Math-Net.Ru

Общероссийский математический портал

А. А. Nechaev, А. V. Abornev, Нелинейные перестановки пространства над конечным полем, порожденные линейными преобразованиями модуля над кольцом Галуа, *Матем. вопр. криптогр.*, 2013, том 4, выпуск 2, 81–100

DOI: <https://doi.org/10.4213/mvk85>

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: 54.80.73.141

26 апреля 2023 г., 13:37:20

УДК: 512.643

Nonlinear permutations of a space over a finite field induced by linear transformations of a module over a Galois ring*

A. A. Nechaev¹, A. V. Abornev²

¹Academy of Cryptography of the Russian Federation, Moscow

²LLC «Certification Research Center», Moscow

Получено 18.IX.2012

Nonlinear permutations of m -dimensional vector space $P^{(m)}$ over a finite field $P = \text{GF}(q)$ induced by linear transforms of a module $R^{(m)}$ over a Galois ring $R = \text{GR}(q^2, p^2)$, $q = p^r$, are constructed. The transforms constructed by iteration of linear recurrent transforms are studied separately. Some applications in cryptography are discussed.

Key words: digit-permutable matrix, DP-matrix, digit-permutable polynomial, DP-polynomial, Galois ring, block ciphering system

Нелинейные перестановки пространства над конечным полем, порожденные линейными преобразованиями модуля над кольцом Галуа

А. А. Нечаев¹, А. В. Аборнев²

¹Академия криптографии Российской Федерации, Москва

²ООО «Центр сертификационных исследований», Москва

Аннотация. Построены нелинейные перестановки m -мерного векторного пространства $P^{(m)}$ над конечным полем $P = \text{GF}(q)$, порожденные линейными отображениями модуля $R^{(m)}$ над кольцом Галуа $R = \text{GR}(q^2, p^2)$, $q = p^r$. Отдельно рассматриваются отображения, порожденные итерациями линейных рекуррентных преобразований. Обсуждаются некоторые криптографические применения.

Ключевые слова: матрица перестановки разрядов, DP-матрица, многочлен перестановки разрядов, DP-многочлен, кольцо Галуа, блочные системы шифрования

Citation: *Mathematical Aspects of Cryptography*, 2013, vol. 4, no. 2, pp. 81–100 (Russian).

© 2013 A. A. Nechaev, A. V. Abornev

* The research was carried out with financial support of the Academy of Cryptography of the Russian Federation

1. Introduction

Let $R = \text{GR}(q^2, p^2)$, $q = p^r$, be a Galois ring of cardinality q^2 and characteristic p^2 with identity e . The set $P = \Gamma(R) = \{a \in R: a^q = a\}$ is called *p-adic digit set* of a ring R . Any element $a \in R$ has *p-adic decomposition*

$$a = a_0 + pa_1, \quad a_s = \gamma_s(a) \in P, \quad s \in \{0, 1\}. \quad (1)$$

We call the functions $\gamma_s: R \rightarrow P$, $s \in \{0, 1\}$, *digit functions* (in a digit set P). The digit set P has cardinality q , is closed relative to the multiplication “ $\cdot$ ” on R and algebra $(P, \oplus, \cdot)$ with the addition $a \oplus b = \gamma_0(a + b)$ is a field.

Let $R_{m,m}$ be a set of $m \times m$ -matrices over R . For a matrix $A = (a(i, j)) \in R_{m,m}$ we can consider also the decomposition $A = A_0 + pA_1 = \gamma_0(A) + p\gamma_1(A)$, $A_s = (\gamma_s(A))$, $s = 0, 1$.

Let $\oplus, \odot$ be matrix operations over the field P and “+”, “ $\cdot$ ” be matrix operations over the ring R . Any $A \in R_{m,m}$ defines a mapping $\pi_A: P^{(m)} \rightarrow P^{(m)}$ such that for all $y^\perp \in P^{(m)}$

$$\pi_A(y^\perp) = \gamma_1(A \cdot y^\perp) = \gamma_1(A_0 \cdot y^\perp) \oplus (A_1 \odot y^\perp) = (\psi_1(y^\perp), \dots, \psi_m(y^\perp))^T, \quad (2)$$

where $\psi_1, \dots, \psi_m$ are coordinate functions and T is a transpose operation. We call π_A a *nonlinear* map if it is not a homomorphism of the group $(P^{(m)}, \oplus)$.

First of all we represent the following essentially new result.

Theorem 1. *For any $m > 1$ there exists an invertible matrix A such that π_A is a nonlinear permutation of the space $P^{(m)}$.*

The proof of Theorem 1 follows from the results given below.

If π_A is a permutation, then the system of functions $\psi_1, \dots, \psi_m$ in (2) is called *orthogonal* [1]. We call A a *digit-permutable matrix* (or *DP-matrix*) and π_A a *(linearly generated by A) digit permutation* on $P^{(m)}$.

The coordinate functions $\psi_1, \dots, \psi_m$ in (2) are polynomials over the field P of the form

$$\psi_i(y^\perp) = \gamma_1(a_0(i1)y_1 + \dots + a_0(im)y_m) \oplus l_i(y^\perp), \quad i = 1, \dots, m, \quad (3)$$

where $l_i(y^\perp) = a_1(i1)y_1 \oplus \dots \oplus a_0(im)y_m$ is a linear function and γ_1 is a homogeneous polynomial of degree q over P . In particular for $p = 2$

$$\gamma_1(a_0(i1)y_1 + \dots + a_0(im)y_m) = \sigma_2(a_0(i1)y_1, \dots, a_0(im)y_m)^h, \quad (4)$$

where $h = 2^{r-1}$, $\sigma_2(x_1, \dots, x_m) = \bigoplus_{1 \leq s < t \leq m} x_s x_t$ is an elementary symmetric polynomial of order 2 (see [2]).

In general, the coordinate function $\psi_i(y^\perp)$ is not linear iff i -th row $\vec{A}(i)$ of the matrix A contains more than one invertible element.

Let

$$S(F) = \begin{pmatrix} 0 & e & 0 & \dots & 0 \\ 0 & 0 & e & \dots & 0 \\ & & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & e \\ f_0 & f_1 & f_2 & \dots & f_{m-1} \end{pmatrix} \quad (5)$$

be an accompanying matrix of a polynomial $F(x) = x^m - \sum_{i=0}^{m-1} f_i x^i \in R[x]$. For applications DP-matrices of the form $A = S(F)^m$ are of great interest. We call such matrices *recursively generated*. In this case a permutation π_A has effective recursive realization.

It is interesting to investigate cryptographic primitives of the form $(\pi_A G)^k \subset \mathfrak{S}(P^{(m)})$, where G is some regular subgroup of the symmetric group $\mathfrak{S}(P^{(m)})$, e. g. G is a regular representation of the group $(P^{(m)}, \oplus)$ or a cyclic group.

So we consider as important the problem of construction (for sufficiently large alphabet $P^{(m)}$) invertible DP-matrices A such that:

- π_A is a nonlinear permutation;
- the *indicator of 2-transitivity*: $d_2(\pi_A G) = \min\{k \geq 1 : (\pi_A G)^k \text{ is 2-transitive}\}$ is small enough [3];
- the group $\langle \pi_A G \rangle$ contains the alternating group $\mathfrak{A}(P^{(m)})$.

2. Theorems on DP-matrices

Corner DP-matrices. It is possible to describe a large family of invertible DP-matrices A such that the system of coordinate functions (2) of π_A have a triangular form and each coordinate function depends linearly on the last variable. Evidently, such a system defines a permutation.

