Quasigroups and Related Systems **26** (2018), 109 – 120

Non-commutative finite associative algebras of 3-dimensional vectors

Dmitriy Moldovyan, Nicolai Moldovyan and Victor Shcherbacov

Abstract. Properties of the non-commutative finite associative algebras of 3-dimensional vectors are presented. An interesting feature of these algebras is mutual associativity of all modifications of the defined parameterized multiplication operation and existence of a large set of single-side unit elements. In the ordinary case one unique two-side unit element is connected with every element of the algebra, except the elements that are square roots of zero element. It is shown that the used method suites for defining finite non-commutative associative algebras of arbitrary dimension $m \geqslant 2$. The considered finite associative algebras are interesting for cryptographic applications.

1. Introduction

Finite non-commutative associative algebras (FNAAs) are interesting for applications in design of public-key cryptoschemes characterized in using hidden conjugacy search problem (called also discrete logarithm problem in hidden cyclic group) [2, 3, 6]. In literature there are considered different FNAAs defined over finite vector spaces with dimensions $m = 4, 6$, and 8. The main attention was paid to the case $m = 4$ that provides lower computational difficulty of multiplication operation in the FNAA while defining vector spaces over the same finite field $GF(p)$. Recently it has been introduced the 2-dimension FNAA [4].

In the present paper it is shown that the method for defining 2-dimension FNAA can be generalized and used to define m-dimensional FNAAs for an arbitrary value $m \geqslant 2$. Some properties of the FNAA relating to the case $m = 3$ are investigated. Other types of 3-dimension non-commutative algebras with associative multiplication operation are defined as well. All investigated FNAAs contain only local unit elements, therefore defining the discrete logarithm problem in a hidden group [2] on the base of such FNAAs has some peculiarities that are discussed in relation of cryptographic application of the considered finite algebras.

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: finite associative algebra, difficult problem, homomorphism, non-commutative group, non-commutative ring, public-key cryptoscheme.
The reported study was funded by Russian Foundation for Basic Research (project #18-07-00932).

2. Unit elements in 3-dimensional FNAA

Suppose $\mathbf{e}$, $\mathbf{i}$, and $\mathbf{j}$ are some formal basis vectors and $a, b, c \in GF(p)$, where prime $p \geqslant 3$, to be coordinates. Three-dimensional vectors are denoted as $a\mathbf{e}+b\mathbf{i}+c\mathbf{j}$ or as (a, b, c). Terms $\tau\mathbf{v}$, where $\tau \in GF(p)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \mathbf{j}\}$ are called components of the vector.

Addition of two vectors (a, b, c) and (x, y, z) is defined as addition of the corresponding coordinates, i.e., with the following formula $(a, b, c) + (x, y, z) = (a + x, b + y, c + z)$.

The multiplication operation in finite 3-dimensional vector space is defined with the formula

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) =$$
$$= ax(\mathbf{e}\circ\mathbf{e})+bx(\mathbf{i}\circ\mathbf{e})+cx(\mathbf{j}\circ\mathbf{e})+ay(\mathbf{e}\circ\mathbf{i})+by(\mathbf{i}\circ\mathbf{i})+cy(\mathbf{j}\circ\mathbf{i})+az(\mathbf{e}\circ\mathbf{j})+bz(\mathbf{i}\circ\mathbf{j})+cz(\mathbf{j}\circ\mathbf{j}),$$

where products of different pairs of formal basis vectors $\mathbf{e}$, $\mathbf{i}$, and $\mathbf{j}$ are to be replaced by some one-component vector in accordance with the basis-vector multiplication table (BVMT) shown in Table 1. The left basis vector defines the row and the right one defines the column. At the intersection of the row and column we have the value of the product of two formal basis vectors.

