Quasigroups and Related Systems **26** (2018), 263 – 270

Unified method for defining finite associative algebras of arbitrary even dimensions

Nikolay Moldovyan

Abstract. There is introduced a general method for defining finite associative algebras of arbitrary even dimension. The method consists in defining the multiplication operation in the finite vector space of even dimension with using some unified basis vector multiplication table. In the cases $m = 2$ and $m = 4$ the constructed algebras are commutative rings. In the cases $m \geqslant 6$ the algebras are non-commutative rings. Finite non-commutative associative algebras of dimension greater or equal to 6 are useful for defining discrete logarithm problem in hidden cyclic group which is attractive as primitive of the post-quantum cryptographic algorithms and protocols.

1. Introduction

One of the actual problems in the area of cryptography relates to construction of the post-quantum public-key cryptoschemes [2, 10].

The computational difficulty of the discrete logarithm problem (DLP) in hidden cyclic group defined in a finite non-commutative algebra was proposed as primitive for designing post-quantum cryptoschemes [5, 7, 9]. However, it has been shown in [1] that for the known implementations of mentioned hard problem the last can be reduced to DLP in finite fields. Therefore, to provide high security (against cryptanalysis with using quantum computers) of the cryptoschemes based on computational difficulty of DLP in hidden group one should define the last problem in some other finite non-commutative associative algebras (FNAAs) [1]. Unfortunately, in the literature few m-dimensional FNAAs are presented for cases $m = 2$ [3], $m = 3$ [4], $m = 4$ [5], and $m = 8$ [6].

In this paper, a unified method for defining FNAAs of arbitrary even dimension $m \geqslant 6$ is introduced. The method consists in defining the multiplication operation in the m-dimensional vector space by using basis vector multiplication table (BVMT) of some general type. The proposed BVMT defines an operation for multiplying the vectors in all cases of the even dimension m. It is shown that this operation is associative, non-commutative for $m \geqslant 6$ and commutative for $m = 2$ and $m = 4$.

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

2. Defining FNAAs of even dimensions

Suppose $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are m formal basis vectors and $a_o, a_1, \ldots a_{m-1} \in GF(p^d)$ (where $p \geqslant 2$ is a prime number and $d \geqslant 1$ is a natural number) are coordinates of the vector A that is represented in the following two forms:

$$A = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \cdots + a_{m-1}\mathbf{e}_{m-1};$$
$$A = (a_0, a_1, \ldots, a_{m-1}).$$

Terms $a_i\mathbf{e}_i$, where $i = 0, 1, \ldots, m-1$, are called components of the vector.

Addition of two vectors $A = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$ and $B = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ is defined in the usual form by

$$A + B = \sum_{i=0}^{m-1} (a_i + b_i)\,\mathbf{e}_i.$$

Note that $+$ denotes the addition operation in the m-dimensional vector space and the addition operation in the field $GF(p^d)$.

The multiplication operation $\circ$ of two m-dimensional vectors A and B as elements of some finite associative algebra is defined with the following formula

$$A \circ B = \left(\sum_{i=0}^{m-1} a_i\mathbf{e}_i\right) \circ \left(\sum_{j=0}^{m-1} b_j\mathbf{e}_j\right) = \sum_{j=0}^{m-1}\sum_{i=0}^{m-1} a_i b_j \mathbf{e}_i \circ \mathbf{e}_j, \tag{1}$$

where the product $\mathbf{e}_i \circ \mathbf{e}_j$ for all possible pairs of the values i and j is to be replaced by some one-component vector in accordance with the BVMT shown in Table 1, where $\mu \in GF(p^d)$ is some fixed value called structural coefficient, assuming that the left basis vector $\mathbf{e}_i$ defines the row and the right one $\mathbf{e}_j$ defines the column. Thus, the intersection of the ith row and jth column gives the value of the product $\mathbf{e}_i \circ \mathbf{e}_j$.

The structure of the Table 1 is described as follows. For every even value i the ith row represents result of the left rotation of the initial row $(\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{m-1})$ by i positions. The $(i+1)$th row represents result of the right rotation of the sequence of the single-component vectors $\mu\mathbf{e}_0, \mathbf{e}_{m-1}, \mu\mathbf{e}_{m-2}, \ldots, \mu\mathbf{e}_2, \mathbf{e}_1$ by $i+1$ positions, where the structural coefficient μ is written at the basis vectors having even numbers.

