Computer Science and Information Technology 2(8): 331-338, 2014 http://www.hrpub.org
DOI: 10.13189/csit.2014.020803

Recursive Construction of *n*-gonal Codes on the Basis of Block Design

Tkachenco V.G.[1,*], Sinyavsky O.V.[2]

[1]Odessa National Academy of Telecommunications named after O.S.Popov, 65029, Odessa, str. Kovalska 1, Ukraine
[2]Military Academy (Odessa), 65009, Odessa, str. Fontansky road, 10, Ukraine

Abstract In the article are defined nonlinear *n*-gonal block codes. The methods of constructing *n*-gonal codes are considered. Suggest efficient universal recursive methods of constructing codes great length on the basis of block design for error-correcting code. On the basis of these methods can be constructed error-correcting codes for any predetermined number of errors. Among the codes with a predetermined length codeword and a predetermined number of units in the word, these codes will have a maximum number of codewords. Dignity of these codes is speed of encoding and decoding. Also possibility of fast change of a code without change of tables of encoding and decoding. This makes it possible to use these in cryptosystems.

Keywords Error-correcting Code, Nonlinear *N*-gonal Codes, Steiner System, Affine Plane, Projective Plane, Projective-affine *BIB* Expansion

1. Introduction

In the progress of transmitting information on telecommunication networks there is a problem of error correction. Control of integrity of data and error correction — important tasks at many levels of work with information. One means of solving these problems is the use of error-correcting codes.

To date, developed many different error-correcting codes, which differ from each other by structure, redundancy, encoding and decoding algorithms ([1] … [4]). On the basis of monotone Boolean functions constructed a number of cryptosystems [5 - 8] with error correction. In particular, in the system based on triangular codes for construction codes great lengths used a recursive method [6].

However the recursive method used in [6] does not allow to build codes, if number of units in a code word more than 3.

The aim of this work is to develop a recursive method for constructing of error-correcting code great length, which has a maximum power and corrects any predetermined number of errors and has a high speed encoding and decoding.

2. Theoretical Foundations of *n*-gonal Codes

In this article as codewords we will consider vectors of length n $\tilde{p} = (p_1, ..., p_i, ..., p_n)$, which components accept values from a set $\{0,1\}$, and the number unit a component is equal in a vector to *k*. Such codewords have Hamming weight (number of units in a codeword) equal *k*. In Hamming distance (code distance) between two codewords $\tilde{p}$ and $\tilde{s}$ the number is called $\rho(\tilde{p},\tilde{s})$ equal to number a component in which they differ [1]. Length of a code we will call length of a codeword. In total such codewords with weight of *k* can be C_n^k. Code distances between different words in this case can be 2, 4, 6, …, 2*k*. For correcting codes only codewords with distance 4, 6, …, 2*k* are applicable. The number of codewords is called as code power. Such codes with code distance 2*k* are uninviting, as their power is small and is always equal $\left[\frac{n}{k}\right]$. In any such pair of codewords there are no conterminous single bits. Let's consider further the maximum codes with $\rho(\tilde{p},\tilde{s}) \geq 2k-2$, as they correct the maximum number of errors. From determination of Hamming distance follows that in such codes for each pair of codewords of the general there can be only one unit. It is easy to present such codes in the form of monotonous Boolean functions of a rank n, weight 1 and power m, where m equally to code power. [6-8]]

For research of such codes it is possible to use block designs.

In [9-11] the following definitions of the block design, *BIB* of the block design, the affine and projective planes are given.

Definition. The balanced incomplete block design (or simply the block design) $B(v,b,r,k,\lambda)$ is called such placement of *v* of different elements on *b* to blocks that each block contains precisely *k* of the different elements, each element appears precisely in *r* different blocks and each pair of different elements b_i, b_j appears precisely in λ

blocks.

Example 1. For $v=7, b=7, r=3, k=3, \lambda=1$ we have such blocks:

b0:	(0,	1,	3)
b1:	(1,	2,	4)
b2:	(2,	3,	5)
b3:	(3,	4,	6)
b4:	(4,	5,	0)
b5:	(5,	6,	1)
b6:	(6,	0,	2)

Definition. The block design balanced with respect to pairs (elements) of $BIB\left(v,\left(b_1,...,b_m\right),\left(k_1,...,k_m\right),\lambda\right)$ is called such placement of v of elements on $b=\sum_1^m b_i$ to blocks that: 1) b_i blocks contains on $k_i < v$ of different elements at some $i = 1..., m$; 2) each pair of elements appears together precisely in λ blocks.

Any block design or *BIB* the block design is a code. In this case numbers of single bits of codewords correspond to block elements, and codewords correspond to blocks in this block design. Thus, since. $\rho\left(\tilde{a},\tilde{b}\right)\geq 2k-2$, that no 2 blocks in the constructed count have the general pairs of elements. It is obvious that number λ corresponds to Hamming distance, namely: $\rho\left(\tilde{a},\tilde{b}\right)=2\left(k-\lambda\right)$.

