Math-Net.Ru

Общероссийский математический портал

А. В. Аборнев, Рекурсивно-порождаемые перестановки двоичного пространства, *Матем. вопр. криптогр.*, 2014, том 5, выпуск 2, 7–20

DOI: <https://doi.org/10.4213/mvk112>

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: 54.92.164.108

26 апреля 2023 г., 07:18:19

Recursively-generated permutations of a binary space

A. V. Abornev

LLC "Certification Research Center", Moscow

Received 25.09.2013

Nonlinear permutations of a vector space $GF(2)^m$ of any dimension $m \neq 2^t, t \in \mathbb{N}$, induced by iterations of linear transformation over the ring $R = \mathbb{Z}_4$ with characteristic polynomial $F(x) \in R[x]$, $F(x) \equiv (x \oplus e)^m \pmod{2}$, are studied.

Keywords: digit-permutable polynomial, DP-polynomial, permutation.

Рекурсивно-порождаемые перестановки двоичного пространства

А. В. Аборнев

ООО "Центр сертификационных исследований", Москва

Аннотация. В работе изучаются нелинейные перестановки векторного пространства $GF(2)^m$ произвольной размерности $m \neq 2^t, t \in \mathbb{N}$, порождаемые итерациями линейного преобразования над кольцом $R = \mathbb{Z}_4$, заданного характеристическим многочленом $F(x) \in R[x]$, $F(x) \equiv (x \oplus e)^m \pmod{2}$.

Ключевые слова: разрядно-подстановочный многочлен, РП-многочлен, перестановка.

1 Introduction

Let $R = \mathbb{Z}_4$. A subset $P = \Gamma(R) = \{0, e\}$ is called a *binary digit set* of the ring R . Any element $a \in R$ has a *binary decomposition*

$$a = a_0 + 2a_1, \quad a_s = \gamma_s(a) \in P, \quad s \in \{0, 1\}. \quad (1)$$

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

Let $F(x) \in R[x]$ be a monic polynomial of degree m ,

$$F(x) = x^m - f_{m-1}x^{m-1} - \dots - f_1x - f_0, \quad (2)$$

$L_R(F)$ be a family of all linear recurrent sequences (LRS) over the ring R with characteristic polynomial $F(x)$, and $u \in L_R(F)$. Then

$$u(i + m) = \sum_{s=0}^{m-1} f_s u(i + s), \quad i \geq 0. \quad (3)$$

Using the decomposition (1) we have $u(i) = u_0(i) + 2u_1(i)$, $u_0(i), u_1(i) \in P$, $i \geq 0$. Let us denote by $u[\overline{i, i+k}]$ the vector $(u(i), u(i+1), \dots, u(i+k))$ for all $i \in \mathbb{N}_0, k \in \mathbb{N}$, and by $L'_R(F)$ the set of linear recurrent sequences $u \in L_R(F)$ such that $u_1[\overline{0, m-1}] = \overrightarrow{0}$.

Consider the mapping $\pi_F: P^{(m)} \rightarrow P^{(m)}$ given by

$$\pi_F(x^\downarrow) = u_1[\overline{m, 2m-1}]^T, \quad \text{where } u \in L'_R(F), \quad u_0[\overline{0, m-1}]^T = x^\downarrow, \quad (4)$$

and T is a transpose operator.

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

It was proved in [1] that there exist polynomials $F(x)$ such that the mapping π_F is a bijection. Such polynomials are called *digit-permutable* (or *DP-polynomials*). A DP-polynomial is said to be *nontrivial* if π_F is a nonlinear permutation.

From (3) it follows that for any LRS $u \in L_R(F)$ the first digit sequence satisfies the relation

$$u_1(i + m) = \sum_{s=0}^{m-1} \oplus \gamma_1(f_s) u_0(i + s) \oplus \sum_{s=0}^{m-1} \oplus \gamma_0(f_s) u_1(i + s) \oplus \gamma_1 \left(\sum_{s=0}^{m-1} \gamma_0(f_s) u_0(i + s) \right), \quad (5)$$

where according to [2] the digit function $\gamma_1(x_1 + \dots + x_m)$ has the form

$$\gamma_1(x_1 + \dots + x_m) = \sigma_2(x_1, \dots, x_m) = \sum_{1 \leq s < t \leq m} x_s x_t. \quad (6)$$

Therefore in (5)

$$\gamma_1 \left(\sum_{s=0}^{m-1} \gamma_0(f_s) u_0(i+s) \right) = \sigma_2(\gamma_0(f_0) u_0(i), \dots, \gamma_0(f_{m-1}) u_0(i+m-1)).$$

Hence a DP-polynomial F is nontrivial if and only if the row $(\gamma_0(f_0), \dots, \gamma_0(f_{m-1}))$ contains at least two nonzero elements.