For all pairs of integers $i, j \in \{0, 1, , \ldots, m-1\}$ Table 1 defines the following simple formula for product of the basis vectors $\mathbf{e}_i$ and $\mathbf{e}_j$:

$$\mathbf{e}_i \circ \mathbf{e}_j = \begin{cases} \mathbf{e}_{i+j}, \text{for even } i \\ \mathbf{e}_{i-j}, \text{for odd } i \text{ and even } j \\ \mu\mathbf{e}_{i-j}, \text{for odd } i \text{ and odd } j \end{cases} \tag{2}$$

It is supposed that in formula (2) addition and subtraction are performed modulo m. Using (1) and (2) one can easily prove the following statement.

Proposition 2.1. *The multiplication operation defined by Table* 1 *is associative.*

Proof. Using formula (1) for product of three vectors A, B, and $C = \sum_{k=0}^{m-1} c_k \mathbf{e}_k$ one can get the following

$$\begin{aligned}(A \circ B) \circ C &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \sum_{k=0}^{m-1} a_i b_j c_k \, (\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k; \\ A \circ (B \circ C) &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \sum_{k=0}^{m-1} a_i b_j c_k \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) \, .\end{aligned} \tag{3}$$

Thus, it is sufficient to show that for arbitrary possible triple (i, j, k) the following formula holds

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) \, . \tag{4}$$

We have the following cases.

Case 1: each one of the values i and j is even (k is even or odd). Then from (2) one gets

$$\begin{aligned}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k &= \mathbf{e}_{i+j} \circ \mathbf{e}_k = \mathbf{e}_{i+j+k}; \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) &= \mathbf{e}_i \circ \mathbf{e}_{j+k} = \mathbf{e}_{i+j+k}.\end{aligned}$$

Case 2: the value i is even and the each of the values j and k is odd.

$$\begin{aligned}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k &= \mathbf{e}_{i+j} \circ \mathbf{e}_k = \mu \mathbf{e}_{i+j-k}; \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) &= \mathbf{e}_i \circ (\mu \mathbf{e}_{j-k}) = \mu \mathbf{e}_{i+j-k}.\end{aligned}$$

Case 3: each one of the values i and k is even and the values j is odd.

$$\begin{aligned}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k &= \mathbf{e}_{i+j} \circ \mathbf{e}_k = \mathbf{e}_{i+j-k}; \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) &= \mathbf{e}_i \circ \mathbf{e}_{j-k} = \mathbf{e}_{i+j-k}.\end{aligned}$$

Case 4: every one of the values i, j, and k is odd .

$$\begin{aligned}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k &= \mu \mathbf{e}_{i-j} \circ \mathbf{e}_k = \mu \mathbf{e}_{i-j+k}; \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) &= \mathbf{e}_i \circ (\mu \mathbf{e}_{j-k}) = \mu \mathbf{e}_{i-j+k}.\end{aligned}$$

Case 5: each one of the values i and j is odd and the value k is even.

$$\begin{aligned}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k &= \mu \mathbf{e}_{i-j} \circ \mathbf{e}_k = \mu \mathbf{e}_{i-j+k}; \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) &= \mathbf{e}_i \circ \mathbf{e}_{j-k} = \mu \mathbf{e}_{i-j+k}.\end{aligned}$$

Case 6: the value i is odd and each one of the values j and k is even.

$$\begin{aligned}(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k &= \mathbf{e}_{i-j} \circ \mathbf{e}_k = \mathbf{e}_{i-j-k}; \\ \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) &= \mathbf{e}_i \circ \mathbf{e}_{j+k} = \mathbf{e}_{i-j-k}.\end{aligned}$$

Case 7: each one of the values i and k is odd and the value j is even.