Table 1 defines non-commutative associative multiplication of the vectors $V = (a, b, c) = a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$ and $X = (x, y, z) = x\mathbf{e} + y\mathbf{i} + z\mathbf{j}$. The BVMT contains structural coefficients $\mu, \tau, \lambda \in GF(p)$ defining different modifications of the multiplication operation, i.e., the last is parameterized. The defined non-commutative multiplication operation is characterized in the mutual associativity of all its modifications, i.e., for the considered FNAA of 3-dimensional vectors the following statement is valid:

Proposition 1. *Suppose $\circ$ and $\star$ are two arbitrary modifications of the vector multiplication operation, which correspond to different triples of structural coefficients $(\mu_1, \tau_1, \lambda_1)$ and $(\mu_2, \tau_2, \lambda_2) \neq (\mu_1, \tau_1, \lambda_1)$. Then for arbitrary three vectors A, B, and C the following formula $(A \circ B) \star C = A \circ (B \star C)$ holds.*

Proof of this statement consists in straightforward using of the definition of the multiplication operation and Table 1.

Table 1: The BVMT defining associative multiplication in the finite vector space of the dimension $m = 3$ ($\mu \neq 0$; $\tau \neq 0$; $\lambda \neq 0$)

$\circ$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$
$\mathbf{e}$	$\mu\mathbf{e}$	$\tau\mathbf{e}$	$\lambda\mathbf{e}$
$\mathbf{i}$	$\mu\mathbf{i}$	$\tau\mathbf{i}$	$\lambda\mathbf{i}$
$\mathbf{j}$	$\mu\mathbf{j}$	$\tau\mathbf{j}$	$\lambda\mathbf{j}$

Structure of Table 1 is similar to structure of the BVMT used for defining the 2-dimension FNAA [4] (see Table 2), i.e., every cell in every fixed row contains the

same formal basis vector and every cell in every fixed column contains the same structural coefficient.

Table 2: The basis-vector multiplication table for the case $m = 2$ [4]

$\circ$	$\mathbf{e}$	$\mathbf{i}$
$\mathbf{e}$	$\mu\mathbf{e}$	$\tau\mathbf{e}$
$\mathbf{i}$	$\mu\mathbf{i}$	$\tau\mathbf{i}$

Finding the right-side unit elements in the considered 3-dimension FNAA is connected with solving the vector equation

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) = a\mathbf{e} + b\mathbf{i} + c\mathbf{j}, \tag{1}$$

where $V = a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$ is an arbitrary vector and $X = x\mathbf{e} + y\mathbf{i} + z\mathbf{j}$ is the unknown one.

Equation (1) can be reduced to the following system of three linear equations:

$$\begin{cases} \mu ax + \tau ay + \lambda az = a, \\ \mu bx + \tau by + \lambda bz = b, \\ \mu cx + \tau cy + \lambda cz = c. \end{cases} \tag{2}$$

Solution of the system (2) defines the following set of the local right-side unit elements

$$E_r = (x,\ y,\ z) = \left(x,\ y,\ \lambda^{-1}(1 - \mu x - \tau y)\right), \tag{3}$$

where x and y take on all possible values in $GF(p)$. Every value E_r from set (3) represents a global right-side unit element acting on all 3-dimensional vectors of the considered FNAA.

The vector equation

$$(x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) \circ (a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) = a\mathbf{e} + b\mathbf{i} + c\mathbf{j} \tag{4}$$

that defines the left-side unit elements can be reduced to the following system of three linear equations:

$$\begin{cases} (\mu a + \tau b + \lambda c)x = a, \\ (\mu a + \tau b + \lambda c)y = b, \\ (\mu a + \tau b + \lambda c)z = c. \end{cases} \tag{5}$$

Solving the system (5) one gets the following statement.

Proposition 2. *To every vector $V = (a, b, c)$, such that $\mu a + \tau b + \lambda c \neq 0$, there corresponds a unique local left-side unit vector*

$$E_l = (x, y, z) = \left(\frac{a}{\mu a + \tau b + \lambda c}, \frac{b}{\mu a + \tau b + \lambda c}, \frac{c}{\mu a + \tau b + \lambda c}\right). \tag{6}$$

It is easy to show that the local left-side unit element is contained in the set (3), i.e., it is equal to the local bi-side unit of the vector V.

