Math-Net.Ru

Общероссийский математический портал

V. V. Vlasova, M. A. Pudovkina, Групповые свойства блочных алгоритмов шифрования российских стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.12-2015, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 2, 59–70

DOI: <https://doi.org/10.4213/mvk256>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.157.27.8

26 апреля 2023 г., 18:30:15

Group Properties of Block Ciphers of the Russian Standards GOST R 34.11-2012 and GOST R 34.12-2015

V. V. Vlasova¹, M. A. Pudovkina²

¹ Kaspersky Lab, Moscow

² Bauman Moscow State Technical University, Moscow

Получено 03.11.2017

Abstract. A group generated by the set of the round functions is often used to describe properties of a block cipher. The results obtained by A.S.Maslov in 2007 are used to prove that round functions of Kuznyechik and Stribog generate the alternating groups. We prove a theorem on the mixing properties of linear transformations and apply this theorem to the family of Stribog-like ciphers (Stribog, Anubis, etc.).

Key words: GOST R 34.11–2012, GOST R 34.12–2015, Kuznyechik, Stribog, permutation groups, alternating group, linear transformation of block cipher.

Групповые свойства блочных алгоритмов шифрования российских стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.12-2015

В. В. Власова¹, М. А. Пудовкина²

¹ АО «Лаборатория Касперского», Москва

² Московский государственный технический университет имени Н. Э. Баумана, Москва

Аннотация. Группа, порожденная множеством раундовых функций, часто используется для описания свойств блочного шифра. С помощью теоремы об условиях знакопеременности группы, порожденной раундовыми преобразованиями XSL-шифра, полученной в 2007 г. А. С. Масловым, доказана знакопеременность групп, порожденных раундовыми функциями алгоритма блочного шифрования Кузнечик и алгоритма блочного шифрования, используемого в функции хеширования Стрибог. В частности, для линейных преобразований в Стрибог-подобных алгоритмах (Стрибог, Anubis и др.) установлена примитивность графа, ассоциированного с этими преобразованиями.

Ключевые слова: ГОСТ Р 34.11–2012, ГОСТ Р 34.12–2015, Кузнечик, Стрибог, группы подстановок, знакопеременная группа, линейное преобразование блочного алгоритма шифрования

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 2, pp. 59–70 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

1. Introduction

Round functions of most contemporary block ciphers may be represented as compositions of functions of X-, L- and S-layers, where X-layer is a key addition layer, S-layer realizes S-boxes mappings and L-layer is a linear transformation. Such block ciphers are called XSL-ciphers. This principle underlies many official standards, such as AES [1] (adopted by NIST as FIPS PUB 197), Whirlpool hash function [2] (included in ISO/IEC 10118-3:2004), the Russian standards GOST R 34.11-2012 [3] and GOST R 34.12-2015 [4].

Group properties of XSL-ciphers are widely discussed [5–10]. In [5] a group theoretic approach to the design and analysis of cryptographic systems has been discussed.

It was proved by Wernsdorf [11] that the permutation group G generated by the round functions of DES is the alternating group. In his later paper [7] he used ad hoc methods to prove that the group G of AES is alternating. Some years later, Sparr and Wernsdorf [8] have given another (permutation group theoretic) proof. They also have obtained a set of sufficient conditions for the group G to be alternating. Another sets of such sufficient conditions have been given in [9] and [10].

The conditions given in [9] represent the slightly changed conditions of primitivity of the group G proposed earlier by the same authors [6]. Also in [9] it was shown that AES satisfies the given conditions. It should be noted that the key schedule isn't taken into account in mentioned works.

If the group G of an XSL-cipher is alternating, then several possible regularities such as the existence of non-trivial factor groups or a too small diversity of occurring permutations may be excluded for this cipher (the alternating group is a large, simple, primitive and multiple transitive permutation group).

In this paper we use the results obtained in [10] to prove that the groups generated by round functions of Kuznyechik and Stribog are the alternating groups. We get the new matrix representation of the linear transformations of the ciphers. Also we describe properties of the linear transformations and generalize them for the family of Stribog-like ciphers (Stribog, Anubis, etc.). We prove a theorem in which the mixing properties of linear transformations of such ciphers are considered.