Theorem 2. Let $m \in \mathbb{N}$, $R = \text{GR}(q^2, p^2)$, $q = p^r$, $p \geq 2$. Then any matrix

$$A = \begin{pmatrix} * & \dots & * & u_1 & pv_1 \\ * & \dots & u_2 & pv_2 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ u_{m-1} & pv_{m-1} & \dots & 0 & 0 \\ pv_m & 0 & \dots & 0 & u_m \end{pmatrix}, \quad (6)$$

where $u_1, \dots, u_{m-1}, v_1, \dots, v_m \in R^*$, $u_m \in P^*$, is an invertible DP-matrix. Coordinate functions of π_A are of a form

$$\psi_m(y^\perp) = v_m y_1, \quad \psi_j(y^\perp) = \hat{\psi}_j(y_1, \dots, y_{m-j}) \oplus v_j y_{m-j+1}, \quad j = 1, \dots, m-1,$$

for some functions $\hat{\psi}_1, \dots, \hat{\psi}_{m-1}$.

DP-matrices over $R = \text{GR}(q^2, 4)$. Let $q = 2^r$, $A = A_0 + 2A_1$, $A_s h = (a_s(ij)) \in P_{m,m}$, $s = 0, 1$. Substituting x_i^2 for y_i ($i = 1, \dots, m$), in (3) and using (4), we obtain that for $h = 2^{r-1}$ the orthogonality of the initial system (2) is equivalent to the orthogonality of the following system of quadratic functions of variables $\vec{x} = (x_1, \dots, x_m)$:

$$g_i(\vec{x}) = \sigma_2(a_0^h(i1)x_1, \dots, a_0^h(im)x_m) \oplus d_i(\vec{x}), \quad i = 1, \dots, m, \quad (7)$$

where

$$d_i(\vec{x}) = \bigoplus_{s=1}^m a_1(is)x_s^2, \quad i = 1, \dots, m, \quad (8)$$

are *diagonal* quadratic functions. Any orthogonal system (7) evidently corresponds to some DP-matrix. So the problem of construction of DP-matrices is reduced to the problem of construction of orthogonal systems (7).

Recall some definitions from [4], [5]. For every quadratic function $g: P^m \rightarrow P$ a bilinear function $f: P^m \times P^m \rightarrow P$ of the form

$$f(\vec{x}, \vec{y}) = g(\vec{x} \oplus \vec{y}) \oplus g(\vec{x}) \oplus g(\vec{y}) \quad (9)$$

is called a *bilinear function associated to* g .

The set of all quadratic functions associated to the same bilinear function f is a set of all functions of the form $g(\vec{x}) \oplus d(\vec{x})$, where $d: P^m \rightarrow P$ is a diagonal quadratic function. A subspace $V_f^\perp = \{\vec{a} \in P^m: f(P^m, \vec{a}) = 0\}$ is called the *kernel* of f . According to (9), we obtain that

$$\forall a, b \in P, \quad \forall \vec{u} \in V_f^\perp, \quad g(a\vec{x} \oplus b\vec{u}) = a^2g(\vec{x}) \oplus b^2g(\vec{u}). \quad (10)$$

Let $g_1, \dots, g_k$ be some system of quadratic functions with corresponding associated bilinear functions $f_1, \dots, f_k$. Denote by $\mathcal{L}(g_1, \dots, g_k)$ the set containing $\vec{0}$ and all the vectors $\vec{b} \in P^m$ satisfying a condition

$$\exists (c_1, \dots, c_k) \in P^k \setminus \{\vec{0}\}: \vec{b} \in V_{c_1f_1 \oplus \dots \oplus c_kf_k}^\perp, \quad (c_1g_1 \oplus \dots \oplus c_kg_k)(\vec{b}) \neq 0. \quad (11)$$

We offer the following approach to construction of orthogonal systems of quadratic functions.

Let us consider a system

$$g_1(x_1, \dots, x_m), \dots, g_k(x_1, \dots, x_m) \quad (12)$$

of quadratic functions and a system of diagonal quadratic functions

$$d_{k+1}, \dots, d_m. \quad (13)$$

Note that a subspace

$$K = \{\vec{x}: d_i(\vec{x}) = 0, i \in \{k+1, \dots, m\}\} \quad (14)$$

satisfies the condition $\dim K \geq k$, and $\dim K = k$ if and only if a system (13) is linearly independent.

Theorem 3. *For a system (12) the following conditions are equivalent:*

1. *There exists a system of diagonal quadratic forms (13) such that*

$$g_1, \dots, g_k, d_{k+1}, \dots, d_m \quad (15)$$

is an orthogonal system.

2. *There exists a system of diagonal quadratic forms (13) such that a subspace (14) satisfies the conditions*

$$\dim K = k, \quad K \subseteq \mathcal{L}(g_1, \dots, g_k). \quad (16)$$

3. *There exists a subspace $K \leq {}_P P^m$ satisfying (16).*

Recall that polynomial $g \in P[x_1, \dots, x_m]$ is called *balanced* if for each $a \in P$ the equation $g(\vec{x}) = a$ has $|P|^{m-1}$ solutions.

The simplest example of orthogonal system (15) is given in the following theorem.

Theorem 4. *A quadratic function g_1 (in particular, a function of type (7)) can be supplemented by some system $d_2, \dots, d_m$ of diagonal quadratic functions (8) to a bijection*

$$\Pi = (g_1, d_2, \dots, d_m): P^m \rightarrow P^m, \quad (17)$$

if and only if g_1 is a balanced function.

If r is odd or $r < m$, then there exists a diagonal quadratic function d_1 on the space P^m such that $g_1 = \sigma_2(x_1, \dots, x_r) \oplus d_1$ is a balanced function.

For the case $k \geq 2$ we have the following general condition sufficient for the existence of orthogonal system of the form (15). Let, as before, $f_1, \dots, f_k$ be the system of bilinear functions associated to $g_1, \dots, g_k$ correspondingly and

$$V_0^\perp = V_{f_1}^\perp \cap \dots \cap V_{f_k}^\perp. \quad (18)$$

It is evident that $V_0^\perp$ is a subspace of ${}_P P^m$. Let us note that a mapping

$$\bar{g} = (g_1, \dots, g_k): P^m \rightarrow P^k \quad (19)$$

is a semilinear function on $V_0^\perp$ since (10) imply

$$\forall a, b \in P, \quad \forall \vec{u}, \vec{v} \in V_0^\perp, \quad \bar{g}(a\vec{u} \oplus b\vec{v}) = a^2 \bar{g}(\vec{u}) \oplus b^2 \bar{g}(\vec{v}). \quad (20)$$

So $\bar{g}(V_0^\perp)$ is a subspace of ${}_P P^k$.

Theorem 5. *If a system (12) satisfy the condition*

$$\dim_P \overline{g}(V_0^\perp) = k, \quad (21)$$

then there exists an orthogonal system of functions of the form (15).

