

## Algebraic fields and rings as a digital signal processing tool

Dinara Kutlimuratovna Matrassulova<sup>1</sup>, Yelizaveta Sergeevna Vitulyova<sup>1</sup>,  
Sergey Vladimirovich Konshin<sup>1</sup>, Ibragim Esenovich Suleimenov<sup>2</sup>

<sup>1</sup>Department of Radio engineering, electronics and telecommunications,

Almaty University of Power Engineering and Telecommunications, Almaty, Republic of Kazakhstan

<sup>2</sup>National Engineering Academy of the Republic of Kazakhstan, Almaty, Republic of Kazakhstan

### Article Info

#### Article history:

Received Nov 6, 2021

Revised Sep 3, 2022

Accepted Oct 5, 2022

#### Keywords:

Algebraic rings

Fourier transform

Galois fields

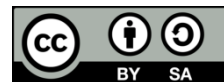
Multivalued logics

Signal processing

### ABSTRACT

It is shown that algebraic fields and rings can become a very promising tool for digital signal processing. This is mainly due to the fact that any digital signals change in a finite range of amplitudes and, therefore, there are only a finite set of levels that can correspond to the amplitudes of a signal reduced to a discrete form. This allows you to establish a one-to-one correspondence between the set of levels and such algebraic structures as fields, rings, etc. This means that a function that takes values in any of the algebraic structures containing a finite set of elements can serve as a model of a signal reduced to a discrete form. A special case of such a signal model are functions that take values in Galois fields. It is shown that, along with Galois fields, in certain cases, algebraic rings contain zero divisors can be used to construct signal models. This representation is convenient because in this case it becomes possible to independently operate with the digits of the number that enumerates the signal levels. A simple and intuitive method for constructing rings is proposed, based on an analogy with the method of algebraic extensions.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Yelizaveta Sergeevna Vitulyova

Department of Radio engineering, electronics and telecommunications

Almaty University of Power Engineering and Telecommunications after Gumarbek Daukeyev

126/1 Baitursynova Street, 050013, Almaty, Republic of Kazakhstan

Email: lizavita@list.ru

## 1. INTRODUCTION

In various branches of information theory, in particular, in the theory of coding and decoding, as well as for the purposes of pattern recognition, Galois fields are widely used, both binary [1], [2] and non-binary [3]-[5], and one of their main areas of application is coding theory [6], [7], including the creation of error correction codes [8], [9], and the development of pattern recognition methods [10].

Galois fields are finite commutative algebraic skew fields, i.e., sets that are closed under the operations of addition, multiplication, subtraction, and division (with the exception of division by zero). Any of these operations, applied to two elements of the Galois field, also gives an element of this field, despite the fact that the total number of elements is finite, which, as shown in [11], creates quite definite advantages for digital signal processing that varies in a finite range amplitude. The simplest examples of Galois fields are the result of a homomorphic mapping of the ring of integers onto the ring of residue classes modulo some prime number.

Researchers in [12]-[14] it was shown that there is a very close relationship between the theory of error-correcting coding and the theory of neural networks, which are also often used for digital signal processing [15], [16]. This creates quite definite prospects for the practical use of multivalued logics, which are actively being developed at the present time [17], [18]. They, in particular, are associated with the use of

multivalued logics in electronics [19], [20], as well as with the creation of neural networks, the state of the outputs of the elements of which corresponds to the variables of non-binary logic. The operations carried out by such networks can be described in terms of non-binary Galois fields, since for many multivalued logics it is possible to establish a one-to-one correspondence [21], [22] between the values of a logical variable and the elements of the Galois field, which, by definition, contains a finite number of elements.

The advantages of using non-binary Galois fields for digital signal processing are especially clearly demonstrated by the results of [11], [23]. It was shown that the spectra of digital signals taking values in a finite range of amplitudes can be conveniently constructed by assigning to each signal level a certain element of the field. In particular, in [11], an example was considered when the number of such levels is 17. It is important that the spectra of signals obtained in terms of functions taking values in Galois fields, in contrast to the spectra obtained, for example, based on the Walsh basis [24] and its modifications [25], [26], fit into the same range of amplitudes as original signal. Moreover, as follows from [23], using spectra of this type, a complete “digital” analog of the convolution theorem can be formulated and proved. It is appropriate to emphasize that the classical (“analogue”) convolution theorem [27] is, in turn, the basis of such concepts as the amplitude-frequency characteristic, which are widely used in radio engineering.

Thus, it can be argued that at present there is already a clearly traced tendency expressing in the close integration of such an area of information theory as digital signal processing (including the development of methods for error-correcting coding) and neural networks, and the use of such algebraic structures as Galois fields plays an important role here.

As is known, a more general algebraic structure are algebraic rings, which now are also actively used in coding theory [28], [29] too. Otherwise, Galois fields (finite commutative bodies) can be considered as specific algebraic rings, obeying additional axioms and contain only a finite number of elements. From the point of view of the theory of algebras, algebraic structures, on which more and more weakened requirements are imposed, are applied in the theory of coding. In particular, there are works in the literature that describe the use of non-associative algebraic structures in coding theory [30]. We emphasize that, unlike algebraic fields, algebraic rings have zero divisors, which, as will be clear from what follows, can also be used for digital signal processing.

