UDK 681.3:519.15

V. Riznyk
National University "Lviv Polytechnic",
Department of Automated Control Systems

CODES OF SPATIAL SYMMETRIC-ASYMMETRIC SETS

It is shown possibility for application a new class of spatial sets using multidimensional symmetrical and non-symmetrical combinatorial configurations "Ideal Ring Bundles" (IRB)s for vector data coding with minimal number of the digit weights. Mutual connection theory of the symmetrical and asymmetrical sets with algebraic structures in Galois fields is developed.

Keywords - code, symmetrical and asymmetrical set, Galois field, optimization, vector data coding, information technology.

Introduction

Many current issues of computer engineering and information technology due to the skillful use of mathematical models and optimization methods of converting information based on the properties of multidimensional combinatorial configurations ideal type of ring v'yazanok (SCR) [1] as a convenient mathematical models for the design information technologies with enhanced functionality transformation forms of information in the form of vector data. Investigation of the properties of these models it is advisable to take into account the fundamental laws of the universe, which are based on the law of spatial symmetry. Particular attention should be paid to the symmetrical design of ordered sets and their subsets asymmetric. We propose to develop the scientific basis of the theory of spatial symmetrychno-asymmetric sets of information technology on the basis of the idea of proportionality symmetric and asymmetric structures, using greater clarity their geometric interpretation.

Formulation of the problem

Among the problems associated with the development of the theory of multidimensional combinatorial configurations ideal type of ring v'yazanok (SCR), an important question arises synthesis of multidimensional codes with optimal weight distribution of discharges by the criterion of minimizing the number of bits. These problems expedient to solve using combinatorial optimization methods of multidimensional structures using correlation theory SCR and algebraic theory of finite fields with the projection of the latter on the spatial properties of symmetric patterns and their asymmetric substructure.

The purpose of the study

The aim of the study is to identify the connection between structure and SCR structure algebraic Galois fields involving geometric interpretations of symmetric and asymmetric Galois fields SCR structures, development of algorithm synthesis vector codes using the classical theory of symmetric sets and their subsets in the asymmetric structure of algebraic Galois fields to empower practical application of methods of encoding and converting vector data into information technology.

Spatial structure symmetrical asymmetrical groups

Under the existing diversity of interpretations "perfect" combinatorial structures through cyclic flow charts, difference sets, finite affine, projective plane etc [2] structure type SCR is useful to compare the properties of algebraic Galois fields. Here is a list of some of them [3]:

1) for every degree prime p and any $n \geq 1$ there exists a unique up to isomorphism finite field $GF(p^n)$, is a field with a finite number of elements where GF means Galois Field;

2) field $GF(p^n)$ can be represented as the set of all residue classes modulo an arbitrary polynomial $f(x)$ degree *n* irreducible over the field $GF(p)$;

3) polynomial $f(x)$ degree $n \geq 1$ with coefficients from the field $GF(p)$ is irreducible over the field $GF(p)$, if it can not be written as $f(x) = A(x) \cdot B(x)$, where $A(x)$ and $B(x)$ polynomials over $GF(p)$;

4) in field $GF(q^s)$ all its $q^S - 1$ nonzero elements are different and form a cyclic group under multiplication operation ;

5) field automorphism $GF(q^s)$ form a cyclic group of order s, which is generated by the automorphism $\alpha : x \to x^p$ for any $x \in GF(q^s)$.

Comparing the properties of classical combinatorial configurations with the structure of IKB [1], we can see that the SCR described parameters S_n, n, R, де S_n – sum of the elements of the ideal ring bundles, *n*- number of elements, *R* - number of ring amounts to the same numerical values.

SCR synthesis algorithm is as follows:

1) find an irreducible over the field $GF(p^s)$ polynomial;

2) determine the initial element x of the field with the maximum possible period of said element and calculate the degree $x^0, x^1, \ldots, x^z$, ($z=q^{s-2}$), which should "run through" all the values of nonzero elements $GF(p^s)$;

3) constructed an algebraic structure $GF(p^s)$ determine numerical values of the elements SCR.

To investigate the combinatorial properties of extended Galois fields using SCR advisable to use the graphical display of the last.