In [1] following classes of DP-polynomials was constructed. Let us introduce notations

$$F_0(x) = x^m \oplus \sum_{s=0}^{m-1} \gamma_0(f_s) x^s \in P[x],$$

$$F_1(x) = \sum_{s=0}^{m-1} \gamma_1(f_s) x^s \in P[x].$$

Theorem 1 ([1]). *Let $R = \mathbb{Z}_4$ and $F(x) \in R[x]$ be a monic 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*

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

(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 $F_1(e) = 0$.*

In this paper we generalize the statement (b) of Theorem 1 to the case of any $m \in \mathbb{N}$, $m \geq 3$.

So below $F(x) \equiv (x - e)^m \pmod{2R}$ is a monic polynomial of degree $m \geq 3$ over the ring R . We can present it in a form

$$F(x) = C(x - e), \quad C(x) = x^m - 2c_{m-1}x^{m-1} - \dots - 2c_0 \in R[x]. \quad (7)$$

Our main result:

Theorem 2. *Let $R = \mathbb{Z}_4$. A polynomial $F(x) \in R[x]$ of the form (7) having degree $m \geq 3$ is a DP-polynomial if and only if $F(e) \neq 0$, that is if $c_0 = e$.*

Note that a DP-polynomial (7) is nontrivial iff $m \neq 2^t$, $t \in \mathbb{N}$.

2 Proof of the necessity

Let us prove that if $c_0 = 0$ than the polynomial (7) is not digit-permutable. Since $c_0 = 0$, it follows that $F(x) = (x - e)G(x)$. Then the sequences

$$u = (0, \dots, 0, 0, \dots, 0, \dots),$$

$$v = (e, \dots, e, e, \dots, e, \dots)$$

belong to $L'_R(F)$. Therefore the map π_F given by (4) is not a bijection, because $u_0[\overline{0, m-1}] \neq v_0[\overline{0, m-1}]$, but

$$\pi_F(u_0[\overline{0, m-1}]) = u_1[\overline{m, 2m-1}] = (0, \dots, 0);$$

$$\pi_F(v_0[\overline{0, m-1}]) = v_1[\overline{m, 2m-1}] = (0, \dots, 0).$$

This means that $F(x)$ is not a DP-polynomial.

3 Proof of the sufficiency

Suppose that $c_0 = e$ and show that $F(x)$ is a DP-polynomial. In this case the polynomial

$$C(x) = x^m - 2c_{m-1}x^{m-1} - \dots - 2c_1x - 2c_0 \in R[x], \quad c_0 = e, \quad (8)$$

is an Eisenstein polynomial [3, 4, 5] and a quotient ring $R[x]/(C(x))$ is isomorphic to the extension $\mathcal{E} = R[\pi]$ of the ring R generated by a root π of the polynomial $C(x)$. According to [3, 4, 5], $R[\pi]$ is a chain ring with the lattice of all ideals

$$\mathcal{E} > \pi\mathcal{E} > \dots > \pi^m\mathcal{E} = 2\mathcal{E} > \dots > \pi^{2m-1}\mathcal{E} > \pi^{2m}\mathcal{E} = 4\mathcal{E} = 0.$$

The module ${}_R\mathcal{E}$ is a free R -module of rank m with a basis

$$e, \pi, \dots, \pi^{m-1}. \quad (9)$$

3.1 Representation of LRS via trace function

Any $\xi \in \mathcal{E}$ has unique representation

$$\xi = \xi_0 + \xi_1\pi + \dots + \xi_{m-1}\pi^{m-1}, \quad \xi_0, \dots, \xi_{m-1} \in R. \quad (10)$$

The map $\text{Tr} : \mathcal{E} \rightarrow R$ taking ξ to ξ_{m-1} is a (*generalized Frobenius*) trace or $\mathcal{GF}$ -trace (see [6]), that is

- (a) $\text{Tr}(x)$ is an epimorphism of R -modules,
- (b) $\text{Ker}(\text{Tr})$ does not contain any nonzero ideal of $\mathcal{E}$.

Notice that the element $\theta = \pi + e$ is a root of the polynomial $F(x) = C(x - e)$. Any $\xi \in T$ defines a sequence

$$u(i) = \text{Tr}(\xi\theta^i), \quad i \in \mathbb{N}_0. \quad (11)$$

Proposition 3. *The sequence (11) belongs to $L_R(F)$ and for any LRS $u \in L_R(F)$ there exists unique $\xi \in \mathcal{E}$ satisfying condition (11).*

Proof. For each sequence (11) consider a sequence

$$v(i) = u(i+m) - f_{m-1}u(i+m-1) - \dots - f_1u(i+1) - f_0u(i), \quad i \geq 0.$$

Using property (a) of the function Tr , we obtain

$$\begin{aligned} v(i) &= \text{Tr}(\xi\theta^{i+m}) - \sum_{k=0}^{m-1} f_k \text{Tr}(\xi\theta^{i+k}) = \\ &= \text{Tr}\left(\xi\theta^{i+m} - \sum_{k=0}^{m-1} f_k \xi\theta^{i+k}\right) = \text{Tr}(\xi F(\theta)) = \text{Tr}(0) = 0. \end{aligned} \quad (12)$$

Therefore u satisfies condition (3), that is $u \in L_R(F)$.