A complete description of orthogonal systems of the form (15) is an open problem even for $k = 2$. Below for any $m > 2$ we describe systems of two quadratic functions of special form

$$\begin{cases} g_1(x_1, \dots, x_m) = \sigma_2(x_1, \dots, x_k) \oplus d_{11}x_1^2 \oplus \dots \oplus d_{1m}x_m^2, \\ g_2(x_1, \dots, x_m) = \sigma_2(x_s, \dots, x_t) \oplus d_{21}x_1^2 \oplus \dots \oplus d_{2m}x_m^2, \end{cases} \quad (22)$$

where $1 < s \leq k < t \leq m$, which can be supplemented by some diagonal quadratic functions $d_3, \dots, d_m$ to an orthogonal system

$$\begin{aligned} g_1 &= \sigma_2(x_1, \dots, x_k) \oplus d_{11}x_1^2 \oplus \dots \oplus d_{1m}x_m^2, \\ g_2 &= \sigma_2(x_s, \dots, x_t) \oplus d_{21}x_1^2 \oplus \dots \oplus d_{2m}x_m^2, \\ d_3 &= d_{31}x_1^2 \oplus \dots \oplus d_{3m}x_m^2, \\ &\vdots \\ d_m &= d_{m1}x_1^2 \oplus \dots \oplus d_{mm}x_m^2. \end{aligned} \quad (23)$$

Such a system defines a DP-matrix $A = A_0 + 2A_1 \in R_{m,m}$, where $A_1 = (d_{ij})$, A_0 is any invertible matrix of the form

$$A_0 = \begin{pmatrix} \underbrace{e \dots \dots e}_k 0 \dots \dots 0 \\ \underbrace{0 \dots 0}_{s-1} \underbrace{e \dots \dots e}_{t-s+1} 0 \dots \dots 0 \\ \dots \end{pmatrix}$$

and for each $i \in \{3, \dots, m\}$ the i -th row of A_0 contains exactly one nonzero element.

Denote by $f_{n,l}(\vec{x}, \vec{y})$, $1 \leq n < l \leq m$, a bilinear function associated to $\sigma_2(x_n, \dots, x_l)$ on P^m . For numbers s, k, t from (22) we define the kernel: $V_0^\perp = V_{f_{1,k}}^\perp \cap V_{f_{s,t}}^\perp$.

The following result is given without the proof (in view of restrictions on the article size). The notation $a \stackrel{2}{\equiv} b$ will be used instead of $a \equiv b \pmod{2}$.

Theorem 6. *A system of functions (23) is orthogonal if and only if there exists a pair of vectors $\vec{u}, \vec{v} \in P^m$ satisfying one of the following conditions 1–5:*

1. (a) $\vec{u}, \vec{v} \in V_0^\perp$

- (b) two vectors $(g_1(\vec{u}), g_2(\vec{u})), (g_1(\vec{v}), g_2(\vec{v}))$ are linearly independent over P .
2. For some $(c_1, c_2) \in P^2 \setminus \{\vec{0}\}$
- (a) $\vec{u} \in V_0^\perp, \vec{v} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp \setminus V_0^\perp,$
- (b) $(g_1(\vec{u}), g_2(\vec{u})) \neq (0, 0), (c_1 g_1 \oplus c_2 g_2)(\vec{u}) = 0, (c_1 g_1 \oplus c_2 g_2)(\vec{v}) \neq 0.$
3. (a) $s - 1 \stackrel{2}{\equiv} t - k \stackrel{2}{\equiv} k - s + 1 \stackrel{2}{\equiv} 1$ and

$$\begin{aligned}\vec{u} &= (0, \dots, 0, 0, \dots, 0, e, \dots, e, *, \dots, *), \\ \vec{v} &= (\underbrace{e, \dots, e}_{s-1}, \underbrace{0, \dots, 0}_{k-s+1}, \underbrace{0, \dots, 0}_{t-k}, *, \dots, *); \end{aligned}$$

- (b) $g_2(\vec{v}) \neq 0$ and a polynomial $D_1(x) = g_1(\vec{u}) \oplus x g_2(\vec{u}) \oplus x^2 g_1(\vec{v}) \oplus x^3 g_2(\vec{v})$ has no roots in P .
4. (a) $s - 1 \stackrel{2}{\equiv} t - k \stackrel{2}{\equiv} 1, k - s + 1 \stackrel{2}{\equiv} 0$, and

$$\begin{aligned}\vec{u} &= (e, \dots, e, e, \dots, e, \delta_1, \dots, \delta_1, *, \dots, *), \\ \vec{v} &= (\underbrace{\delta_2, \dots, \delta_2}_{s-1}, \underbrace{e, \dots, e}_{k-s+1}, \underbrace{e, \dots, e}_{t-k}, *, \dots, *), \end{aligned}$$

where $\delta_1 \neq e, \delta_2 \neq e$.

- (b) $g_2(\vec{v}) \neq 0$ and a polynomial $D_2(x) = g_1(\vec{u}) \oplus x_{\delta_1 \oplus e}^{\delta_2 \oplus e} g_2(\vec{u}) \oplus x^2 g_1(\vec{v}) \oplus x_{\delta_1 \oplus e}^{3\delta_2 \oplus e} g_2(\vec{v})$ has no roots in P .
5. (a) $s - 1 \stackrel{2}{\not\equiv} t - k, k - s + 1 \stackrel{2}{\equiv} 0$ and

$$\begin{aligned}\vec{u} &= (\delta_1, \dots, \delta_1, \delta_1, \dots, \delta_1, \delta_2, \dots, \delta_2, *, \dots, *), \\ \vec{v} &= (\underbrace{\delta_1, \dots, \delta_1}_{s-1}, \underbrace{\delta_2, \dots, \delta_2}_{k-s+1}, \underbrace{\delta_2, \dots, \delta_2}_{t-k}, *, \dots, *), \end{aligned}$$

where $\delta_1 = (s - 1)e, \delta_2 = (t - k)e$;

- (b) $g_2(\vec{v}) \neq 0$ and a polynomial $D_3(x) = g_1(\vec{u}) \oplus x g_2(\vec{u}) \oplus x^2 g_1(\vec{v}) \oplus x^3 g_2(\vec{v})$ has no roots in P .

Recursively generated DP-matrices. Let $F(x) = x^m - \sum_{i=0}^{m-1} f_i x^i \in R[x]$, $S(F)$ be an accompanying matrix for $F(x)$ of the form (5). We call $F(x)$

a *DP-polynomial* if $A = S(F)^m$ is a DP-matrix. Let $L_R(F)$ be a family of all linear recurrent sequences over the ring R with characteristic polynomial $F(x) \in R[x]$ and $u \in L_R(F)$. Then

$$u(i+m) = \sum_{k=0}^{m-1} f_k u(i+k), \quad i \geq 0. \quad (24)$$

Using the decomposition (1) we have $u = u_0 + 2u_1$, where u_0, u_1 are digit sequences of u over P . Let us denote $u_s[\overline{i, i+k}] = (u_s(i), \dots, u_s(i+k))$ for every $s \in \{0, 1\}$, $i, k \in \mathbb{N}_0$. Permutation π_A generated by a DP-polynomial $F(x)$ for any $u \in L_R(F)$ such that $u_1[\overline{0, m-1}] = (0, \dots, 0)$ gives the following equality

$$\pi_A(u_0[\overline{0, m-1}]^T) = u_1[\overline{m, 2m-1}]^T. \quad (25)$$

Therefore the value $\pi_A(u_0[\overline{0, m-1}]^T)$ may be computed just by the calculation of m elements $u[\overline{m, 2m-1}]$ of LRS $u \in L_R(F)$.

Below we describe a class of DP-polynomials $F(x)$ such that corresponding permutations are nonlinear. We use the notations

$$F_0(x) = x^m \bigoplus_{i=0}^{m-1} \bigoplus_{i=0}^{m-1} \gamma_0(f_i) x^i, \quad F_1(x) = \bigoplus_{i=0}^{m-1} \gamma_1(f_i) x^i.$$

Theorem 7. Let $R = \mathbb{Z}_4$, $F(x) \in R[x]$ be a polynomial of degree $m \geq 3$.