We emphasize that from the point of view of using multivalued logics for digital signal processing (especially taking into account the results of [12]-[14], where it was shown that there is a deep connection between the nature of the functioning of neural networks and algorithms for error-correcting coding), the weakening of the axioms imposed on the used algebraic structures is of undoubted interest. Namely, if the variables of multivalued logic are assigned to the elements of the Galois field, then this obviously imposes very strict restrictions on the structure of logic. In particular, any operation on logical variables in this case can be represented through a function of variables taking values in the Galois field, and this function itself also takes values in this field. From the point of view of the development of artificial intelligence systems, gradually approaching human intelligence [31], [32], such a limitation is indeed very strict [33].

Namely, *onepaquu*, that human thinking uses, are not always compatible with each other. The simplest mapping of incompatibility of logical operations can obviously be realized using algebraic structures containing zero divisors. As shown in this paper, usage of algebraic structures containing zero divisors may significantly expand the capabilities of the new method for digital signal processing, previously proposed in [11], [23]. Specifically, this paper considers a simple and intuitive way to construct algebraic rings with zero divisors, which significantly expands the capabilities of the digital signal processing method proposed earlier in [11], [23].

Specifically, in the present paper, on the basis of the proposed method for constructing algebraic rings, another kind of generalized Rademacher functions is constructed. Note that the Rademacher functions are the basis for constructing the Walsh basis, which, as noted above, is widely used in applications [25], [26]. The need to pass from the Rademacher functions to the Walsh functions is due to the fact that the Rademacher functions, in contrast to the Walsh functions, do not form a complete basis suitable for the use of spectral methods. However, the Walsh functions, although they form a complete basis, nevertheless, they cannot be considered as a direct “digital” analogue of the harmonic functions. In particular, they do not have the corresponding symmetry properties with respect to the shift operation of the current discrete variable [23]. The generalized Rademacher functions proposed in [11], on the contrary, can be considered as a complete “digital” analogue of harmonic functions, which allows us to formulate and prove a “digital” analogue of the classical convolution theorem [23].

The generalized Rademacher functions proposed in [11] have a certain disadvantage. Namely, the number of cycles on which they form a complete basis must be exactly equal to the number of nonzero elements in the used Galois field, which imposes certain restrictions on the use of such functions in applications. The transition to the use of generalized Rademacher functions that take values in algebraic extensions of simple Galois fields makes it possible to significantly weaken restrictions of this kind. The same problem is also solved by using allebraic rings, whose extensions are constructed according to a specific method proposed in this

paper. Note that the method of algebraic extensions in classical algebra is applied to fields. Its use for extending rings in order to construct orthogonal bases of functions taking values in finite algebraic structures is proposed for the first time.

**2. METHOD**

The method of algebraic extensions is one of the main tools for constructing fields, including Galois fields. Simplifying somewhat, a formal root of an unsolvable equation is added to the set of elements of the original field. The most famous example is the transition from real numbers to complex ones, when an imaginary unit is introduced into consideration, which is the root of an irreducible (undecidable in real numbers) (1):

$$x^2 + 1 = 0 \tag{1}$$

and the complex numbers are written as the sum as (2):

$$c = a + ib \tag{2}$$

where  $i$  - is the root of the irreducible (1).

In a similar way, one can construct extensions of Galois fields, which, as shown in [11], [23], allow one to construct analogs of Rademacher functions, which are direct analogs of harmonic functions. The restriction is that the number of clock cycles on which the complete basis formed from analogues of the Rademacher functions proposed in [11], [23] should be exactly equal to the number of nonzero elements of the used Galois field. Consequently, the transition to fields containing a greater number of elements is also of practical interest.

Let us show how exactly one can construct analogs of the Rademacher functions proposed in [11], [23], but containing a greater number of elements using the concrete example-Galois field  $GF(5)$ . All Galois fields  $GF(5)$  are isomorphic. For convenience, we will use a field containing elements  $(-2, -1, 0, 1, 2)$ . Addition and multiplication (Tables 1 and 2) are defined according to rules similar to those used in [34].

Table 1. Multiplication table for elements of the Galois field  $GF(5)$  in the representation

$$GF(5) = (-2, -1, 0, 1, 2)$$

*	-2	-1	1	2
-2	-1	2	-2	1
-1	2	1	-1	-2
1	-2	-1	1	2
2	1	-2	2	-1

Table 2. Addition table for elements of the Galois field  $GF(5)$  in the representation

$$GF(5) = (-2, -1, 0, 1, 2)$$

+	-2	-1	1	2
-2	1	2	-1	0
-1	2	-2	0	1
1	-1	0	2	-2
2	0	1	-2	-1

From the point of view of digital signal processing, the addition rules (Table 2) have the following meaning. Figure 1 shows two groups of 5 levels each. The arrows show examples when the element "1" and the element "2" are added to the element of the Galois field  $GF(5)$  corresponding to a certain level. It can be seen that the result of these operations leads to the transition to the next group of levels, i.e., the rules presented in Table 2 have a clear meaning: they correspond to mod5 addition operations for the case when negative numbers are used.

The transition from the field  $GF(5)$  to the field  $GF(5^2)$ , which contains 25 elements, allows one to display two-digit numbers in the number system with base 5. Fields can be constructed by the method of algebraic extensions. Let us apply it for the specific case of the field  $GF(5)$ .

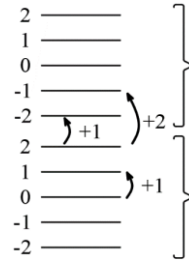


Figure 1. Illustration for the addition rules in the Galois field  $GF(5)$

In the considered Galois field, the (1) has a solution, more precisely, two solutions. These are the elements «-2» and «2», which directly follows from Table 1. Therefore, it is not permissible to use it when using the method of algebraic extensions in the classical form. Therefore, we will use the (3):

$$x^2 + 2 = 0 \tag{3}$$

which in the considered field  $GF(5)$  has no solutions.