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_{i-j} \circ \mathbf{e}_k = \mu \mathbf{e}_{i-j-k};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ \mathbf{e}_{j+k} = \mu \mathbf{e}_{i-j-k}.$$

Thus, in all cases formula (4) is valid and therefore, Proposition 2.1 holds. □

Proposition 2.2. *The vector* $U = (u_0, u_1, \ldots, u_i, \ldots, u_{m-1})$, *where* $u_0 = 1$ *and* $u_i = 0$ *for* $i = 1, 2, \ldots, m-1$, *is the bi-side unit of the* m*-dimensional finite associative algebra in which the multiplication operation is defined by Table* 1.

Proof. Using formula (1) for products $A \circ U$ and $U \circ A$, where A is an arbitrary vector of the m-dimensional FNAA, one can get

$$A \circ U = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i u_j (\mathbf{e}_i \circ \mathbf{e}_j) = \sum_{i=0}^{m-1} \sum_{j=0}^{0} a_i u_j (\mathbf{e}_i \circ \mathbf{e}_j) = \sum_{i=0}^{m-1} a_i u_0 \mathbf{e}_{i \pm 0} = A;$$
$$U \circ A = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} u_i a_j (\mathbf{e}_i \circ \mathbf{e}_j) = \sum_{i=0}^{0} \sum_{j=0}^{m-1} u_0 a_j (\mathbf{e}_0 \circ \mathbf{e}_j) = \sum_{j=0}^{m-1} a_j \mathbf{e}_j = A.$$

Thus, $A \circ U = U \circ A = A$. □

Table 1: The BVMT for defining m-dimensional FNAA (addition and subtraction is performed modulo m; the value i is even; j is odd)

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	...	$\mathbf{e}_j$	...	$\mathbf{e}_{m-1}$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	...	$\mathbf{e}_j$	...	$\mathbf{e}_{m-1}$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mu\mathbf{e}_0$	$\mathbf{e}_{m-1}$	...	$\mu\mathbf{e}_{1-j}$	...	$\mu\mathbf{e}_2$
...	...	...	...	...	...	...	...
$\mathbf{e}_i$	$\mathbf{e}_i$	$\mathbf{e}_{i+1}$	$\mathbf{e}_{i+2}$	...	$\mathbf{e}_{i+j}$	...	$\mathbf{e}_{i+m-1}$
$\mathbf{e}_{i+1}$	$\mathbf{e}_{i+1}$	$\mu\mathbf{e}_i$	$\mathbf{e}_{i-1}$	...	$\mu\mathbf{e}_{i+1-j}$	...	$\mu\mathbf{e}_{i+1-(m-1)}$
...	...	...	...	...	...	...	...
$\mathbf{e}_{m-1}$	$\mathbf{e}_{m-1}$	$\mu\mathbf{e}_{m-2}$	$\mathbf{e}_{m-3}$	...	$\mu\mathbf{e}_{j-(m-1)}$	...	$\mu\mathbf{e}_0$

It is easy to see that for the cases $m = 2$ and $m = 4$ Table 1 defines finite algebras with commutative multiplication operation. For even dimensions $m \geqslant 6$ the defined finite algebras are non-commutative. Indeed, in a general case the operation $\circ$ is non-commutative. For example, for even i and odd j we have

$$\mathbf{e}_i \circ \mathbf{e}_j = \mathbf{e}_{i+j};$$
$$\mathbf{e}_j \circ \mathbf{e}_i = \mathbf{e}_{j-i}.$$

In the case of 4-dimensional vectors one can define FNAAs insetting some additional structural coefficient equal to $p-1$ in several cells of the BVMT as it is shown in Table 2 for the following variants:

Table 2: Defining the 4-dimensional FNAAs

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\tau\mu\mathbf{e}_0$	$\tau\epsilon\mathbf{e}_3$	$\epsilon\mu\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\sigma\mathbf{e}_3$	$\sigma\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\sigma\tau\mu\mathbf{e}_2$	$\sigma\epsilon\tau\mathbf{e}_1$	$\epsilon\mu\mathbf{e}_0$

i) $\epsilon = p-1; \tau = \sigma = 1$,
ii) $\sigma = p-1; \tau = \epsilon = 1$,
iii) $\tau = p-1; \epsilon = \sigma = 1$, and
iv) $\sigma = \mu = p-1; \tau = \epsilon = 1$.
Note the last case represents the finite algebra of quaternions [7].