Definition. Correcting ability – the characteristic of a code which is equal to the maximum number of corrected errors in codewords.

Is defined as $\left[\frac{d-1}{2}\right]$, where d – the minimum distance between codewords.

As number of codewords, at which $\rho\left(\tilde{a},\tilde{b}\right)=2k$ it is not enough, the greatest correcting ability of a code is reached, when $\lambda=1$ also it is equal $\left[\frac{2(k-1)-1}{2}\right]=\left[\frac{2k-3}{2}\right]$

What follows we consider only the block designs with $\lambda=1$, i.e. Steiner systems.

In the offered method creation of correcting codes the projective and affine planes will be used.

Definition. System $PG\left(2,n\right)$, having finite number of points is called as the projective plane of an order n, if satisfies to the following axioms:

Through two different points of *P* and *Q* of the plane there passes a straight line, and, only one.

Any two straight lines have the general point.

There are three points which are not lying on one straight line.

Each straight line contains not less than three points

Generally projective plane of an order n has n^2+n+1 points and as much straight lines. Each line contains $n+1$ points, and each point belongs $n+1$ straight line.

Definition. System $EG\left(2,n\right)$, having finite number of points is called as the affine plane of an order n, if satisfies to the following axioms:

For any two different points there is only one straight line containing these points.

Crossing of two different straight lines contains exactly one point.

There is a set from four points, any three of which do not belong to one straight line.

Generally projective plane of an order n has n^2 points and n^2+n straight lines. Each line contains n points, and each point belongs $n+1$ straight line.

The affine and projective planes are block designs in which each block consists of numbers of points being on some straight line.

Let's make definition n-gonal code.

Definition 1. n-gonal code is called the Steiner system in which each block contains n elements.

n-gonal codes are block and nonlinear as a difference of any codewords are not a code.

Before describing a recursive method of creation of codes on the basis of block designs we will enter the following definitions.

Definition 2. Projective expansion of Steiner system *A*0(*v*, *b*, *r*, *k*) is called the Steiner system *C*0 obtained by combining blocks *b* of the projective planes *B*0(*k* (*k* – 1) + 1, *k* (*k* – 1) + 1, *k*, *k*) = *PG* (2, *k* – 1), constructed for each block of Steiner system *A*0.

Definition 3. Affine expansion of Steiner system *A*0(*v, b, r, k*) is called the Steiner system *C*0 obtained by combining blocks *b* of the affine planes *B*0((*k* – 1) (*k* – 1), *k* (*k* – 1), *k*, *k* – 1) = *EG* (2, *k* – 1), constructed for each block of Steiner system *A*0.

Definition 4. The projective-affine expansion *BIB* of Steiner system *A*0(*v*, (*b*1, *b*2), (*k*, *k*+1)) is called the Steiner system *C*0 obtained by combining *b*1 blocks of the projective planes *B*0(*k* (*k* – 1) + 1, *k* (*k* – 1) + 1, *k*, *k*) = *PG* (2, *k* – 1), constructed for each block from *k* of elements, and *b*2 of the affine planes *B*0(*k*·*k*, *k* (*k* + 1), *k* + 1, *k*) = *EG* (2, *k*), constructed for each block from *k* + 1 element of Steiner system *A*0.

3. Recursive Methods of Constructing *n*-gonal Codes

Let's describe a recursive method of creation of block designs on an example of creation of a code in length 64 of a code in length 21.

Example 2. As the block design of *A*0 of length 21 we will take the projective plane of the 4th order of *PG* (2,4) *v* = 21, *b* = 21, *r* = 5, *k* = 5, $\lambda=1$

1) (1,2,7,9,19)

2) (2,3,8,10,20)
3) (0,3,4,9,11)
4) (0,1,6,8,18)
5) (1,4,5,10,12)
6) (2,5,6,11,13)
7) (3,6,7,12,14)
8) (4,7,8,13,15)
9) (5,8,9,14,16)
10) (6,9,10,15,17)
11) (7,10,11,16,18)
12) (8,11,12,17,19)
13) (9,12,13,18,20)
14) (0,10,13,14,19)
15) (1,11,14,15,20)
16) (0,2,12,15,16)
17) (1,3,13,16,17)
18) (2,4,14,17,18)
19) (3,5,15,18,19)
20) (4,6,16,19,20)
21) (0,5,7,17,20)

Let set E, consists 0 and pairs (x,y), where $0 \le x \le 20,\ 0 \le y \le 2$. Let's construct the blocks containing 0, as follows: $\left(0,(x,0),(x,1),(x,2)\right)$. Such blocks we will call the allocated blocks. In pairs (x, y) as elements x we will take elements of the block of 1 block design of $A0$: (1,2,7,9). As a result we will receive 16-element set $E1$. Let's renumber all pairs (x, y) as follows $(0,0)=1$, $(1,0)=2$, …, $(0,1)=22$, ... , $(20,2)=63$. As a result we will receive such set of $E1$ = {0,1,2,7,9,19,22,23,28,30,40,43,44,49,51,61}. On this set we will construct $B1$ block design – the affine plane of the 4th order of EG (2,4) v = 16, b = 20, r=5, k = 4, $\lambda = 1$.