(a) If $F_0(x) = x^m \oplus x^{m-1} \oplus x \oplus e$, then $F(x)$ is a DP-polynomial if and only if

$$(F_0(x), e \oplus F_1(x)) = e, \quad (F_0(x), x \oplus F_1(x)) = e. \quad (26)$$

(b) If $m = 2^t - 1$ for some $t \in \mathbb{N}$, $F_0(x) = (x \oplus e)^m$, then $F(x)$ is a DP-polynomial if and only if $F_1(e) = 0$.

Properties of cryptographic primitives. Permutations induced by DP-matrices and DP-polynomials are computationally simple and are nonlinear for large enough alphabet $P^{(m)}$.

Let $R = \mathbb{Z}_{p^m}$, $P = \{0, 1, \dots, p-1\}$. We identify vectors $v^\downarrow = (a_1, \dots, a_m)^T \in P^{(m)}$, $m > 1$, with elements $a = a_1 + a_2 p + \dots + a_m p^{m-1} \in R$ and consider a regular cyclic subgroup $G < \mathfrak{S}(P^{(m)})$ generated by the cycle $t = (0, 1, 2, \dots, p^m - 1)$. Let $A \in R_{m,m}$ be a DP-matrix. We have the following results on the properties of the set of permutations $(\pi_A G)^k$.

Define the oriented graph $\mathcal{G}(\pi_A)$ with a vertex set $\{1, \dots, m\}$ and with an edge from s to i whenever $s \leq i$ or the function ψ_i in (3) depends on a variable y_s

essentially. The graph $\mathcal{G}(\pi_A)$ may be easily reconstructed by the matrix A . An edge from s to i exists in the following cases only:

- (a) $s \leq i$,
- (b) $a_1(is) \neq 0$,
- (c) $a_0(is) \neq 0$ and a row $(a_0(i1), \dots, a_0(im))$ has more than 1 nonzero coordinate.

Below we use the S-Conjecture: all the finite simple groups are known (see [6], [7]).

Theorem 8. *Let the graph $\mathcal{G}(\pi_A)$ described above be strongly connected.*

1. *If $p = 2$ and $2^m - 1$ is a composite number, then $\langle \pi_A G \rangle = \mathfrak{S}(P^{(m)})$.*
2. *If $p \geq 3$, S-Conjecture is true, and*

$$p^m \notin \left\{ 11, 23, \frac{p_1^n - 1}{p_1 - 1}, p_1^3 + 1, d^{d(2n+1)} + 1 : p_1 \text{ is a prime}, d \in \{2, 3\}, n \geq 1 \right\}, \quad (27)$$

then $\langle \pi_A G \rangle \supseteq \mathfrak{A}(P^m)$.

Corollary 1. *Let $p = 2, 2^m - 1$ be a composite number. If π_A is a permutation corresponding to a corner matrix of the form (6) or to a DP-polynomial from theorem 7, then $\langle \pi_A G \rangle = \mathfrak{S}(P^{(m)})$.*

Results of calculations on PC. Let now G_1 be a regular representation of the group $(\mathbb{Z}_p^{(m)}, +)$ in $\mathfrak{S}(\mathbb{Z}_p^{(m)})$ and G_2 be a regular representation of the group $(\mathbb{Z}_{p^m}, +)$ in $\mathfrak{S}(\mathbb{Z}_p^{(m)})$. Below we present examples of DP-matrices A such that π_A is nonlinear and $\langle \pi_A G \rangle \supset \mathfrak{A}(\mathbb{Z}_p^{(m)})$, $G \in \{G_1, G_2\}$.

We study the properties of the *transition matrix of differences*

$$Q_G(\pi_A) = \frac{1}{p^m} (\nu_{a^\downarrow, b^\downarrow})_{(p^m-1) \times (p^m-1)},$$

where $a^\downarrow, b^\downarrow \in \mathbb{Z}_p^{(m)} \setminus 0$ and $\nu_{a^\downarrow, b^\downarrow}$ is a number of solutions $x^\downarrow \in \mathbb{Z}_p^{(m)}$ of the equation

$$\pi_A(x^\downarrow + a^\downarrow) - \pi_A(x^\downarrow) = b^\downarrow,$$

where $+, -$ are operations of group G .

The following parameters of the matrix $Q_G(\pi_A)^k$ are of interest:

$D = D(k)$ — the density of nonzero elements,

Δ — the difference between maximal and minimal elements,

Max — a maximal element.

Note that

$$D(k) = 1 \iff Q_G(\pi_A)^k > 0 \iff d_2(\pi_A G) \leq k + 1,$$

and $d_2(\pi_A G) \geq 3$ in the cases considered according to [3].

1. A DP-matrix corresponding to an orthogonal system of quadratic functions of the form (23). Let $R = \mathbb{Z}_4$, $m = 8$,

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} + 2 \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Parameters of matrices $Q_G(\pi_A)^k$, $G \in \{G_1, G_2\}$:

$G = G_1 \cong \mathbb{Z}_2^8$				$G = G_2 \cong \mathbb{Z}_{2^8}$			
k	D	Δ	Max	k	D	Δ	Max
1	0.0136	—	1.0000	1	0.3533	—	0.3750
6	0.9990	—	0.0200	2	0.9833	—	0.1262
7	1	0.0117	0.0126	3	1	0.0512	0.0518
10	1	0.0020	0.0053	6	1	0.0011	0.0047
$\langle \pi_A G_1 \rangle = \mathfrak{A}(\mathbb{Z}_2^8)$				$\langle \pi_A G_2 \rangle = \mathfrak{S}(\mathbb{Z}_2^8)$			

2. A corner DP-matrix.

Let $R = \mathbb{Z}_4$, $m = 8$.

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} + 2 \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Parameters of matrices $Q_G(\pi_B)^k$, $k \in \{1, \dots, 9\}$, $G \in G_1, G_2$:

$G = G_1 \cong \mathbb{Z}_2^8$				$G = G_2 \cong \mathbb{Z}_{2^8}$			
k	D	Δ	Max	k	D	Δ	Max
1	0.0732	—	1.0000	1	0.2961	—	0.5000
4	0.9999	—	0.0179	2	0.9967	—	0.0478
5	1	0.0086	0.0104	3	1	0.0117	0.0129
10	1	0.000009	0.0039	6	1	0.000091	0.0039
$\langle \pi_B G_1 \rangle = \mathfrak{A}(\mathbb{Z}_2^8)$				$\langle \pi_B G_2 \rangle = \mathfrak{S}(\mathbb{Z}_2^8)$			

3. Recursively generated DP-matrix.

Let $R = \mathbb{Z}_4$, $m = 8$, $F(x) = x^8 - x^7 - 2x^5 - 2x^3 - x - 1$.

$$C = S(F)^m = \begin{pmatrix} 1 & 1 & 0 & 2 & 0 & 2 & 0 & 1 \\ 1 & 2 & 1 & 2 & 2 & 2 & 2 & 1 \\ 1 & 2 & 2 & 3 & 2 & 0 & 2 & 3 \\ 3 & 0 & 2 & 0 & 3 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 2 & 0 & 2 & 0 & 2 & 1 & 1 \\ 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 3 & 2 & 2 & 2 & 2 & 2 & 0 \end{pmatrix}.$$

Parameters of matrices $Q_G(\pi_C)^k$, $k \in \{1, \dots, 9\}$, $G \in G_1, G_2$:

$G = G_1 \cong \mathbb{Z}_2^8$				$G = G_2 \cong \mathbb{Z}_{2^8}$			
k	D	Δ	Max	k	D	Δ	Max
1	0.1298	-	1.0000	1	0.4927	-	0.1445
2	0.4761	-	0.5000	2	1	0.0215	0.0218
6	0.9998	-	0.0664	3	1	0.0033	0.0060
7	1	0.0344	0.0354	4	1	0.0004	0.0041
9	1	0.0168	0.0194	5	1	0.000096	0.0039
$\langle \pi_C G_1 \rangle = \mathfrak{A}(\mathbb{Z}_2^8)$				$\langle \pi_C G_2 \rangle = \mathfrak{S}(\mathbb{Z}_2^8)$			