In view of $|\mathcal{E}| = |R|^m = |L_R(F)|$, to finish the proof of the Proposition it is sufficient to show that different sequences (11) correspond to different elements $\xi \in \mathcal{E}$. For this according to property (a) of the function Tr , it is enough to prove that (11) is nonzero sequence for any $\xi \neq 0$.

Let $\xi \in \mathcal{E}$ and

$$\text{Tr}(\xi\theta^k) = 0, \quad k = 0, 1, \dots \quad (13)$$

Since the system of elements (9) is a basis of the module $\mathcal{E}_R$, then the system $e, \theta = e + \pi, \dots, \theta^{m-1} = (e + \pi)^{m-1}$ is also a basis of this module. Therefore any $\alpha \in \mathcal{E}$ has a representation $\alpha = ea_0 + \theta a_1 + \dots + \theta^{m-1}a_{m-1}$, $a_0, \dots, a_{m-1} \in R$ and, by (13), it follows that $\text{Tr}(\xi\alpha) = \sum_{s=0}^{m-1} \text{Tr}(\xi\theta^s) a_s = 0$. Thus the ideal $\xi\mathcal{E}$ of the ring $\mathcal{E}$ satisfies the condition $\text{Tr}(\xi\mathcal{E}) = 0$ and, by property (b) of a trace function, $\xi\mathcal{E} = 0$, that is $\xi = 0$. $\square$

3.2 Representation of the vector $u[\overline{0, 2m-1}]$ in terms of ξ

From the definition (4) of a map π_F it follows that $F(x)$ is a DP-polynomial iff any sequence $u \in L'_R(F)$ is uniquely determined by the vector $u_1[\overline{0, 2m-1}]$. Therefore to prove a sufficiency of the condition of the Theorem 2 it is enough to prove that an element ξ from (11) may be uniquely reconstructed from the vector $u_1[\overline{0, 2m-1}]$.

Now we represent the vector $u[\overline{0, 2m-1}]$ in terms of $\xi^\downarrow = (\xi_{m-1}, \dots, \xi_0)$ from (10). Since $\binom{k}{i} = 0$, where $k < i$, then for $k \geq 0$ we have

$$\text{Tr}(\xi\theta^k) = \text{Tr}(\xi(\pi + e)^k) = \sum_{i=0}^{2m-1} \binom{k}{i} \text{Tr}(\pi^i \xi). \quad (14)$$

Let $i \in \overline{0, m-1}$. Since π is a root of the polynomial $C(x)$ then $\pi^{m+i} = \pi^i \pi^m = \pi^i(2c_{m-1}\pi^{m-1} + \dots + 2c_1\pi + 2c_0)$ and from $2\pi^m = 0$ it follows that

$$\pi^{m+i} = 2c_{m-1-i}\pi^{m-1} + \dots + 2c_1\pi^{i+1} + 2c_0\pi^i, \quad i \in \overline{0, m-1}. \quad (15)$$

Hence for $i \in \overline{1, m-1}$ we have

$$\begin{aligned} \text{Tr}(\pi^i \xi) &= \text{Tr}(\pi^i (\xi_{m-1} \pi^{m-1} + \dots + \xi_1 \pi + \xi_0)) = \\ &= \text{Tr}((\pi^{m-1} 2c_{m-1-(i-1)} \xi_{m-1} + \dots) + \dots + \\ &+ \text{Tr}((\pi^{m-1} 2c_{m-1} \xi_{m-1-(i-1)} + \dots)) + \text{Tr}(\pi^{m-1} \xi_{m-1-i}) = \\ &= 2c_{m-1-(i-1)} \xi_{m-1} + \dots + 2c_{m-1} \xi_{m-1-(i-1)} + \xi_{m-1-i}, \end{aligned}$$

that is

$$\text{Tr}(\pi^i \xi) = (2c_{m-1-(i-1)}, \dots, 2c_{m-1}, e, 0, \dots, 0)(\xi_{m-1}, \dots, \xi_0)^T. \quad (16)$$

Now for $i \in \overline{0, m-1}$ we obtain

$$\begin{aligned} \text{Tr}(\pi^{m+i} \xi) &= \\ &= \text{Tr}((2c_{m-1-i} \pi^{m-1} + \dots + 2c_0 \pi^i)(\xi_{m-1} \pi^{m-1} + \dots + \xi_1 \pi + \xi_0)) = \\ &= 2c_0 \xi_{m-1-i} + \dots + 2c_{m-1-i} \xi_0 = \\ &= (0, \dots, 0, 2c_0, \dots, 2c_{m-1-i})(\xi_{m-1}, \dots, \xi_0)^T. \quad (17) \end{aligned}$$