1.1) (0,1,22,43)
1.2) (0,2,23,44)
1.3) (0,7,28,49)
1.4) (0,9,30,51)
1.5) (0,19,40,61)
1.6) (1,2,9,28)
1.7) (2,7,40,43)
1.8) (7,9,23,61)
1.9)(1,23,30,40)
1.10) (2,22,51,61)
1.11) (7,22,30,44)
1.12) (23,43,49,51)
1.13) (9,19,43,44)
1.14) (9,22,40,49)
1.15) (28,30,43,61)
1.16) (28,40,44,51)
1.17) (1,44,49,61)
1.18) (2,19,30,49)
1.19) (1,7,19,51)
1.20) (19,22,23,28)

The allocated blocks in the block design of B1 are the blocks containing 0, i.e. with numbers 1.1-1.5

Similarly on the block of 2 block designs of $A0$ PG (2,4) we build a set of E2 = {0,2,3,8,10,20,23,24,29,31,41,44,45, 50,52,62}. On this set we will construct $B2$ block design – the affine plane of the 4th order of EG (2,4) v = 16, b = 20, r=5, k = 4, $\lambda = 1$ by means of such replacement of elements of the block design of $B1$ (according to a lemma 3):

1->>> 2->>> 3, 7---> 8, 9---> 10, 19---> 20, 22---> 23---> 24, 28---> 29, 30---> 31, 40---> 41, 43---> 44---> 45, 49---> 50, 51---> 52, 61---> 62

2.1) (0,2,23,44)
2.2) (0,3,24,45)
2.3) (0,8,29,50)
2.4) (0,10,31,52)
2.5) (0,20,41,62)
2.6) (2,3,10,29)
2.7) (2,8,20,52)
2.8) (2,24,31,41)
2.9) (2,45,50,62)
2.10) (3,8,41,44)
2.11) (3,20,31,50)
2.12) (3,23,52,62)
2.13) (8,10,24,62)
2.14) (8,23,31,45)
2.15) (10,20,44,45)
2.16) (10,23,41,50)
2.17) (20,23,24,29)
2.18) (24,44,50,52)
2.19) (29,31,44,62)
2.20) (29,41,45,52)

The allocated blocks in the block design of $B2$ are blocks 2.1-2.5

Having used thus everything 21 blocks of block design $A0$, we will receive 21 affine plane into which 420 blocks will enter. Thus not allocated blocks will not have repeating pairs of such blocks will be $15 \cdot 21 = 315$. Now, we will add blocks on which there are crossings of block designs Bi and Bj, $1 \le i, j \le 21, i \ne j$. Such crossings will occur only on the allocated blocks (a lemma 1). Such blocks in all Bj will be $21 \cdot 5 = 105$. But on a lemma of such blocks will be 21. Therefore we will have in the sum 315 + 21 = 336 not being crossed blocks. Thus, we have received all blocks of Steiner system C0 with parameters v = 64, b = 336, r = 21, k= 4.

For construction distribution from an example 1 on any Steiner systems previously we will prove 3 lemmas.

Lemma 1. Any not allocated block can enter only into one of Steiner systems Bi.

Proof. As as $A0$ the system, any 2 ai and aj blocks from $A0$ is considered Steiner either are not crossed, or have one general element. In the first case of a set of Ei and Ej have one general element equal to 0, so Steiner of system Bi and Bj, constructed of elements of these sets, have no general blocks. In the second case ai and aj blocks have the general element x, and sets of Ei and Ej have as the general elements 0 and pair (x,y) where x it is constant, and y can accept all admissible values. In Ei and Ej there is so much in total general elements, how many they contain in one block of Steiner systems Bi and Bj. All these general elements enter into one allocated block, the general for Steiner systems Bi

and *Bj*. It proves that *Bi* and *Bj* have no general not allocated blocks.

Lemma 2. Any two distinct blocks of Steiner systems *Bi* and *Bj* do not contain the general pair of elements.

Proof. On construction the allocated blocks have no general pair and no pair from the allocated block can enter into not allocated block. Let's allow 2 not allocated blocks from *Bi* and *Bj* contain the general pair of elements. Then this pair is the general for sets of *Ei* and *Ej*, so according to a lemma 1 the general enters into the allocated block, for *Bi* and *Bj*. Then *Bi* contains the allocated and not allocated blocks with the general pair of elements. It contradicts that *Bi* is Steiner system. The lemma is proved.

Lemma 3. Any Steiner system *Bi* obtained by renumbering the elements of Steiner systems *B*1.

