Quasigroups and Related Systems **30** (2022), 133 − 140

https://doi.org/10.56415/qrs.v30.11

Structure of a finite non-commutative algebra set by a sparse multiplication table

Dmitriy Moldovyan, Alexandr Moldovyan, Nikolay Moldovyan

Abstract. Four-dimensional finite non-commutative associative algebras represent practical interest as algebraic support of post-quantum digital signature algorithms, especially algebras with two sided global unit, set by sparse basis vectors multiplication tables. A new algebra of the latter type, set over the field $GF(p)$, is proposed and its structure is investigated. The studied algebra is described as a set of $p^2 + p + 1$ commutative subalgebras of three different types. All subalgebras intersect strictly in the subset of scalar vectors. Formulas are derived for the number of subalgebras of each type.

1. Introduction

Development of practical post-quantum (PQ) public-key digital signature algorithms is one of current challenges in the area of cryptography, which attracts considerable attention from the research community [8, 9]. Among computationally difficult problems used as a basic primitive of PQ signature algorithms, the hidden discrete logarithm problem (HDLP) is of interest for the development of PQ signature schemes having high performance and comparetively small size of the public key and signature [1, 3, 5]. Usually the HDLP is set in finite non-commutative associative algebras (FNAAs).

Recently [2], FNAAs defined with a sparse basis vector multiplication table (BVMT) have been proposed to get higher performance of the HDLP-based signature algorithms. The structure of the FNAAs used as algebraic support play significant role in the design of PQ HDLP-based signature schemes [1, 6].

The present paper introduces a new 4-dimensional FNAA set by a sparse BVMT over the ground field $GF(p)$, where p is an odd prime, and examines its structure from the point of view of decomposition into commutative subalgebras denoted as Ψ.

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50

Keywords: non-commutative algebra, finite associative algebra, single-sided units, post-quantum cryptography, public-key cryptoscheme, signature scheme, discrete logarithm problem, hidden logarithm problem

2. Introduced 4-dimensional algebra

Suppose a finite 4-dimensional vector space is defined over the ground finite field $GF(p)$, where $p \geq 3$. Then defining additionally the vector multiplication that is distributive at the right and at the left relatively the addition operation one gets a finite 4-dimensional algebra. An algebra element A can be denoted in the following two forms: $A = (a_0, a_1, a_2, a_3)$ and $A = \sum_{i=0}^{3} a_i\mathbf{e}_i$, where $a_0, a_1, a_2, a_3 \in GF(p)$ are called coordinates; $\mathbf{e}_0$, $\mathbf{e}_1$, $\mathbf{e}_2$, $\mathbf{e}_3$ are basis vectors.

The vector multiplication operation of two 4-dimensional vectors A and B is defined as $AB = \sum_{i=0}^{3}\sum_{j=0}^{3} a_ib_j(\mathbf{e}_i\mathbf{e}_j)$, where every of the products $\mathbf{e}_i\mathbf{e}_j$ is to be replaced by a single-component vector $\lambda\mathbf{e}_k$, where $\lambda \in GF(p)$, indicated in the cell at the intersection of the ith row and jth column of so called BVMT, like the proposed sparse Table 1. To define associative vector multiplication operation the BVMT should define associative multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k) : (\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k)$.

Table 1 with the structural constant $\lambda \neq 0$ defines the associative vector multiplication operation. Solving the vector equations $AX = X$ and $XA = A$, where $X = (x_0, x_1, x_2, x_3)$ is the unknown, one can easily prove that the 4-dimensional FNAA set by Table 1 contains global two-sided unit $E = (0, 0, 1, 1)$.

Consider the vector equation $AX = A$ that is reduced to the following system of four linear equations in $GF(p)$:

$$\begin{cases} a_3x_0 + a_0x_2 = 0; \\ a_0x_3 + a_2x_1 = 0; \\ \lambda a_1x_0 + a_2x_2 = 1; \\ \lambda a_0x_1 + a_3x_3 = 1. \end{cases} \tag{1}$$

If the system (1) has solution, then the vector A is invertible. It is easy to derive the following invertibility (non-invertibility) condition:

$$\lambda a_0a_1 \neq a_2a_3 \qquad (\lambda a_0a_1 = a_2a_3). \tag{2}$$

The condition (2) defines (see, for examle, [1]) the following value of the order Ω of the algebra multiplicative group (the number of invertible vectors contained in the algebra):

$$\Omega = p(p-1)\left(p^2-1\right). \tag{3}$$

3. Structure of the algebra

To study the structure of the FNAA set by Table 1, we apply the method used earlier in [1] . Consider the set of the vectors X that are permutable with a fixed vector $A = (a_0, a_1, a_2, a_3)$. The vectors $X = (x_0, x_1, x_2, x_3)$ can be computed as solutions of the vector equation $A \circ X = X \circ A$. Evidently, if X and X' are

Table 1

The BVMT setting the studied 4-dimensional FNAA; $\lambda \neq 0$.