Let us introduce into consideration the root of (3), which may be interpreted as a logical imaginary unit. Then the algebraic extension of the field  $GF(5)$  (in this case, the field  $GF(5^2)$ ) will contain exactly 25 elements representable in the form (2), and in this formula  $a$  and  $b$  should be understood as elements of the original field  $GF(5)$ , and under  $i$  is the root of (3). In accordance with the methodology proposed in [11], [23], the set of generalized Rademacher functions forming a complete basis on a set of 24 clock cycles can be constructed based on the fact that for any element  $\zeta$  of an arbitrary Galois field containing  $n + 1$  elements,

$$\zeta^n = 1 \tag{4}$$

let us form next sequences:

$$\begin{aligned} w_1 &= (1, \theta, \theta^2, \theta^3, \dots, \theta^{23}) \\ w_2 &= (1, \theta^2, \theta^{2^2}, \theta^{2^3}, \dots, \theta^{2^{23}}) \\ w_{23} &= (1, \theta^{2^3}, \theta^{2^{3 \cdot 2}}, \theta^{2^{3 \cdot 3}}, \dots, \theta^{2^{3 \cdot 23}}) \end{aligned} \tag{5}$$

where  $\theta = 1 - i$ , as follows from (5), there are exactly 23 such sequences, more generally,  $n - 1$ . Complementing set of these sequences with the sequence:

$$w_0 = (1, 1, 1, 1, \dots, 1), \tag{6}$$

consisting only of ones, we obtain a set of 24 sequences, each element of which contains, generally speaking, the real and imaginary parts in the above sense.

The number of sequences in the constructed set is equal to  $n$ -the number of nonzero elements of the considered Galois field (in the case under consideration  $n = 24$ ). We emphasize that, by virtue of (4), all degrees appearing in (5), de facto, do not exceed 23. Otherwise, the products of integers (degrees) included in them are calculated  $mod 24$ . This also implies that for each sequence  $w_k$  from the constructed set, one can specify the conjugate sequence  $w_{\tilde{k}}$  from the same set:

$$(w_k, w_{\tilde{k}}) = (1, 1, 1, 1, \dots, 1), \tag{7}$$

where  $(a, b)$ -direct product of two sequences  $a$  and  $b$ :

$$(a, b) = (a_1 b_1, a_2 b_2, \dots, a_n b_n), \tag{8}$$

specifically, the value of  $\tilde{k}$  is determined from the condition as shown in (9).

$$k \equiv \tilde{k} (mod 24) \tag{9}$$

The number  $\tilde{k}$  is uniquely determined by  $k$ . Indeed, in the Galois field, each nonzero element has an inverse element, moreover, a unique one. Accordingly, the second element of the sequence  $w_{\tilde{k}}$  is the inverse element to the second element of the sequence  $w_k$ , which is uniquely determined; the same is true for the other

elements by the construction of these sequences. Further, in an arbitrary Galois field, there is a general theorem for the sum of powers, used, among other things, in [11], [23]:

$$1 + \zeta + \zeta^2 + \dots + \zeta^{n-1} = \begin{cases} "n", \zeta = 1 \\ 0, \zeta \neq 1 \end{cases} \tag{10}$$

where  $n$  is the number of nonzero elements in the given Galois field.

We emphasize that in the formula (10) the number " $n$ " appears only formally, since the summation should be performed precisely in the sense of addition in this particular field, and " $n$ " is far from necessarily its element. The number " $n$ " in the formula (10), accordingly, is no more than a symbol implying the summation of " $n$ " ones. Consequently, in the considered Galois field,

$$\sum_{j=0}^{j=23} w_k^{(j)} w_{\tilde{k}}^{(j)} = \begin{cases} "23", k = \tilde{k} \\ 0, k \neq \tilde{k} \end{cases} \tag{11}$$

in (11) can be interpreted as an orthogonality condition in the same sense as for harmonic functions: the function  $\exp(ikt)$  is considered as conjugate with respect to the function  $\exp(-ikt)$  and vice versa. In other words, in the interval containing 24 measures, the generated sequences really constitute a complete basis. Based on (11), acting by analogy with [11], [23], one can go directly to the spectral representation of the signal in the form:

$$\vec{u} = \sum_{j=0}^{j=7} z_j \vec{w}_j \tag{12}$$

where  $\vec{u}$  is a sequence of 24 elements of the Galois field  $GF(5^2)$ , which can also be interpreted as a piecewise constant function taking values in this field with the number of values equal to 25. Of course, this representation is valid only for functions that take a value in the Galois field  $GF(5^2)$  and are given on an interval of 24 ticks, but it can be generalized to any other prime numbers and their powers. The amplitudes of the spectral components, which are also elements of the considered Galois field, are expressed in terms of the function  $\vec{u}$  as (13):

$$z_k = (\vec{u}, \vec{w}_{\tilde{k}}) = \sum_{i=0}^{i=7} z_i (\vec{w}_i, \vec{w}_{\tilde{k}}) \tag{13}$$

which follows directly from formula (11). Examples of generalized Rademacher functions corresponding to the field  $GF(5^2)$ , are shown in Figure 2. The left column shows the real parts of the specified functions, the right-the imaginary.