Let $\left\langle \begin{smallmatrix} i \\ j \end{smallmatrix} \right\rangle = \binom{i}{j} e \in R$, $i, j \in \mathbb{N}_0$, and

$$B^{(N)} = \left(\left\langle \begin{smallmatrix} i \\ j \end{smallmatrix} \right\rangle \right) \in R_{N,N}, \quad i, j \in \overline{0, N-1}. \quad (18)$$

Such matrices (18) are called *Pascal matrices* [7]. Denote by B the matrix $B^{(2m)}$. Substitute relations (16), (17) in (14) and consider the vector

$$u^\downarrow = (u(0), u(1), \dots, u(m-1), u(m), \dots, u(2m-1))^T.$$

Then the first $2m$ elements of the sequence u satisfy the equality

$$u^\downarrow = B C \xi^\downarrow, \quad (19)$$

where

$$B = \left(\begin{array}{cccc|cccc} \langle \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \rangle & 0 & & & 0 & \dots & 0 & \\ \langle \begin{smallmatrix} 1 \\ 0 \end{smallmatrix} \rangle & \langle \begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \rangle & & & \vdots & & \vdots & \\ \vdots & \vdots & \ddots & & & & & \\ \langle \begin{smallmatrix} m-1 \\ 0 \end{smallmatrix} \rangle & \langle \begin{smallmatrix} m-1 \\ 1 \end{smallmatrix} \rangle & \dots & \langle \begin{smallmatrix} m-1 \\ m-1 \end{smallmatrix} \rangle & 0 & \dots & 0 & \\ \hline \langle \begin{smallmatrix} m \\ 0 \end{smallmatrix} \rangle & \langle \begin{smallmatrix} m \\ 1 \end{smallmatrix} \rangle & \dots & \langle \begin{smallmatrix} m \\ m-1 \end{smallmatrix} \rangle & \langle \begin{smallmatrix} m \\ m \end{smallmatrix} \rangle & & 0 & \\ \vdots & \vdots & & & & \ddots & & \\ \langle \begin{smallmatrix} 2m-1 \\ 0 \end{smallmatrix} \rangle & \langle \begin{smallmatrix} 2m-1 \\ 1 \end{smallmatrix} \rangle & \dots & \langle \begin{smallmatrix} 2m-1 \\ m-1 \end{smallmatrix} \rangle & \langle \begin{smallmatrix} 2m-1 \\ m \end{smallmatrix} \rangle & \dots & \langle \begin{smallmatrix} 2m-1 \\ 2m-1 \end{smallmatrix} \rangle & \end{array} \right) \in R_{2m,2m}, \quad (20)$$

$$C = \begin{pmatrix} e & 0 & \cdots & 0 \\ 2c_{m-1} & e & \cdots & 0 \\ & \ddots & \ddots & \\ 2c_1 & & \ddots & e \\ \hline 2c_0 & 2c_1 & & 2c_{m-1} \\ \vdots & \ddots & \ddots & \\ 0 & & 2c_0 & 2c_1 \\ 0 & & 0 & 2c_0 \end{pmatrix} \in R_{2m,m}, \quad (21)$$

and $\xi^\downarrow = (\xi_{m-1}, \dots, \xi_0)^T$.

3.3 Representation of the vector $u_1[\overline{0, 2m-1}]$ in terms of ξ

Using (19), we represent the vector $u_1^\downarrow = u_1[\overline{0, 2m-1}]^T$ in terms of $\xi^\downarrow = \xi_0^\downarrow + 2\xi_1^\downarrow$, $\xi_0^\downarrow, \xi_1^\downarrow \in P^{(m)}$. We will use decompositions $B = B_0 + 2B_1$, $C = C_0 + 2C_1$ of matrices B, C , where $B_j = \gamma_j(B)$, $C_j = \gamma_j(C)$, $j = 0, 1$, are digit matrices over the field P (see (1)). Denote by $\odot, \oplus$ multiplication and addition operations over the field P correspondingly. From (19) we obtain

$$u_1^\downarrow = \gamma_1(BC\xi^\downarrow) = B_1 \odot C_0 \odot \xi_0^\downarrow \oplus B_0 \odot C_1 \odot \xi_0^\downarrow \oplus B_0 \odot C_0 \odot \xi_1^\downarrow \oplus \gamma_1(B_0 C_0 \xi_0^\downarrow). \quad (22)$$

Lemma 4. *The matrix $B_0 = \gamma_0(B)$ is invertible over P and $B_0^{-1} = B_0$.*

Proof. As it was already noticed the matrix B is a lower triangular Pascal matrix modulo 4. It is known [8, 9] that B is invertible and

$$B^{-1} = \left((-1)^{i+j} \left\langle \begin{matrix} i \\ j \end{matrix} \right\rangle \right), \quad i, j \in \overline{0, 2m-1}. \quad (23)$$

Therefore $B_0^{-1} = B_0$. Direct proof of (23) follows from well known orthogonality property of binomial coefficients

$$\sum_{k=0}^n (-1)^{j+k} \binom{k}{j} \binom{i}{k} = \delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases} \quad (24)$$