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	0	$\lambda\mathbf{e}_3$	$\mathbf{e}_0$	0
$\mathbf{e}_1$	$\lambda\mathbf{e}_2$	0	0	$\mathbf{e}_1$
$\mathbf{e}_2$	0	$\mathbf{e}_1$	$\mathbf{e}_2$	0
$\mathbf{e}_3$	$\mathbf{e}_0$	0	0	$\mathbf{e}_3$

solutions, then $X \pm X'$ and XX' are also solutions. Therefore the set of solutions (Ψ_A) is a subalgebra. The said vector equation can be reduced to the following system of three linear equations with the unknowns x_0, x_1, x_2, and x_3:

$$\begin{cases} (a_3 - a_2)\,x_0 + a_0x_2 - a_0x_3 = 0; \\ (a_2 - a_3)\,x_1 - a_1x_2 + a_1x_3 = 0; \\ a_1x_0 - a_0x_1 = 0. \end{cases} \tag{4}$$

Depending on the values a_0, a_1, a_2, and a_3, the following cases should be considered.

I. $a_0 = a_1 = 0$. The system (4) reduces to

$$\begin{cases} (a_3 - a_2)\,x_0 = 0; \\ (a_2 - a_3)\,x_1 = 0. \end{cases}$$

If $a_2 \neq a_3$, then $x_0 = x_1 = 0$ one gets the solution space

$$X = (x_0, x_1, x_2, x_3) = (0, 0, i, j)\,, \tag{5}$$

where $i, j = 0, 1, \ldots p-1$. The set (5) describes a subalgebra Ψ_A of order p^2, which contains $2p-1$ different non-invertible vectors of the forms $(0, 0, i, 0)$ and $(0, 0, 0, j)$. Multiplicative group Γ_1 of this subalgebra has order $\Omega_1 = p^2 - (2p-1) = (p-1)^2$. One can show that the group Γ_1 possesses 2-dimensional cyclicity (in terms of [7]), i. e., its minimum generator system includes two vectors of the order $p - 1$.

If $a_3 = a_2$, (the algebra element A is a scalar vector), then the solution space of the system (4) includes all vectors of the algebra.

II. $a_0 \neq 0$; $a_1 = 0$. We have The system (4) can be reduced to

$$\begin{cases} x_3 = x_2 + \dfrac{a_3 - a_2}{a_0}x_0; \\ x_1 = 0 \end{cases}$$

and the solution space of the system (4) is described as follows:

$$X = (x_0, x_1, x_2, x_3) = \left(i,\ 0,\ j,\ j + \frac{a_3 - a_2}{a_0}i\right), \tag{6}$$

where $i, j = 0, 1, \ldots p-1$. The latter set includes non-invertible vectors satisfying the condition $j\left(j + \frac{a_3 - a_2}{a_0} i\right) = 0$. The latter condition sets the following two subsets of non-invertible vectors: i) $X = \left(i,\ 0,\ 0,\ \frac{a_3-a_2}{a_0} i\right)$ and ii) $X = \left(i,\ 0,\ -\frac{a_3-a_2}{a_0} i,\ 0\right)$, which intersect in the zero vector $(0, 0, 0, 0)$.

II,a) $a_2 \neq a_3$. This subcase corresponds to subalgabra Ψ_A of order p^2 which includes $2p - 1$ non-invertible vectors and multiplicative group Γ_1 of order $\Omega_1 = (p-1)^2$.

