Computer Science Journal of Moldova, vol.**25**, no.3(75), 2017

Non-commutative finite associative algebras of 2-dimensional vectors

Alexander Moldovyan, Nicolay Moldovyan, Victor Shcherbacov

Abstract

In this paper properties of the non-commutative finite associative algebra of two-dimensional vectors are presented. Interesting features of algebra are mutual associativity of all modifications of the defined parameterized multiplication operation and existing of a large set of single-side unit elements. In the ordinary case one unique two-side unit element is connected with each element of the algebra, except the elements that are square roots from zero element. There are also presented four different variants of defining commutative associative algebras of 2-dimension vectors. For the case of commutativity the algebra has common unit element for all its elements.

Keywords: finite algebra; ring; Galois field; vector; associative multiplication; parameterized multiplication; cryptoscheme

AMS: 16U60, 11G20, 11T71

1 Introduction

Finite non-commutative associative algebras (FNAA) are interesting for applications in the desin of the public-key cryptoschemes characterized in using the hidden conjugacy search problem (called also discrete logarithm problem in hidden commutative subgroup) [1]–[3]. In the literature there are considered different FNAA defined over the 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 the multiplication operation in the FNAA, while defining the vector spaces over the same finite field $GF(p)$.

In the present paper it is shown that the FNAA can be defined over the vector spaces of the dimensions less than 4. There are introduced two possible variants of defining the FNAA of two-dimensional vectors and investigated some properties of such FNAA. There are also described in brief four possible variants of defining the commutative associative algebras of two-dimensional vectors.

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

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

The multiplication of two vectors $a\mathbf{e} + b\mathbf{i}$ and $x\mathbf{e} + y\mathbf{i}$ is defined by the following formula

$$(a\mathbf{e} + b\mathbf{i}) \circ (x\mathbf{e} + y\mathbf{i}) = ax\mathbf{e} \circ \mathbf{e} + bx\mathbf{i} \circ \mathbf{e} + ay\mathbf{e} \circ \mathbf{i} + by\mathbf{ii},$$

where $\circ$ denotes the vector multiplication operation and each product of two basis vectors is to be replaced by some basis vector or by a one-component vector in accordance with the so called basis-vector multiplication table (BVMT) which defines associative (commutative and non-commutative) multiplication of the two-dimensional vectors. In the paper there are considered two variants of the BVMT presented in Table 1 (Section 2) and Table 2 (Section 3) for defining FNAA and four variants of the BVMT presented in Tables 3, 4, 5, and 6 (Section 4) for defining commutative finite algebras.

2 Algebra with unique local right-side unit elements

The multiplication of two-dimensional vectors defined by Table 1, where $\mu \neq 0$ and $\tau \neq 0$, is a parameterized operation, different modifications of which correspond to different pairs of values of the so called structural coefficients μ and τ. As compared with the case of

Table 1. The basis-vector multiplication table for the case $m = 2$

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

the commutative finite algebra of the 2-dimensional vectors [4], the defined non-commutative multiplication operation is characterized in the mutual associativity of all its modifications.

Statement 1. Suppose $\circ$ and $\star$ are two arbitrary modifications of the vector multiplication operation, which correspond to different pairs of structural coefficients (μ_1, τ_1) and $(\mu_2, \tau_2) \neq (\mu_1, \tau_1)$. 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 of straightforward calculations using the definition of the multiplication operation and Table 1.

To find the right unit element of the considered FNAA, one can solve the following vector equation

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

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

Equation (1) can be reduced to solving the following system of two linear equations in $GF(p)$:

$$\begin{cases} (a\mu + b\tau)x = a \\ (a\mu + b\tau)y = b. \end{cases} \tag{2}$$

In the case $a\mu + b\tau \neq 0$ this system has a unique solution

$$\begin{cases} x = \dfrac{a}{a\mu + b\tau} \\ y = \dfrac{b}{a\mu + b\tau}. \end{cases} \tag{3}$$

All vectors (a,b) such that $a\mu + b\tau \neq 0$ have only one right unit element. In the general case the right unit elements corresponding to different vectors are different, therefore these unit elements can be called local, since they act only in frame of some sufficiently restricted subset of the two-dimensional vectors. There does not exist global right unit element, i.e. right unit acting over the whole two-dimensional vector space. The following is evident:

Statement 2. Suppose $V = (a,b)$ be a vector such that $a\mu + b\tau \neq 0$. Then the vector

$$E_r = \left(\frac{a}{a\mu + b\tau}, \quad \frac{b}{a\mu + b\tau} \right) \tag{4}$$

acts as local right unit in the following subset of two-dimensional vectors $V, V^2, ..., V^i, ...$, where i is an arbitrary integer.

