371×10^{-5}	$5.32168354 \times 10^{-4}$	$1.63272940 \times 10^{-4}$	$1.00034176 \times 10^{-4}$
18	1.75778×10^{-5}	$5.24102890 \times 10^{-4}$	$1.87672767 \times 10^{-4}$	$9.68045141 \times 10^{-5}$
20	1.06987×10^{-5}	$5.11365042 \times 10^{-4}$	$1.96620564 \times 10^{-4}$	$9.11743047 \times 10^{-5}$
22	6.89244×10^{-6}	$5.02705835 \times 10^{-4}$	$1.95326371 \times 10^{-4}$	$8.48346025 \times 10^{-5}$
24	4.64338×10^{-6}	$4.95408412 \times 10^{-4}$	$1.88110195 \times 10^{-4}$	$7.82445308 \times 10^{-5}$
26	3.2436×10^{-6}	$4.79257173 \times 10^{-4}$	$1.77894848 \times 10^{-4}$	$7.19221628 \times 10^{-5}$
28	2.33481×10^{-6}	$4.57258208 \times 10^{-4}$	$1.68454993 \times 10^{-4}$	$6.60500281 \times 10^{-5}$
30	1.72369×10^{-6}	$4.36575324 \times 10^{-4}$	$1.66609101 \times 10^{-4}$	$6.05393376 \times 10^{-5}$
32	1.30035×10^{-6}	$4.16986323 \times 10^{-4}$	$1.68211020 \times 10^{-4}$	$5.55637826 \times 10^{-5}$
34	9.9951×10^{-7}	$4.07554148 \times 10^{-4}$	$1.66476378 \times 10^{-4}$	$5.11186757 \times 10^{-5}$
36	7.80948×10^{-7}	$3.98553616 \times 10^{-4}$	$1.61975108 \times 10^{-4}$	$4.71277254 \times 10^{-5}$
38	6.19047×10^{-7}	$3.89937352 \times 10^{-4}$	$1.55695118 \times 10^{-4}$	$4.35295404 \times 10^{-5}$
40	4.97045×10^{-7}	$3.79043787 \times 10^{-4}$	$1.48455870 \times 10^{-4}$	$4.03147068 \times 10^{-5}$
42	4.03692×10^{-7}	$3.68207383 \times 10^{-4}$	$1.140940754 \times 10^{-4}$	$3.74421915 \times 10^{-5}$
44	3.31277×10^{-7}	$3.57807948 \times 10^{-4}$	$1.35077161 \times 10^{-4}$	$3.48991385 \times 10^{-5}$
46	2.74405×10^{-7}	$3.48489916 \times 10^{-4}$	$1.33429372 \times 10^{-4}$	$3.33221165 \times 10^{-5}$
48	2.29236×10^{-7}	$3.40974622 \times 10^{-4}$	$1.31913843 \times 10^{-4}$	$3.17809110 \times 10^{-5}$
50	1.92994×10^{-7}	$3.32276709 \times 10^{-4}$	$1.29915008 \times 10^{-4}$	$3.08847539 \times 10^{-5}$

Table 2: The maximums of the probability of undetected errors for $k = 3$, CRC-12, CRC-ANSI and CRC-CCITT. The block length n is expressed in bits.

$1/2$ if the block length is 12, while CRC-ANSI and CRC-CCITT will have rate $1/2$ if the block length is 16. Since $1.46302 \times 10^{-4} < 4.92904790 \times 10^{-4}$, our code has smaller probability of undetected errors than CRC-12 when the rates and block lengths are equal. Also, since $3.11371 \times 10^{-5} < 1.63272940 \times 10^{-4}$ and $3.11371 \times 10^{-5} < 1.00034176 \times 10^{-4}$, we conclude that our code has smaller probability of undetected errors than CRC-ANSI and CRC-CCITT for equal rates and block-lengths. Further, we can decrease the probability of undetected errors for our code without changing the rate. Namely, if we divide the message into blocks with greater length, the probability of undetected errors will be even smaller, and the code rate will be still $\frac{1}{2}$. Practically, the probability of undetected errors for our code can be made arbitrary small (as explained in subsection 3.1). On the other side, CRC code does not have this property. It is well known fact that the probability of undetected errors for CRC codes with c redundant bits tends to 2^{-c} when block length tend to infinity. Also, for fixed n, the probability of undetected

errors tends to 2^{-c} when p increases. For this reason the probability of undetected errors for CRC codes can not be made arbitrary small.