Proof. Steiner systems *B*1 and *Bi* are under construction of a_1 and a_i blocks of Steiner system *A*0. Let's unequivocally display *a1* block elements on a_i block elements. Thus the general element of 2 blocks (if it is) is mapping on itself. To elements of a_1 and a_i blocks there correspond components *x* in pairs (*x*,*y*), belonging to sets to *E1* and *Ei.* In such a mapping obtained uniquely renumbering of the elements of *E*1 to the elements of *Ei*. Thus from Steiner system *B1* obtained the Steiner system *Bi*.

In the proof of lemmas 1-3 that in an example 1 in quality *Bi* and *Bj* the affine planes undertake is not used. Therefore lemmas 1-3 are fair, when *Bi* and *Bj* is Steiner systems

Let's extend construction from an example 2 to a case of the any v and k.

Theorem 1. If there is Steiner system *A*0(*v*, *b*, *r*, *k*) and there is an affine plane *k*-1st order $B0((k-1)^2, k(k-1), k, k-1) = EG(2, k-1)$, exists the affine expansion $C0(v(k-2)+1, b \cdot k(k-2)+v, v, k-1)$ of Steiner system *A*0. The affine planes *Bi* exist for $k-1$ look p^i, where *p* – simple number.

Proof. According to a lemma 1 at *b* the affine planes *Bi* there are $b \cdot k(k-1) - b \cdot k$ of not allocated blocks. Adding to them *v* of the allocated blocks we will receive that the affine expansion *C*0 of Steiner system *A*0 contains $b \cdot k(k-2)+v$ of blocks. Into all these blocks on construction enter $v(k-2)+1$ elements, as *x* in pairs (*x*,*y*) changes generally from 0 to $v-1$, and *y* from 0 to $k-3$. Each pair (*x*,*y*) is included into $r \cdot (k-1)$ not allocated blocks and in one allocated block. 0 enters into *v* of the allocated blocks. As in any Steiner system is carried out $r \cdot (k-1)+1 = v$, each element of the affine expansion *C*0 enters into *v* of blocks, and pair of elements $((x_1,y_1), (x_2,y_2))$ according to a lemma 2 is included only into one block. $b \cdot k(k-2)+v$ blocks contains in all $b \cdot k(k-2) \cdot (k-1) \cdot (k-2)/2 + v \cdot (k-1) \cdot (k-2)/2$ pairs. As for block designs $b \cdot k = v \cdot r$, number of pairs equally $v \cdot (v-1) \cdot (k-2)^2/2 + v \cdot (k-1) \cdot (k-2)/2 = v^2 \cdot (k-2)^2/2 + v \cdot (k-2)/2$, i.e. to number of pairs, which form $v(k-2)+1$ elements. It proves that *C*0 Steiner system.

In a case when $v = 40$, this theorem it is impossible to apply that. From the block design with $v = 13$ to construct the block design $v = 40$ it is possible by means of the projective plane.

Theorem 2. If there is Steiner system *A*0(*v*, *b*, *r*, *k*) and there is a projective plane *k*-1st order $B0(k(k-1)+1, k(k-1)+1, k, k) = PG(2,k-1)$, exists the projective expansion $C0(v(k-1)+1, b(k-1) \cdot (k-1)+v, v, k)$ of Steiner system *A*0. The projective plane *B*0 exists for $k-1$ look p^i, where *p* – simple number. Steiner system *B*0 is symmetric.

Proof. According to a lemma 1 at *b* the projective planes B*i* there are $b \cdot (k(k-1)+1) - b \cdot k$ of not allocated blocks. Adding to them *v* of the allocated blocks we will receive that the projective extension *C*0 of the block design of *A*0 contains $b(k-1)2+v$ of blocks. In all of these blocks by construction includes $(k-1)+1$ elements, as *x* in pairs (*x*,*y*) changes generally from 0 to *v*-1, and *y* from 0 to $k-3$. Each pair (*x*,*y*) is included into $r \cdot (k-1)$ not allocated blocks and in one allocated block. 0 enters into v of the allocated blocks. As in any Steiner system is carried out $r \cdot (k-1)+1 = v$, each element of the projective *C*0 expansion enters into *v* of blocks, and pair of elements $((x_1,y_1), (x_2,y_2))$ according to a lemma 2 is included only into one block. In all $b(k-1)2+v$ blocks contains $b(k-1)^2 \cdot k \cdot (k-1)/2 + v \cdot k \cdot (k-1)/2$ pairs. As for block designs $b \cdot k = v \cdot r$, number of pairs equally $v \cdot (v-1) \cdot (k-1)^2/2 + v \cdot k \cdot (k-1)/2 = v \cdot (k-1)(v \cdot (k-1)+1)/2$, i.e. to number of pairs, which form $v(k-1)+1$ elements. It proves that *C*0 Steiner system.