An algorithm for constructing graphical models SCR is as follows:

1) the parameters SCR find original irreducible polynomial over Galois field corresponding degree;

2) determine the initial polynomial expanded field and calculate all nonzero elements of the field;

3) build a graph whose vertices are the elements $x^0, x^1, \ldots, x^z$, ($z= q^{s-2}$);

4) built on top of the column to choose, which correspond to the same values of the coefficients for any of the fixed degrees;

5) combining all pairs of vertices adjacent edges get a graphical display of SCR as a polygon.

For example, SCR with parameters $S_n = (q^{s+1} - 1)/(q-1) = 21$, $n = (q^s - 1)/(q-1) = 5$, $R = (q^{s-1} - 1)/(q-1) = 1$, де $q = 2^2$, $s = 2$, $GF(q^{s+1}) = GF(2^6)$, field $GF(2^2)$ 0, 1, c, c+1, where $c^2+c+1=0$, can be viewed as an extension of the field $GF(2)$. The initial element *x* of the field $GF(2^6)$ satisfies the equation $f(x) = x^3 + cx^2 + cx + c = 0$, де $f(x)$ – irreducible polynomial over the field $GF(2^2)$ [2]. Denoting for convenience of calculation $c + 1 = d$, easy to find all the elements of the field (Table 1).

Table 1

Elements of field $GF(2^6)$, formed irreducible polynomial $f(x) = x^3 + cx^2 + cx + c = 0$

$x = x;$

$x^2 = x^2$

$x^3 = c + cx + cx^2$

$x^4 = d + x + x^2$

$x^5 = c + x + dx^2$

$x^6 = 1 + d$

$x^7 = x + dx^2$

$x^8 = 1 + x$

$x^9 = x + x^2$

$x^{10} = c + cx + dx^2$

$x^{11} = 1 + (c+1)x + dx^2$

$x^{12} = 1 + cx^2$

$x^{13} = c + 1 + cx + dx^2$

$x^{14} = 1 + cx + dx^2$

$x^{15} = 1 + dx^2$

$x^{16} = 1 + x^2$

$x^{17} = c + dx + cx^2$

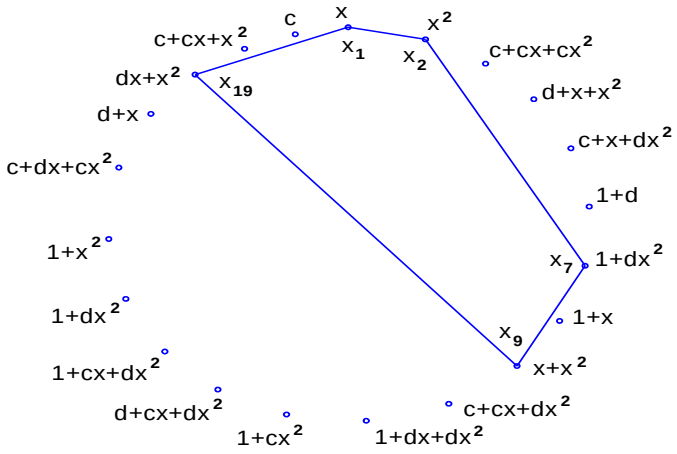
$x^{18} = d + x$

$x^{19} = dx + x^2;$

$x^{20} = c + cx + x^2;$

$x^{21} = c.$

In symmetric null graph whose vertices are the elements $x^1, x^2, x^3, ..., x^{21}$, easy to find peaks, which correspond to zero coefficients at a fixed value of the power x^i the right side of equations. For i =1 this corresponds to the set of vertices $x^1, x^2, x^7, x^9, x^{19}$, forming an asymmetrical pentagon (n=5) in symmetric field the graph з S_n=21 vertices (pict.1).



Pict.1. Diagram of SCR (1,3,10,2,5) with parameters S_n = 21, n = 5, R = 1 в $GF(2^6)$

Consider the mapping of SCR parameters $n = 4, R = 1, S_n = 13$. In this case, the initial element x field $GF(3^2)$ satisfies the equation $f(x) = x^3 - x - 1$, де $f(x)$ – irreducible polynomial over the field $GF(3^2)$, $p = 3$, $s = 2$. The elements of this field are summarized in Table 2.