Let us consider the sequence $V, V^2, \ldots, V^i$ (for $i = 1, 2, 3, \ldots$). If the vector V is not a zero-divisor relatively some of its power (zero-divisors are considered below, where it is shown that vectors satisfying the condition $a\mu + b\tau + c\lambda \neq 0$ are not zero-divisors), then for some two integers h and $k > h$ we have $V^k = V^h$ and $V^k = V^{k-h} \circ V^h = V^h \circ V^{k-h} = V^{k-h} \circ V^h$. Thus, the mentioned sequence is periodic and for some integer ω (that can be called order of the vector V) the equality $V^\omega = V^{k-h} = E'$ holds, where E' is a bi-side local unit such that $V^i \circ E' = E' \circ V^i = V^i$ holds for all integers i.

Thus, taking into account that the local right-side unit element corresponding to the vector V is a unique one, we can conclude the following:

Proposition 3. *Suppose $V = (a, b, c)$ is a vector such that $a\mu + b\tau + c\lambda \neq 0$. Then the vector E_r described with the formula (6) acts as a unique bi-side local unit element E' in the subset $\{V, V^2, \ldots, V^i, \ldots\}$, and the value E' can be computed as some power of V.*

Thus, the element E_l defined by the vector $V = (a, b, c)$ acts on vectors $V, V^2, \ldots, V^i$ as a local bi-side unit for an arbitrary integer $i \geqslant 1$.

Example. The last fact can be illustrated by the following computations using the values

$p = 99161514659781804607 1879$, $\mu = 3176589117$, $\tau = 1$, $\lambda = 8766554$, and

$$N = (a, b, c) = (8654389874321123, 35172879913271, 185758463523115).$$

Computation of the value E' as $E' = N^{p^2-1}$ and using formula (6) from Statement 2 gives the same result

$$E' = (73697875749428423568471, 45051144211088924326 1952, 50136619611775872069 0571).$$

Finding the right-side zero-divisors for the vector $V = (a, b, c)$ is connected with consideration of the vector equation

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) = (0, 0, 0)$$

that can be reduced to the following system of equations:

$$\begin{cases} (\mu x + \tau y + \lambda z)a = 0, \\ (\mu x + \tau y + \lambda z)b = 0, \\ (\mu x + \tau y + \lambda z)c = 0. \end{cases} \tag{7}$$

Solution of system (7) defines the following set of the right-side zero-divisors

$$D_r = (x,\ y,\ z) = \left(x,\ y,\ \lambda^{-1}(-\mu x - \tau y)\right), \tag{8}$$

where x and y take on all values in $GF(p)$. Every value D_r from set (8) represents a global right-side zero-divisor acting on all 3-dimensional vectors of the considered FNAA. Formula (8) describes the vectors to which no left-side unit corresponds. Below it is shown that formula (8) describes square roots of zero vector $(0,0,0)$.

The vector equation

$$(x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) \circ (a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) = (0,0,0)$$

that defines the left-side zero-divisor can be reduced to the following system of three linear equations:

$$\begin{cases} (\mu a + \tau b + \lambda c)x = 0, \\ (\mu a + \tau b + \lambda c)y = 0, \\ (\mu a + \tau b + \lambda c)z = 0. \end{cases} \tag{9}$$

Solving system (9) one gets the following statement.

Proposition 4. *To every vector $V = (a,b,c)$ such that $\mu a + \tau b + \lambda c \neq 0$, there corresponds no left-side zero-divisor, except $(0,0,0)$. Every vector of the considered FNAA acts on vectors $V' = (a',b',c')$, such that $\mu a' + \tau b' + \lambda c' = 0$, as a left-side zero-divisor.*

Consideration of the vector equation

$$D \circ D = (0,0,0),$$

where $D = (x,y,z)$ is unknown, leads to solving the system

$$\begin{cases} (\mu x + \tau y + \lambda z)x = 0, \\ (\mu x + \tau y + \lambda z)y = 0, \\ (\mu x + \tau y + \lambda z)z = 0, \end{cases}$$

that defines the following set of square roots of the zero vector $(0,0,0)$:

$$D = \left(x,\ y,\ -\lambda^{-1}(\mu x + \tau y)\right),$$

where x and y take on all values in $GF(p)$. Thus, vectors $V = (a',b',c')$, coordinates of which satisfy condition $\mu a' + \tau b' + \lambda c' = 0$, are square roots of zero.