Example 3. From block design *A*0(13, 13, 4, 4) and the same block design *B*0(13, 13, 4, 4) we will receive block design *C*0(40, 130, 13, 4). Let block designs of *A*0 and *B*0 the such:

1)	(1, 2, 3, 4)		8)	(3, 6, 10, 11)
2)	(1, 5, 6, 7)		9)	(3, 5, 9, 13)
3)	(1, 8, 9, 10)		10)	(3, 7, 8, 12)
4)	(1, 11, 12, 13)		11)	(4, 5, 10, 12)
5)	(2, 5, 8, 11)		12)	(4, 6, 8, 13)
6)	(2, 6, 9, 12)		13)	(4, 7, 9, 11)
7)	(2, 7, 10, 13)			

From the block 1 we will receive just as in an example the 2nd block design *B*1(13, 13, 4, 4). From it renumbering of elements we will receive block designs *B*2 – *B*13. As a result we will receive 117 not allocated and 13 allocated blocks of block design *C*0.

Repeatedly applying the theorem 2 to $C0(40,130,13,4) = A1$ we will receive infinite sequence of Steiner systems:

$$A0(13,13,4,4) \Rightarrow A1(40,130,13,4) \Rightarrow \ldots$$

$$\Rightarrow A3(364,11011,121,4) \Rightarrow$$

$$\Rightarrow \ldots \Rightarrow Ai(9841,8069620,3280,4) \Rightarrow \ldots$$

In a case, when $v = 52$ 1 and 2 it is impossible to apply the theorem. But it is possible to construct Steiner system with $v = 52$, using Steiner *A*0 system

Theorem 3. If there is *BIB* Steiner system *A*0(*v*, (*b*1, *b*2), (*k*, *k* + 1)), exists the projective plane *k*-1rd order $B0(k(k-1)+1, k(k-1)+1, k, k) = PG(2, k-1)$ and exists the affine *k*rd plane of an order of $D0(k \cdot k, k(k+1), k+1, k) = EG(2, k)$, exists the projective and affine expansion $C0(v(k-1)+1, b1$

$(k-1)\,(k-1)+b2\,(k\cdot k-1)+v, v, k)$ *BIB* of Steiner system $A0$. Both planes exist for $k-1$ look $p_1^{i_1}\cdot i_1$ and look k $p_2^{i_2}$, where p_1 and p_2 – simple numbers.

Proof. According to a lemma 1 in $b1$ projective and $b2$ the affine planes Bi are present at $b1\cdot(k(k-1)+1)-b1\cdot k+b2\cdot k(k+1)-b2\cdot(k+1)$ not allocated blocks. Adding to them v of the allocated blocks we will receive that the projective and affine $C0$ extension of the block design of $A0$ contains $b1(k-1)^2+b2(k^2-1)+v$ of blocks. Enter into all these blocks on construction $v(k-1)+1$ elements, as x in pairs (x,y) changes generally from 0 to v-1, and y from 0 to $k-2$. Each pair (x,y) enters in $r(k-1)+k$ not allocated blocks and in one allocated block. 0 enters into v of the allocated blocks. As in any Steiner system is carried out $r\cdot(k-1)+1=v$, each element of the projective $C0$ expansion enters into v of blocks, and pair of elements $((x_1,y_1),(x_2,y_2))$ according to a lemma 2 is included only into one block. In all $b1(k-1)^2+b2(k^2-1)+v$ blocks contains $b1(k-1)^2\cdot k\cdot(k-1)/2+b2(k^2-1)\cdot k\cdot(k-1)/2+v\cdot k\cdot(k-1)/2$ pairs. As for block designs $(b1+b2)\cdot k=v\cdot r$, number of pairs equally $v\cdot(v-1)\cdot(k-1)^2/2+v\cdot k\cdot(k-1)/2=v\cdot(k-1)(v\cdot(k-1)+1)/2$, i.e. to number of pairs, which form $v(k-1)+1$ elements. It proves that $C0$ Steiner system.

Example 4. Let *BIB* block design $A0(v=17, (b1=16, b2=4), (k=4, k+1=5))$ is set:

a1)	(0,	1,	2,	3,	4)
a2)	(0,	5,	6,	7,	8)
a3)	(0,	9,	10,	11,	12)
a4)	(0,	13,	14,	15,	16)
a5)	(1,	5,	9,	13)	
a6)	(1,	6,	10,	14)	
a7)	(1,	7,	11,	15)	
a8)	(1,	8,	12,	16)	
a9)	(2,	5,	10,	15)	
a10)	(2,	6,	9,	16)	
a11)	(2,	7,	12,	13)	
a12)	(2,	8,	11,	14)	
a13)	(3,	5,	11,	16)	
a14)	(3,	6,	12,	15)	
a15)	(3,	7,	9,	14)	
a16)	(3,	8,	10,	13)	
a17)	(4,	5,	12,	14)	
a18)	(4,	6,	11,	13)	
a19)	(4,	7,	10,	16)	
a20)	(4,	8,	9,	15)	

projective plane of the 3rd order $B0(13, 13, 4, 4)$ and affine plane of the 4th order $D0(16, 20, 5, 4)$. From $A0$, $B0$ and $D0$ it is possible to construct the projective and affine expansion $C0(52, 221, 17, 4)$. Namely, from blocks a_1-a_4 block designs $A0$ we will receive 4 affine planes $D1-D4(13, 13, 4, 4)$ (as in an example 2) which will give 144 not allocated blocks, and from other blocks of scheme $A0$ we will receive 16 projective planes $B5-B20(16, 20, 5, 4)$ (as in an example 3) which will give 60 not allocated and 17 allocated blocks (on construction) the projective-affine expansion $C0(52, 221, 17, 4)$.

