Proceedings of the Steklov Institute of Mathematics, Vol. 218, 1997, pp. 332–339.
Translated from Trudy Matematicheskogo Instituta imeni V. A. Steklova, Vol. 218, 1997, pp. 335–342.

Distribution of Signs in a Sequence of Rectangular Matrices over a Finite Field

V. I. Nechaev

Received February, 1997

This article deals with the problem of distribution of the collections s of fixed signs on a given segment of a row or a column in a sequence of rectangular matrices which satisfy the linear recurrence equation over a finite field and the number of coincidence of these collections.

The problem of the number of the collections s $(< n)$ of signs on a full period of a maximal linear recurrent sequence of order n was considered by Laksov [8] and Zierler [10] and the problem of number of occurences of a fixed sign on a part of the period of a maximal linear recurrent sequence was studied by Lidl and Niderreiter [3] and [9]. The problem of the occurence of a fixed collection of signs as successive values of a maximal linear recurrent sequence was considered by N. M. Korobov. In this article we use the approach to the study of linear recurrent sequences which was described, for the first time, in the articles [4–7].

Notation and terms. Assume that p is a prime number, $\mathbb{N}$ is the set of positive integers, $\mathbb{Z}$ is the set of integers, $\mathbb{C}$ is the set of complex numbers; $n, s, q, X \in \mathbb{N}$, $\mathbb{F} = \mathbb{F}_q = \mathrm{GF}(q)$ is a finite field of q elements, $p \mid q$; $\mathbf{V}_n$ is an n-dimensional vector space over the field $\mathbb{F}$; $\alpha \bullet \beta$ is the inner product of the vectors α and β in the space $\mathbf{V}_n$; $\mathbf{V}_n^*$ is the set of nonzero vectors of the space $\mathbf{V}_n$; $M\bullet$ is a linear operator on the space $\mathbf{V}_n$ for any square matrix M of order n over the field $\mathbb{F}_q$, as well as on the space $\mathbf{V}_{n,k}$ of rectangular $n \times k$ matrices; E_n is the identity $n \times n$ matrix; $\Box_{n,k}$ is zero matrix on the space $\mathbf{V}_{n,k}$, $\Box_{n,1} = \theta^{(n)}$ is the null-vector of the space $\mathbf{V}_{n,1} = \mathbf{V}_n$; $a_1, \dots, a_n \in \mathbb{F}$, $a_n \neq 0$, $f = \lambda^n - a_1\lambda^{n-1} - a_2\lambda^{n-2} - \cdots - a_n$ is the characteristic polynomial of a linear recurrence equation of the form

$$\delta_{x+n} = a_1\delta_{x+n-1} + a_2\delta_{x+n-2} + \cdots + a_n\delta_x, \quad x \in \mathbb{Z}, \qquad \delta_0, \delta_1, \dots, \delta_{n-1} \in \mathbb{F}. \tag{1}$$

By the symbol $\delta = \{\delta_x\}_{x=-\infty}^{+\infty} = \{\delta_x\}_x$ we denote any solution of equation (1). The nonzero solution $\delta = \{\delta_x\}_{x=-\infty}^{+\infty}$ over the field $\mathbb{F}$ of equation (1) is called a maximal linear recurrent sequence if its primitive period, i.e., the least natural period, is equal to $q^n - 1$; $\operatorname{ord} f$ is the order of the polynomial over the field $\mathbb{F}$, i.e., the least positive integer t such that $x^t - 1$ is divisible by the polynomial f; the polynomial f over the field $\mathbb{F} = \mathbb{F}_q$ is said to be primitive if $\operatorname{ord} f = q^{\deg f} - 1$; $\rho^{(j)} = \{\rho_x^{(j)}\}_{x=0}^{\infty}$ for every $j = 0, 1, \dots, n-1$ is the solution of equation (1) with the initial values

$$\rho_x^{(j)} = \begin{cases} 1 & \text{for } x = j \\ 0 & \text{for } x \neq j, \end{cases} \qquad 0 \le x \le n-1;$$

β_x and Δ_x are n-dimensional vectors, for all integers x, defined by the conditions

$$\beta_x = \left\| \begin{matrix} \rho_x^{(0)} \\ \rho_x^{(1)} \\ \vdots \\ \rho_x^{(n-2)} \\ \rho_x^{(n-1)} \end{matrix} \right\|, \qquad \Delta_x = \left\| \begin{matrix} \delta_x \\ \delta_{x+1} \\ \vdots \\ \delta_{x+n-2} \\ \delta_{x+n-1} \end{matrix} \right\|.$$

Assume, furthermore, that

$$A = \left\| \begin{matrix} 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \\ a_n & a_{n-1} & \dots & a_2 & a_1 \end{matrix} \right\|$$

is a matrix of equation (1), $B = A^T$ is the transposite of the matrix A. Thus, $B = [\beta_1, \beta_2, \dots, \beta_n]$, i.e., the vectors $\beta_1, \beta_2, \dots, \beta_n$ are columns of the matrix B; $b_1, b_2, \dots, b_s \in \mathbb{F}$; $m, m_1, m_2, \dots, m_s \in \mathbb{Z}$.