3. Proofs of theorems

3.1. Proof of theorem 3

1 $\iff$ 2. Any system of functions (15) defines a map

$$\Pi = (g_1, \dots, g_k, d_{k+1}, \dots, d_m): P^m \rightarrow P^m.$$

Lemma 1 ([1]). *The map Π is a permutation if and only if for every $(c_1, \dots, c_m) \in P^m \setminus \{\vec{0}\}$ a function $c_1 g_1 \oplus \dots \oplus c_k g_k \oplus c_{k+1} d_{k+1} \oplus \dots \oplus c_m d_m$ is balanced.*

A set $K = \{\vec{x} \in P^m : d_i(\vec{x}) = 0, i \in \{k+1, \dots, m\}\}$ is a subspace of P^m , $\dim K \geq k$. If $\dim K > k$, then the system of functions $d_{k+1}, \dots, d_m$ is linearly dependent and in view of Lemma 1 the map Π is not a permutation.

Evidently the map Π is a bijection if and only if for every nonzero $\vec{b} \in P^m$ the equation

$$\Pi(\vec{x} \oplus \vec{b}) \oplus \Pi(\vec{x}) = \vec{0} \quad (28)$$

has no solutions in P^m . Let $f_1, \dots, f_k$ are bilinear functions associated to $g_1, \dots, g_k$. From (9) it follows that $g_i(\vec{x} \oplus \vec{b}) \oplus g_i(\vec{x}) = f_i(\vec{x}, \vec{b}) \oplus g_i(\vec{b})$, $i = 1, \dots, k$, and (28) is equivalent to the system of conditions

$$\begin{cases} f_i(\vec{x}, \vec{b}) = g_i(\vec{b}), & i = 1, \dots, k, \\ d_j(\vec{b}) = 0, & j = k+1, \dots, m. \end{cases}$$

Therefore Π is a bijection if and only if $\dim K = k$ and for every $\vec{b} \in K \setminus \{\vec{0}\}$ the system of equations

$$f_i(\vec{x}, \vec{b}) = g_i(\vec{b}), \quad i = 1, \dots, k,$$

has no solutions in P^m . The last condition is equivalent to the existence of $(c_1, \dots, c_k) \in P^k \setminus \{\vec{0}\}$ such that $c_1 f_1(\vec{x}, \vec{b}) \oplus \dots \oplus c_k f_k(\vec{x}, \vec{b}) = 0$ and $c_1 g_1(\vec{b}) \oplus \dots \oplus c_k g_k(\vec{b}) \neq 0$, that is $\vec{b} \in \mathcal{L}(g_1, \dots, g_k)$.

2 $\Rightarrow$ 3. Is evident.

3 $\Rightarrow$ 2. Under the condition (16) we can construct a system of diagonal quadratic functions $d_{k+1}, \dots, d_m$ such that $K = \text{Ker}(d_{k+1}, \dots, d_m)$. Then corresponding Π is a bijection. Theorem 3 is proved.

3.2. Proof of theorem 4

If the function $F = (g_1, d_2, \dots, d_m)$ is a permutation, then according to lemma 1 a quadratic function g_1 is balanced.

Let now g_1 be a balanced quadratic function. Then, according to [1, 4, 5], g_1 is equivalent to a canonical form

$$h = x_1 x_2 \oplus x_3 x_4 \oplus \dots \oplus x_{2s-1} x_{2s} \oplus x_{2s+1}^2, \quad s \leq \lfloor m/2 \rfloor. \quad (29)$$

Any quadratic function (29) is balanced. Therefore, it is enough to prove the theorem for $g_1 = h$. In this case the set $\mathcal{L}(g_1)$ defined by (11) contains a 1-dimensional subspace K generated by the vector $\vec{E}_{2s+1} = (\underbrace{0, \dots, 0}_{2s}, e, 0, \dots, 0)$.

The first statement of theorem 4 is proved.

The second statement is evident.

3.3. Proof of theorem 5

Theorem 3, a system of quadratic functions $g_1, \dots, g_k$ may be supplemented by some diagonal quadratic functions $d_{k+1}, \dots, d_m$ to the orthogonal system (15) iff there exists a subspace $K < {}_P P^m$ satisfying the condition (16).

Under the condition of theorem there exist elements $\vec{u}_1, \dots, \vec{u}_k \in V_0^\perp$ such that the system of vectors $\vec{g}(\vec{u}_1), \dots, \vec{g}(\vec{u}_k)$ is linearly independent. Since $\vec{g}$ is semilinear function on $V_0^\perp$ it means that a subspace $K = {}_P(\vec{u}_1, \dots, \vec{u}_k)$ of subspace $V_0^\perp \leq {}_P P^m$ satisfies the first condition in (16).

The second condition for K in (16) is proved by the following way. From the construction it is obvious that the mapping $\vec{g}$ induces isomorphism of K on $\vec{g}(V_0^\perp)$. Let $\vec{b} \in K \setminus \{\vec{0}\}$. Then $\vec{g}(\vec{b}) = (g_1(\vec{b}), \dots, g_k(\vec{b})) \neq \vec{0}$. Therefore $g_s(\vec{b}) \neq 0$ for some $s \in \{1, \dots, k\}$ and since by definition $\vec{b} \in V_0^\perp \subseteq V_{f_s}^\perp$ we have $\vec{b} \in \mathcal{L}(g_1, \dots, g_k)$.

3.4. Proof of theorem 7

We need the following general result. Let $F(x) \in R[x]$ be a monic polynomial of degree m , $S = \gamma_0(S(F))$, $\vec{F}_j = \gamma_j((f_0, f_1, \dots, f_{m-1})) \in P^m$, $j = 0, 1$, and

$$g_1(\vec{x}) = \sigma_2(\vec{F}_0 \wedge \vec{x}) \oplus \vec{F}_1 \odot x^\perp, \quad (30)$$

where $\wedge$ is a coordinate-wise multiplication of vectors, $\odot$ is a matrix multiplication over the field P , and $x^\perp = \vec{x}^T$.

Lemma 2. *A monic polynomial $F(x) \in R[x]$ of degree m is a DP-polynomial if and only if the system of functions*

$$\left\{ h_i(x^\perp) = g_1(\vec{x} \odot (S^T)^{i-1}), \quad i = 1, \dots, m, \right. \quad (31)$$

over P is orthogonal¹.

¹ Some classes of orthogonal systems of type (31) with g_1 essentially depending on variables x_1, x_2, x_3 were studied in [9].