Table 2

Elements of field $GF(3^2)$, formed by the irreducible polynomial $f(x) = x^3 - x - 1$

$x^1 = x$

$x^2 = x^2$

$x^3 = x + 1$

$x^4 = x^2 + x$

$x^5 = x^2 + x + 1$

$x^6 = x^2 + 2x + 1$

$x^7 = 2x^2 + 2x + 1$

$x^8 = 2x^2 + 2$

$x^9 = x + 2$

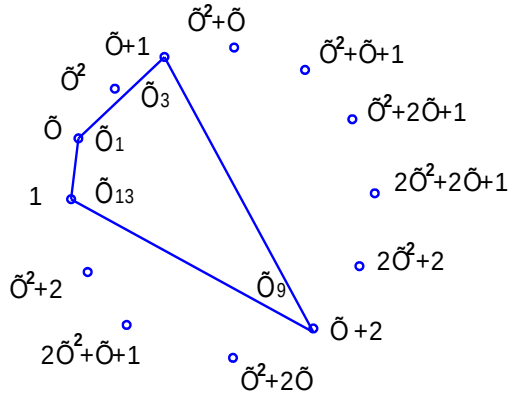
$x^{10} = x^2 + 2x$

$x^{11} = 2x^2 + x + 1$

$x^{12} = x^2 + 2$

$x^{13} = 1$

In symmetric null graph (Pict. 2) vertices x^1, x^3, x^9, x^{13} correspond to the same zero coefficients of the powers x^2, and inscribed in this rectangle asymmetric graph with parameters reflecting the SCR S_n=13, n=4, R=1 in field $GF(3^2)$.



Pict.2. Diagram of SCR with parameters S_n =13, n = 4, R = 1, formed by a polynomial

$$f(x) = x^3 - x - 1.$$

In pict.2 SCR can be seen as a quadrilateral (n = 4), adjacent vertices is asymmetrically spaced at a distance, forming a sequence (1,2,6,4) in symmetric field the graph of S_n =13 vertices.

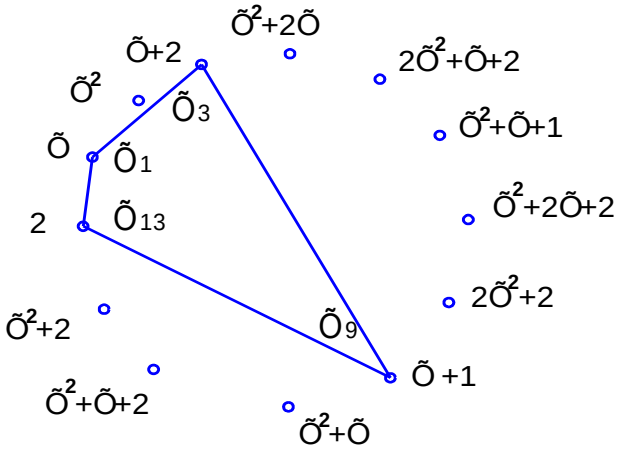
For irreducible polynomial $f(x) = x^3 - x - 2$ table of the elements field $GF(3^2)$ takes the form (Table 3).

Table3

Elements of field $GF(3^2)$, formed by the irreducible polynomial $f(x) = x^3 - x - 2$

$x = x$
$x^2 = x^2$
$x^3 = x + 2$
$x^4 = x^2 + 2x$
$x^5 = 2x^2 + x + 2$
$x^6 = x^2 + x + 1$
$x^7 = x^2 + 2x + 2$
$x^8 = 2x^2 + 2$
$x^9 = x + 1$
$x^{10} = x^2 + x$
$x^{11} = x^2 + x + 2$
$x^{12} = x^2 + 2$
$x^{13} = 2$

Circular graph for this case is shown in Pict. 3.



Pict.3. Diagram of SCR with parameters S_n=13, n=4, R=1, founded irreducible polynomial

$$f(x) = x^3 - x - 2$$

In pict.3 SCR can be seen as an asymmetric quadrilateral (n=4), adjacent vertices which are separated by distance, forming a sequence (1,2,6,4) symmetric field $GF(3^2)$.