The paper is organized as follows. In Section 2 we provide some necessary notions and results from the graph theory. In Section 3 we review some results of [10] on groups generated by round functions of XSL-ciphers. In Section 4 we describe some properties of linear transformations of such ciphers regarding their mixing properties. In Section 5 we give the descriptions of Kuznyechik and Stribog and also prove that the groups generated by their round functions are the alternating groups.

2. Definitions and notation

We use 0_m to denote the zero element of $GF(2^m)$ and 1_m to denote the multiplicative identity element of $GF(2^m)$. Let V_l be the l -dimensional vector space over the field $GF(2)$. There is a natural correspondence between elements of $GF(2)^l$ and V_l ; thus, we will identify them. Let $S(V_l)$ and $A(V_l)$ denote the symmetric and the alternating group acting on V_l , respectively. Also note that elements from V_{mn} may be represented as vectors from the Cartesian product V_m^n . Therefore we will identify this representations. Symbol $||$ means strings concatenation.

The set of all $p \times q$ matrices over $GF(u)$ is denoted by $M_{p,q}(u)$. We will write $M_p(u)$ instead of $M_{p,p}(u)$.

Elements $\alpha = (\alpha_0, \dots, \alpha_{pq-1}) \in GF(u)^{pq}$ are identified with matrices $\beta = (\beta_{ij}) \in M_{p,q}(u)$ via the mapping $GF(u)^{pq} \rightarrow M_{p,q}(u)$, defined by $\beta_{ij} = \alpha_{qi+j}$ for all $i \in \{0, \dots, p-1\}$ and $j \in \{0, \dots, q-1\}$.

Definition. A strongly connected digraph Γ with an adjacency matrix $\mathbf{a}$ is called *primitive* if there is an integer r such that all entries of $\mathbf{a}^r$ are non-zero.

Definition. For a linear transformation $a: V_m^n \rightarrow V_m^n$, we will assign a digraph $\Gamma(a)$ with a set of vertices $\{1, \dots, n\}$ and a set of edges X , where edge $(i, j) \in X$ exists if and only if $\beta_j = a(\alpha_i)$ and β_j essentially depends on α_i for all $\alpha_1, \dots, \alpha_n \in GF(2^m)$. We say that digraph $\Gamma(a)$ is a *graph of essential dependence* of a linear transformation a .

3. Properties of Generated Group

In papers [8–10] conditions have been provided ensuring that the group generated by round functions of XSL-ciphers is the alternating group. In this section we give the theorem proved in [10].

We consider a block cipher with a set of all round keys K and a round function $g_k: V_{mn} \rightarrow V_{mn}$, $k \in K$, which is given as

$$g_k: \alpha \mapsto a \circ s \circ x[k](\alpha),$$

where $a, s, x[k]: V_{mn} \rightarrow V_{mn}$ are functions with the following properties:

- a is an invertible linear transformation over a general linear group of a vector space V_{mn} ,
- s is a parallel application of n bijective S-box mappings $s_i: V_m \rightarrow V_m$ defined by $s: (\alpha_1, \dots, \alpha_n) \mapsto (s_1(\alpha_1), \dots, s_n(\alpha_n))$ for all $i \in \{1, \dots, n\}$;
- $x[k]$ is a XOR-addition with a round key $k \in V_{mn}$, i. e. $x[k]: \alpha \mapsto \alpha \oplus k$.

Let G be a group generated by the set $\{g_k \mid k \in K\}$ of all round functions. In this paper properties of the round subkeys caused by the key schedule are neglected. The sufficient conditions for the equality

$$G = \langle g_k \mid k \in K \rangle = A(V_{mn})$$

are shown below.

Let $\Gamma(a)$ be a graph of essential dependence of a linear transformation $a: V_m^n \rightarrow V_m^n$.