□ Consider a map $H = (h_1, \dots, h_m): P^{(m)} \rightarrow P^{(m)}$ defined by (31) and a map $\alpha: P^{(m)} \rightarrow P^{(m)}$ defined by the rule

$$\alpha(x_0, \dots, x_{m-1}) = (y_0, \dots, y_{m-1})^T, \quad y_i = x_i \bigoplus_{k=0}^{i-1} f_{m-1-k,0} x_k. \quad (32)$$

Note that α is a bijection. Now in order to prove lemma it is enough to show that if $A = S(F)^m$ then

$$\pi_A = \alpha^{-1} \circ H, \quad (33)$$

where $\circ$ is a composition. We shall use the representation of π_A in a form (25). Let

$$L'_R(F) = \{u \in L_R(F): u_1[\overline{0, m-1}] = \vec{0}\}.$$

Then according to (25), the map π_A is completely defined by a condition

$$\forall u' \in L'_R(F): \pi_A(u'_0[\overline{0, m-1}]^T) = u'_1[\overline{m, 2m-1}]^T. \quad (34)$$

From (24) and decomposition (1) we obtain that the first digit sequence of any $u' \in L_R(F)$ satisfy the relations

$$\begin{aligned} u'_1(i+m) &= \left(\bigoplus_{k=0}^{m-1} f_{k0} u'_1(i+k) \right) \oplus \\ &\oplus \left(\bigoplus_{k=0}^{m-1} f_{k1} u'_0(i+k) \right) \oplus \gamma_1 \left(\bigoplus_{k=0}^{m-1} f_{k0} u'_0(i+k) \right) \end{aligned} \quad (35)$$

and therefore the sequence

$$v(i) = u'_1(i+m) \oplus \left(\bigoplus_{k=0}^{m-1} f_{k0} u'_1(i+k) \right) \quad (36)$$

satisfy the relation

$$v(i) = \gamma_1 \left(\bigoplus_{k=0}^{m-1} f_{k0} u'_0(i+k) \right) \oplus \left(\bigoplus_{k=0}^{m-1} f_{k1} u'_0(i+k) \right). \quad (37)$$

Note that (36) and the condition $u'_1[\overline{0, m-1}] = \vec{0}$ imply

$$\begin{aligned} v(i) &= u'_1(i+m) \oplus \left(\bigoplus_{k=m-i}^{m-1} f_{k0} u'_1(i+k) \right), \quad i = 0, \dots, m-1; \\ v[\overline{0, m-1}]^T &= \alpha(u'_1[\overline{m, 2m-1}]^T). \end{aligned} \quad (38)$$

On the other hand using (4) and (37) we receive

$$v(i) = \sigma_2 \left(\vec{F}_0 \wedge u'_0[\overline{i, i+m-1}] \right) \oplus \vec{F}_1 \odot u'_0[\overline{i, i+m-1}]^T. \quad (39)$$

From (24) it follows that

$$u'_0[\overline{i, i+m-1}] = u'_0[\overline{0, m-1}] \odot (S^T)^i, \quad i \geq 0.$$

Hence (39) implies

$$v(i) = \sigma_2 \left(\vec{F}_0 \wedge \left(u'_0[\overline{0, m-1}] \odot (S^T)^i \right) \right) \oplus \vec{F}_1 \odot S^i \odot u'_0[\overline{0, m-1}]^T.$$

Now using (30), we have

$$\begin{aligned} v(i-1) &= g_1(u'_0[\overline{0, m-1}] \odot (S^T)^{i-1}) = h_i(u'_0[\overline{0, m-1}]), \quad i = 1, \dots, m, \\ v[\overline{0, m-1}]^T &= H(u'_0[\overline{0, m-1}]^T). \end{aligned} \quad (40)$$

Finally, (33) follows from (38), (40), (34). Lemma 2 is proved. $\square$

Proof of the statement (a) of theorem 7. Below we will use the identities $g_1(\vec{x}) = g_1(x^\downarrow)$, $\sigma_2(\vec{x}) = \sigma_2(x^\downarrow)$. Let $F_0(x) = x^m \oplus x^{m-1} \oplus x \oplus e$. Then

$$S = \begin{pmatrix} 0 & e & 0 & \dots & 0 & 0 \\ 0 & 0 & e & \dots & 0 & 0 \\ & \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & 0 & e \\ e & e & 0 & \dots & 0 & e \end{pmatrix}, \quad (41)$$

$$S^{i-1}x^\downarrow = \begin{pmatrix} x_i \\ x_{i+1} \\ \vdots \\ x_1 \oplus x_i \oplus x_m \end{pmatrix}, \quad 2 \leq i < m, \quad S^{m-1}x^\downarrow = \begin{pmatrix} x_m \\ x_1 \oplus x_2 \oplus x_m \\ \vdots \\ x_1 \oplus x_{m-1} \oplus x_m \end{pmatrix}, \quad (42)$$

a function (30) is $g_1(x^\downarrow) = \sigma_2(x_1, x_2, x_m) \oplus \vec{F}_1 \odot x^\downarrow = (x_1 \oplus x_m)(x_1 \oplus x_2) \oplus x_1 \oplus \vec{F}_1 \odot x^\downarrow$, and simple calculations show that a system (31) has a form

$$\begin{cases} h_1(x^\downarrow) = (x_1 \oplus x_m)(x_1 \oplus x_2) \oplus x_1 \oplus \vec{F}_1 \odot x^\downarrow, \\ h_i(x^\downarrow) = (x_1 \oplus x_m)(x_i \oplus x_{i+1}) \oplus x_i \oplus \vec{F}_1 \odot S^{i-1} \odot x^\downarrow, \quad 2 \leq i < m, \\ h_m(x^\downarrow) = (x_1 \oplus x_m)(x_1 \oplus x_2) \oplus x_m \oplus \vec{F}_1 \odot S^{m-1} \odot x^\downarrow. \end{cases} \quad (43)$$

Consider a map $H = (h_1, \dots, h_m)^T: P^{(m)} \rightarrow P^{(m)}$ and introduce the notation

$$S_{\vec{F}_1} = \begin{pmatrix} \vec{F}_1 \\ \vec{F}_1 \odot S \\ \vdots \\ \vec{F}_1 \odot S^{m-1} \end{pmatrix}.$$

Let $\mathcal{A}_\delta = \{x^\downarrow \in P^{(m)} : x_1 \oplus x_m = \delta\}$, $\delta \in \{0, 1\}$. Then (43) implies that

$$H(x^\downarrow) = \begin{cases} (E \oplus S_{\vec{F}_1}) \odot x^\downarrow, & \text{if } x^\downarrow \in \mathcal{A}_0, \\ (S \oplus S_{\vec{F}_1}) \odot x^\downarrow, & \text{if } x^\downarrow \in \mathcal{A}_1. \end{cases} \quad (44)$$

In view of the evident equality $S_{\vec{F}_1} = F_1(S)$ we obtain that

$$H(x^\downarrow) = \begin{cases} u(S) \odot x^\downarrow, & \text{if } x^\downarrow \in \mathcal{A}_0, \ u(x) = e \oplus F_1(x), \\ v(S) \odot x^\downarrow, & \text{if } x^\downarrow \in \mathcal{A}_1, \ v(x) = x \oplus F_1(x). \end{cases} \quad (45)$$

According to lemma 2 we need to prove that H is a bijection iff condition (26) is true.

The condition (26) means that matrices $E \oplus F_1(S)$, $S \oplus F_1(S)$ are invertible. We can prove that (26) implies reversibility of H using the following general result of U. A. Vasiliev, B. M. Kloss and O. E. Nazarov (1963).

Theorem 9. *Let $T_\delta: P^{(m)} \rightarrow P^{(m)}$, $\delta = 0, 1$, are bijections and $\tau: P^{(m)} \rightarrow P = \mathbb{Z}_2$. Then a mapping $M: P^{(m)} \rightarrow P^{(m)}$ of the form*

$$M(x^\downarrow) = T_{\tau(x^\downarrow)}(x^\downarrow), \quad (46)$$

is a bijection iff

$$\forall x^\downarrow \in P^m, \quad \tau(T_0(x^\downarrow)) = \tau(T_1(x^\downarrow)). \quad (47)$$

In our case we put $T_\delta(x^\downarrow) = (S^\delta \oplus F_1(S))x^\downarrow$, $s = 0, 1$, $\tau(x^\downarrow) = x_1 \oplus x_m$ for all $x^\downarrow \in P^m$. Then, by (45), we have $H(x^\downarrow) = T_{\tau(x^\downarrow)}(x^\downarrow)$.