□

Multiplying both sides of (22) by the matrix $B_0^{-1} = B_0$ from the left, we get

$$B_0 \odot u_1^\downarrow = B_0 \odot B_1 \odot C_0 \odot \xi_0^\downarrow \oplus C_1 \odot \xi_0^\downarrow \oplus C_0 \odot \xi_1^\downarrow \oplus B_0 \odot \gamma_1(B_0 C_0 \xi_0^\downarrow). \quad (25)$$

We can consider the equation (25) as a system of equations

$$\begin{pmatrix} h_0(\xi_0^\downarrow, \xi_1^\downarrow) \\ \vdots \\ h_{2m-1}(\xi_0^\downarrow, \xi_1^\downarrow) \end{pmatrix} = B_0 \odot u_1^\downarrow \quad (26)$$

on variables $\xi_0^\downarrow, \xi_1^\downarrow$, where

$$h_j(\xi_0^\downarrow, \xi_1^\downarrow) : P^{(m)} \times P^{(m)} \rightarrow P, \quad j \in \overline{0, 2m-1},$$

are functions derived from (25). Now describe the left hand side of (26) in more detail.

3.4 Separation of variables $\xi_0^\downarrow$ and $\xi_1^\downarrow$

From (21) it follows that $C = C_0 + 2C_1$, where matrices C_0, C_1 over the field P are divided into $m \times m$ -blocks:

$$C_0 = \begin{pmatrix} E \\ 0 \end{pmatrix}, \quad C_1 = \begin{pmatrix} C'' \\ C''' \end{pmatrix}. \quad (27)$$

Hence in (25)

$$C_0 \odot \xi_1^\downarrow = \begin{pmatrix} \xi_1^\downarrow \\ 0^\downarrow \end{pmatrix}, \quad C_1 \odot \xi_0^\downarrow = \begin{pmatrix} C'' \odot \xi_0^\downarrow \\ C''' \odot \xi_0^\downarrow \end{pmatrix}. \quad (28)$$

Describe the summand $B_0 \odot B_1 \odot C_0 \odot \xi_0^\downarrow$ of the equality (25). Using (20), we get

$$B_0 \odot B_1 = \begin{pmatrix} B' & 0 \\ B'' & * \end{pmatrix}, \quad B', B'' \in P_{m,m}.$$

Then (27) implies

$$B_0 \odot B_1 \odot C_0 \odot \xi_0^\downarrow = \begin{pmatrix} B' \odot \xi_0^\downarrow \\ B'' \odot \xi_0^\downarrow \end{pmatrix}. \quad (29)$$

For the last summand in (25) we will use notations

$$B_0 \odot \gamma_1(B_0 C_0 \xi_0^\downarrow) = \begin{pmatrix} g_0(\xi_0^\downarrow) \\ \vdots \\ g_{2m-1}(\xi_0^\downarrow) \end{pmatrix}. \quad (30)$$

Here $g_0, \dots, g_{2m-1}$ are known functions. Then, substituting equalities (28), (29), (30) in (25), we obtain for the left hand side of the system (26)

$$\begin{pmatrix} h_0(\xi_0^\downarrow, \xi_1^\downarrow) \\ \vdots \\ h_{m-1}(\xi_0^\downarrow, \xi_1^\downarrow) \end{pmatrix} = B' \odot \xi_0^\downarrow \oplus C'' \xi_0^\downarrow \oplus \xi_1^\downarrow \oplus \begin{pmatrix} g_0(\xi_0^\downarrow) \\ \vdots \\ g_{m-1}(\xi_0^\downarrow) \end{pmatrix}, \quad (31)$$

$$\begin{pmatrix} h_m(\xi_0^\downarrow, \xi_1^\downarrow) \\ \vdots \\ h_{2m-1}(\xi_0^\downarrow, \xi_1^\downarrow) \end{pmatrix} = C''' \odot \xi_0^\downarrow \oplus B'' \odot \xi_0^\downarrow \oplus \begin{pmatrix} g_m(\xi_0^\downarrow) \\ \vdots \\ g_{2m-1}(\xi_0^\downarrow) \end{pmatrix}. \quad (32)$$

So the system (26) may be represented as a system of two systems of equations

$$B' \odot \xi_0^\downarrow \oplus C' \xi_0^\downarrow \oplus \xi_1^\downarrow \oplus \begin{pmatrix} g_0(\xi_0^\downarrow) \\ \vdots \\ g_{m-1}(\xi_0^\downarrow) \end{pmatrix} = B_{01} u_1^\downarrow, \quad (33)$$

$$C'' \odot \xi_0^\downarrow \oplus B'' \odot \xi_0^\downarrow \oplus \begin{pmatrix} g_m(\xi_0^\downarrow) \\ \vdots \\ g_{2m-1}(\xi_0^\downarrow) \end{pmatrix} = B_{02} u_1^\downarrow, \quad (34)$$

where $\begin{pmatrix} B_{01} \\ B_{02} \end{pmatrix} = B_0$. Now it is sufficient to prove that under the condition $c_0 = e$ the vector $\xi_0^\downarrow$ is uniquely determined by the system of equations (34), because then the vector $\xi_1^\downarrow$ may be uniquely reconstructed from the system (33).