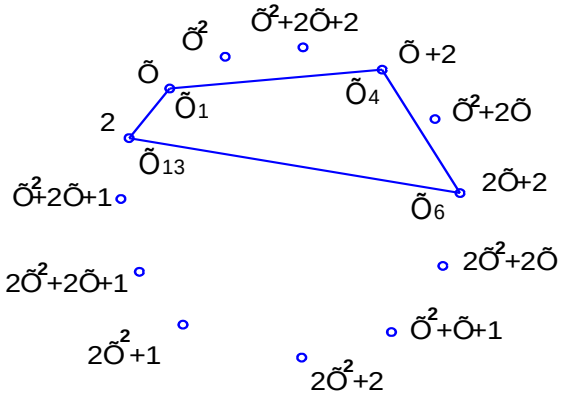
For irreducible polynomial $f(x) = x^3 - x^2 - 2x - 2$ equation for $x, x^2, ..., x^{13}$ acquire the following form (Table. 4):

Table 4

Elements of field $GF(3^2)$, formed by the irreducible polynomial $f(x) = x^3 - x^2 - 2x - 2$

$x = x$	$x^8 = x^2 + x + 1$
$x^2 = x^2$	$x^9 = 2x^2 + 2$
$x^3 = x^2 + 2x + 2$	$x^{10} = 2x^2 + 1$
$x^4 = x + 2$	$x^{11} = 2x^2 + 2x + 1$
$x^5 = x^2 + 2x$	$x^{12} = x^2 + 2x + 1$
$x^6 = 2x + 2$	$x^{13} = 2$
$x^7 = 2x^2 + 2x$	

Choosing the graph (Pict. 4) top x^i $(i = 1,..., n)$, values which correspond to the same zero coefficients at a fixed x^2, easy to establish that these vertices are x, x^4, x^6, x^{13}.



Pict.4. Diagram of SCR with parameters S_n =13, n = 4, R = 1, founded irreducible polynomial $f(x) = x^3 - x^2 - 2x - 2$

In Pict.4 SCR can be seen as an asymmetric quadrilateral (n=4), adjacent vertices which are separated each other at a distance, forming a sequence (1,3,2,7) symmetric field $GF(3^2)$.

Multidimensional Vector SCR Codes

Establish the connection multidimensional vector SCR codes to standard combinatorial structures [2], selecting for example the formation of vector code combinations based on three-dimensional ideal ring v'yazanok (3D-SCR). To construct a three-dimensional coding systems will present its model as a sequence of ordered 3-tuples integer ((k_{11}, k_{21}, k_{31}), (k_{12}, k_{22}, k_{32}), ... , (k_{1i}, k_{2i}, k_{3i}), ... , (k_{1n}, k_{2n}, k_{3n})), which is closed on itself in the form of a ring circuit. In general, the number of k_{11}, k_{21}, k_{31}, k_{12}, k_{22}, k_{32}, ... , k_{1i}, k_{2i}, k_{3i}, ... , k_{1n}, k_{2n}, k_{3n} this model can take any values. However, when it comes to the optimal coding system messages in the form of combinations of three-dimensional vectors, you must follow these requirements:

1) the number of all ordered sequences (3-tuple) should not be repeated;
2) All 3D vector sum placed next 3-tuples must not be repeated;
3) the set of all 3-tuples with the set of all sums consistently placed 3-tuples must complete the three-dimensional coordinates of the nodes cyclic matrix.

In 3D vector arithmetic sum understands result of adding numbers selected from each of the n-3 tuples with similar serial numbers, and the addition is carried out at the appropriate modules whose values are determined by the size of a cyclic matrix on the number of units in each of its coordinatesi .

Let $(k_{11}, k_{21}, k_{31}) = (0,1,0)$; $(k_{12}, k_{22}, k_{32}) = (0,2,3)$; $(k_{13}, k_{23}, k_{33}) = (1,1,2)$;
$(k_{14}, k_{24}, k_{34}) = (0,2,2)$; $(k_{15}, k_{25}, k_{35}) = (1,0,3)$; $(k_{16}, k_{26}, k_{36}) = (1,1,1)$.