II,b) $a_2 = a_3$. This subcase corresponds to a subalgabra Ψ_A of order p^2, which includes p non-invertible vectors of the form $(i, 0, 0, 0)$ and contains a multiplicative group Γ_2 of order $\Omega_2 = p^2 - p = p(p-1)$. It is easy to prove that the group Γ_2 is cyclic

III. $a_0 = 0$; $a_1 \neq 0$. The system (4) reduces to

$$\begin{cases} x_3 = x_2 + \dfrac{a_3 - a_2}{a_1} x_1; \\ x_0 = 0 \end{cases}$$

and the solution space of the system (4) is described as follows:

$$X = (x_0, x_1, x_2, x_3) = \left(0,\ i,\ j,\ j + \frac{a_3 - a_2}{a_1} i\right), \tag{7}$$

where $i, j = 0, 1, \ldots p-1$. The set (7) includes non-invertible vectors satisfying the condition $j\left(j + \frac{a_3-a_2}{a_0} i\right) = 0$ which sets the following two subsets of non-invertible vectors: i) $X = \left(0,\ i,\ 0, \frac{a_3-a_2}{a_0} i\right)$ and ii) $X = \left(0,\ i,\ -\frac{a_3-a_2}{a_0},\ 0\right)$.

III,a) $a_2 \neq a_3$. This subcase corresponds to a subalgabra Ψ_A of order p^2 which includes $2p - 1$ non-invertible vectors and multiplicative group Γ_1 of order $\Omega_1 = (p-1)^2$.

III,b) $a_2 = a_3$. This subcase corresponds to a subalgabra Ψ_A of order p^2, which includes p non-invertible vectors of the form $(0, i, 0, 0)$ and contains a cyclic multiplicative group of the Γ_2 type and of order $\Omega_2 = p(p-1)$.

IV. $a_0 \neq 0$; $a_1 \neq 0$. One can write $x_1 = x_0 a_1 a_0^{-1}$. At the latter condition the firs and the second equations in (4) have the same solutions, therefore, the system (4) reduces to

$$\begin{cases} (a_3 - a_2)\, x_0 + a_0 x_2 - a_0 x_3 = 0; \\ x_1 = \dfrac{a_1}{a_0} x_0 \end{cases}$$

and the solution space of the system (4) is described as follows:

$$X = (x_0, x_1, x_2, x_3) = \left(i,\ \frac{a_1}{a_0} i,\ j, j + \frac{a_3 - a_2}{a_0} i\right), \tag{8}$$

where $i, j = 0, 1, \dots p - 1$. Taking into account the non-invertibility condition in (2), for non-invertible vectors from the set (8) one can write

$$\lambda \frac{a_1}{a_0} i^2 = j^2 + \frac{a_3 - a_2}{a_0} ji;$$

$$i^2 - \frac{a_3 - a_2}{\lambda a_1} ji - \frac{a_0}{\lambda a_1} j^2 = 0; \tag{9}$$

Fixing the value of j, one gets the following solutions of the latter quadratic equation

$$i = \frac{a_3 - a_2 \pm \sqrt{\Delta}}{2\lambda a_1} j, \text{ where } \Delta = (a_3 - a_2)^2 + 4\lambda a_0 a_1. \tag{10}$$

IV,a) $\Delta \neq 0$ is a quadratic residue in $GF(p)$. The number of non-invertible vectors in the set (8) equals to $2p-1$ and the multiplicative group of the subalgebra Ψ_A represented by the set (8) is attributed to the Γ_1 type.

IV,b) $\Delta \neq 0$ is a quadratic non-residue in $GF(p)$. The set (8) includes the single non-invertible vector $(0, 0, 0, 0)$ and represents a finite field that is isomorphic to the $GF(p^2)$ field. The multiplicative group Γ_3 of this subalgebra is cyclic and has order equal to $\Omega_3 = p^2 - 1$.

IV,c) $\Delta = 0$. The number of non-invertible vectors in the set (8) equals to p and the set (8) is a Ψ_A subalgebra that includes multiplicative group of the Γ_2 type and of order $\Omega_2 = p(p - 1)$.

Note that for a non-invertible vector A we have $\lambda a_0 a_1 = a_2 a_3$. Therefore, in the latter case $\Delta = (a_3 + a_2)^2$ and, if $a_3 \neq -a_2$, the set (8) contains $2p - 1$ non-invertible vectors (including A) and represents an algebra with multiplicative group of the Γ_1 type, which possesses 2-dimensional cyclicity and has order equal to $(p - 1)^2$. If $a_3 = -a_2$, then the multiplicative group of the Ψ_A subalgebra is attributed to the Γ_2 type.

Thus, every algebra element A that is not a scalar vector defines a subalgebra Ψ_A of order p^2. Suppose the set of scalar vectors is denoted as Σ. Evidently, Σ is contained in every subalgebra Ψ_A. The next Proposition 1 shows that every subalgebra Ψ_A defined by a vetor $A \notin \Sigma$ is commutative.