Let us consider the sequence $V, V^2, ..., V^i$ (for $i = 1, 2, 3, ...$). If the vector V is not a zero-divisor relatively some its power (zero-divisors are considered below and it is shown that vectors satisfying condition $a\mu + b\tau \neq 0$ are not zero-divisors), then for some two integers h and $k > h$ we have $V^k = V^h$ and $V^k = V^{k-h} \circ V^h = V^h \circ V^{k-h}$, i.e. the mentioned sequence is periodic and for some integer ω (that can be called order of the vector V) it holds that $V^\omega = E'$, where E' is 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 unit element corresponding to the vector V is unique one can conclude the following:

Statement 3. Suppose $V = (a,b)$ be a vector such that $a\mu + b\tau \neq 0$. Then the vector E_r described by formula (4) acts as a unique bi-side local unit element E' in the subset $\left\{V, V^2, ..., V^i, ...,\right\}$ and the value E' can be computed as some power of V.

The following computational example illustrates this fact: for $p = 16832914260232697023$ and $\mu = 276474637$; $\tau = 948576254546$ we have

$$\begin{aligned} &N = (a,b) = \\ &(17235252752952, 29124252511124). \end{aligned} \tag{5}$$

Computation of the value E' as $E' = N^{p-1}$ and by using formula (3)

gives the same result

$$E' = \\ (12597150130467515608, 9876457378547066970). \tag{6}$$

To find the left unit elements of the considered FNAA one can solve the following vector equation:

$$(x\mathbf{e} + y\mathbf{i}) \circ (a\mathbf{e} + b\mathbf{i}) = (a\mathbf{e} + b\mathbf{i}). \tag{7}$$

Equation (7) can be reduced to solving the following system of two linear equations in $GF(p)$:

$$\begin{cases} a\mu x + a\tau y = a \\ b\mu x + b\tau y = b. \end{cases} \tag{8}$$

The last system defines the following set of the left unit elements:

$$E_l = (x,\ y) = \left(x,\ \tau^{-1}(1-x)\right), \tag{9}$$

where x takes on all possible values in $GF(p)$. Each element of the last set acts on all elements of the considered FNAA as the left unit, i.e. elements of set (9) are global left unit elements. Substituting the value $x = a(a\mu + b\tau)^{-1}$ in (9) one can show that all local right units are contained in the set of the (global) left unit elements. This is in compliance with Statement 3.

Let us consider the question of existence of the right and left zero-divisors. The first case is connected with solving the vector equation

$$(a\mathbf{e} + b\mathbf{i}) \circ (x\mathbf{e} + y\mathbf{i}) = (0, 0), \tag{10}$$

where $V = (a\mathbf{e} + b\mathbf{i})$ is an arbitrary vector different from (0,0) and $X = (x\mathbf{e} + y\mathbf{i})$ is the unknown one.

Equation (10) can be reduced to solving the following system of two linear equations in $GF(p)$:

$$\begin{cases} (a\mu + b\tau)x = 0 \\ (a\mu + b\tau)y = 0. \end{cases} \tag{11}$$

In the case of the vectors V, the coordinates of which satisfy condition $a\mu + b\tau \neq 0$, this system has a unique solution $(x, y) = (0, 0)$ that represents zero of the considered FNAA. Each two-dimensional vector acts on the vectors V such that $a\mu + b\tau = 0$ as the right zero-divisor.

Consideration of the case of the left zero-divisors is connected with solving the vector equation

$$(x\mathbf{e} + y\mathbf{i}) \circ (a\mathbf{e} + b\mathbf{i}) = (0, 0), \tag{12}$$

that can be reduced to the following system of two linear equations in $GF(p)$:

$$\begin{cases} a\mu x + a\tau y = 0 \\ b\mu x + b\tau y = 0. \end{cases} \tag{13}$$

One can see that each of the vectors

$$D_l = \left(x, -\tau^{-1}\mu x\right),$$

where x takes on all values in $GF(p)$, acts on each element of the considered FNAA as the left zero-divisor.

Some zero-divisor D satisfying equation

$$D^2 = D \circ D = (0, 0)$$

can be called square root from zero of the FNAA. Finding such elements is connected with solving the vector equation

$$(x\mathbf{e} + y\mathbf{i}) \circ (x\mathbf{e} + y\mathbf{i}) = (0, 0),$$

connected with the following system of two linear equations in $GF(p)$

$$\begin{cases} \mu x^2 + \tau xy = 0 \\ \mu xy + \tau y^2 = 0. \end{cases} \tag{14}$$

For the last system we have the following solutions that define the set of the square roots from zero element $(0, 0)$:

$$D = (x,\ y) = \left(x,\ -\mu\tau^{-1}x\right), \tag{15}$$

where $x = 0, 1, ..., p - 1$. Taking into account the condition of Statement 2 one can conclude that elements, to which no right unit element corresponds, are square roots from the zero vector $(0, 0)$.