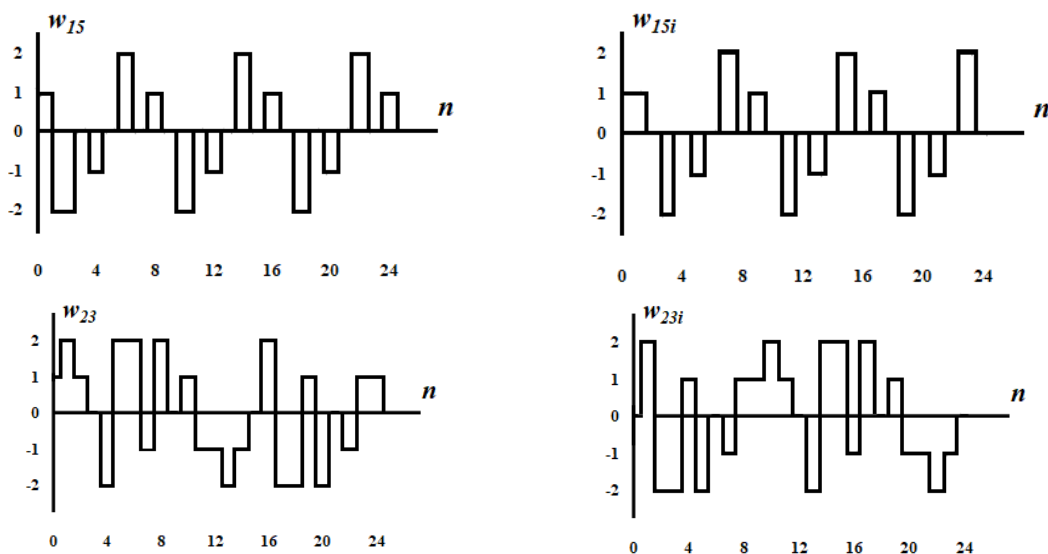


Figure 2. Examples of real and imaginary parts of generalized Rademacher functions corresponding to the field  $GF(5^2)$

It can be seen that there are examples of functions whose period is less than 24. This is due to the fact that the multiplicative group of the field under consideration has subgroups. We also emphasize that the sequences under consideration were constructed starting from the field element  $\theta = 1 - i$ . Correctly it should be interpreted as a primitive root of one. Finding primitive roots for an arbitrary Galois field, generally speaking, is a non-trivial problem, but it makes no sense to solve it for the purposes pursued, since in formulas (5) all elements of the field are used as the second elements of the sequences, therefore it is easier to find the primitive root by the method of enumeration options by computing means.

Further, the Galois fields  $GF(5^n)$  correspond to the representation of numbers in the base 5 number system, just as the fields  $GF(2^n)$  correspond to their binary representation. Indeed, any integer can be represented in the form

$$a \dots bc \leftrightarrow a \cdot 5^n + \dots + b \cdot 5^1 + c \cdot 5^0 \tag{14}$$

where the letter designations correspond to one of the elements of the field  $GF(5)$ , more precisely its mapping to the set  $(-2, -1, 0, 1, 2)$ .

Such a number record can be matched with an element of the Galois field formed by the rule:

$$a \dots bc \leftrightarrow a + \dots + b \cdot \theta^{n-2} + c \cdot \theta^{n-1} \tag{15}$$

where  $\theta$  is a primitive element of the field  $GF(5^n)$ , the degrees of which are generated by all elements of the given field. In particular, numbers in representation (14) containing two digits are represented by the elements of the Galois field  $GF(5^2)$ , considered above.

$$ab \leftrightarrow a + ib \tag{16}$$

In this way, the use of the method of algebraic extensions makes it possible to construct generalized Rademacher functions for signals whose number of cycles is a power of a prime number. This essentially removes the restrictions that arise when simple Galois fields are used. In particular, since the power of a prime number can be chosen arbitrarily, the generalized Rademacher functions proposed earlier can be constructed for intervals that also contain a significant number of cycles.

Further, as emphasized in the introduction, in classical algebra the method of algebraic extensions is applied to algebraic fields. However, it is quite applicable to the construction of specific algebraic rings, which also solve the problem under consideration, i.e., the above restrictions on the number of cycles, more precisely, on the relationship of this number with the number of amplitude levels of the digital signals involved in the consideration, substantially violate.

### 3. RESULTS AND DISCUSSION

It was emphasized that (1) in the field  $GF(5)$  is solvable. Therefore, starting from it, it is impossible to use the method of classical algebraic extensions. Nevertheless, let us introduce a logical imaginary unit as an additional root of (1) in the field  $GF(5)$ . More precisely, since in (1) is square, there will be two additional roots. Let us denote them  $\pm i$ , interpreting  $i$  as a logical imaginary unit. Using representation (2) for the elements of the set that is formed after the addition of a logical imaginary unit, it is easy to show that for such a set all the axioms of the rings are satisfied, and at the same time, zero divisors appear in it. Indeed, consider two elements:

$$e_1 = -2 + i, e_2 = -2 - i \tag{17}$$

direct computation shows (18).

$$e_1 \cdot e_2 = (-2 + i)(-2 - i) = 2 \cdot 2 + 1 = -1 + 1 = 0 \tag{18}$$

Moreover, it is also proved by direct calculations that the elements  $e_1$  and  $e_2$  are idempotent, and their sum is equal to one as (19) to (21).