Since under the condition (26) T_0, T_1 are bijections it is sufficient to show that H satisfy (47). By the definition of τ we receive

$$\tau(T_0(x^\downarrow)) = \tau(x^\downarrow \oplus F_1(S) \odot x^\downarrow) = x_1 \oplus x_m \oplus \tau(F_1(S) \odot x^\downarrow)$$

and using (5) we finally obtain

$$\tau(T_1(x^\downarrow)) = \tau(S \odot x^\downarrow \oplus F_1(S) \odot x^\downarrow) = x_2 \oplus x_1 \oplus x_2 \oplus x_m \oplus \tau(F_1(S) \odot x^\downarrow) = \tau(T_0(x^\downarrow)).$$

According to theorem 9 the mapping H is bijection.

The direct proof of the theorem is following. Let $e^\downarrow = (e, \dots, e)^T$.

Lemma 3. For every $x^\downarrow \in P^{(m)}$, $\delta \in \{0, 1\}$ the following conditions are equivalent:

- (a) $x^\downarrow \in \mathcal{A}_\delta$,
- (b) $(S^{m-1} \oplus E) \odot x^\downarrow = \delta e^\downarrow$,
- (c) $x^\downarrow = (S \oplus E) \odot y^\downarrow \oplus (\delta, 0, \dots, 0)^T$ for some $y^\downarrow \in P^{(m)}$.

Proof. (a) $\Rightarrow$ (b) It is enough to note that the first row of matrix $(S^{m-1} \oplus E)$ is $(e, 0, \dots, 0, e)$.

(b) $\Leftrightarrow$ (c) Each vector of the form (c) satisfies the condition (b) since $(S^{m-1} \oplus E) \odot (S \oplus E) = F_0(S) = 0$. Since $\text{rank}(S \oplus E) = m-1$ and $(S^{m-1} \oplus E) \neq 0$ the number of vectors satisfying (c) equals to the number of solutions of the equation (b).

(b) $\Rightarrow$ (a) Obvious, since $\delta e^\downarrow = x_1 \oplus x_m$ in (b).

Lemma 4. H is a bijection iff $H(\mathcal{A}_\delta) = \mathcal{A}_\delta$, $\delta = 0, 1$.

□ If $x^\downarrow \in \mathcal{A}_0$, then according to lemma 3(c) $x^\downarrow = (S \oplus E) \odot y^\downarrow$ for some $y^\downarrow \in P^{(m)}$ and $H(x^\downarrow) = u(S) \odot (S \oplus E) \odot y^\downarrow = (S \oplus E) \odot (u(S) \odot y^\downarrow) \in \mathcal{A}_0$. Therefore $H(\mathcal{A}_0) \subseteq \mathcal{A}_0$. Now lemma is evident. □

Let us show that (26) imply reversibility of H . According to (26) matrices $u(S)$, $v(S)$ are invertible. If $x^\downarrow \in \mathcal{A}_1$, then

$$\begin{aligned} (E \oplus S^{m-1}) \odot H(x^\downarrow) &= (E \oplus S^{m-1}) \odot (v(S) \odot ((E \oplus S) \odot y^\downarrow \oplus (e, 0, \dots, 0)^T)) = \\ &= (E \oplus S^{m-1}) \odot v(S) \odot (e, 0, \dots, 0)^T = v(S) \odot e^\downarrow = S \odot e^\downarrow \oplus F_1(S) \odot e^\downarrow. \end{aligned} \quad (48)$$

In view of (26) $F_1(e) = \vec{F}_1 \odot e^\downarrow = 0$ and since $S \odot e^\downarrow = e^\downarrow$, then $F_1(S) \odot e^\downarrow = \vec{F}_1 \odot e^\downarrow = 0$. Therefore $(E \oplus S^{m-1}) \odot H(x^\downarrow) = e^\downarrow$ and $H(\mathcal{A}_1) \subset \mathcal{A}_1$. So H is a bijection.

Conversely, let H be a bijection. Let us show that (26) is true. According to lemma 4 we have $H(\mathcal{A}_\delta) = \mathcal{A}_\delta$, $\delta = 0, 1$. Let us suppose that $(u(x), F_0(x)) \neq e$. Then $u(S)$ is not invertible but in view of (45) $\text{Ker } u(S) \cap \mathcal{A}_0 = \{0^\downarrow\}$. Hence there exists $\eta^\downarrow \in \mathcal{A}_1$ such that $u(S) \odot \eta^\downarrow = 0^\downarrow$ and in view of the equality $v(S) = (E \oplus S) \oplus u(S)$ according to Lemma 3 we have

$$H(\eta^\downarrow) = v(S)\eta^\downarrow = (E \oplus S) \odot \eta^\downarrow \oplus u(S) \odot \eta^\downarrow = (E \oplus S) \odot \eta^\downarrow \in \mathcal{A}_0.$$

Therefore $(u(x), F_0(x)) = e$.

Now we show that $(v(x), F_0(x)) = e$ (or, equivalently, that $v(S)$ is invertible). Since $\mathcal{A}_1 = \mathcal{A}_0 \oplus E_1^\perp$ and $\dim \mathcal{A}_0 = m - 1$ then $\mathcal{A}_1$ contains a linearly independent system $w_1^\perp, \dots, w_m^\perp$. Therefore in view of the equality $v(S) \odot \mathcal{A}_1 = \mathcal{A}_1$ there exists a solution $X \in P_{m,m}$ of the equation $v(S) \odot X = (w_1^\perp, \dots, w_m^\perp)$, that is $v(S)$ is invertible.

A statement (a) of the Theorem is proved.

Proof of the statement (b) of theorem 7. Let $F_0(x) = (x \oplus e)^m$, $m = 2^t - 1$. In this case $\vec{F}_0 = (e, \dots, e)$ and in (30) $g_1(\vec{x}) = \sigma_2(\vec{x}) \oplus \vec{F}_1 \odot x^\perp$. Note that $\sigma_2(\vec{x} \odot S^T) = \sigma_2(S \odot x^\perp) = \sigma_2(x_2, \dots, x_m, x_1 \oplus \dots \oplus x_m) = \sigma_2(x_2, \dots, x_m, x_1) \oplus (x_2 \oplus \dots \oplus x_m)(x_2 \oplus \dots \oplus x_m) = \sigma_2(\vec{x}) \oplus \vec{\eta} \odot x^\perp$, where $\vec{\eta} = (0, e, \dots, e)$. Therefore $\sigma_2(S^{i-1} \odot x^\perp) = \sigma_2(x^\perp) \oplus \vec{\eta} \odot (E \oplus S \oplus \dots \oplus S^{i-2}) \odot x^\perp$. Then the system of functions (31) has a form

$$\begin{aligned} h_1(x^\perp) &= g_1(\vec{x}) = \sigma_2(\vec{x}) \oplus \vec{F}_1 \odot x^\perp, \\ h_i(x^\perp) &= \sigma_2(\vec{x}) \oplus \vec{\eta} \odot (E \oplus S \oplus \dots \oplus S^{i-2}) \odot x^\perp \oplus \vec{F}_1 \odot S^{i-1} \odot x^\perp, \quad i = 2, \dots, m. \end{aligned}$$