In this case, the system for encoding 3D vectors by six (n=6) code combinations takes the following form: ((0,1,0), (0,2,3), (1,1,2), (0,2,2), (1,0,3), (1,1,1)):

If for each 3D coordinate values of lattice modules to choose an appropriate number of 2, 3, 5, we can obtain the following combinations as sums of consecutive 3-tuples:

(0, 0, 0) ≡ (0,1,0) + (0,2,3) + (1,1,2) + (0,2,2) +(1,0,3),
(0, 0, 1) ≡ (0,2,2) + (1,0,3) + (1,1,1),
(0, 0, 2) ≡ (1,1,2) + (0,2,2) + (1,0,3),
(0, 0, 3) ≡ (0,1,0) + (0,2,3),
(0, 0, 4) ≡ (0,2,2) + (1,0,3) + (1,1,1) + (0,1,0) + (0,2,3),
(0, 1, 0) ≡ (0,1,0),
(0, 1, 1) ≡ (0,2,2) + (1,0,3) + (1,1,1) + (0,1,0),
(0, 1, 2) ≡ (1,0,3) + (1,1,1) + (0,1,0) + (0,2,3),
(0, 1, 3) ≡ (1,1,1) + (0,1,0) + (0,2,3) + (1,1,2) + (0,2,2),
(0, 1, 4) ≡ (0,1,3) + (1,1,1),
(0, 2, 0) ≡ (0,2,3) + (1,1,2) + (0,2,2) + (1,0,3),
(0, 2, 1) ≡ (1,1,1) + (0,1,0) + (0,2,3) + (1,1,2),
(0, 2, 2) ≡ (0, 2, 2), і т.д.
……..…….

It is easy to see that the set on 3-tuples exhausts the coordinates of three-dimensional lattice, where one of the coordinates is gaining values of integers in the range from 0 to 1, the second - from 0 to 2, the third - from 0 to 4 Thus, an ordered sequence of ring 3 -kortezhiv ((0,1,0), (0,2,3), (1,1,2), (0,2,2), (1,0,3), (1,1,1)) - is an example of building a system for encoding a plurality of three-dimensional lattice vectors of size 2×3×5, which looks like a 3D torus, using only six (n = 6) code bits.

Call ring vector sum of the amount of any number (from 1 to n-1) sequentially ordered t- measurable vectors n-ring sequence. Ring n-ordered sequence t- dimensional vectors, where the set of circular vector sums exhausts the set of values of all coordinates t- dimensional lattice fixed number of times, called t-measurable ideal ring bundles (tD- IKB), and created this system of cyclically ordered sequence of vectors - perfect t- dimensional code.

The results of theoretical and experimental studies indicate that there is a large number of multi-SCR. This fact opens up opportunities for the design of new information systems and advanced computer technologies through the use of multi-dimensional vector code.

Prospects for the development of high-performance encoding vector data

Perfect example of a multi-cyclic relations in information and communication systems is the so-called "monolithic code" [1]. When monolithic understand the code combinations which are based on sequences of similar information symbols ("units" or "zero"), so the appearance among them at least one "zero" of "units", or conversely, points to the emergence of errors without the need for additional control Check to ensure high performance in detecting and correcting errors. Ensuring maximum power is achieved through an appropriate code distribution vector of weighted discharges. Under these conditions, exhaust monolithic code set ways of forming combinations that minimizes its information redundancy. Studies related to the problem of multidimensional systems design and coding signal conversion to vector form monolithic code, make it possible to develop information technology hardware and software with enhanced

functionality based on single and multi-SCR, designing effective systems convert information form , development of specialized processors for multidimensional computer arithmetic.

The study of geometrical properties of space-symmetric asymmetric groups include expanding the use of optimized vector monolithic codes in areas of science and technology, which are implemented system-wide principles based on the theory of combinatorial configurations: mathematics (vector algebra, group theory), computer engineering, cryptography, information -vymiryuvalniy technology, computer technology, radio physics, communication systems.

Conclusions

Results of the study combinatorial properties of SCR involving geometric interpretations symmetrical structure of algebraic Galois fields and asymmetric structures reveal the relationship SCR SCR theory of the classical theory of symmetric groups and their asymmetric configuration in the symmetric structure of algebraic Galois fields, indicating that the geometric nature of single and multi-SCR reveals a fundamental role of spatial symmetrical asymmetrical structural relations in the theory of optimal encoding vector data and creates opportunities for the design of new devices and systems for vector information technologies with improved characteristics.

1. Різник В.В. Синтез оптимальних комбінаторних систем.- Львів., «Вища школа», 1989.- 168 с. 2. Холл М. Комбинаторика. — М., «Мир», 1970. 3. Свердлик М.Б. Оптимальные дискретные сигналы. — М., 1975.