3.5 Construction of the vector $\xi_0^\downarrow$

In this section we will prove that the system of functions (32) has a triangular form:

$$\begin{cases} h_m = h_m(\xi_0^\downarrow, \xi_1^\downarrow) &= c_0 \xi_{m-1,0} \oplus \tilde{h}_m(\xi_{m-2,0}, \dots, \xi_{0,0}), \\ h_{m+1} = h_{m+1}(\xi_0^\downarrow, \xi_1^\downarrow) &= c_0 \xi_{m-2,0} \oplus \tilde{h}_{m+1}(\xi_{m-3,0}, \dots, \xi_{0,0}), \\ &\vdots \\ h_{2m-2} = h_{2m-2}(\xi_0^\downarrow, \xi_1^\downarrow) &= c_0 \xi_{1,0} \oplus \tilde{h}_{2m-2}(\xi_{0,0}), \\ h_{2m-1} = h_{2m-1}(\xi_0^\downarrow, \xi_1^\downarrow) &= c_0 \xi_{0,0}, \end{cases} \quad (35)$$

for some functions $\tilde{h}_j$, $j \in \overline{m, 2m-2}$. Then the condition $c_0 = e$ implies that the vector $\xi_0^\downarrow$ is uniquely reconstructed from the system (34).

Consider every item of (32). Combining (21) and (27), we get

$$C'' \odot \xi_0^\downarrow = \begin{pmatrix} \xi_{m-1,0} \oplus c_1 \xi_{m-2,0} \oplus \dots \oplus c_{m-1} \xi_{0,0} \\ \vdots \\ \xi_{1,0} \oplus c_1 \xi_{0,0} \\ \xi_{0,0} \end{pmatrix}. \quad (36)$$

Let us show that the matrix $B'' = (b''_{ij}), i, j \in \overline{1, m}$, from (29) satisfies conditions $b''_{ij} = 0$ for all $1 \leq j < i \leq m$, that is all elements on the main diagonal and under the main diagonal of B'' are zeros.

Let $\binom{i}{j}_s = \gamma_s \left(\binom{i}{j} \right)$, $s = 0, 1$. The matrix $B_0 \odot B_1$ is described in the following lemma.

Lemma 5. Let $B_0 \odot B_1 = (b_{ij})$, $i, j \in \overline{0, 2m-1}$. Then

(a) for all $i, j \in \overline{1, 2m-1}$ the following relations hold

$$b_{i,j} = b_{i-1,j-1} \oplus \bigoplus_{k=j}^{i-1} \binom{i-1}{k}_0 \binom{k}{j}_0 \binom{k}{j-1}_0; \quad (37)$$

(b) if $i \geq j + m$, then $b_{i,j} = 0$.

Proof. (a) $B_0 = \binom{i}{j}_0$, $B_1 = \binom{i}{j}_1$. For $i, j \in \overline{1, 2m-1}$, $i > j$, we have

$$b_{i,j} = \sum_{k=j}^i \bigoplus \binom{i}{k}_0 \binom{k}{j}_1. \quad (38)$$

Using obvious equalities

$$\begin{aligned} \binom{i}{k}_0 &= \binom{i-1}{k}_0 \oplus \binom{i-1}{k-1}_0, \\ \binom{i}{k}_1 &= \binom{i-1}{k}_1 \oplus \binom{i-1}{k-1}_1 \oplus \binom{i-1}{k}_0 \binom{i-1}{k-1}_0, \end{aligned}$$

we obtain

$$\begin{aligned} b_{i,j} &= \sum_{k=j}^i \bigoplus \left(\binom{i-1}{k}_0 \oplus \binom{i-1}{k-1}_0 \right) \binom{k}{j}_1 = \\ &= \sum_{k=j}^{i-1} \bigoplus \binom{i-1}{k}_0 \binom{k}{j}_1 \oplus \\ &= \sum_{k=j}^i \bigoplus \binom{i-1}{k-1}_0 \left(\binom{k-1}{j}_1 \oplus \binom{k-1}{j-1}_1 \oplus \binom{k-1}{j}_0 \binom{k-1}{j-1}_0 \right). \quad (39) \end{aligned}$$