Evidently, the system (31) is orthogonal if and only if the system

$$\begin{cases} g_1(\vec{x}) = \sigma_2(\vec{x}) \oplus \vec{F}_1 \odot x^\perp, \\ d_i = h_i \oplus h_{i-1} = \vec{\eta} \odot S^{i-2} \odot x^\perp \oplus \vec{F}_1 \odot (S^{i-1} \oplus S^{i-2}) \odot x^\perp, \quad i = 2, \dots, m, \end{cases} \quad (49)$$

is orthogonal. Note that here the functions $d_2, \dots, d_m$ are linear. Consider the mapping $\Pi = (g_1, d_2, \dots, d_m)$. According to theorem 3 (in the case $k = 1$), the system (49) is orthogonal iff system $d_i(\vec{x}), i = 2, \dots, m$, is linearly independent and for a bilinear function f associated to h_1 there exists a vector $\vec{b} \in P^m \setminus \{\vec{0}\}$ such that

$$d_i(\vec{b}) = 0, \quad i = 2, \dots, m, \quad f(\vec{b}, \vec{y}) = 0, \quad h_1(\vec{b}) = e. \quad (50)$$

Firstly, we will prove that the system $d_i(\vec{x}), i = 2, \dots, m$, is linearly independent iff $F_1(e) = 0$. Let $\vec{e} = (e, 0, \dots, 0)$. Note that $\vec{\eta} = \vec{e} \odot (S \oplus E)$, $\vec{F}_1 = \vec{e} \odot F_1(S)$ and $\vec{e} = \vec{e} \odot \sum_{i=0}^{m-1} S^i$. Then (49) implies that

$$\begin{aligned} d_i(\vec{x}) &= (\vec{\eta} \oplus \vec{F}_1 \odot (S \oplus E)) \odot S^{i-2} \odot x^\perp = (\vec{e} \oplus \vec{F}_1) \odot (S \oplus E) \odot S^{i-2} \odot x^\perp = \\ &= \vec{e} \odot \left(\sum_{j=0}^{m-1} S^j \oplus F_1(S) \right) \odot (S \oplus E) \odot S^{i-2} \odot x^\perp. \end{aligned} \quad (51)$$

Hence the system $d_i(\vec{x})$, $i = 2, \dots, m$, is linearly independent iff for each polynomial $C(x) \in R[x] \setminus \{0\}$, $\deg C(x) < m - 1$, the condition

$$\vec{\varepsilon} \odot \left(\sum_{i=0}^{m-1} S^i \oplus F_1(S) \right) \odot (S \oplus E) \odot C(S) \neq \vec{0}$$

is true. As $F_0(x) = (x \oplus e)^m$ is a minimal polynomial of a vector ε relative to the accompanying matrix S then the last condition is equivalent to the condition

$$\forall C(x) \in R[x] \setminus \{0\}, \deg C(x) < m - 1 :$$

$$F_0(x) \nmid \left(\sum_{i=0}^{m-1} x^i \oplus F_1(x) \right) \odot (x \oplus e) \odot C(x).$$

Since we can choose $C(x) = (x \oplus e)^{m-2}$ it is equivalent to the condition

$$\left(x \oplus e, \sum_{i=0}^{m-1} x^i \oplus F_1(x) \right) = e,$$

i. e. to the condition $F_1(e) = 0$.

Now let us show that $\vec{b} = \vec{e} = (e, \dots, e)$ satisfy (50). As $(S \oplus E)b^\downarrow = 0^\downarrow$ then (49) implies $d_i(\vec{b}) = 0$, $i = 2, \dots, m$.

Note that a bilinear function f associated to $h_1(x^\downarrow) = \sigma_2(\vec{x}) \oplus \vec{F}_1 \odot x^\downarrow$ is of a form

$$f(\vec{x}, \vec{y}) = \sum_{s=1}^m \sum_{\substack{t=m \\ t \neq s}}^m x_s y_t = \vec{x}(E \oplus I)y^\downarrow, \quad I = (e)_{m,m}.$$

Since $m = 2^t - 1$ the equality $f(\vec{b}, \vec{y}) = 0$ is evident, direct computations show that $\sigma_2(\vec{b}) = \binom{m}{2}e = e$, $\vec{F}_1 b^\downarrow = 0$, that is $h_1(\vec{b}) = 0$. So (50) is proved.

3.5. Proofs of theorem 8 and corollary 1

Since the graph $\mathcal{G}(\pi_A)$ is strongly connected then the group $\langle \pi_A G \rangle$ is primitive ([10, 11]).

1. According to a classification [12] of primitive groups containing 2^m -cycle, if $p = 2$ and the number $2^m - 1$ is composite, then $\langle \pi_A G \rangle = \mathfrak{S}(P^{(m)})$.

2. It is known that for $p > 2$ any primitive group that contains a cycle of prime-power length p^a is 2-transitive, except the case $a = 1$ [7, 13].

S-Conjecture implies that all the 2-transitive permutation groups are known and therefore list of such groups in papers [6, 7] is exhaustive. According to this list, if $p > 2$ satisfies the condition (27), then $\langle \pi_A G \rangle \supset \mathfrak{A}(P^m)$.

Theorem 8 is proved.

If π_A satisfy conditions of corollary 1, then its first coordinate function $\psi_1(y^\perp)$ in (2) depends on variable x_m essentially. Therefore corresponding graph $\mathcal{G}(\pi_A)$ is strongly connected. So $\langle \pi_A G \rangle = \mathfrak{S}(P^{(m)})$ follows from the assertion 1 of theorem 8.

Список литературы

1. *Lidl R., Niederreiter H.* Finite Fields. — Cambridge University Press, second edition, 1997.
2. *Kuzmin A. S., Nechaev A. A.* Linear recurring sequences over Galois rings // Algebra and Logic. — 1995. — V. 34. No 2. — P. 87–100.
3. *Gluhov M. M.* On numerical parameters associated with the definition of finite groups by systems of generating elements // Trudy po diskretnoi matematike, v. 1. — M. : TVP, 1997. — P. 43–66 (in Russian).
4. *Diedonné J.-A.* La Géométrie des Groupes Classiques // Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5. — Springer-Verlag, 1971.
5. *Kuzmin A. S., Nechaev A. A.* Trace-function on a Galois ring in coding theory // Lect. Notes Comput. Sci., v. 1255. — Springer-Verlag, 1997.
6. *Cameron P. J.* Finite permutation groups and finite simple groups. — Bull. London Math. Soc., 1981. — V. 13. No 1. — P. 1–22.
7. *Pogorelov B. A.* Permutation groups. I. (A survey for 1981-1995) // Trudy po diskretnoi matematike, v. 2. — M. : TVP, 1998. — P. 237–281 (in Russian).
8. *Pogorelov B. A.* Bases of permutation groups theory. I. General questions. — Moscow, 1986. — 316 pp. (in Russian).
9. *Nikonov V. G., Sarantsev A. V.* On the complexity of joint realization of Boolean functions regular systems in DNF basis // Mathematical Aspects of Cryptography. — 2010. — V. 1, No.3. — P. 45–65 (in Russian).
10. *Nechaev A. A.* Criterion for the completeness of systems of functions of p^n -valued logic containing operations of addition and multiplication modulo p^n // Metody Diskretnogo Analiza. — 1980. — V. 34. — P. 74–87 (in Russian).
11. *Gluhov M. M.* On 2-transitive products of regular permutation groups // Trudy po diskretnoi matematike, v. 3. — M. : Fizmatlit, 2000. — P. 37–52 (in Russian).
12. *Pogorelov B. A.* Primitive permutation group that contain a 2^m -cycle // Algebra i Logika. — 1980. — V. 19. No. 2. — P. 147–155 (in Russian).
13. *Knapp W.* On Burnside's method // J. Algebra. — 1995. — V. 175. — P. 644–660.