$$e_1 \cdot e_1 = (-2 + i)(-2 + i) = 2 \cdot 2 - 1 - i(2 \cdot 2) = -2 + i = e_1 \tag{19}$$

$$e_2 \cdot e_2 = (-2 - i)(-2 - i) = 2 \cdot 2 - 1 + i(2 \cdot 2) = -2 - i = e_2 \tag{20}$$

$$e_1 + e_2 = (-2 + i) + (-2 - i) = -2 \cdot 2 = 1 \quad (21)$$

This result corresponds to one of the general theorems of the theory of algebraic ideals, according to which there is a variety of rings  $R$  (specifically, semisimple rings with the minimality condition) that decompose into a direct sum of ideals  $r_i$

$$R = r_1 + r_2 + \dots + r_n \quad (22)$$

each of these ideals is generated by idempotent elements  $e_i$ :

$$r_i = Re_i \quad (23)$$

which mutually cancel each other:

$$e_i e_j = 0, i \neq j; e_i e_i = e_i \quad (24)$$

and their sum is equal to one of the rings  $R$  as (25).

$$\sum_i e_i = 1 \quad (25)$$

Any element of the set obtained by extending the field  $GF(5)$  by adding additional roots of the reducible (in this field) (1) can be represented in the form:

$$a = b_1 + ib_2 \quad (26)$$

it follows from relations (18)-(21) that the element  $a$  can also be represented in the form:

$$a = a_1 e_1 + a_2 e_2 = -2(a_1 + a_2) + i(a_1 - a_2) \quad (27)$$

and,

$$a_1 = b_1 - 2b_2, a_2 = b_1 + 2b_2 \quad (28)$$

let us show that the representation of the ring  $R$  in the form (22) can be used for digital signal processing. Indeed, along with the representation of signal levels through the elements of the Galois field [11], [23], one can use a signal model in which different elements of the  $R$  ring correspond to different discrete levels. This approach, in particular, makes it possible to naturally build a signal model, which will include the digits of the numerical representation in the form (15) or similar.

$$U(t) = \sum_i u_i(t) e_i \quad (29)$$

where  $U(t)$  – signal model, i.e., time function taking values in the ring  $R$ ,  $u_i(t)$  – are time functions taking values in the original field (for the example under consideration, this is the field  $GF(5)$ ),  $e_i$  are idempotent elements of the ring  $R$ .

The convenience of using the signal model (29) is, in particular, as follows. With such a representation of the signal, it is possible to operate not with the spectrum of the signal as a whole, but with its partial spectra, each of which belongs to a certain category (in a certain number system, the choice of which is uniquely determined by the chosen Galois field). Indeed, in this case, one can compose the following expressions for the partial components of the digital spectrum:

$$\langle e_i f_k(t), U(t) \rangle = \langle f_k(t), u_i(t) \rangle e_i \quad (30)$$

where  $\langle f_1(t), f_2(t) \rangle$  denotes an operation that plays the same role as the scalar product of two functions in calculating the spectra, the functions describing which take real or complex values.

Specifically, in (30), one can use, for example, spectra calculated in Galois fields in accordance with the technique [20], [21]. The adequacy of the proposed approach to the use of models of signals through the elements of rings that decompose into sums of ideals can be additionally demonstrated using the matrix

representation of the elements of the rings used. Consider a particular case of the ring constructed above over the field  $GF(5)$ .

Let's compose the product of its two elements according to the usual rules for operating with complex numbers (recall that the additional root of the reduced equation is interpreted as a logical imaginary unit):

$$C = AB = (A_1 + iA_2)(B_1 + iB_2) = A_1B_1 - A_2B_2 + i(A_2B_1 + A_1B_2) \tag{31}$$

consequently,

$$C_1 = A_1B_1 - A_2B_2, C_2 = A_2B_1 + A_1B_2 \tag{32}$$

based on (32), each element of  $A$  can be associated with a matrix defined by the next formula as (33).

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} A_1 & -A_2 \\ A_2 & A_1 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \tag{33}$$

In particular, the following matrices correspond to the unit and logical imaginary unit:

$$1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{34}$$

consequently, for idempotent elements of the ring, the representation in (35) and (36).

$$e_1 = -2 + i \leftrightarrow \hat{E}_1 = \begin{pmatrix} -2 & -1 \\ 1 & -2 \end{pmatrix} \tag{35}$$

$$e_2 = -2 - i \leftrightarrow \hat{E}_2 = \begin{pmatrix} -2 & 1 \\ -1 & -2 \end{pmatrix} \tag{36}$$

Is valid, where all elements of the matrices belong to  $GF(5)$ . It can be shown by direct calculation that matrices (35) and (36) annihilate each other:

$$\begin{pmatrix} -2 & -1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} -2 \cdot (-2) - 1 \cdot (-1) & -2 \cdot 1 - 1 \cdot (-2) \\ 1 \cdot (-2) - 1 \cdot (-2) & 1 \cdot 1 - 2 \cdot (-2) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \tag{37}$$

in the same way, it is proved that these matrices are idempotent.

$$\hat{E}_i \hat{E}_i = \hat{E}_i, i = 1,2 \tag{38}$$

Consequently, in the ring of 2 by 2 matrices defined over the field  $GF(5)$ , one can single out a subset that is a finite ring decomposing into ideals generated by two mutually annihilating idempotent elements. All elements of this ring can be represented as (39).

$$\hat{A} = a_1 \begin{pmatrix} -2 & -1 \\ 1 & -2 \end{pmatrix} + a_2 \begin{pmatrix} -2 & 1 \\ -1 & -2 \end{pmatrix}, a_i \in GF(5) \tag{39}$$

This allows us to write the following expression for the model of a discrete signal that changes in the range of amplitudes corresponding to numbers in the number system (14) and has two digits.