Proposition 1. *Suppose $A \notin \Sigma$, $X, X' \in \Psi_A$. Then $XX' = X'X$.*

Proof. Consequtively, fix every of the sets (5), (6), (7), and (8). For every of the latter four cases, select arbitrary two elements X and X' contained in the fixed set and, using Table 1, compute the vectors $V_1 = XX'$ and $V_2 = X'X$. For every of the cases one gets $V_1 = V_2$. □

Proposition 2. *Suppose $A \notin \Sigma$, $X \in \Psi_A$, and $X \notin \Sigma$. Then Ψ_X coinside with Ψ_A.*

Proof. Suppose $X' \in \Psi_A$. Since $X \in \Psi_A$, due to Proposition 1, we have $XX' = X'X$, i. e., $X' \in \Psi_X$. Respectively, if $X' \in \Psi_X$, then, taking into account that $A \in \Psi_X$ and Proposition 1, we have $AX' = X'A$, i. e., $X' \in \Psi_A$. □

Due to Proposition 2, one can see that every non-scalar vector X is contained in a unique Ψ subalgebra, namely, in subalgebra Ψ_X.

One has the following three types of the commutative Ψ subalgebras: Ψ_1, Ψ_2, and Ψ_3, characterized in structure of thier multiplicative group, namely, multiplicative group of a Ψ_h subalgebra represents a group of the Γ_h type, where $h = 1, 2, 3$.

4. Number of the Ψ_1, Ψ_2, and Ψ_3 subalgebras

The studied 4-dimensional FNAA has order p^4 and contains exactly three types of commutative subalgebras of order p^2. Due to Proposition 2, one can see that arbitrary two of the said subalgebras intersect exactly in the set of scalar vectors and every non-scalar vector is included in a unique Ψ subalgebra. Every Ψ subalgebra contains $p^2 - p$ unique non-scalar vectors. The studied FNAA contains $p^4 - p$ unique non-scalar vectors, therefore for the number η of the Ψ subalgebras one gets the following formula:

$$\eta = \frac{p^4 - p}{p^2 - p} = p^2 + p + 1. \tag{11}$$

Suppose k, t, and u denote numbers of different subalgebras of the Ψ_1, Ψ_2, and Ψ_3 types, correspondingly. Then we have $\eta = k + t + u$,

$$k + t + u = p^2 + p + 1. \tag{12}$$

Consider the multiplicative groups of the types Γ_1, Γ_2, and Γ_3. The values k, t, and u are equal to the numbers of different Γ_1, Γ_2, and Γ_3 groups, correspondingly. Taking into account that the set Σ includes $p-1$ invertible vectors and the orders of the Γ_1, Γ_2, and Γ_3 groups are equal to $(p-1)^2$, $p(p-1)$, and $\left(p^2 - 1\right)$, one can write

$$(\Omega_1 - (p-1))\,k + (\Omega_2 - (p-1))\,t + (\Omega_3 - (p-1))\,u = \Omega - (p-1);$$
$$\left((p-1)^2 - (p-1)\right)k + (p(p-1) - (p-1))\,t + \left(p^2 - 1 - (p-1)\right)u =$$
$$= p(p-1)(p^2-1) - (p-1);$$

$$(p-2)k + (p-1)t + pu = p^3 - p - 1. \tag{13}$$

Every fixed Ψ_2 subalgebra contains $p-1$ unique nonzero non-invertible vectors N such that $\Psi_N = \Psi_2$. To find the value t, consider the number of non-invertible vectors A relating to the Case IV,c), i. e. $a_0 \neq 0$; $a_1 \neq 0$; $\Delta = 0$, which define the commutative subalgebras containing multiplicative groups of the Γ_2 type. Such vectors satisfy the conditions $a_2a_3 = \lambda a_0 a_1 \neq 0$ and $\Delta = (a_3 + a_2)^2 = 0$. From the latter condition we have $a_3 = -a_2$. Thus, the Case IV,c) gives $(p-1)^2$ different vectors $A = \left(i, -j^2\lambda^{-1}i^{-1}, j, -j\right)$, where $i, j = 1, 2, \ldots p-1$, which define the subalgebras Ψ_A of the Ψ_2 type. Each of the subcases II,b) and III,b) gives other

$p-1$ unique vectors A composing a unique subalgebra of the Ψ_2 type. Totally, we have $(p-1)^2+2(p-1)=(p-1)(p+1)$ unique non-invertible vectors defining all subalgebras of the Ψ_2 type. Every subalgebra of the Ψ_2 type contains $p-1$ of the said non-invertible vectors and t algebras contain all vectors A: $t(p-1)=(p-1)(p+1)$, therefore,

$$t=p+1. \tag{14}$$

From (12), (13), and (14) we have

$$k=\frac{p(p+1)}{2};\quad u=\frac{p(p-1)}{2}. \tag{15}$$

Table 2

Setting the studied 4-dimensional FNAA studied in [1]; $\lambda \neq 0$.