From all presented above, we can conclude that the advantage of the code considered in this paper compared with CRC code is that it has a smaller probability of undetected errors and it allows to make the probability of undetected errors arbitrarily small, which is not a case with CRC code.

6.2 Comparison with Hamming code

Error-detecting codes except for checking the accuracy of the data transmitted through a noise channels, are also used to check the accuracy of the data stored in a computer memory. One such code that is often used in computer memory is Hamming code. Certainly, the code can be used in data transmission, also. Its probability of undetected errors is examined in [12]. Results obtained in [12] are given in Table 3. General conclusion is that our code has much smaller probability of undetected errors. But, the price we pay for such a small probability of undetected errors is that we add more redundant characters compared with Hamming code. Now, it is matter of choice what is more important to the user. If it is the speed of transmission (i.e. memory space), than Hamming code goes first. But, if the accuracy of the data is more important, then our code has an advantage.

name	block length	no. redundant bits	max.probability
Hamming (7,4)	4	3	1.1718750×10^{-1}
Hamming (15,11)	11	4	6.2469482×10^{-2}
Hamming (31,26)	26	5	3.1250000×10^{-2}
Hamming (63,57)	57	6	1.5625000×10^{-2}
Hamming (127,120)	120	7	7.8125000×10^{-3}
Hamming (255,247)	247	8	3.906250×10^{-3}

Table 3: The number of information characters (block length), the number of redundant characters and the maximum of the probability of undetected errors for Hamming codes (from [12]). The block length is expressed in bits.

6.3 Comparison with Reed-Muller code

Reed-Muller is one of the oldest codes. It is first of all error-correcting code, but it can be used for error-detection solely. The code has two parameters and is denoted as $R(r, m)$. Ability of the code to detect errors depends on the parameters r and m. Some special cases are studied in [14]. For a given parameters r and m, the block length (length of the information block) is $\sum_{i=0}^{r} \binom{m}{i}$, while the number of redundant symbols is $2^m - \sum_{i=0}^{r} \binom{m}{i}$. Length of the coded block is 2^m.

- *First-order* $R(1,m)$ *code*

For first-order $R(1,m)$ code in [14] is obtained the following formula for the probability of undetected errors:

$$f_{R1}(m,p) = (2^{m+1}-2)(p(1-p))^{2^{m-1}} + p^{2^m} \tag{18}$$

The formula for the probability of undetected errors is a function of the code parameter m and the bit-error rate p.

Comparing formulas (17) and (18) we can conclude that $R(1,m)$ code has much smaller probability of undetected errors. But, on the other side, the $R(1,m)$ code on $m+1$ information bits adds 2^m-m-1 redundant bits. This implies that when m increases, the number of redundant bits exponentially grows and this code adds much more redundant characters then our code. For example, for $m=10$, the code adds 1013 redundant bits on 11 information bits . For this reason, despite the low probability of undetected errors of $R(1,m)$ code, our code is more practical for coding.

- $R(2,m)$ *code*

In [14] is also derived approximative formula for the probability of undetected errors for $R(2,m)$ code. This code on $\frac{m(m-1)}{2}+m+1$ information bits adds $2^m-\frac{m(m-1)}{2}-m-1$ redundant bits. For $m=5$, the code on 16 information bits adds 16 redundant bits, so the rate is $1/2$. Our code has rate $1/2$, so code rates are equal. Since it is most reasonable to compare the codes with same rate, we will compare $R(2,5)$ with our code. In Figure 5 is given the graphic of the probability of undetected errors of $R(2,5)$ code. The maximum of this probability is 9.49253×10^{-6}. If we use our code for coding, we can separate the message into blocks with length greater than 22 (in bits) and code these blocks separately. Then our code will have smaller probability of undetected errors. This means that when transmission speeds are equal (i.e. code rates are equal) our code is better for coding since its probability of undetected errors can be made smaller.