$$\hat{U}(t) = u_1(t) \begin{pmatrix} -2 & -1 \\ 1 & -2 \end{pmatrix} + u_2(t) \begin{pmatrix} -2 & 1 \\ -1 & -2 \end{pmatrix} \tag{40}$$

In (41) can also be considered as a special case of the general representation of a digital signal through a function that takes values in a commutative ring that decomposes into ideals. A similar matrix representation also exists for the case when a function that is a signal model takes a value in the Galois field  $GF(5^2)$ . It should be emphasized that the number of elements corresponding to the used matrix representation differs from the number  $5^4$ , which is equal to the total number of  $2 \times 2$  matrices over the field  $GF(5)$ . This is due to the fact that matrices are used precisely as a representation of specific elements of the ring, i.e., from their complete set, only those are selected that display the properties of the elements of the ring under consideration. More broadly, it can be argued that there is a fairly wide choice of signal models in which, instead of a function that takes values corresponding to a certain set of discrete levels, functions that take values corresponding to a certain set



of matrices are considered. Such a representation can also be interpreted as an operator representation of a signal, since it is always possible to establish a one-to-one correspondence between matrices and operators.

Signal models of this kind, first of all, can find application in systems where classical methods of digital signal processing are combined with processing based on neural networks [35], [36]. Neural networks currently used for this purpose de facto use binary logic, but this is not required. Moreover, as shown in [13], [14], there are quite definite prerequisites for switching to neural networks using multivalued logic. In the cited works, it was also shown that there is a very close relationship between algorithms that de facto use neural networks and algorithms for error-correcting coding.

From this point of view, the operator (matrix) representation of the form (40) is also of interest. Indeed, the classical methods of error-correcting coding [37] use the factor of redundant information. Instead of a sequence containing a certain number of characters, a sequence containing more characters is used, which allows you to identify or eliminate the error. The transition to a signal model in a form similar to (40) also de facto implies the introduction of redundant information. In particular, the set of 2 by 2 matrices over the Galois field  $GF(5)$  contains  $5^4$  elements, while the field (or ring) that is mapped to this set contains  $5^2$  elements.

#### 4. CONCLUSION

Accordingly, in this paper, it is shown that a variety of algebraic structures can be used for digital signal processing, for example, Galois fields obtained by the method of algebraic extensions, as well as algebraic rings containing zero divisors. The possibility of their use is determined by the fact that for a finite range of amplitude variation, the number of prescriptive signal levels is finite and each of these levels can be assigned a field or ring element. Accordingly, the signal model becomes a function of time that takes values in an algebraic field or an algebraic ring. All of these structures have a matrix representation, but their properties are different, which allows them to be used for different purposes. So, algebraic rings containing zero divisors can be used for those digital processing methods in which it is required to operate with the digits of a number separately. Such rings can be constructed by a modernized method of algebraic extensions, in which a "logical unit" is used as an analogue of a primitive element, which is an additional formal root of a solvable equation.




#### REFERENCES

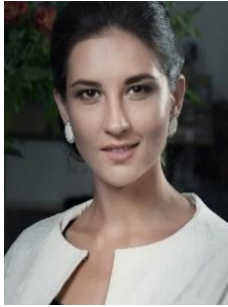
- [1] D. Shah and T. Shah, "Binary Galois field extensions dependent multimedia data security scheme," *Microprocessors and Microsystems*, vol. 77, p. 103181, 2020, doi: 10.1016/j.micpro.2020.103181.
- [2] T. Pruss, P. Kalla, and F. Enescu, "Equivalence verification of large Galois field arithmetic circuits using word-level abstraction via Gröbner bases," *DAC '14: Proceedings of the 51st Annual Design Automation Conference*, 2014, pp. 1-6, doi: 10.1145/2593069.2593134.
- [3] H. P. Thi and H. Lee, "Basic-set trellis min-max decoder architecture for nonbinary LDPC codes with high-order Galois fields," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 3, pp. 496-507, 2018, doi: 10.1109/TVLSI.2017.2775646.
- [4] H. P. Thi, C. D. The, N. P. Xuan, H. D. Tuan, and H. Lee, "Simplified variable node unit architecture for nonbinary LDPC decoder," *2019 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, 2019, pp. 213-216. doi: 10.1109/APCCAS47518.2019.8953111.
- [5] T. Liu and X. Chen, "Deep learning-based belief propagation algorithm over non-binary finite fields," *2020 International Conference on Wireless Communications and Signal Processing (WCSP)*, 2020, pp. 164-169. doi: 10.1109/WCSP49889.2020.9299875.
- [6] P. Liu, Z. Pan, and J. Lei, "Parameter identification of reed-solomon codes based on probability statistics and Galois field Fourier transform," *IEEE Access*, vol. 7, pp. 33619-33630, 2019, doi: 10.1109/ACCESS.2019.2904718.
- [7] L. Tang, Q. Huang, Z. Wang, and Z. Xiong, "Low-complexity encoding of binary quasi-cyclic codes based on Galois Fourier transform," *2013 IEEE International Symposium on Information Theory*, 2013, pp. 131-135, doi: 10.1109/ISIT.2013.6620202.
- [8] M. Poolakkaparambil, J. Mathew, A. M. Jabir, and S. P. Mohanty, "An investigation of concurrent error detection over binary Galois fields in CNTFET and QCA technologies," *2012 IEEE Computer Society Annual Symposium on VLSI*, 2012, pp. 141-146, doi: 10.1109/ISVLSI.2012.57.
- [9] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano, "Entanglement-assisted quantum error-correcting codes over arbitrary finite fields," *Quantum Inf Process*, vol. 18, no. 4, p. 116, 2019, doi: 10.1007/s11128-019-2234-5.
- [10] S. Shivashanka, M. Kudari, and P. S. Hiremath, "A Galois field-based texture representation for face recognition," *International Journal of Applied Engineering Research*, vol. 13, no. 18, pp. 13460-13465, 2018.
- [11] I. Moldakhan, D. Matrassulova, D. Shaltykova, and I. Suleimenov, "Some advantages of non-binary Galois fields for digital signal processing," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 23, no. 2, pp. 871-878, 2021, doi: 10.11591/ijeecs.v23.i2.pp871-878.
- [12] Y. S. Vitulyova, A. S. Bakirov, D. B. Shaltykova, and I. E. Suleimenov, "Prerequisites for the analysis of the neural networks functioning in terms of projective geometry," *IOP Conference Series: Materials Science and Engineering*, vol. 946, no. 1, p. 012001, 2020, doi: 10.1088/1757-899X/946/1/012001.
- [13] A. Bakirov and I. Suleimenov, "On the possibility of implementing artificial intelligence systems based on error-correcting code algorithms," *Journal of Theoretical and Applied Information Technology*, vol. 99, no. 1, pp. 83-99, 2021.
- [14] I. E. Suleimenov, A. S. Bakirov, D. K. Matrassulova, "A technique for analyzing neural networks in terms of ternary logic," *Journal of Theoretical and Applied Information Technology*, vol. 99, no. 11, pp. 2537-2553, 2021.