Taking into account Proposition 4 and finiteness of the considered vector space it is easy to see that the vector V, such that $\mu a + \tau b + \lambda c \neq 0$, generates periodic sequence $V, V^2, \ldots, V^i$, where $i = 1,2,3,\ldots$, and for some value $i = \omega$ we have $V^\omega = E'$, where $E' = E_l$ is the local bi-side unit determined by coordinates of the vector V in accordance with the formula (6) from Proposition 2.

Like in the case of FNAA of two-dimensional vectors, non-commutative associative multiplication of the 3-dimensional vectors can be defined alternatively with Table 3 that represents transposition of the Table 1. It is easy to see that Table 3 defines the FNAA having the properties very close to the properties of the

considered FNAA of 3-dimensional vectors. Indeed, suppose V and W to be arbitrary 3-dimensional vectors and $\circ$ and $\star$ to be the vector multiplication operations defined with Table 1 and Table 3 respectively. Then

$$V \circ W = W \star V.$$

The proof of this fact consists in straightforward using of the definition of the multiplication operation and the indicated two BVMTs.

Table 3: Alternative BVMT defining associative multiplication in the finite vector space of the dimension $m = 3$

$\circ$	**e**	**i**	**j**
e	μ**e**	μ**i**	μ**j**
i	τ**e**	τ**i**	τ**j**
j	λ**e**	λ**i**	λ**j**

4. Particular variants of 3-dimensional FNAAs

Except Tables 1 and 3, other particular BVMTs defining 3-dimension FNAAs are possible, which can be attributed to the type of unbalanced BVMTs. If the BVMT is such that while multiplying two input vectors the **e**-coordinate does not influence the **i**- and **j**-coordinates of the output vector, then the BVMT is called **e**-unbalanced. Similar definitions can be formulated for **i**- and **j**-unbalanced BVMTs. In such sense the BVMTs presented by Table 1 and 3 can be called balanced. Four different unbalanced BVMTs and formulas for describing local unit elements (left-side E_l, right-side E_r, and bi-side E' ones) for the vector $V = (a, b, c)$ relating to the FNAAs defined with these BVMTs, are presented bellow.

Table 4: The **j**-unbalanced BVMT

$\circ$	**e**	**i**	**j**
e	μ**e**	μ**i**	**0**
i	τ**e**	τ**i**	**0**
j	μ**j**	τ**j**	**0**

Case of Table 4. The set of the left-side local unit elements of the vector $V = (a, b, c)$ such that $\tau \neq 0$ and $\mu a + \tau b \neq 0$, is described as follows:

$$E_l = \left(h, \frac{1 - \mu h}{\tau}, \frac{c}{\mu a + \tau b}\right),$$

where $h = 0, 1, \ldots, p-1$.

The set of the right-side local units of the vector V is described as follows (where $h = 0, 1, \ldots, p-1$):

$$E_r = \left(\frac{a}{\mu a + \tau b}, \frac{b}{\mu a + \tau b}, h \right).$$

For the vector V there exists only one local bi-side unit:

$$E' = \left(\frac{a}{\mu a + \tau b}, \frac{b}{\mu a + \tau b}, \frac{c}{\mu a + \tau b} \right).$$

Table 5: The **e**-unbalanced BVMT

$\circ$	**e**	**i**	**j**
e	**0**	**0**	**0**
i	μ**e**	μ**i**	τ**i**
j	τ**e**	μ**j**	τ**j**

Case of Table 5. The set of the left-side local units corresponding to the vector $V = (a, b, c)$ such that $\mu b + \tau c \neq 0$, is described by the following formula (where $h = 0, 1, \ldots, p-1$):

$$E_l = \left(h, \frac{b}{\mu b + \tau c}, \frac{c}{\mu b + \tau c} \right).$$

The set of the right-side local units of the vector V is described by the following formula ($h = 0, 1, \ldots, p-1$):

$$E_r = \left(\frac{a}{\mu b + \tau c}, h, \frac{1}{\tau} - \frac{\mu}{\tau} h \right).$$

The single local bi-side unit of the vector V is

$$E' = \left(\frac{a}{\mu b + \tau c}, \frac{b}{\mu b + \tau c}, \frac{c}{\mu b + \tau c} \right).$$