For specific cases k can exist and other recurrent ways of creation of codes. In particular, for a case $k=3$ in [7] are proved the theorem A and the theorem B, and also Moore's theorem is provided.

Theorem A. Exists a triangular code with words of code length k (k is odd and $k\not\equiv 5(\bmod 6)$) power $m=\frac{k(k-1)}{6}$. Then there is a triangular code with words of code length $n=2k$ power $4m=\frac{n(n-2)}{6}$.

Theorem B. There are systems of triples of Steiner of orders of v_1 and v_2: $S_1(v_1, b_1, r_1,3)$ and $S_2(v_2, b_2, r_2,3)$. Then there is Steiner a system $S\left(v_1v_2,\frac{v_1v_2(v_1v_2-1)}{6},\frac{v_1v_2-1}{2},3\right)$.

Moore's theorem. Let there are systems of triples of Steiner of orders v_1 and v_2: $S_1(v_1, b_1, r_1,3)$ and $S_2(v_2, b_2, r_2,3)$. Let also either $v_3=1$, or v_3 is order of system of triples of Steiner $S_3(v_3, b_3, r_3,3)$ which is a subsystem in S_2. Then it is possible to construct system of triples of Steiner $S(v, b, r, 3)$ with $v=v_3+v_1(v_2-v_3)$, containing v_1 of subsystems of an order of v_2 and at least on one subsystem of orders $v1$ and v_3 (if v_3 is not equal 1).

For a case $k=4$ it is possible to prove the theorem similar to the theorem B:

Theorem 4. Let there are systems of fours Steiner's of orders v_1 and v_2: $S_1(v_1, b_1, r_1,4)$ and $S_2(v_2, b_2, r_2,4)$. Then there is Steiner a system

$$S(v,b,r,4)=S\left(v_1v_2,\frac{v_1v_2(v_1v_2-1)}{12},\frac{v_1v_2-1}{3},4\right).$$

Proof. We form of the elements S_1 and S_2 $v=v_1v_2$ pairs. Of these pairs we will build the four of Steiner system S. At the first stage we take any element a_i from S_1 and any block (b,c,d,e) from S_2. We form the four of pairs $((a,b),(a,c),(a,d),(a,e))$, such the fours exists v_1b_2. Also at the second stage we take any block (a,b,c,e) from S_1 and any element d from S_2. We form the four of pairs $((a,d),(b,d),(c,d),(e,d))$. Such the fours exists v_2b_1. At the third stage we take any block from (a,b,c,d) S_1 and any block (e,f,g,h) from S_2. It is possible to form 24 four of these pairs of 2 blocks. Let's order pairs in each of 24 fours on four elements (a,b,c,d). Then the second elements of pairs in each of 24 fours represent shift of elements of the

four (e,f,g,h). 24 it is possible to choose from these only 12 which have no general pairs. For this purpose it is necessary to take only even shifts (e,f,g,h). Let's list these 12 fours: $((a,e),(b,f),(c,g),(d,h))$, $((a,e),(b,g),(c,h),(d,f))$, $((a,e),(b,h),(c,f),(d,g))$, $((a,f),(b,e),(c,h),(d,g))$, $((a,f),(b,g),(c,e),(d,h))$, $((a,f),(b,h),(c,g),(d,e))$, $((a,g),(b,e),(c,f),(d,h))$, $((a,g),(b,f),(c,h),(d,e))$, $((a,g),(b,h),(c,e),(d,f))$, $((a,h),(b,e),(c,g),(d,f))$, $((a,h),(b,f),(c,e),(d,g))$, $((a,h),(b,g),(c,f),(d,e))$. In total for Steiner systems S_1 and S_2 it is possible to receive $12b_1b_2$ such fours.

Let's show that it Steiner system. As no 2 four from S_1 or S_2 have the general pairs, cannot have the general pairs any 2 four from these constructed $12b_1b_2$ fours.