- [15] M. H. Rahmani, F. Almasganj, and S. A. Seyyedsalehi, "Audio-visual feature fusion via deep neural networks for automatic speech recognition," *Digital Signal Processing*, vol. 82, pp. 54-63, 2018, doi: 10.1016/j.dsp.2018.06.004.
- [16] F. N. Khan *et al.*, "Joint OSNR monitoring and modulation format identification in digital coherent receivers using deep neural networks," *Optics Express*, vol. 25, no. 15, p. 17767, 2017, doi: 10.1364/OE.25.017767.
- [17] A. Karpenko and N. Tomova, "Bochvar's three-valued logic and literal paralogics: their lattice and functional equivalence," *Logic and Logical Philosophy*, vol. 26, no. 2, pp. 207-235, 2017, doi: 10.12775/LLP.2016.029.
- [18] A. Schumann, "Logical determinacy versus logical contingency. the case of Łukasiewicz's three-valued logic," *Studia Humana*, vol. 8, no. 2, pp. 8-15, 2019, doi: 10.2478/sh-2019-0012.
- [19] K. Kobashi, R. Hayakawa, T. Chikyow, and Y. Wakayama, "Multi-valued logic circuits based on organic anti-ambipolar transistors," *Nano Letters*, vol. 18, no. 7, pp. 4355-4359, 2018, doi: 10.1021/acs.nanolett.8b01357.
- [20] S. A. Hosseini and S. Etezadi, "A novel very low-complexity multi-valued logic comparator in nanoelectronics," *Circuits, Systems, and Signal Processing*, vol. 39, no. 1, pp. 223-244, 2020, doi: 10.1007/s00034-019-01158-2.
- [21] H. Wu, L. He, X. Li, Y. Bai, and M. Zhang, "Design of AB2 in Galois fields based on multiple-valued logic," *Journal of Beijing Institute of Technology*, vol. 28, no. 4, pp. 764-769, 2019, doi: 10.15918/j.jbit1004-0579.18160.
- [22] A. Kuchansky, A. Biloshchytskyi, Y. Andrashko, S. Biloshchytska, Y. Shabala, and O. Myronov, "Development of adaptive combined models for predicting time series based on similarity identification," *Eastern-European Journal of Enterprise Technologies*, vol. 1, no. 4 (91), pp. 32-42, 2018, doi: 10.15587/1729-4061.2018.121620.
- [23] E. S. Vitulyova, D. K. Matrassulova, and I. E. Suleimenov, "New application of non-binary Galois fields Fourier transform: digital analog of convolution theorem," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 23, no. 3, pp. 1718-1726, 2021, doi: 10.11591/ijeecs.v23.i3.pp1718-1726.
- [24] Y. Lu and Y. Desmedt, "Walsh transforms and cryptographic applications in bias computing," *Cryptography and Communications*, vol. 8, no. 3, pp. 435-453, 2015, doi: 10.1007/s12095-015-0155-4.
- [25] D. E. Dutkay and G. Picioroaga, "Generalized Walsh bases and applications," *Acta Applicandae Mathematicae*, vol. 133, no. 1, pp. 1-18, 2013, doi: 10.1007/s10440-013-9856-x.
- [26] J. Irion and N. Saito, "The generalized Haar-Walsh transform," *2014 IEEE Workshop on Statistical Signal Processing (SSP)*, 2014, pp. 472-475, doi: 10.1109/SSP.2014.6884678.
- [27] A. Domínguez "A history of the convolution operation [Retrospectroscope]," *IEEE pulse*, vol. 6, no. 1, pp. 38-49, 2015, doi: 10.1109/MPUL.2014.2366903.
- [28] H. Jagadeesh, R. Joshi, and M. Rao, "Group secret-key generation using Algebraic rings in wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1538-1553, 2021, doi: 10.1109/TVT.2021.3054031.
- [29] A. Razaq, I. Rasool, M. Ahmad, A. Yousaf, and S. Masood, "A novel Finite rings based Algebraic scheme of evolving secure s-boxes for images encryption," *Multimedia Tools and Applications*, 2021, doi: 10.1007/s11042-021-10587-8.
- [30] V. Markov, A. V. Mikhalev, and A. Nechaev, "Nonassociative Algebraic structures in cryptography and coding," *Fundamental and Applied Mathematics*, vol. 21, pp. 99-123, 2020, doi: 10.1007/s10958-020-04685-5.
- [31] I. E. Suleimenov, Y. S. Vitulyova, A. S. Bakirov, and O. A. Gabrielyan, "Artificial intelligence: what is it?," *ICCTA '20: Proceedings of the 2020 6th International Conference on Computer and Technology Applications*, 2020, pp. 22-25, doi: 10.1145/3397125.3397141.
- [32] Y. S. Vitulyova, A. S. Bakirov, S. T. Baipakbayeva, and I. E. Suleimenov, "Interpretation of the category of 'complex' in terms of dialectical positivism," *IOP Conference Series: Materials Science and Engineering*, vol. 946, no. 1, p. 012004, 2020, doi: 10.1088/1757-899X/946/1/012004.
- [33] I. E. Suleimenov, D. K. Matrassulova, I. Moldakhan, Y. S. Vitulyova, S. B. Kabdushev, and A. S. Bakirov, "Distributed memory of neural networks and the problem of the intelligence's essence," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 11, no. 1, pp. 510-520, 2022, doi: 10.11591/eei.v11i1.3463.
- [34] I. Suleimenov, A. Bakirov, and I. Moldakhan, "Formalization of ternary logic for application to digital signal processing," in *International Scientific Conference Energy Management of Municipal Facilities and Sustainable Energy Technologies EMMFT 2019. EMMFT 2019. Advances in Intelligent Systems and Computing*, V. Murgul and V. Pukhkal, Eds. Cham: Springer, 2021, pp. 26-35.
- [35] Y. Tu and Y. Lin, "Deep neural network compression technique towards efficient digital signal modulation recognition in edge device," *IEEE Access*, vol. 7, pp. 58113-58119, 2019, doi: 10.1109/ACCESS.2019.2913945.
- [36] M. Zahid and Z. Meng, "Recent advances in neural network techniques for channel equalization: a comprehensive survey," *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, 2018, pp. 178-182, doi: 10.1109/iCCECE.2018.8658818.
- [37] M.A. Belhamra and El. M. Soudi, "Error correcting network codes," *Computer Networks*, vol. 197, p. 108277, 2021, doi: 10.1016/j.comnet.2021.108277.

