BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 2(87), 2018, Pages 95–100
ISSN 1024–7696

General Method for Defining Finite Non-commutative Associative Algebras of Dimension $m > 1$

A. A. Moldovyan

Abstract. General method for defining non-commutative finite associative algebras of arbitrary dimension $m \geq 2$ is discussed. General formulas describing local unit elements (the right-, left-, and bi-side ones), square roots of zero and zero divisors are derived. For arbitrary value m the single bi-side unit corresponds to every element of the algebra, except the square roots from zero. Various modifications of the multiplication operation can be assigned using different sets of the values of structural coefficients. It is proved that all of the modifications are mutually associative.

Mathematics subject classification: 94A60, 16Z05, 14G50, 11T71, 16S50.
Keywords and phrases: Finite associative algebra, non-commutative algebra, structural coefficient, mutual associativity, local unit.

1 Introduction

Finite non-commutative rings and associative algebras attract attention of cryptographers due to their potential application for designing post-quantum public-key cryptoschemes [1] based on computational difficulty of the discrete logarithm problem in hidden cyclic group [2, 3].

Recently finite non-commutative associative algebras (FNAAs) of dimensions $m = 2$ [4] and $m = 3$ [5] have been introduced. Those FNAAs are defined with using basis vector multiplication tables (BVMTs) which have similar structure.

In present paper it is shown that the mentioned method for defining 2- and 3-dimensional FNAAs can be extended for the case of arbitrary dimension. General type of BVMT for defining FNAAs is presented and it is shown that many properties of such FNAAs can be described with unified formulas that are derived.

2 Defining m-dimensional FNAA

Suppose $\mathbf{e}_1$, $\mathbf{e}_2$, ... $\mathbf{e}_m$ are some formal basis vectors and $v_1, v_2, \dots v_m \in GF(p)$, where prime $p \geq 3$, are coordinates of the m-dimensional vectors V which are denoted as $v_1\mathbf{e}_1 + v_2\mathbf{e}_2 + \cdots + v_m\mathbf{e}_m$ or as $(v_1, v_2, \dots, v_m)$. Terms $v_i\mathbf{e}_i$, where $i = 1, 2, \dots, m$, are called components of the vector.

Addition of two vectors $A=\sum_{i=1}^{m} a_i\mathbf{e}_i$ and $B=\sum_{i=1}^{m} b_i\mathbf{e}_i$ is defined as addition of the corresponding coordinates, i.e., with the following formula

$$A+B=\sum_{i=1}^{m}(a_i+b_i)\mathbf{e}_i,$$

where $+$ denotes the addition operation of both the m-dimensional vectors and the values of the field $GF(p)$. The multiplication operation in m-dimensional FNAAs (denoted as $\circ$) is defined with the formula

$$A\circ B=\left(\sum_{i=1}^{m} a_i\mathbf{e}_i\right)\circ\left(\sum_{i=1}^{m} b_i\mathbf{e}_i\right)=\sum_{j=1}^{m}\sum_{i=1}^{m}(a_ib_j)(\mathbf{e}_i\circ\mathbf{e}_j), \tag{1}$$

where products of different pairs of formal basis vectors $\mathbf{e}_i\circ\mathbf{e}_j$ are to be replaced by some one-component vector in accordance with the BVMT shown in Table 1, where $\mu_i\in GF(p)$ for $i=1,\ 2,\ ...,\ m$ are some fixed structural coefficients, assuming that the left basis vector defines the row and the right one defines the column. Thus, the intersection of the ith row and jth column gives the value of the product $\mathbf{e}_i\circ\mathbf{e}_j$.

Table 1. The BVMT for defining m-dimensional FNAA

$\circ$	$\mathbf{e}_1$	$\mathbf{e}_2$	...	$\mathbf{e}_i$	...	$\mathbf{e}_m$
$\mathbf{e}_1$	$\mu_1\mathbf{e}_1$	$\mu_2\mathbf{e}_1$	...	$\mu_i\mathbf{e}_1$	...	$\mu_m\mathbf{e}_1$
$\mathbf{e}_2$	$\mu_1\mathbf{e}_2$	$\mu_2\mathbf{e}_2$	...	$\mu_i\mathbf{e}_2$	...	$\mu_m\mathbf{e}_2$
...	...	...	...	...	...	...
$\mathbf{e}_i$	$\mu_1\mathbf{e}_i$	$\mu_2\mathbf{e}_i$	...	$\mu_i\mathbf{e}_i$	...	$\mu_m\mathbf{e}_i$
...	...	...	...	...	...	...
$\mathbf{e}_m$	$\mu_1\mathbf{e}_m$	$\mu_2\mathbf{e}_m$	...	$\mu_i\mathbf{e}_m$	...	$\mu_m\mathbf{e}_m$