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	0	0	$\mathbf{e}_3$
$\mathbf{e}_1$	0	$\mathbf{e}_1$	$\mathbf{e}_2$	0
$\mathbf{e}_2$	$\mathbf{e}_2$	0	0	$\lambda\mathbf{e}_1$
$\mathbf{e}_3$	0	$\mathbf{e}_3$	$\lambda\mathbf{e}_0$	0

Table 3

Setting the studied 4-dimensional FNAA studied in [6]; $\lambda \neq 0$.

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	0	0
$\mathbf{e}_1$	0	0	$\lambda\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\lambda\mathbf{e}_3$	0	0
$\mathbf{e}_3$	0	0	$\mathbf{e}_2$	$\mathbf{e}_3$

5. Disscussion and conclusion

In several HDLP-based digital signature algorithms on FNAAs there are used hidden groups possessing 2-dimensional cyclicity [5, 6, 1] and issues about existance and number of such groups have critical significance. The results obtained on the study of the structure of the 4-dimensional FNAA defined by Table 1 show that this algebra contains a sufficiently large number of groups with two-dimensional cyclicity. Therefore, the said algebra can be used as an algebraic support of the mentioned digital signature algorithms. Previously [6, 1], a similar study was performed for the algebras specified in Tables 2 and 3. The results of this work and of [6, 1] are mainly coincided, namely, the structure of algebras set by sparse Tables 1,2 and 3 is described from a single position. Each of these algebras is divided into commutative subalgebras of order p^2, which are attributed exacly to the following three types Ψ_1, Ψ_2, and Ψ_3. The number of the subalgebras of every type is described by the formulas (14) and (15). One can expect that other 4-dimensional FNAAs set by other sparse basis vector multiplication tables also possesses the same structure, however, the finite quaternion-like algebras [4] possess another structure.

Study of the structure of the FNAAs used as algebraic support of the HDLP-based signature schemes appears to be an important stage of the development of the said cryptoschemes.

References

[1] **D.N. Moldovyan**, *A practical digital signature scheme based on the hidden logarithm problem*, Computer Sci. J. Moldova, **29** (2021), no. 2, 206 – 226.

[2] **D.N. Moldovyan, A.A. Moldovyan, N.A. Moldovyan**, *Post-Quantum signature schemes for efficient hardware implementation*, Microprocessors and Microsystems, **80** (2021), 103487.

[3] **D.N. Moldovyan, A.A. Moldovyan, N.A. Moldovyan**, *An enhanced version of the hidden discrete logarithm problem and its algebraic support*, Quasigroups and Related Systems, **29** (2021), 97 – 106.

[4] **N.A. Moldovyan**, *Signature schemes on algebras, satisfying enhanced criterion of post-quantum security*, Bull. Acad. Sci. Moldova. Mathematics, **2(93)** (2020), 62 – 67.

[5] **N.A. Moldovyan, A.A. Moldovyan**, *Candidate for practical post-quantum signature scheme*, Vestnik Saint Petersburg Univ., Applied Math., Computer Sci.,. Control Processes, **16** (2020), 455 – 464.

[6] **N.A. Moldovyan, A.A. Moldovyan**, *Digital signature scheme on the 2x2 matrix algebra*, Vestnik Saint Petersburg Univ., Applied Math., Computer Sci., Control Processes, **17** (2020), 254 – 261.

[7] **N.A. Moldovyan, P.A. Moldovyanu**, *New primitives for digital signature algorithms*, Quasigroups and Related Systems, **17** (2009), 271 – 282.

[8] **D. Moody**, *NIST Status Update on the 3rd Round*, 2021. Available at: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf (accessed November 4, 2021).

[9] *Post-quantum cryptography*, Lecture Notes in Computer Sci., **11505**, (2019).

Received November 8, 2021

St. Petersburg Federal Research Center of the Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg, Russia
E-mail: nmold@mail.ru