Next suppose that χ is a character of the additive group of the field $\mathbb{F}$ and χ_0 is the principal character of the same group, $e_t(x) = \exp(2\pi i x/t)$.

It is important to note for what follows that the set of solutions of equation (1) forms an n-dimensional vector space over the field $\mathbb{F}$ of ordinary operators on sequences, the primitive period of any solution of equation (1) divides the order of the characteristic polynomial of this equaltion and is equal to it if the characteristic polynomial is a primitive polynomial over the field $\mathbb{F}$ [9]. The polynomial f is primitive over the field $\mathbb{F}$ if and only if $\operatorname{ord} f = q^n - 1$. The primitive polynomial over the field $\mathbb{F}$ is irreducible over the same field. The order of the characteristic polynomial f of the square matrix C over a finite field is equal to the order of this matrix ($\operatorname{ord} f = \operatorname{ord} C$).

Lemma 1. *$\delta_{x+y} = \beta_x \bullet \Delta_y$ holds for all integers x, y.*

Proof. Indeed, the relation

$$\delta_{x+y} = \delta_y \rho_x^{(0)} + \delta_{y+1} \rho_x^{(1)} + \dots + \delta_{y+n-1} \rho_x^{(n-1)} \tag{2}$$

is valid for $x = 0, 1, \dots, n-1$ for every fixed y, and therefore the solutions δ_{x+y} and $\beta_x \bullet \Delta_y$ of equation (1) are equal for n successive values of the variable x.

Lemma 2. *The solutions $\{\delta_{x+h}\}_x, \dots, \{\delta_{x+g}\}_x$ of equation (1) are linearly independent over the field $\mathbb{F}$ if and only if the vectors $\beta_h, \dots, \beta_g$ of the space $\mathbf{V}_n$ are linearly independent over the field $\mathbb{F}$.*

Proof. It follows from Lemma 1.

Lemma 3. *For all integers x we have*

(1) $A^x \bullet \Delta_0 = \Delta_x$,
(2) $B^x \bullet \beta_0 = \beta_x$.

Proof. (1) follows from the easily verifiable relation $A \bullet \Delta_x = \Delta_{x+1}$.

(2) Setting $\delta_y = \rho_y^{(j)}$, where $0 \le j \le n-1$, in relation (2), we obtain

$$\rho_{x+y}^{(j)} = \rho_y^{(j)} \times \rho_x^{(0)} + \rho_{y+1}^{(j)} \times \rho_x^{(1)} + \dots + \rho_{y+n-1}^{(j)} \times \rho_x^{(n-1)}.$$

It follows that

$$\rho_{x+y}^{(j)} = \rho_1^{(0)} \times \rho_y^{(j)} + \rho_1^{(1)} \times \rho_{y+1}^{(j)} + \cdots + \rho_1^{(n-1)} \times \rho_{y+n-1}^{(j)}$$

for all $y \in \mathbb{Z}$. Thus $B \bullet \beta_y = \beta_{y+1}$.

Lemma 4. *The vectors $\beta_1, \beta_2, \ldots, \beta_n$ are linearly independent over the field $\mathbb{F}$.*

Proof. Indeed,

$$\| \beta_1 \quad \beta_2 \quad \ldots \quad \beta_n \| = \left\| \begin{matrix} 0 & 0 & \ldots & 0 & a_n \\ 1 & 0 & \ldots & 0 & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & a_2 \\ 0 & 0 & \ldots & 1 & a_1 \end{matrix} \right\| .$$

Lemma 5. *Let γ be a nonzero vector of the space $\mathbf{V}_n$. Then*

$$(B^x \bullet \gamma) \bullet \Delta_y = \gamma \bullet \Delta_{x+y} \tag{3}$$

for every integer x, y.

Proof. Since the vectors $\beta_1, \beta_2, \ldots, \beta_n$ are linearly independent, it follows that the relation $\gamma = c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n$ holds true for certain $c_1, c_2, \ldots, c_n$. Identity (3) can be direcly verified.