For all integers $i,j\in\{1,2,\dots,m\}$ Table 1 defines the following simple formula for product of the basis vectors $\mathbf{e}_i$ and $\mathbf{e}_j$:

$$\mathbf{e}_i\circ\mathbf{e}_j=\mu_j\mathbf{e}_i. \tag{2}$$

Using (1) and (2) one can easily get the formula for product of the m-dimensional vectors A and B :

$$A\circ B=\sum_{i=1}^{m}\left(a_i\sum_{j=1}^{m}\mu_jb_j\right)\mathbf{e}_i=\left(\sum_{j=1}^{m}\mu_jb_j\right)\sum_{i=1}^{m}a_i\mathbf{e}_i. \tag{3}$$

The formula (3) shows the product $A\circ B$ is equal to the result of multiplying the right operand by scalar $\lambda_B=\sum_{j=1}^{m}\mu_jb_j$ defined by the second operand.

In general case the operation $\circ$ is non-commutative. Indeed, from (3) for A and $B\neq A$ we have

$$\{A \circ B = B \circ A\} \Rightarrow \left\{\forall i : \frac{a_i}{b_j} = \frac{\lambda_A}{\lambda_B}\right\} \Rightarrow \{A = \rho B\}\,. \tag{4}$$

The formula (4) shows the multiplication of vectors A and B is commutative only in particular cases when the second operand can be expressed as the result of multiplying the first one by some scalar $\rho \in GF(p)$.

The operation $\circ$ is associative. Moreover all possible different modifications of the multiplication operation are mutually associative. Indeed, suppose in Table 1 two arbitrary sets of the values of the structural coefficients $\{\mu_1, \mu_2, \dots, \mu_m\}$ and $\{\mu'_1, \mu'_2, \dots, \mu'_m\}$ define the multilication operation modifications $\circ$ and $\star$ respectively. Then from the formula (3) for vectors A, B, and $C = \sum_{k=1}^{m} c_k \mathbf{e}_k$ we have the following

$$(A \circ B) \star C = \left(\left(\sum_{j=1}^{m} \mu_j b_j\right) A\right) \star C = \left(\sum_{k=1}^{m} \mu'_k c_k\right)\left(\sum_{j=1}^{m} \mu_j b_j\right) A;$$

$$A \circ (B \star C) = A \circ \left(\left(\sum_{k=1}^{m} \mu'_k c_k\right) B\right) = \left(\sum_{k=1}^{m} \mu'_k c_k\right)\left(\sum_{j=1}^{m} \mu_j b_j\right) A$$

$$\Rightarrow (A \circ B) \star C = A \circ (B \star C)\,.$$

Analogous FNAAs can be defined with using Table 2 that is transposition of Table 1.

Table 2. Alternative BVMT for defining non-commutative associative multiplication in m-dimensional finite vector space

$\circ$	$\mathbf{e}_1$	$\mathbf{e}_2$	...	$\mathbf{e}_i$	...	$\mathbf{e}_m$
$\mathbf{e}_1$	$\mu_1\mathbf{e}_1$	$\mu_1\mathbf{e}_2$	...	$\mu_1\mathbf{e}_i$	...	$\mu_1\mathbf{e}_m$
$\mathbf{e}_2$	$\mu_2\mathbf{e}_1$	$\mu_2\mathbf{e}_2$	...	$\mu_2\mathbf{e}_i$	...	$\mu_2\mathbf{e}_m$
...	...	...	...	...	...	...
$\mathbf{e}_i$	$\mu_i\mathbf{e}_1$	$\mu_i\mathbf{e}_2$	...	$\mu_i\mathbf{e}_i$	...	$\mu_i\mathbf{e}_m$
...	...	...	...	...	...	...
$\mathbf{e}_m$	$\mu_m\mathbf{e}_1$	$\mu_m\mathbf{e}_2$	...	$\mu_m\mathbf{e}_i$	...	$\mu_m\mathbf{e}_m$

Defining the multiplication operation with using Table 2 gives algebras with similar properties. Indeed, suppose $\circ$ and $*$ are the multiplication operations defined with Table 1 and Table 2 respectively. Then it is easy to prove that for two arbitrary m-dimensional vectors A and B the following formula holds:

$$A \circ B = B * A.$$

To prove this fact note that from definition of the multiplication operation and Table 2 one gets

$$\mathbf{e}_i * \mathbf{e}_j = \mu_i \mathbf{e}_j \Rightarrow B * A = \left(\sum_{i=1}^{m} \mu_i b_i\right) \sum_{j=1}^{m} a_j \mathbf{e}_j = \lambda_B A = A \circ B.$$

In the next section we consider properties of the FNAAs defined by Table 1.

3 Unit elements and zero divisors

Finding the left-side unit elements relatively to some vector A is connected with solving the vector equation

$$X \circ A = A \Rightarrow \lambda_A X = A, \tag{5}$$

where $X = \sum_{i=1}^{m} x_i \mathbf{e}_i$ is the unknown vector.