- $R(m-2,m)$ *code*

The last case of Reed-Muller codes that we will consider are $R(m-2,m)$ codes. These codes on 2^m-m-1 information bits add $m+1$ redundant bits. As we can see, these codes add small redundance, but on the other side they have big probability of undetected errors. The probability of undetected errors given in [14] is:

$$f_R(m,p) = \frac{1}{2^{m+1}}\left(1+(2^{m+1}-2)(1-2p)^{2^{m-1}}+(1-2p)^{2^{m+1}}\right)-(1-p)^{2^{m+1}} \tag{19}$$

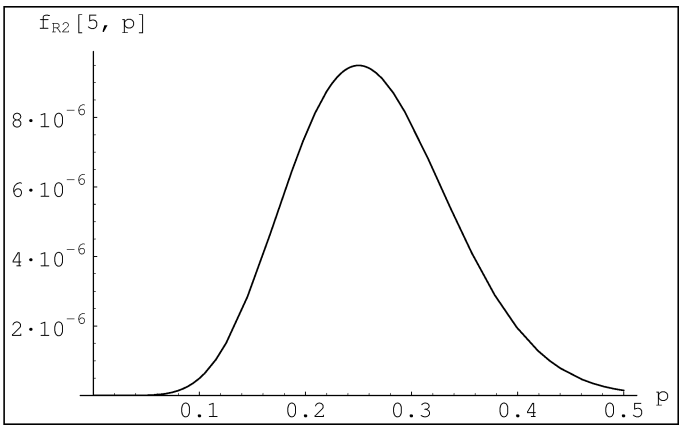

Figure 5: Probability of undetected errors for $R(2,5)$ code

Comparing (17) and (19) we can conclude that the code considered in this paper always has smaller probability of undetected errors. In Table 4 are given maximums of the probability of undetected errors for $R(m-2,m)$ code for different values of m. Comparing these values with the corresponding values for our code (case $k=3$) from Table 2, we can see that our code has much smaller maximums of the functions of the probability of undetected errors.

m	$n=2^m-m-1$	no. redundant bits	$R(m-2,m)$
4	11	5	3.12347×10^{-2}
5	26	6	1.5625×10^{-2}
6	57	7	7.8125×10^{-3}
7	120	8	3.90625×10^{-3}
8	247	9	1.95313×10^{-3}

Table 4: The maximums of the probability functions for $R(m-2,m)$ codes

Here we have similar situation as with Hamming code. It depends what is more important to the user: If it is the transmission speed, then $R(m-2,m)$ will be chosen, while if it is accuracy of the data, then our code will be chosen.

7. Conclusion

In this paper we derived a formula for the probability of undetected errors for the code defined in [4], when $A=\{0,1,2,3\}$ and when $k=3$. An important property of the code is that the probability of undetected errors can be made arbitrary small and we explain how it can be done. Also, in this paper we give a classification

of quasigroups of order 4 according to goodness for the code with $k = 3$. We compare the cases of the codes over the set $A = \{0, 1, 2, 3\}$ when $k = 2$ and when $k = 3$. We saw that the best set of quasigroups of order 4 suitable for the code with $k = 3$ contains only linear fractal quasigroups, as the code with $k = 2$. The both codes, have the same rates, but the probability of undetected errors for the code with $k = 3$ is much smaller. Since, addition of one more character in the definition of each redundant character will slightly increase the coding time, but the probability of undetected errors is much smaller, we conclude that the code with $k = 3$ is better for coding. Our next goal is to find the optimal value for k for the model defined in [4].