Denote by Σ the last sum in (39). Changing limits of summation, we obtain

$$\begin{aligned} \Sigma &= \sum_{k=j-1}^{i-1} \bigoplus \binom{i-1}{k}_0 \left(\binom{k}{j}_1 \oplus \binom{k}{j-1}_1 \oplus \binom{k}{j}_0 \binom{k}{j-1}_0 \right) = \\ &= \sum_{k=j-1}^{i-1} \bigoplus \binom{i-1}{k}_0 \binom{k}{j}_1 \oplus \sum_{k=j-1}^{i-1} \bigoplus \binom{i-1}{k}_0 \binom{k}{j-1}_1 \oplus \sum_{k=j-1}^{i-1} \bigoplus \binom{i-1}{k}_0 \binom{k}{j}_0 \binom{k}{j-1}_0. \end{aligned}$$

Now using (38) and the condition $\binom{j-1}{j} = 0$, we get

$$\Sigma = \sum_{k=j}^{i-1} \bigoplus \binom{i-1}{k}_0 \binom{k}{j}_1 \oplus b_{i-1,j-1} \oplus \sum_{k=j}^{i-1} \bigoplus \binom{i-1}{k}_0 \binom{k}{j}_0 \binom{k}{j-1}_0.$$

Combining this with (39), we obtain

$$b_{i,j} = \sum_{k=j}^{i-1} \bigoplus \binom{i-1}{k}_0 \binom{k}{j}_1 \oplus \Sigma = b_{i-1,j-1} \oplus \sum_{k=j}^{i-1} \bigoplus \binom{i-1}{k}_0 \binom{k}{j}_0 \binom{k}{j-1}_0.$$

That is the relation (37) holds.

(b) From (38) it follows that $b_{i,0} = 0$ for $i \in \overline{0, 2m-1}$. In view of (37) it is enough to prove the equality

$$\sum_{k=j}^{i-1} \binom{i-1}{k}_0 \binom{k}{j}_0 \binom{k}{j-1}_0 = 0. \quad (40)$$

Using the subset-of-a-subset identity [11]

$$\binom{i-1}{k}_0 \binom{k}{j}_0 = \binom{i-1}{j}_0 \binom{i-j-1}{k-j}_0, \quad (41)$$

we get

$$\begin{aligned} \sum_{k=j}^{i-1} \binom{i-1}{k}_0 \binom{k}{j}_0 \binom{k}{j-1}_0 &= \binom{i-1}{j}_0 \sum_{k=j}^{i-1} \binom{i-j-1}{k-j}_0 \binom{k}{j-1}_0 = \\ &= \binom{i-1}{j}_0 \sum_{k=0}^{i-j-1} \binom{i-j-1}{k}_0 \binom{k+j}{j-1}_0. \end{aligned} \quad (42)$$

Now if we prove that for all $s, t, i \in \mathbb{N}$, where $s > t$, the condition

$$\sum_{k=0}^s \binom{s}{k}_0 \binom{k+i}{t}_0 = 0 \quad (43)$$

holds, then using $i \geq j+m$ and $i-j-1 \geq m-1 > j-1$ we will obtain that the last sum in (42) equals to zero, that is (40) holds.

Let $t \in \mathbb{N}$. Consider a binomial sequence $e^{[t]}(k) = \binom{k}{t}_0$, $k \geq 0$ (see [10]). It is known that $e^{[t]} \in L_P((x \oplus e)^{t+1})$. This implies that for $s > t$ the sequence $z = (x \oplus e)^s e^{[t]}$ equals to zero sequence. But

$$z(i) = (x \oplus e)^s e^{[t]}(i) = \sum_{k=0}^s \binom{s}{k}_0 e^{[t]}(i+k) = \sum_{k=0}^s \binom{s}{k}_0 \binom{k+i}{t}_0. \quad (44)$$

The equality (43) and the Lemma are proved. $\square$

Since

$$B_0 \odot B_1 = \begin{pmatrix} B' & 0 \\ B'' & * \end{pmatrix}, \quad B', B'' \in P_{m,m},$$

then the statement (b) of Lemma 5 means that in the matrix B'' all elements on the main diagonal and under the main diagonal are zeros.

To finish the proof of a sufficiency of the condition of the Theorem we have to describe the last summand in (32).

Lemma 6. Let $g_0, \dots, g_{2m-1}$ be functions from (30). Then

$$\begin{cases} g_m(\xi_0^\downarrow) &= g_m(\xi_{m-2,0}, \dots, \xi_{0,0}), \\ g_{m+1}(\xi_0^\downarrow) &= g_{m+1}(\xi_{m-3,0}, \dots, \xi_{0,0}), \\ &\vdots \\ g_{2m-2}(\xi_0^\downarrow) &= g_{2m-2}(\xi_{0,0}), \\ g_{2m-1}(\xi_0^\downarrow) &= 0. \end{cases} \quad (45)$$