3 Algebra with unique local left-side unit elements

The FNAA of two-dimensional vectors with the multiplication operation defined by Table 2 , where $\mu \neq 0$ and $\tau \neq 0$, has properties analogous to the properties of the FNAA described in Subsection 2.1, for example Statement 1 is valid.

Table 2. Alternative BVMT for the case $m = 2$

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

Consideration of the vector equations defining the right and left unit elements, the right and left zero divisors, and square roots from zero $(0,0)$ have given the following statements.

Statement 4. Each two-dimensional vector from the set

$$E_r = (x,\ y) = \left(x,\ \tau^{-1}(1-x)\right), \tag{16}$$

where x takes on all possible values in $GF(p)$, represents a global right-side unit element.

Statement 5. Suppose $V = (a, b)$ be a vector such that $a\mu + b\tau \neq 0$. Then the vector

$$E_l = \left(\frac{a}{a\mu + b\tau},\ \ \frac{b}{a\mu + b\tau}\right) \tag{17}$$

is a unique local left-side unit for all vectors from the following set $\left\{V, V^2, ..., V^i, ...\right\}$, where i is an arbitrary integer.

Statement 6. A unique local bi-side unit element $E' = E_l$ acts in the set $\left\{V, V^2, ..., V^i, ...\right\}$, where i is an arbitrary integer and vector $V = (a, b)$ is such that $a\mu + b\tau \neq 0$. The value E' can be computed as $E' = V^{\omega}$ for some integer ω.

Statement 7. Each two-dimensional vector acts on the vectors $V = (a, b)$ such that $a\mu + b\tau = 0$ as the left zero-divisor.

Statement 8. Each of the vectors

$$D_r = \left(x, -\tau^{-1}\mu x\right),$$

where x takes on all values in $GF(p)$, acts on each element of the considered FNAA as the right-side zero-divisor.

4 Commutative finite algebras of two-dimensional vectors

Finite commutative associative algebras (FCAA) of two-dimensional vectors can be defined using the following BVMT presented in Tables 3, 4, 5, and 6, where $\mu \neq 0$ and $\tau \neq 0$.

Table 3. The BVMT defining FCAA with the unit element $(1, 0)$

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

The case relating to Table 3 was described in [4], where it has been shown that the algebra represents a finite ring with the unit element $(1, 0)$, if the structural coefficient τ is a quadratic residue modulo p, or finite field $GF(p^2)$, if τ is a quadratic non-residue.

Table 4. The BVMT defining FCAA with the unit element $(0, \tau^{-1})$

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

Table 5. Unbalanced BVMT defining FCAA with the unit element $(0, \tau^{-1})$

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

Table 6. Unbalanced BVMT defining commutative algebra with the unit element $\left(0, \mu^{-1}\right)$

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

Let us consider the case relating to Table 4. The vector equation for finding the unit element of the considered FCAA is as follows

$$(a\mathbf{e} + b\mathbf{i}) \circ (x\mathbf{e} + y\mathbf{i}) = (a\mathbf{e} + b\mathbf{i}), \tag{18}$$

where $X = (x\mathbf{e} + y\mathbf{i})$ is unknown.

Using Table 4, equation (18) can be reduced to solving the following system of two linear equations in $GF(p)$:

$$\begin{cases} \tau bx + \tau ay = a \\ \mu ax + \tau by = b. \end{cases} \tag{19}$$

In the case $\Delta = \tau^2 b^2 - \tau\mu a^2 \neq 0$ the system has a unique solution $(x, y) = \left(0, \tau^{-1}\right)$. The indicated inequality takes place for all elements $(a, b) \neq (0, 0)$ in the following two cases

i) τ is a quadratic non-residue and μ is a quadratic residue; ii) τ is a quadratic residue and μ is a quadratic non-residue.

In the last two cases all two-dimensional vectors $V = (a, b) \neq (0, 0)$ are invertible and the considered FCAA represents the finite field $GF(p^2)$.

If conditions i) and ii) do not take place, for some vectors $V = (a, b)$ we have $\Delta = \tau^2 b^2 - \tau\mu a^2 = 0$. Such vectors are not invertible and the FCAA represents a finite ring.

For the non-invertible vector $(a, b) \neq (0, 0)$ we have the following set of local unit elements: $E_x = \left(x, \tau^{-1}a^{-1}(a - \tau bx)\right)$, where $x = 0, 1, 2, ..., p - 1$. Except one non-invertible, all other local unit elements are invertible, and $E_0 = E = \left(0, \tau^{-1}\right)$ represents the global unit element of the FCAA, i.e. the vector acting as a unit element for all elements of the FCAA. The non-invertible local unit element is defined by the following formula:

$$E_n = \left(\frac{a}{\tau b + a\sqrt{\mu\tau}}, \frac{1}{\tau} - \frac{b}{\tau b + a\sqrt{\mu\tau}}\right). \tag{20}$$

Statement 9. The local unit element E_n acts in the set $\left\{V, V^2, ..., V^i, ...\right\}$, where i is an arbitrary integer and vector $V = (a, b)$ is such that $\tau^2 b^2 - \mu\tau a^2 = 0$, and the value E_n can be computed as $E_n = V^\omega$ for some integer ω.