For a vector $\alpha = (\alpha_1, \dots, \alpha_n)$, $\alpha \in V_m^n$, we will assign a set

$$I(\alpha) = \{i \in \{1, \dots, n\} \mid \alpha_i \neq 0_m\}.$$

If I is a subset of vertices of the digraph $\Gamma(a)$, then $J(I)$ denotes the set of ends of edges which starts at the set I .

With each permutations s_i , $i \in \{1, \dots, n\}$, we associate permutations

$$s_{i,k,k'}: \alpha \mapsto s_i^{-1} \circ x[k'] \circ s_i \circ x[k](\alpha),$$

where $k, k' \in V_m$. Let $H(s_i) = \langle s_{i,k,k'} \mid k, k' \in V_m^2 \rangle$ be a group generated by such permutations.

Theorem 1 ([10]). *Suppose that the following conditions hold:*

- 1) *digraph $\Gamma(a)$ is primitive,*
- 2) *for any set $L \subseteq \{1, \dots, n\}$*

$$\max_{\{\alpha \in V_{mn} \mid I(\alpha) = L\}} |I(a(\alpha))| \geq |L|,$$

where the inequality is strict if $|J(I)| > |I|$,

- 3) *groups $H(s_1), \dots, H(s_n)$ are 2-transitive, and there exists a permutation $s \in \bigcup_{i=1}^n H(s_i)$ such that*

$$|\{\alpha \in V_m \mid s(\alpha) = \alpha\}| \notin \{0, 2^0, 2^1, 2^2, \dots, 2^m\}.$$

Then G is equal to the alternating group on V_{mn} .

4. Properties of linear transformations

The first condition required by Theorem 1 is related to the properties of a linear transformation. We describe a way to define a linear transformation of some XSL-ciphers (Stribog, Anubis, etc.). In Theorem 2 we show that the first condition is valid for such ciphers. This theorem refers to a graph of essential dependence of a linear transformation. The obtained results may be used to analyse mixing properties of a linear transformation of an XSL-cipher.

Definition. A linear transformation $a: GF(2^m)^{p^2} \rightarrow GF(2^m)^{p^2}$ is called $\tilde{T}$ -transformation, if a may be represented as a composition of mappings t and l ($a = l \circ t$), where:

- t is the transpose of a matrix from a set $M_p(2^m)$, i.e. $t(\alpha) = \beta$, if and only if $\beta_{ij} = \alpha_{ji}$, where $\alpha, \beta \in M_p(2^m)$, $i, j \in \{1, \dots, p\}$,
- l is an invertible linear transformation over $M_p(2^m)$, that may be represented as a right multiplication by a fixed matrix $\mathbf{d} \in M_p(2^m)$, i.e. $l(\alpha) = \alpha \cdot \mathbf{d}$ for all $\alpha \in M_p(2^m)$.

Theorem 2. Let $a = l \circ t$ be a $\tilde{T}$ -transformation and the matrix $\mathbf{d}$ (corresponding to the transformation l) does not contain zero elements. Then the digraph $\Gamma(a)$ of essential dependence of the transformation a is primitive.

The proof is given in Appendix A.

5. Application to block ciphers Kuznyechik and Stribog

In this section we apply the results obtained in Section 4 to block ciphers underlying GOST R 34.11-2012 and GOST R 34.12-2015. Hereinafter the block cipher underlying GOST R 34.11-2012, we will call the Stribog block cipher.

We begin by giving brief descriptions of Kuznyechik and Stribog.

5.1. The description of Kuznyechik

Kuznyechik is specified by the Russian Federal standard GOST R 34.12-2015. It is an iterative block cipher with a block length of 128 bits and a key length of 256 bits. Transformations of X-, S-, and L-layers are applied for encryption throughout several iterations.

X-layer is a key addition layer defined as $x[k]: V_{128} \rightarrow V_{128}$,

$$x[k](\alpha) = k \oplus \alpha \quad \text{for all } k, \alpha \in V_{128}.$$

S-layer is an S-box layer defined by the mapping $s: V_{128} \rightarrow V_{128}$, $s(\alpha) = (s'(\alpha_{15}), \dots, s'(\alpha_0))$, where $\alpha = (\alpha_{15}, \dots, \alpha_0) \in V_8^{16}$, $s' \in S(V_8)$.