Table 6: The **i**-unbalanced BVMT

$\circ$	**e**	**i**	**j**
e	**e**	**i**	**j**
i	**0**	**0**	**0**
j	**j**	**i**	**e**

Case of Table 6. The set of the left-side local units corresponding to the vector $V = (a, b, c)$ such that $a + b \neq 0$, is described by the following formula (where $h = 0, 1, \ldots, p-1$):

$$E_l = (1, h, 0)\,.$$

There exists only one local right-side unit E_r corresponding to the vector $V = (a, b, c)$, which is equal to the local bi-side unit E':

$$E_r = E' = \left(1, \frac{b}{a+b}, 0\right).$$

Table 7: Alternative **i**-unbalanced BVMT

$\circ$	**e**	**i**	**j**
e	μ**e**	μ**i**	τ**e**
i	μ**i**	**0**	τ**i**
j	μ**j**	τ**i**	τ**j**

Case of Table 7. The set of the right-side local units of the vector $V = (a, b, c)$, where $\tau \neq 0$ and $\mu a + \tau c \neq 0$, is described as follows (where $h = 0, 1, \ldots, p-1$):

$$E_l = \left(h, 0, \frac{1}{\tau} - \frac{\mu}{\tau}h\right).$$

There exists only one local left-side unit E_l for the vector V, which is equal to the local bi-side unit E':

$$E_r = E' = \left(\frac{a}{\mu a + \tau c}, 0, \frac{c}{\mu a + \tau c}\right).$$

We note that Tables 1 and 3 define some new unbalanced BMVTs, when one of structural coefficients is equal to zero. For FNAAs defined with every one of the considered unbalanced BVMTs (see Tables 4 to 7) Proposition 1 is not valid. However Proposition 1 is valid for FNAAs defined by unbalanced BVMTs obtained by taking one structural coefficient equal to zero in Tables 1 and 3.

5. Discussion and potential application

One of the interesting properties of the investigated FNAAs is mutual associativity of all modifications of the parameterized non-commutative multiplication operation.

In the literature, parameterized commutative multiplication operation for the cases $m = 2$ and $m = 3$ [5] does not possess such property. Like in BVMTs used

in [4] for defining 2-dimensional FNAAs, each of Tables 1 and 3 represents m repetitions of the sequence of m basis vectors which are written as strings or as columns of the table. Every cell of the given column in Table 1 and every cell of the given row in Table 3 contains the same structural coefficient. In general case coefficients relating to different columns in Table 1 and different rows in Table 3 are different.

It is easy to check that BVMT with such structure defines associative non-commutative multiplication in finite vector space having arbitrary dimension m. We have preliminary considered the properties of the FNAA of the vectors having dimensions $m = 4, 5, 6$. Properties of such FNAAs resemble the results described in Sections 2 and 3, including mutual associativity of the modifications of the multiplication operation parameterized with different sets of structural coefficients. Detailed consideration of the cases $m > 3$ represents interest for independent research. One can expect that for $m > 3$ there are significantly more variants of different BVMT defining associative non-commutative multiplication operation. An example relating to the case $m = 4$ is presented in [2], though the modifications of the parameterized multiplication operation of that example are not mutually associative.

The FNAA considered in [2] represents a finite non-commutative ring with (global) bi-side unit. One can expect that in the cases $m \geq 4$, when designing different types of BVMTs, it is possible to construct FNAAs having qualitatively different properties.

During execution of the described research we have performed many different computational experiments to check practically the results of analytic consideration. Only results of computing local bi-side unit elements as an integer power of the corresponding vectors have been presented in the paper, since such computational experiment is more interesting due to its indirect connection with the results of analytic consideration of the systems of linear equations defining properties of the multiplication operation.

In the case of FNAA defined with balanced BVMT described by Table 1 one can remark the following. If some vector $V = (a, b, c)$ satisfies the condition $\mu a + \tau b + \lambda c \neq 0$, then for arbitrary integer i the vector V^i can not act as the right zero-divisor relatively all 3-dimensional vectors, except $(0, 0, 0)$.