Uniting the fours, the constructed on 1, 2 and 3 stages, we receive that in Steiner system S is available $b = v_1b_2 + v_2b_1 + 12b_1b_2$ blocks. For any block designs formulas are carried out: $bk = vr$, $r = \frac{\lambda(v\ ?\ 1)}{k\ ?\ 1}$. For Steiner systems with $k = 4$ these formulas look like: $4b = vr$, $r = \frac{v-1}{3}$. From here follows $b = \frac{v(v-1)}{12}$. Substituting this expression instead of $b_1 = \frac{v_1(v_1-1)}{12}$ and $b_2 = \frac{v_2(v_2-1)}{12}$ we receive $b = v_1b_2 + v_2b_1 + 12b_1b_2 = \frac{v_1v_2(v_1v_2-1)}{12}$, that is equal to number a fours in Steiner system S. The number of repetitions of each element is equal in these four $r = 4\frac{b}{v} = 4\frac{v_1b_2 + v_2b_1 + 12b_1b_2}{v_1v_2} = 4\frac{b_1}{v_1} + 4\frac{b_2}{v_2} + 48\frac{b_1b_2}{v_1v_2} = \frac{v_1v_2-1}{3}$. The theorem is proved.

As the Hamming distance between any codewords is not less $2(k-1)$, such quadrangular code can correct that $\left[\frac{2k-3}{2}\right]$ symbols of a transferred codeword. Codewords in the table of coding are ordered on increase.

4. Algorithms of Encoding and Decoding of *n*-gonal Codes

Decoding is carried out by means of the table (the two-dimensional massif) where in headings of lines and columns numbers of single bits, and in the table of number of codewords will be written down. We determine the transferred information message by numbers of two bits of a codeword. Thus numbers of columns correspond lsb, and numbers of lines to the msb of the transferred message.

EXAMPLE 5. Detection of one error. Let's consider a code with $k = 4$ and length n, on the channel cryptosystem two messages 2 and 1 are transferred. These messages are coded by two codewords (according to table 2): 0000 … 01110001 and 0000 … 00001111, i.e. all it is transferred $2n$ bat. Let two codewords 0000 … 0110001 and 000 … 10001111 have been accepted. At reception numbers of bits of codewords for the 1st codeword are defined these are bits: 0, 4, 5, for the 2nd – 0, 1, 2, 3, 7. Let's apply the decoding table (table 3) to definition of the devoted message corresponding to the first codeword. Number of lowest single bit of the transferred word is equal 0, and number of the highest is 5. On crossing of the corresponding line and a column is 2. It means that the message 2 is transferred. The error of transfer for the 1st codeword is corrected.

Let's consider, how there is a decoding in case instead of four single bits 5 single bits were accepted, on an example of the second codeword. It is possible to form 10 pairs of single bits of the 2nd codeword: (0; 1), (0; 2), (0; 3), (1; 2), (1; 3), (2; 3), (0; 7), (1; 7), (2; 7), (3; 7). To these pairs in the table of decoding there correspond the transferred messages: 1, 1, 1, 1, 1, 1, 4, 6, 9, 10. Six of the messages found in the table are identical and equal 1. It means that 6 first pairs of bits form the second codeword, i.e. the codeword 0000 … 00001111 has been transferred. The error of transfer for the 2nd codeword is corrected. It is possible to show that in case of reception of 5 bits instead of 4 it is enough to find in tables for the received pairs two conterminous messages, i.e. in the given example instead of 6 pairs was enough to check only pairs (0; 1) and (0; 2). At worst it is enough to check 6 pairs that demands 6 readings from table 2.

It is simple to count up, how many on the average it is necessary to check pairs in this case. Let's designate through x a random variable – number of checked pairs, p – probabilities of values x. Values p_i we will find on a formula $p_i = \frac{C_6^1 \cdot C_4^{i-2}}{C_{10}^{i-1}} \cdot \frac{5}{10-i+1}$. We have the probability distribution of this random variable:

Table 1. Distribution law of the random variable

x_i	2	3	4	5	6
p_i	0.333333	0.333333	0.214286	0.095238	0.02381

Mathematical expectation mx = 3.14. Therefore, in this case on the average it is necessary to check 3 pairs of bits.

Table 2. Coding table

The transferred message	Codeword											
	Binary look											
1	0	0	0	0	…	0	0	0	0	1	1	1	1
2	0	0	0	0	…	0	1	1	1	0	0	0	1
3	1	0	0	1	…	0	0	0	0	0	0	0	1
4	0	1	1	0	…	1	0	0	0	0	0	0	1
5	0	0	1	1	…	0	0	0	1	0	0	1	0
6	0	0	0	0	…	1	0	1	0	0	0	1	0
7	1	1	0	0	…	0	1	0	0	0	0	1	0
8	0	1	0	1	…	0	0	1	0	1	0	0	0
9	0	0	0	1	…	1	1	0	0	0	1	0	0
10	1	0	0	0	…	1	0	0	1	1	0	0	0
11	0	0	1	0	…	0	1	0	0	1	0	0	0
12	0	1	0	0	…	0	0	0	1	0	1	0	0
13	1	0	1	0	…	0	0	1	0	0	1	0	0
…	…	…	…	…	…	…	…	…	…	…	…	…	…
n	0	0	0	0	…	0	0	0	0	0	0	0	0