The L-layer transformation $a_1: V_{128} \rightarrow V_{128}$ is based on a linear-feedback shift register with a given feedback function $l': V_8^{16} \rightarrow V_8$. The function l' is given by the polynomial of degree 16 over $GF(2^8)$ with irreducible polynomial $p_k(x) = x^8 + x^7 + x^6 + x + 1$.

Depending on the values of round keys $k_1, \dots, k_{10}$ the encryption algorithm is a substitution $e_{k_1, \dots, k_{10}}: V_{128} \rightarrow V_{128}$ is defined as follows:

$$e_{k_1, \dots, k_{10}}(\alpha) = x[k_{10}] \circ \prod_{i=1}^9 (a_1 \circ s \circ x[k_i](\alpha)),$$

where $\alpha, k_i \in V_{128}$ for all $i \in \{1, \dots, 10\}$.

Let $g_k: V_{128} \rightarrow V_{128}$ be a round function of Kuznyechik

$$g_k: \alpha \mapsto a_1 \circ s \circ x[k](\alpha), \quad \text{where } \alpha, k \in V_{128}.$$

Further, we will consider the group $G = \langle g_k \mid k \in K \rangle$ generated by the set of all round functions of Kuznyechik. Note that properties of the key scheduling algorithm are not taken into account.

5.2. The description of Stribog

Stribog is specified by the Russian Federal standard GOST R 34.11–2012. The hash procedure is based on a block cipher with block size of 512 bits and provides digest sizes of 256 and 512 bits. The transformations of X-, S-, P- and L-layer are used to calculate the hash code of a message from V^* .

X-layer is a round constants addition layer defined as $x[k]: V_{512} \rightarrow V_{512}$,

$$x[k](\alpha) = k \oplus \alpha, \quad \text{for all } k, \alpha \in V_{512}.$$

S-layer is an S-box layer defined by the mapping $s: V_{512} \rightarrow V_{512}$, $s(\alpha) = (s'(\alpha_{63}), \dots, s'(\alpha_0))$, where $\alpha = (\alpha_{63}, \dots, \alpha_0) \in V_8^{64}$, $s' \in S(V_8)$.

The P-layer transformation $V_{512} \rightarrow V_{512}$ is defined by the mapping $t: \alpha \mapsto \beta$, $\beta = (\beta_{63} \parallel \dots \parallel \beta_0) = (\alpha_{\tau(63)} \parallel \dots \parallel \alpha_{\tau(0)})$, where $\tau \in S(\{0, 1, \dots, 63\})$.

The L-layer transformation $V_{512} \rightarrow V_{512}$ is defined by the mapping $l: \alpha \mapsto \beta$, $\beta = (\beta_7 \parallel \dots \parallel \beta_0) = (l''(\alpha_7) \parallel \dots \parallel l''(\alpha_0))$, where $l'': V_{64} \rightarrow V_{64}$ is a right multiplication by the matrix $\mathbf{d}_s \in M_{64}(2)$.

The hash code value of a message from V^* is calculated via iterated procedure. The compression function $h_\delta: V_{512} \times V_{512} \rightarrow V_{512}$, $\delta \in V_{512}$, acts on each iteration. The compression function is defined by the rule

$$h_\delta(\eta, \alpha) = f(l \circ t \circ s(\eta \oplus \delta), \alpha) \oplus \eta \oplus \alpha, \quad \eta, \alpha \in GF(2)^{512},$$

where

$$f(k, \alpha) = x[k_{13}] \circ \prod_{i=1}^{12} (l \circ t \circ s \circ x[k_i](\alpha)),$$

for all $\alpha, k_i \in V_{512}$ for all $i \in \{1, \dots, 13\}$.

Let linear transformation $a_2: V_{512} \rightarrow V_{512}$ be a composition of mappings acting on L- and P-layers ($a_2 = l \circ t$). Let $g_k: V_{512} \rightarrow V_{512}$ be a round function of Stribog

$$g_k: \alpha \mapsto a_2 \circ s \circ x[k](\alpha),$$

where $\alpha, k \in V_{512}$.