## BIOGRAPHIES OF AUTHORS






**Dinara Kutlimuratovna Matrassulova**    is PhD student of the Almaty University of Power Engineering and Telecommunications. In 2015 she received a bachelor's degree and in 2017 a master's degree in "Radio engineering, electronics and telecommunications" at the Almaty University of Power Engineering and Telecommunications. She works in the telecommunications company Kcell JCS, as a senior specialist in the field of fixed internet. Actively studies telecommunications, networks, artificial intelligence, neural networks, signal processing. She can be contacted at email: dinara.kutlimuratovna@gmail.com.






**Yelizaveta Sergeevna Vitulyova**    is PhD student at the Almaty University of Power Engineering and Telecommunications after Gumarbek Daukeyev (AUPET). She received her master's degree in 2016 with a degree in radio engineering and communications at the AUPET. From 2016 to present she worked at AUPET as a senior lecturer of the department of Radio engineering, electronics and telecommunications. At the moment she is engaged in research in the field of radio engineering, electronics and telecommunications in accordance with the topic of her PhD thesis "Post-industrial paradigm of development of infocommunication segment in the military-industrial complex of the Republic of Kazakhstan". She can be contacted at email: lizavita@list.ru.



**Sergey Vladimirovich Konshin**    is Candidate of technical sciences (PhD of technical sciences), associate professor of the Higher Attestation Commission of the Republic of Kazakhstan, professor of AUPET. Konshin S.V. has written more than 120 scientific and educational works. The title of "Kurmetti bailanysshy" (Honorable Telecommunication Engineer of Kazakhstan) Vice-rector for educational and methodical work (academic activity). In different years, concurrently conducted examinations as: Expert of the Agency of the Republic of Kazakhstan on Informatization and Communications; Expert of the Agency for the Regulation of Natural Monopolies of the Republic of Kazakhstan (telecommunications); Expert of the Ministry of Education and Science of the Republic of Kazakhstan (on informatization and telecommunications). He can be contacted at email: s.konshin@aes.kz.



**Ibragim Esenovich Suleimenov**    is Professor of the Crimean Federal University named after V.I. Vernadsky (until 2020 - Professor of the Almaty University of Energy and Communications). Graduated from the Physics Department of the Leningrad University named after A.A. Zhdanov in 1986; defended his thesis for the degree of candidate of physical and mathematical sciences in 1989 at the same university. In 2000, he defended his thesis for the degree of Doctor of Chemical Sciences at the Al-Farabi Kazakh National University. Academician of the National Engineering Academy of the Republic of Kazakhstan (since 2016), full professor (since 2018) according to the official certificate of the Ministry of Education and Science of the Republic of Kazakhstan. Actively develops interdisciplinary cooperation, including between natural science and humanities. He pays considerable attention to the interdisciplinary study of intelligence, both using mathematical models and at the level of philosophical interpretation. He can be contacted at email: esenych@yandex.kz.