Table 3. Table decoding

Bits	0	1	2	3	4	5	6	7	…	*n*
0	0	0	0	0	0	0	0	0	…	0
1	1	0	0	0	0	0	0	0	…	0
2	1	1	0	0	0	0	0	0	…	0
3	1	1	1	0	0	0	0	0	…	0
4	2	5	12	10	0	0	0	0	…	0
5	2	6	13	8	2	0	0	0	…	0
6	2	7	9	11	2	2	0	0	…	0
7	4	6	9	10	10	6	9	0	…	0
8	3	6	12	11	12	6	11	6	…	0
9	3	5	9	8	5	8	9	9	…	0
10	4	5	13	11	5	13	11	4	…	0
11	4	7	12	8	12	8	7	4	…	0
12	3	7	13	10	10	13	7	10	…	0
…	…	…	…	…	…	…	…	…	…	0
n	0	0	0	0	0	0	0	0	…	0

Example 6. Detection of two errors. In a considered example chances when:

1. Two units, other zero are accepted.
2. Four units one of which is not on the place are accepted.
3. Six units are accepted.

In the first case at once by two units we determine a transferred codeword.

In the second case we have 3 true (correspond to one transferred message) and 3 incorrect pairs (correspond to different transferred messages). Then it is enough to find to two pair one transferred message. For finding of two pairs from one transferred message it is necessary to check at least 2 and at most 5 pairs. Let's count up, how many on the average it is necessary to check pairs of bits. Let x a random variable – number of checked pairs, p – probabilities of values x. Values p_i we will find on a formula $p_i = \frac{C_3^1 \cdot C_3^{i-2}}{C_6^{i-1}} \cdot \frac{2}{6-i+1}$. We have the probability distribution of this random variable:

Table 4. Distribution law of the random variable

x_i	2	3	4	5
p_i	0.2	0.3	0.3	0.2

Mathematical expectation mx = 3.5. Therefore, in this case on the average it is necessary to check 3-4 pairs of bits.

In the third case we have 6 true (correspond to one transferred message) and 9 incorrect pairs (correspond to different transferred messages). For finding of two pairs from one transferred message it is necessary to check at least 2 and at most 11 pairs.

Let's count up, how many on the average pairs of bits in

this case it is necessary to check. Similarly previous, the distribution law for this random variable:

Table 5. Distribution law of the random variable

x_i	2	3	4	5	6
p_i	0.142857	0.197802	0.197802	0.167832	0.125874
x_i	7	8	9	10	11
p_i	0.083916	0.048951	0.023976	0.008991	0.001998

Mathematical expectation mx = 4.57. Therefore, in the third case on the average it is necessary to check 4-5 pairs of bits.

5. Conclusions

In conclusion, we note the following. The main result is the development of a universal recursive method of constructing codes great length on the basis of Steiner systems. These codes have a maximum power and maximum correcting ability among the codes with a given number of units in the codeword. Is proved a number of properties of such codes, not previously described in the literature. Constructed error-correcting code with simple encoding and decoding algorithms and the ability to change the code for one permutation.

REFERENCES

[1] F.J. MacWilliams, N.J.A. Sloane. The theory of error-correcting codes, North-Holland Publishing Company, Amsterdam, 1977, 744.

[2] R.E. Blahut. Theory and practice of error control codes, Addision-Wesley Publishing Company, London, 1983, 576.

[3] E.R. Berlekamp. Algebraic coding theory, McGraw-Hill Book Company 1968, 480.

[4] David J.C. MacKay. Information Theory, Inference, and Learning Algorithms, Cambridge University Press, 2003.

[5] Ткаченко В.Г. Перечисление типов монотонных булевых функций при синтезе цифровых схем, Наукові праці ОНАЗ ім. О.С. Попова, Одеса, №2, 54 – 69, 2008

[6] Ткаченко В.Г. Синявский О.В., Построение корректирующего кода для криптосистем на основе типов монотонных булевых функций, Наукові праці ОНАЗ ім. О.С. Попова, № 1, 85 – 92, 2010.

[7] Tkachenco V.G. , Sinyavsky O.V. (2014). Construction of Cryptosystem on the Basis of Triangular Codes. Computer Science and Information Technology, 2, 300 - 307. doi: 10.13189/csit.2014.020703.

[8] Tkachenco V.G., Sinyavsky O.V. Construction of cryptosystem on the basis quadrangular codes, Nauka i Studia. Przemyśl, 35 (103), 18–28, 2013.

[9] Marshall Hall, Jr. Combinatorial theory, Blaisdell Publishing Company, Waltham (Massachusetts), 1967, 424.

[10] P.J. Cameron, J.H. van Lint. Graph Theory and Block Designs, Cambridge University Press, 1975, 144.

[11] F. Karteszi. Introduction to Finite Geometries, Akademiai Kiado, Budapest, 1976, 320.