In what follows we will consider the group $G = \langle g_k \mid k \in K \rangle$ generated by the set of all round functions of Stribog. Note that properties of the key scheduling algorithm are not taken into account.

5.3. Group properties of Kuznyechik and Stribog block ciphers

First, we give matrix representations of linear transformations used in Kuznyechik and Stribog.

Linear transformation in Kuznyechik may be represented as right multiplication by the matrix from $M_{16}(2^8)$. Such matrix $\mathbf{m}_k \in M_{16}(2^8)$ has been calculated (see Appendix B).

In GOST R 34.11-2012 the description of L-layer is based on the transformation l which is the right multiplication by a fixed matrix from $M_{64}(2)$.

Binary vectors $\alpha \in V_{512}$ at the input to the linear transformation are considered as elements of $GF(2^8)^{64}$. We will identify vector $\alpha \in V_{512}$ with a matrix $\beta \in M_8(2^8)$ via mapping

$$GF(2^8)^{64} \rightarrow M_8(2^8), \quad \alpha \mapsto \beta,$$

defined by the rule

$$\beta_{ij} = \alpha_{8i+j} \quad \text{for all } i, j \in \{0, \dots, 7\}.$$

As was shown in [12] the L-layer transformation of Stribog may be represented as a left multiplication by the matrix from $M_8(2^8)$. Such matrix has been found in [12]. The multiplication is performed in $GF(2^8)$ with irreducible polynomial

$$p'(x) = x^8 + x^6 + x^5 + x^4 + 1.$$

However calculations using that matrix require the additional conversions of the state bits.

The L-layer transformation of the Stribog block cipher may also be represented as a right multiplication by the matrix $\mathbf{d}_s \in M_8(2^8)$, i. e.

$$\alpha \mapsto \beta, \quad \beta = \alpha \cdot \mathbf{d}_s \quad \text{for all } \alpha, \beta \in M_8(2^8).$$

Such matrix $\mathbf{d}_s \in M_8(2^8)$ has been found using the algorithm described in [12] and given in Appendix B. The multiplication is performed in $GF(2^8)$ with irreducible polynomial

$$p_s(x) = x^8 + x^4 + x^3 + x^2 + 1.$$

The P-layer transformation of Stribog may be represented as a transposition of a matrix from $M_8(2^8)$.

Thus the linear transformation a_2 of Stribog is a $\tilde{T}$ -transformation.

Theorem 3. *For Kuznyechik and Stribog block ciphers the groups G generated by sets of all their round functions are equal to the alternating groups $A(V_{128})$ and $A(V_{512})$ respectively.*

Proof. First, we check the first condition of Theorem 1 for the Kuznyechik block cipher by describing properties of its linear transformation a_1 .

Using the matrix $\mathbf{m}_k \in M_{16}(2^8)$ of the linear transformation a_1 , it is easy to find the graph of essential dependence $\Gamma(a_1)$. Obviously, this graph is primitive if the matrix $\mathbf{m}_k$ does not contain any zero elements.

Secondly, we consider properties of the linear transformation of the Stribog block cipher.

The linear transformation a_2 of Stribog is a $\tilde{T}$ -transformation and its matrix $\mathbf{d}_s$ does not contain zero elements. Therefore, the graph $\Gamma(a_2)$ of essential dependence is primitive according to Theorem 2.

To check the second condition of Theorem 1, we have used Theorem 2 proved in [10]. According to this theorem the condition 2 is satisfied if the inequality

$$2^{mn} < (2^{m-1})^{n-1}(2^m + 2^{m-1} - 2) \quad (1)$$

is true. By means of direct calculations the correctness of inequality (1) has been verified for Kuznyechik and Stribog block ciphers. For Kuznyechik the left-hand side of inequality (1) is $3,4028 \times 10^{38}$ and the right-hand side is $4,7881 \times 10^{38}$. For Stribog, the left-hand side of inequality (1) is $1,3408 \times 10^{154}$ and the right-hand side is $1,5635 \times 10^{154}$.