Also, we compare the code when $k = 3$ with CRC-12, CRC-ANSI, CRC-CCITT, Hamming and some Reed-Muller codes. We conclude that the advantage of the code considered in this paper prior the CRC code is that it has smaller probability of undetected errors when the rates and block lengths are equal. Other big advantage of the code considered in this paper is that the probability of undetected errors can be made arbitrary small which is not case with the CRC code. When compared with first order Reed-Muller code, our code is more practical due to much smaller redundance. The Reed-Muller $R(2, 5)$ code has equal rate as our code. If we divide messages in blocks with length greater or equal than 22, our code will have smaller probability of undetected errors. Comparison with Hamming and Reed-Muller $R(m-2, m)$ codes showed that our code has much smaller probability of undetected errors, but bigger redundance. This means that the code considered in this paper is in advantage in situations when data accuracy is more important than speed of the transmission (or. memory space).

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

References

[1] **T. Baicheva**, *Determination of the best CRC codes with up to 10-bit redundancy*, IEEE Transactions on Communications **56** (2008), 1214 – 1220.

[2] **T. Baicheva, S. Dodunekov, P. Kazakov**, *On the cyclic redundancy-check codes with 8-bit redundancy*, Computer Communication **21** (1988), 1030 – 1033.

[3] **T. Baicheva, S. Dodunekov, P. Kazakov**, *Undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy*, IEE Proc. Commun. **147** (2000), 253 – 256.

[4] **V. Bakeva, N. Ilievska**, *A probabilistic model of error-detecting codes based on quasigroups*, Quasigroups and Related Systems **17** (2009), 135 – 148.

[5] **D. F. Beckley**, *An optimum system with modulo 11*, The Computer Bulletin **11** (1967), 213 – 215.

[6] **G. B. Belyavskaya**, *Check character systems and totally conjugate orthogonal T-quasigroups*, Quasigroups and Related Systems **18** (2010), 7 – 16.

[7] **G. B. Belyavskaya, V. I. Izbash, G. L. Mullen**, *Check Character Systems using Quasigroups: I*, Designs Codes and Cryptography **37** (2005), 215 – 227.

[8] **G. B. Belyavskaya, V. I. Izbash, G. L. Mullen**, *Check Character Systems Using Quasigroups: II*, Designs Codes and Cryptography **37** (2005), 405 – 419.

[9] **G. B. Belyavskaya, V. I. Izbash, V. A. Shcherbacov**, *Check character systems over quasigroups and loops*, Quasigroups and Related Systems **10** (2003), 1 – 28.

[10] **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.

[11] **T. Fujiwara, T. Kasami, S. Lin**, *Error detecting capabilities of the shortened Hamming codes adopted for error detection in IEEE Standard 802.3*, IEEE Transactions on Communications **37** (1989), 986 – 989.

[12] **M. Gupta, J. S. Bhullar, O. P. Vinocha**, *On Probability of undetected error for Hamming codes over q-ary symmetric channel*, J. Communication and Computer **8** (2011), 259 – 263.

[13] **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.

[14] **T. Kløve, T. Kasami, S. Lin**, *Reed-Muller codes for error detection: the good, the bad, and the ugly*, IEEE Transactions on Information Theory **42** (1996), 1615 – 1622.

[15] **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.

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

[17] **G. L. Mullen, V. A. Shcherbacov**, *Properties of codes with one check symbol from a quasigroup point of view*, Izvestiya AN RM. Matematica **3** (2002), 71 – 86.

[18] **G. L. Mullen, V. A. Shcherbacov**, *n-T-quasigroup codes with one check symbol and their error detection capabilities*, Comment. Math. Univ. Carolinae **45** (2004), 321 – 340.

[19] **R. H. Schulz**, *A note on check character systems using Latin squares*, Discrete Mathematics **97** (1991), 371 – 375.

[20] **R. H. Schulz**, *Check character systems over groups and orthogonal Latin squares*, Appl. Algebra in Engineering Communication and Computing **7** (1996), 125 – 132.

[21] **J. Verhoeff**, *Error detecting decimal codes*, Math. Centre Tracts. Math. Centrum Amsterdam **29** (1969).

[22] **K. A. Witzke**, *Exmanination of the undetected error probability of linear block codes*, Thesis: M.A. Sc, University of British Columbia Department of Electrical Engineering (1984).

Received December 11, 2013

Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University, Rugjer Boshkovikj 16, P. O. Box 393, 1000 Skopje, Republic of Macedonia
E-mail: natasa.ilievska@finki.ukim.mk