Each non-invertible vector $(a, b) \neq (0, 0)$ devides zero element $(0, 0)$, i.e. for some element $D_x \neq (0, 0)$ we have $(a, b) \circ D_x = (0, 0)$. Zero divisors $D_x = (x, y)$ connected with the non-invertible vector $(a, b) \neq (0, 0)$ can be computed from the following system of equations

$$\begin{cases} \tau bx + \tau ay = 0 \\ \mu ax + \tau by = 0. \end{cases} \tag{21}$$

The set of the zero divisors D_x is described as follows

$$D_x = \left(x, -ba^{-1}x\right).$$

All values D_x are non-invertible elements of the FCAA.

In the case of defining FCAA by Table 5 we have the folowing system of equations for computing the unit elements:

$$\begin{cases} (\mu a + \tau b)x + \tau ay = a \\ \tau by = b. \end{cases} \tag{22}$$

For all vectors $(a,b) \neq (0,0)$, such that $\mu a + \tau b \neq 0$, system (22) has the same solution $(x,y) = \left(0, \tau^{-1}\right) = E$. The element E is the global unit element of the FCAA defined by Table 5. This FCAA represents a ring with p non-invertible elements N that can be described with the following formular

$$N = \left(x, -\frac{\mu}{\tau}x\right),$$

where $x = 0, 1, 2, ...p-1$.

Each element from the set

$$E_x = \left(x, \tau^{-1}\right)$$

acts as local unit element on all non-invertible elements of the FCAA defined by Table 5.

In the case of defining FCAA by Table 6 we have the following system of equations for computing the unit elements:

$$\begin{cases} \mu a x = a \\ \mu b x + (\mu a + \tau b) y = b. \end{cases} \tag{23}$$

For all vectors $(a,b) \neq (0,0)$, such that $\mu a + \tau b \neq 0$, system (23) has the same solution $(x,y) = \left(\mu^{-1}, 0\right) = E$. The element E is the global unit element of the FCAA defined by Table 6. This FCAA represents a ring with p non-invertible elements N that can be described with the following formula

$$N = \left(x, -\frac{\mu}{\tau}x\right),$$

where $x = 0, 1, 2, ...p-1$.

Each element from the set

$$E_x = \left(\mu^{-1}, y\right)$$

acts as local unit element on all non-invertible elements of the FCAA defined by Table 6.

5 Conclusion

It has been introduced the associative FNAA of the two-dimensional vectors defined over the field $GF(p)$. One of the interesting properties of the investigated FNAA is mutual associativity of all modifications of the parameterized non-commutative multiplication operation. The known in the literature parameterized commutative multiplication operation for the case $m = 2$ [4] do not possess such property.

There are also considered FCAAs defined by four different BVMT, three of them being considered for the first time. The considered six BVMT (two for the non-commutativity case and four for the commutativity case) cover possible variants of defining finite associative algebras of the dimension 2. Other variants of BVMT define non-associative algebras, except some modification of Table 3 in which an additional structural coefficient can be inserted.

Future research in frame of the concerned topic is connected with investigation properties of the associative FNAAs of m-dimensional vectors for cases $m = 3$ and $m = 5$.

References

[1] E. Sakalauskas, P. Tvarijonas and A. Raulynaitis, "Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level," *Informatica*, vol. 18, no. 1, pp. 115–124, 2007.

[2] D. N. Moldovyan, "Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes," *Quasigroups and Related Systems*, vol. 18, no. 2, pp. 165–176, 2010.

[3] D. N. Moldovyan and N. A. Moldovyan, "Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms," *Quasigroups Related Systems*, vol. 18, no. 2, pp. 177–186, 2010.

[4] N. A. Moldovyan and P. A. Moldovyanu, "Vector Form of the Finite Fields $GF(p^m)$," *Bul. Acad. Ştiinţe Repub. Mold. Mat.*, no. 3(61), pp. 1–7, 2009.

Alexander Moldovyan[1], Nicolai Moldovyan[2], Victor Shcherbacov[3]

Received December 6, 2017

[1]Professor/St. Petersburg ITMO University
E–mail: maa1305@yandex.ru

[2]Head of the laboratory/St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
E–mail: nmold@mail.ru

[2]Principal Researcher/Institute of Mathematics and Computer Science of the Academy of Sciences of Moldova
E–mail: victor.scerbacov@math.md