The third condition of Theorem 1 characterizes the properties of S-boxes of a block cipher. S-boxes permutations are the same for Kuznyechik and Stribog. It should be noted that the same permutations are used in each S-box. The difference distribution matrix λ for S-boxes has been found. Then the matrix μ has been calculated by rule $\mu = \lambda \cdot \lambda^T$, where λ^T denotes the transposed matrix λ . For the obtained matrix we assign the graph $\Lambda(s)$ with a set of vertices being the set of all non-zero vectors from V_m , its vertices α and β are connected by an edge if and only if $\mu_{\alpha\beta} > 0$.

According to Theorem 3 proved in [10], a group $H(s)$ is 2-transitive if and only if the graph $\Lambda(s)$ is connected. Connectivity of the graph Λ for S-boxes of Kuznyechik and Stribog has been verified by direct calculations.

Consider the second part of the third condition of Theorem 1. Note that proving it means the existence of elements v of difference distribution matrix λ such that $v \notin \{0, 2^0, 2^1, 2^2, \dots, 2^m\}$. Such elements which are equal to 6, have been found in the calculated matrix λ . $\square$

References

- [1] “Advanced Encryption Standard (AES)”. In: “*FIPS Publication 197*”, 2001, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>.
- [2] *ISO/IEC 10118-3: Information Technology — Security Techniques — Hash-functions — Part 3: Dedicated hash-functions*: Internat. Organiz. for Standardization, 2004.
- [3] *GOST R 34.11–2012. Information technology. Cryptographic data security. Hash-function*, Moscow: Standardinform, 2012, 38 p.
- [4] *GOST R 34.12–2015. Information technology. Cryptographic data security. Block cipher*, Moscow: Standardinform, 2015, 25 p.
- [5] Glukhov M. M., Pogorelov B.A., “On some applications of groups in cryptography”. In: “*Math. and Security of Inform. Technol. (MSU, 2004)*”, Moscow: MCNMO, 2005, 19–31 (In Russian).
- [6] Caranti A., Dalla Volta F., Sala M., Villani F., “Imprimitive permutation groups generated by the round functions of key-alternating block ciphers and truncated differential cryptanalysis” (2006), arXiv: math/0606022v2.
- [7] Wernsdorf R., “The round functions of RIJNDAEL generate the alternating group”. In: “*FSE 2002, Lect. Notes Comput. Sci.*”, **2365**, 2002, 143–148.
- [8] Sparr R., Wernsdorf R., “Group theoretic properties of Rijndael-like ciphers”, *Discrete Appl. Math.*, **126**, 3139–3149.
- [9] Caranti A., Dalla Volta F., Sala M., “An application of the O’Nan-Scott theorem to the group generated by the round functions of an AES-like cipher”, *Des., Codes and Cryptogr.*, **52**:3 (2009), 293–301.
- [10] Maslov A. S., “On sufficient conditions to generate the alternating group by SA-permutations”, *Trudy Inst. Matem. Minsk*, **15**:2 (2007), 58–68 (In Russian), <http://mi.mathnet.ru/timb98>.
- [11] Wernsdorf R., “The one-round functions of the DES generate the alternating group”, *Lect. Notes Comput. Sci.*, **658** (1992), 99–112.
- [12] Kazymyrov O., Kazymyrova V., “Algebraic aspects of the Russian Hash Standard GOST R 34.11–2012”, *Cryptology ePrint Archive*, 2013/556 (2013), <http://eprint.iacr.org/2013/556>.
- [13] Sachkov V. N., Tarakanov V. E., *Combinatorics of Nonnegative Matrices*, Moscow: TVP Sci. Publ., 2000, 452 pp. (in Russian).

Appendix

A. The proof of Theorem 2

As a start, recall the following well-known results from graph theory.

The maximal length of the shortest path between the vertices is called the *diameter* of a graph (digraph). The greatest common divisor of the lengths of the closed paths of the graph (digraph) Γ is called the *period* of Γ .

Theorem 4 ([13]). *Strongly connected graph (digraph) Γ is primitive if and only if its period equals to 1.*

Let $n = pq$.