3. Some properties of the 6-dimensional FNAAs

In the case $m = 6$ the vector equation

$$A \circ X = E$$

can be reduced to the following system of six linear equations with unknowns $x_0, x_1, x_2, x_3, x_4, x_5 \in GF(p^d)$:

$$\begin{cases} a_0x_0 + \mu a_1x_1 + a_4x_2 + \mu a_3x_3 + a_2x_4 + \mu a_5x_5 = 1 \\ a_1x_0 + a_0x_1 + a_3x_2 + a_4x_3 + a_5x_4 + a_2x_6 = 0 \\ a_2x_0 + \mu a_3x_1 + a_0x_2 + \mu a_5x_3 + a_4x_4 + \mu a_1x_5 = 0 \\ a_3x_0 + a_2x_1 + a_5x_2 + a_0x_3 + a_1x_4 + a_4x_5 = 0 \\ a_4x_0 + \mu a_5x_1 + a_2x_2 + \mu a_1x_3 + a_0x_4 + \mu a_3x_5 = 0 \\ a_5x_0 + a_4x_1 + a_1x_2 + a_2x_3 + a_3x_4 + a_0x_5 = 0 \end{cases} \tag{5}$$

If the determinant Δ_A of the system (5) is not equal to zero, then the vector A is invertible and its inverse value A^{-1} can be computed as a solution of (5). If $\Delta_A = 0$, then the vector A is non-invertible one.

If the vector A is invertible, then the sequence $A, A^2, ..., A^i, ...$ (for $i = 1, 2, 3, ...$) is periodic and for some two integers h and $z > h$ we have $A^h = A^z$ and $A^z = A^{z-h} \circ A^h = A^h \circ A^{z-h}$, i.e., for some minimum integer ω (called order of the vector V) the equality $A^\omega = E$ holds. From the last formula one can get $A^{-1} = A^{\omega-1}$.

The performed computational experiments have shown that in the 6-dimensional FNAA defined over the ground field $GF(p)$ for different values p the invertible vectors have orders that divide the value

$$p^2 - 1 = (p-1)(p+1).$$

For defining the DLP in hidden group [5] there are to be used FNAAs that contain elements having sufficiently large prime order. Besides, as it was shown in [6] for designing cryptoschemes base on the DLP in a hidden group one should use vectors order of which does not divide the value $p-1$. To satisfy the mentioned requirements one can choose primes p such that the divisor $q=\frac{p+1}{2}$ is prime. The following example illustrate the last fact:

$p = 134308781033319330362776166404271867531448198177182217544$
$815787332574022955120447255496568284553283676851150 1;$
$q = 671543905166596651813880832021359337657240990885911087724$
$078936662870114775602236277482841422766418384255751.$

We propose the following modification of the DLP in hidden group, which is described by the following formula for computing the public key:

$$Y = V^{\omega-s} \circ N^x \circ V^s, \tag{6}$$

where V is some invertible vector having order equal to $\omega = p^2-1$; N is some non-invertible vector having local order equal to the value $q|p+1$; the pair of integers (s,x) is the private key.

The notion of the local order is connected with the notion of the local unit element E' such that: i) $E' \neq E$ and ii) $E' \circ N = N \circ E' = N$. The performed experiments have shown that in the considered 6-dimensional FNAA there exist non-invertible vectors N' having local order equal to the value p^2-1. Using such vectors one can easily compute the vectors $N = N'^{\frac{p^2-1}{q}}$ that have the required order $q|(p+1)$.

A computationally efficient method for generating non-invertible vectors can be proposed on the base of consideration of the value of the main determinant Δ of the system (5). One can derive the following formula for the determinant Δ :

$$\begin{aligned}\Delta = \frac{1}{4}((a_0+a_2+a_4)^2 - \mu(a_1+a_3+a_5)^2)\times \\ \times ((a_0-a_2)^2 + (a_0-a_4)^2 + (a_2-a_4)^2 - \\ - \mu(a_1-a_3)^2 - \mu(a_1-a_5)^2 - \mu(a_3-a_5)^2)^2\end{aligned} \tag{7}$$