Indeed, assumption $D \circ V^i = (0, 0, 0)$ leads to contradiction with Proposition 4. Therefore the sequence $V, V^2, \ldots V^i, \ldots$, does not contain the vector $(0, 0, 0)$ and is periodic. The last leads to conclusion that such sequence contains local bi-side unit element E' corresponding to V, i.e., for some integer ω we have $V^\omega = E'$. Thus, the subset $\left\{V, V^2, \ldots V^\omega\right\}$ of 3-dimensional vectors represents a cyclic finite group contained in the FNAA.

Mutual associativity of the multiplication modifications represent interest as cryptographic primitive for designing secret key cryptoschemes in which operations are used as key elements.

Regarding the public-key cryptoschemes it is interesting to consider designs based on computational complexity of the hidden conjugacy search problem (that

can be called alternatively the discrete logarithm problem in a hidden cyclic subgroup) in FNAAs of 3-dimensional vectors.

Suppose W to be some vector generating commutative finite multiplicative group having sufficiently large order ω, in which the bi-side local unit element E'' connected with W is the unit of such group.

One can define the following homomorphism $\varphi_{W,t}$ over the subset of elements $\{V_{E''}\}$ of the FNAA which are described as follows $V_{E''} = V \circ E''$, where V takes on all values in the FNAA.

Like standard automorphisms ψ_U of some finite non-commutative ring, which are described by formula $\psi_U(V) = U^{-1} \circ V \circ U$, where U is an invertible element of the ring and V takes on all values in the ring, one can define the homomorphism $\varphi_{W,t}$ as follows:

$$\varphi_{W,t}\left(V_{E''}\right) = W^{\omega-t} \circ V_{E''} \circ W^{t}.$$

To construct public-key cryptoschemes, like that described in [2, 3], one can select some vector G generating a cyclic group (that is a subset of elements of the FNAA) having sufficiently large order g, which satisfies the condition $G \circ W \neq W \circ G$ and use the formula

$$Y = W^{\omega-t} \circ (G \circ E'')^{x} \circ W^{t},$$

where Y is public key and the pair of numbers (t, x) is private key (the integers $t < \omega$ and $x < \omega$ are to be selected at random).

Suppose Y_A and Y_B are public keys of the users A and B respectively. Then they are able to generate a common secret key

$$Z_{AB} = W^{\omega-t_A} \circ (Y_B)^{x_A} \circ W^{t_B} = W^{\omega-t_B} \circ (Y_A)^{x_B} \circ W^{t_B},$$

where (t_A, x_A) and (t_B, x_B) are private keys of the users A and B respectively.

It should be noted that the used balanced BVMTs for defining 3-dimensional FNAAs are particular cases of the BVMTs for defining m-dimensional FNAAs, which are presented as Tables 8 and 9, where $\mu_i \in GF(p)$, $(i = 1, 2, \ldots, m)$ are structural coefficients.

Proposition 5. *The multiplication of the m-dimensional vectors*

$$V = (v_1, v_2, \ldots, v_i, \ldots, v_m) = v_1\mathbf{e}_1 + v_2\mathbf{e}_2 + \ldots + v_i\mathbf{e}_i + \ldots + v_m\mathbf{e}_m$$

for an arbitrary integer $m \geqslant 2$, defined by Tables 8 and 9, is an associative operation.

Table 8: The BVMT for defining m-dimensional FNAA

$\circ$	$\mathbf{e_1}$	$\mathbf{e_2}$	$\ldots$	$\mathbf{e_m}$
$\mathbf{e_1}$	$\mu_1\mathbf{e}_1$	$\mu_2\mathbf{e}_1$	$\ldots$	$\mu_m\mathbf{e_1}$
$\mathbf{e_2}$	$\mu_1\mathbf{e}_2$	$\mu_2\mathbf{e}_2$	$\ldots$	$\mu_m\mathbf{e_2}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$\mathbf{e_m}$	$\mu_1\mathbf{e}_m$	$\mu_2\mathbf{e}_m$	$\ldots$	$\mu_m\mathbf{e}_m$