The $\tilde{T}$ -transformation a may be represented as a right multiplication by the matrix from $M_{n,n}(2^m)$. We will find the matrix $m \in M_{n,n}(2^m)$ such that $a(\beta) = \beta \cdot m$ for all $\beta \in GF(2^m)^n$. Such matrix has a form $m = t \cdot d$, where t and d are matrices from $M_{n,n}(2^m)$ corresponding to transformation t and l_d respectively.

Consider the matrix $t \in M_{n,n}(2^m)$ such as $t(\beta) = \beta \cdot t$ for all $\beta \in GF(2^m)^n$. This matrix $t = (\hat{t}_{ij})$ corresponds to permutation matrix $t = (t_{ij}) \in M_{n,n}(2)$ in such a way that $\hat{t}_{ij} = 0_m$ if $t_{ij} = 0$ and $\hat{t}_{ij} = 1_m$ if $t_{ij} = 1$ for all $i, j \in 0n - 1$. The matrix t exchanges elements with indexes $iq + j$ and $jp + i$, and thus it consists of blocks t_{ij} of size $q \times p$, where $i \in \{0, \dots, p - 1\}$, $j \in \{0, \dots, q - 1\}$. In each block of t_{uv} there is only one non-zero element, which equals t_{vu} . This holds for the matrix $t \in M_{n,n}(2^m)$, i. e. for any arbitrary block t_{uv} we have

$$t = \begin{pmatrix} \vdots & & \\ \dots t_{uv} \dots & & \\ \vdots & & \\ \vdots & & \end{pmatrix}, \quad t_{uv} = \begin{pmatrix} 0 & \vdots & 0 \\ \vdots & \vdots & \vdots \\ \dots \hat{t}_{vu} \dots & & \\ 0 & \vdots & 0 \end{pmatrix}, \quad \hat{t}_{vu} = 1_m,$$

where $u \in 0p - 1, v \in 0q - 1$.

Next, consider the matrix $d \in M_{n,n}(2^m)$ such that $l_d(\beta) = \beta \cdot d$ for all $\beta \in GF(2^m)^n$. The matrix $\hat{d}$ is a quasidiagonal $(pq \times pq)$ -matrix with $p \times p$ blocks. For each $i \in \{0, \dots, q - 1\}$ the block $\hat{d}_{ii}$ is equal to the matrix $d \in M_{p,p}(2^m)$. If the matrix d does not have zero elements, then each block $\hat{d}_{ii}$ does not contain zero elements for all $i \in \{0, \dots, q - 1\}$.

Therefore, matrix $m = t \cdot d$ is a block matrix with $p \times q$ blocks of size $q \times p$. Since j^{th} row of each block t_{ij} contains 1_m , then j^{th} row of each block m_{ij} contain only non-zero elements for all $i \in 0p - 1, j \in 0q - 1$.

Let $\Gamma(a)$ be a graph of essential dependence of transformation a . Its adjacency matrix $\mathbf{a} = (a_{ij})$ may be obtained from the matrix $m = (m_{ij})$ by rule

$$a_{ij} = \begin{cases} 0, & \text{if } m_{ij} = 0_m, \\ 1, & \text{if } m_{ij} \neq 0_m \end{cases}$$

for all $i, j \in \{0, \dots, n-1\}$.

Note that j^{th} row of each block $\mathbf{a}_{ij}$ contains only non-zero elements, $i \in 0p-1$, $j \in 0q-1$. As a result, in digraph Γ there are exactly p edges from each vertex $i \in \{0, \dots, pq-1\}$ to p different vertices with numbers $p(i \bmod q) + u$, where $u \in \{0, \dots, p-1\}$. In two steps vertices with numbers

$$p((p(i \bmod q) + u) \bmod q) + v, \quad u, v \in \{0, \dots, p-1\}$$

may be reached from each vertex i of Γ , $i \in \{0, \dots, pq-1\}$. If $p \geq q$, then all pq vertices of Γ will be reached. If $p < q$, then we reach p^2 different vertices. However, for some finite number $x \in \mathbb{N}$ we have $p^x \geq q$ (and $p^{x-1} < q$). Thus, it may be proved by induction on the number of steps that all pq vertices of Γ will be reached from any vertex in $x+1$ steps. Therefore the digraph Γ is *strongly connected* (and its diameter is equal to $\lceil \log_p q \rceil + 1$). Also, since the digraph Γ has a loop (vertex with number 0 has an edge to oneself), the *period* of Γ is equal to 1. Consequently, the digraph Γ is *primitive*, according to Theorem 4. $\square$