Proof. In view of (30), using the form (27) of C_0 , we have

$$\gamma_1(B_0 C_0 \xi_0^\downarrow) = \begin{pmatrix} \gamma_1 \left(\binom{0}{0}_0 \xi_{m-1,0} \right) \\ \gamma_1 \left(\binom{1}{0}_0 \xi_{m-1,0} + \binom{1}{1}_0 \xi_{m-2,0} \right) \\ \vdots \\ \gamma_1 \left(\binom{m-1}{0}_0 \xi_{m-1,0} + \dots + \binom{m-1}{m-1}_0 \xi_{0,0} \right) \\ \gamma_1 \left(\binom{m}{0}_0 \xi_{m-1,0} + \dots + \binom{m}{m-1}_0 \xi_{0,0} \right) \\ \vdots \\ \gamma_1 \left(\binom{2m-1}{0}_0 \xi_{m-1,0} + \dots + \binom{2m-1}{m-1}_0 \xi_{0,0} \right) \end{pmatrix}.$$

Therefore, by (30), we get

$$g_t(\xi_0^\downarrow) = \sum_{k=0}^t \bigoplus \binom{t}{k}_0 \gamma_1 \left(\binom{k}{0}_0 \xi_{m-1,0} + \dots + \binom{k}{m-1}_0 \xi_{0,0} \right), \quad t \in \overline{1, 2m-1}.$$

By description (6) of the digit function γ_1 , the last equality implies

$$g_t(\xi_0^\downarrow) = \sum_{k=0}^t \bigoplus \binom{t}{k}_0 \sum_{0 \leq i < j < m} \binom{k}{i}_0 \binom{k}{j}_0 \xi_{m-1-i,0} \xi_{m-1-j,0}.$$

Changing the order of summation, we get

$$g_t(\xi_0^\downarrow) = \sum_{0 \leq i < j < m} \xi_{m-1-i,0} \xi_{m-1-j,0} \sum_{k=0}^t \bigoplus \binom{t}{k}_0 \binom{k}{i}_0 \binom{k}{j}_0. \quad (46)$$

Let $0 \leq i < j < m$. Evidently,

$$\sum_{k=0}^t \bigoplus \binom{t}{k}_0 \binom{k}{i}_0 \binom{k}{j}_0 = \sum_{k=j}^t \bigoplus \binom{t}{k}_0 \binom{k}{i}_0 \binom{k}{j}_0.$$

Then, using the subset-of-a-subset identity $\binom{t}{k}_0 \binom{k}{j}_0 = \binom{t}{j}_0 \binom{t-j}{k-j}_0$, we obtain in (46)

$$\sum_{k=j}^t \binom{t}{k}_0 \binom{k}{i}_0 \binom{k}{j}_0 = \binom{t}{j} \sum_{k=j}^t \binom{t-j}{k-j}_0 \binom{k}{i}_0 = \binom{t}{j} \sum_{k=0}^{t-j} \binom{t-j}{k}_0 \binom{k+j}{i}_0. \quad (47)$$

Now (43) implies that if $t - j > i$, then the last sum in (47) and the coefficient at $\xi_{m-1-i,0} \xi_{m-1-j,0}$ in (46) equal to 0. This means that functions g_{m+s} do not depend on variables $\xi_{m-1,0}, \dots, \xi_{m-1-s,0}$, where $s = 0, \dots, m-1$. This proves (45). $\square$

The theorem is completely proved.

Acknowledgments

The author expresses profound gratitude to professor Alexander A. Nechaev for attention and for the help in proving the main result.

References

- [1] *Nechaev A. A., Abornev A. V.* Nonlinear permutations on a space over a finite field induced by linear transformations of a module over a Galois ring // *Mathematical Aspects of Cryptography*. — 2013. — V. 4. No 2. — P. 81–100.
- [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] *Nechaev A. A.* On the structure of finite commutative rings with an identity // *Mathematical Notes*. — 1971. — V. 10. No 6. — P. 840–845.
- [4] *Elizarov V. P.* Finite Rings (foundations of the theory). — Moscow : Gelios-ARV, 2006. — 304 p. (in Russian).
- [5] *Nechaev A. A.* Finite rings with applications // *Handbook of Algebra*. M. Hazewinkel, ed. — Elsevier, 2008. — V. 5. — P. 213–320.
- [6] *Greferath M., Nechaev A.* Generalized Frobenius extensions of finite rings and trace functions // *Information Theory Workshop (ITW)*, 2010 IEEE. Dublin. — P. 1–5.
- [7] *Edwards A.W.F.* Pascal's Arithmetical Triangle: The Story of a Mathematical Idea. — London : Charles Griffin, 1987.

- [8] *Call G. S., Vellman D. J.* Pascal's matrices // Amer. Math. Monthly. — 1993. — V. 100. — P. 372–376.
- [9] *Edelman A., Strang G.* Pascal matrices // Amer. Math. Monthly. — 2004. — V. 111. No 3. — 361–385.
- [10] *Glukhov M. M., Elizarov V. P., Nechaev A. A.* Algebra. — Moscow : Gelios-ARV, 2003. — V. II. — 416 p. (in Russian).
- [11] *Jonathan L. G.* Combinatorial Methods with Computer Applications // Discrete Mathematics and Its Applications. — Chapman and Hall/CRC, 2007. — 664 p.