Table 9: Alternative BVMT for defining m-dimensional FNAA

$\circ$	$\mathbf{e_1}$	$\mathbf{e_2}$	...	$\mathbf{e}_m$
$\mathbf{e_1}$	$\mu_1\mathbf{e}_1$	$\mu_1\mathbf{e}_2$	...	$\mu_1\mathbf{e}_m$
$\mathbf{e_2}$	$\mu_2\mathbf{e}_1$	$\mu_2\mathbf{e}_2$	...	$\mu_2\mathbf{e}_m$
...	...	...	...	...
$\mathbf{e}_m$	$\mu_m\mathbf{e}_1$	$\mu_m\mathbf{e}_2$	...	$\mu_m\mathbf{e}_m$

To prove the last statement it is sufficient to show that for arbitrary ordered set of three basis vectors $\mathbf{e}_i$, $\mathbf{e}_j$ and $\mathbf{e}_k$ the following formula holds:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k)\,.$$

In the case of Table 8 we have

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = (\mu_j\mathbf{e}_i) \circ \mathbf{e}_k = \mu_j\mu_k\mathbf{e}_i$$

and

$$\mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ (\mu_k\mathbf{e}_j) = \mu_j\mu_k\mathbf{e}_i.$$

In the case of Table 9 we have

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = (\mu_i\mathbf{e}_j) \circ \mathbf{e}_k = \mu_i\mu_j\mathbf{e}_k$$

and

$$\mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ (\mu_j\mathbf{e}_k) = \mu_i\mu_j\mathbf{e}_k.$$

5. Conclusion

In the present paper, the 3-dimensional FNAAs are introduced. The used BVMTs define the parameterized non-commutative multiplication operation in finite space of 3-dimensional vectors. They have sufficiently simple structure and represent particular cases of two general-type BVMTs (see Tables 8 and 9) that can be used for defining FNAAs of arbitrary dimension $m \geqslant 2$.

An interesting feature of the considered FNAAs is existence of different sets of elements that act (on some other sets of elements) as the single-side unit elements. Except the elements that are square roots of zero, to every element W of the FNAAs corresponds one two-side unit E''_W. Usually, to different elements correspond different two-side units and therefore the lasts are called local.

For the given local unit E''_W over the subset $\{V \circ E''_W\}$ a homomorphism can be defined and used for constructing public-key cryptoschemes based on computational difficulty of the discrete logarithm problem in a hidden cyclic group of the FNAAs.

Future research in the context of the concerned topic is connected with study of the m-dimensional FNAAs for the cases $m \geqslant 4$, which are defined by Tables 8 and 9. It is also interesting to consider other variants of BVMTs for defining 3-dimensional FNAAs and to investigate the properties of the lasts.

References

[1] **A.S. Kuzmin, V.T. Markov, A.A. Mikhalev, A.V. Mikhalev, A.A. Nechaev**, *Crypto-graphic algorithms on groups and algebras*, J. Math. Sci. **223** (2017), 629 – 641.

[2] **D.N. Moldovyan**, *Non-commutative finite groups as primitive of public-key cryptoschemes*, Quasigroups and Related Systems **18** (2010), 165 – 176.

[3] **D.N. Moldovyan, N.A. Moldovyan**, *Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms*, Quasigroups Related Systems **18** (2010), 177 – 186.

[4] **A.A. Moldovyan, N.A. Moldovyan, and V.A. Shcherbacov**, *Non-commutative finite associative algebras of 2-dimension vectors*, Computer Sci. J. Moldova **25** (2017), 344 – 356.

[5] **N.A. Moldovyan and P.A. Moldovyanu**, *Vector form of the finite fields* $GF(p^m)$, Bul. Acad. Ştiinţe Repub. Mold. Mat. **3** (2009), 57 – 63.

[6] **E. Sakalauskas, P. Tvarijonas, and A. Raulynaitis**, *Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level*, Informatica **18** (2007), 115 – 124.

Received March 29, 2018

D. Moldovyan
St. Petersburg Electrotechnical University "LETI"
Email: maa1305@yandex.ru

N.Moldovyan
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Email: nmold@mail.ru

V. Shcherbacov
Institute of Mathematics and Computer Science of the Academy of Sciences of Moldova
victor.scerbacov@math.md