Taking into account (3) the equation (5) can be reduced to the system of m linear equations which can be described for $i = 1, 2, \ldots, m$ as follows:

$$\lambda_A x_i = a_i. \tag{6}$$

System (6) shows that for the vectors A, such that $\sum_{i=1}^{m} \mu_i a_i \neq 0$, there exists the following single solution

$$E_l = (x_1, x_2, \ldots, x_i, \ldots, x_m), \text{where } \forall i = 1, 2, \ldots, m: \; x_i = a_i \left(\sum_{i=1}^{m} \mu_i a_i\right)^{-1}. \tag{7}$$

Finding the right-side unit elements relatively to some vector A is connected with solving the equation

$$A \circ X = A \Rightarrow \lambda_X A = A. \tag{8}$$

Taking into account (8) one can conclude that there exists a set of the right-side units which is described as follows

$$E_r = (x_1, x_2, \ldots, x_i, \ldots, x_m), \tag{9}$$

where $x_1, x_2, \ldots, x_i, \ldots, x_{m-1} \in \{0, 1, \ldots, p-1\}$ are arbitrary integers and $x_m = \mu_m^{-1}\left(1 - \sum_{i=1}^{m-1} \mu_i x_i\right)$. Evidently, the set (9) describes the right-side unites for arbitrary vectors A. We can say that formula (9) describes the set of global right-side units.

The element E_l is contained in the set (9), therefore the formula (7) defines the local bi-side unit relatively to vector A.

Finding the left-side zero divisors relatively to the vector A is connected with solving the vector equation

$$X \circ A = (0, 0, \ldots, 0) \Rightarrow \lambda_A X = (0, 0, \ldots, 0). \tag{10}$$

The equation (10) can be reduced to the system of m linear equations which can be described for $i = 1, 2, \ldots, m$ as follows:

$$\lambda_A x_i = 0. \tag{11}$$

The system (11) shows that for the vectors A, such that $\lambda_A = \sum_{i=1}^{m} \mu_i a_i \neq 0$, there exists the single solution $X = (0, 0, \ldots, 0)$. If $\lambda_A = 0$, then (10) holds for arbitrary value X, therefore the vectors D', such that $\lambda_{D'} = 0$, are the right zero divisors.

The equation

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

holds only for such vectors D that satisfy the condition $\lambda_D = \sum_{i=1}^{m} \mu_i d_i = 0$. Such vectors D can be called square roots of zero of the considered FNAAs.

To every vector A that is not a square root from zero there corresponds only one local left-side unit element E_l defined by the formula (7) which acts on the vectors $A, A^2, ..., A^s$ as local bi-side unit $E' = E_l$ for arbitrary integer $s \geq 1$. Taking into account finiteness of the considered FNAAs it is easy to see that the sequence $A, A^2, ..., A^s, \ldots$ is periodic and for some value $i = \omega$ we have $V^{\omega} = E'$. The number of different values A^s generated by the vector A can be called its order, since the set $\{A, A^2, ..., A^{\omega}\}$ represents cyclic group with the group operation $\circ$.

Using (3) one can easily get the formula for computing the value A^s :

$$A^s = A^{s-1} \circ A = (\lambda_A)^{s-1} A. \tag{12}$$

Since $\lambda_A \in GF(p)$ and $(\lambda_A)^{p-1} = 1$, then one gets $A^{p-1} = E'$. Therefore the possible values of the orders of elements in the considered FNAAs are divisors of the value $p - 1$.

4 Conclusion

We have introduced a general method for defining FNAAs for arbitrary dimension $m \geq 2$. It has been proved that in arbitrary fixed FNAA of such type different modifications of the multiplication operation are mutually associative. General formulas describing the right-side, left-side, and bi-side unit elements as well as the right-side and left-side zero divisors have been derived.

References

[1] Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A. *Cryptographic Algorithms on Groups and Algebras.* Journal of Mathematical Sciences, 2017, **223**, No. 5, 629–641.

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

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

[4] Moldovyan A. A., Moldovyan N. A., Shcherbacov V. A. *Non-commutative finite associative algebras of 2-dimensional vectors.* Computer Science Journal of Moldova, 2017, **25**, No. 3, 344–356.

[5] Moldovyan A. A., Moldovyan N. A., Shcherbacov V. A. *Non-commutative finite rings with several mutually associative multiplication operations*, The Fourth Conference of Mathematical Society of the Republic of Moldova dedicated to the centenary of Vladimir Andrunachievici (1917–1997), June 28 – July 2, 2017, Chisinau, Proceedings CMSM4, 2017, p. 133–136.

Alexandr Moldovyan
St. Petersburg Institute for Informatics and Automation
of Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg
Russia

E-mail: *maa1305@yandex.ru*

Received May 02, 2018