A vector $N = (a_0, a_1, a_2, a_3, a_4, a_5)$ is non-invertible if its coordinates satisfy the condition $\Delta = 0$. The expression (7) shows that two different subsets of non-invertible vectors are contained in the considered FNAA. The first subset includes the vectors satisfying the condition

$$(a_0+a_2+a_4)^2 = \mu(a_1+a_3+a_5)^2. \tag{8}$$

The second subset includes the vectors satisfying condition

$$(a_0-a_2)^2 + (a_0-a_4)^2 + (a_2-a_4)^2 = \mu\left((a_1-a_3)^2 + (a_1-a_5)^2 + (a_3-a_5)^2\right).$$

From the equation (8) one obtains that: if the structural coefficient μ is a quadratic non-residue modulo p, then the first subset contains only the zero vector $(0,0,0,0,0,0)$.

If the value μ is a quadratic residue modulo p, then a non-invertible vector $N_1 = (a_0, a_1, a_2, a_3, a_4, a_5)$ contained in the first subset can be found as follows:

1. Generate random values $a_1, a_2, a_3, a_4, a_5 \in GF(p)$.
2. Compute the value $g = \mu\,(a_1 + a_3 + a_5) \bmod p$.
3. Compute the value $a_0 = g - a_2 - a_4 \bmod p$.

If the value μ is a quadratic non-residue modulo p, then a non-invertible vector $N_2 = (a_0, a_1, a_2, a_3, a_4, a_5)$ contained in the second subset can be found as follows:

1. Generate random values $a_1, a_2, a_3, a_4, a_5 \in GF(p)$.
2. Compute the value $h = \mu\left((a_1 - a_3)^2 + (a_1 - a_5)^2 + (a_3 - a_5)^2\right) \bmod p$.
3. Compose the quadratic equation

$$z^2 - z(a_2 + a_4) + \frac{h + (a_2 - a_4)^2 + a_2^2 + a_4^2}{2} \equiv 0 \bmod p. \tag{9}$$

(with the unknown value z) and compute discriminant of the equation (9):

$$d = \left(\frac{a_2 + a_4}{2}\right)^2 - \frac{h + (a_2 - a_4)^2 + a_2^2 + a_4^2}{2}.$$

4. If d is a quadratic residue modulo p, then compute one of the roots of the equation (9): $z_0 = \frac{a_2 + a_4}{2} - \sqrt{d}$. Otherwise go to step 1.
5. Take the value z_0 as the value a_0, i.e., $a_0 = z_0$.

4. Conclusion

A general method for defining FNAAs for arbitrary even dimension $m \geqslant 6$ has been introduced. The method also provides construction of finite associative algebras for cases $m = 2$ and $m = 4$, however the algebras are commutative in those cases. In the case of defining finite associative algebra over 4-dimensional vector space, the non-commutativity of the multiplication operation can be obtained by insetting a structural coefficient equal to $p-1$ in some cells of the proposed general BVMT. As a particular case we have the finite algebra of quaternions.

In the cases $m \geqslant 6$ the algebras are non-commutative rings with a global bi-side unit. The finite algebras of the dimensions $m = 6$ and $m = 8$ are useful as carriers of the discrete logarithm problem in a hidden cyclic group. A modification of the DLP in hidden group has been given, in which non-invertible elements of the FNAA are used. In the case of the 6-dimensional FNAA methods for finding non-invertible vectors have been proposed. Detailed investigation of the properties of the 6- and 8-dimensional FNAAs appear to be a topic of an individual study.

References

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

[2] Lecture Notes Computer Sci., **9606** (2016).

[3] **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.

[4] **A.A. Moldovyan, N.A. Moldovyan and V.A. Shcherbacov**, *Non-commutative finite rings with several mutually associative multiplication operations*, Proc. of 4 Confer. Math. Soc. Republ. Moldova, (2017), 133 – 136.

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

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

[7] **D.N. Moldovyan and N.A. Moldovyan**, *A new hard problem over non-commutative finite groups for cryptographic protocols*, Lecture Notes Computer Sci., **6258** (2010), 183 – 194.

[8] **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.

[9] **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.

[10] **J.A. Smolin, G. Smith and A. Vargo**, *Oversimplifying quantum factoring*, Nature, **499** (2013), 163 – 165.

Received May 10, 2018

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
E-mail: nmold@mail.ru