B. The matrices of linear transformations

The matrix $\mathbf{d}_s$ of the transformation l of Stribog:

$$\begin{pmatrix} 83 & 47 & 8B & 07 & B2 & 46 & 87 & 64 \\ 46 & B6 & 0F & 01 & 1A & 83 & 98 & 8E \\ AC & CC & 9C & A9 & 32 & 8A & 89 & 50 \\ 03 & 21 & 65 & 8C & BA & 93 & C1 & 38 \\ 5B & 06 & 8C & 65 & 18 & 10 & A8 & 9E \\ F9 & 7D & 86 & D9 & 8A & 32 & 77 & 28 \\ A4 & 8B & 47 & 4F & 9E & F5 & DC & 18 \\ 64 & 1C & 31 & 4B & 2B & 8E & E0 & 83 \end{pmatrix}.$$

The multiplication is performed in $GF(2^8)$ with irreducible polynomial

$$p_s(x) = x^8 + x^4 + x^3 + x^2 + 1.$$

The matrix $\mathbf{m}_k$ of the transformation a_1 of Kuznyechik:

CF	$6E$	$A2$	76	72	$6C$	48	$7A$	$B8$	$5D$	27	BD	10	DD	84	94
98	20	$C8$	33	$F2$	76	$D5$	$E6$	49	$D4$	$9F$	95	$E9$	99	$2D$	20
74	$C6$	87	10	$6B$	EC	62	$4E$	87	$B8$	BE	$5E$	$D0$	75	74	85
BF	DA	70	$0C$	CA	$0C$	17	$1A$	14	$2F$	68	30	$D9$	CA	96	10
93	90	68	$1C$	20	$C5$	06	BB	CB	$8D$	$1A$	$E9$	$F3$	97	$5D$	$C2$
$8E$	48	43	11	EB	BC	$2D$	$2E$	$8D$	12	$7C$	60	94	44	77	$C0$
$F2$	89	$1C$	$D6$	02	AF	$C4$	$F1$	AB	EE	AD	BF	$3D$	$5A$	$6F$	01
$F3$	$9C$	$2B$	$6A$	$A4$	$6E$	$E7$	BE	49	$F6$	$C9$	10	AF	$E0$	DE	FB
$0A$	$C1$	$A1$	$A6$	$8D$	$A3$	$D5$	$D4$	09	08	84	EF	$7B$	30	54	01
BF	64	63	$D7$	$D4$	$E1$	EB	AF	$6C$	54	$2F$	39	FF	$A6$	$B4$	$C0$
$F6$	$B8$	30	$F6$	$C4$	90	99	37	$2A$	$0F$	EB	EC	64	31	$8D$	$C2$
$A9$	$2D$	$6B$	49	01	58	78	$B1$	01	$F3$	FE	91	91	$D3$	$D1$	10
EA	86	$9F$	07	65	$0E$	52	$D4$	60	98	$C6$	$7F$	52	DF	44	85
$8E$	44	30	14	DD	02	$F5$	$2A$	$8E$	$C8$	48	48	$F8$	48	$3C$	20
$4D$	$D0$	$E3$	$E8$	$4C$	$C3$	16	$6E$	$4B$	$7F$	$A2$	89	$0D$	64	$A5$	94
$6E$	$A2$	76	72	$6C$	48	$7A$	$B8$	$5D$	27	BD	10	DD	84	94	01

The multiplication is performed in $GF(2^8)$ with irreducible polynomial

$$p_k(x) = x^8 + x^7 + x^6 + x + 1.$$