Lemma 6. *Let $\gamma \in \mathbf{V}_n$, $\chi \neq \chi_0$. Then*

(1) $\displaystyle\sum_{a \in \mathbb{F}} \chi(a \times c) = \begin{cases} q & \text{for } c = 0 \\ 0 & \text{for } c \neq 0; \end{cases}$

(2) $\displaystyle\sum_{\alpha \in \mathbf{V}_n} \chi(\alpha \bullet \gamma) = \begin{cases} q^n & \text{for } \gamma = \theta \\ 0 & \text{for } \gamma \neq \theta. \end{cases}$

Proof. (1) Indeed, if $c \in \mathbb{F}$ and $c \neq 0$, then $a \times c$ together with a runs through all elements of the field $\mathbb{F}$.

(2) If $c_1, c_2, \ldots, c_n \in \mathbb{F}$, then

$$\sum_{a_1, \ldots, a_n \in \mathbb{F}} \chi(a_1 \times c_1 + \cdots + a_n \times c_n) = \sum_{a_1 \in \mathbb{F}} \chi(a_1 \times c_1) \cdots \sum_{a_n \in \mathbb{F}} \chi(a_n \times c_n).$$

This proves the second assertion.

Lemma 7. *Let f be a primitive polynomial over the field $\mathbb{F}$ of degree n, $t = \operatorname{ord} f$, $a \in \mathbb{Z}$, $\gamma \in \mathbf{V}_n$, $\gamma_x = B^x \bullet \gamma$,*

$$\sigma_{a,t}(\delta, y) = \sum_{x=1}^{t} \chi(\gamma \bullet \Delta_x) \times e_t(a \times x).$$

Then

$$\sigma_{a,t}(\delta, y) = \begin{cases} q^{n/2} & \text{for } 1 \leq a < t \\ 1 & \text{for } a = 0. \end{cases}$$

Proof. Since t is the period of any solution of equation (1), we have

$$\sum_{x=1}^{t} \chi(\gamma \bullet \Delta_x) \times e_t(a \times x) = \sum_{x=1}^{t} \chi(\gamma \bullet \Delta_{x+y}) \times e_t\big(a(x+y)\big)$$

for any integer y. Next note that $\gamma \bullet \Delta_{x+y} = \gamma_x \bullet \Delta_y$. Therefore

$$|\sigma_{a,t}(\delta,\gamma)| = \left|\sum_{x=1}^{t} \chi(\gamma \bullet \Delta_{x+y}) \times e_t(a \times x)\right| = \left|\sum_{x=1}^{t} \chi(\gamma_x \bullet \Delta_y) \times e_t(a \times x)\right|.$$

Consequently,

$$\begin{aligned} t|\sigma_{a,t}(\delta,\gamma)|^2 &= \sum_{y=1}^{t}\sum_{x=1}^{t}\sum_{z=1}^{t} \chi\big((\gamma_x - \gamma_z) \bullet \Delta_y\big) \times e_t\big(a \times (x-z)\big) \\ &= \sum_{u=1}^{t}\sum_{z=1}^{t} e_t(a \times u) \sum_{y=1}^{t} \chi\big((\gamma_{u+z} - \gamma_z) \bullet \Delta_y\big) \\ &= \sum_{z=1}^{t} 1 \times \sum_{y=1}^{t} \chi(0) + \sum_{u=1}^{t-1}\sum_{z=1}^{t} e_t(a \times u) \times \sum_{\alpha \in \mathbf{V}^*} \chi\big((\gamma_{u+z} - \gamma_z) \bullet \alpha\big) \\ &= t^2 - t \times \sum_{u=1}^{t-1} e_t(a \times u) = \begin{cases} t & \text{for } a = 0 \\ t^2 + t & \text{for } 1 \le a < t. \end{cases} \end{aligned}$$

Lemma 8. *For any positive integer $t > 12$ and X we have*

$$\left|\sum_{u=1}^{t-1}\sum_{z=1}^{X} e_t(-a \times z)\right| < t \ln t - \frac{t}{2}.$$

Proof. [1, Ch. 3, Question 11c]. See also [3, Lemma 8.10].

Lemma 9. *Let f be a primitive polynomial over the field $\mathbb{F}$ of degree n, $\gamma \in \mathbf{V}_n$, $\gamma \neq \theta$,*

$$\sigma(X) = \sum_{x=1}^{X} \chi(\gamma \bullet \Delta_x).$$

If $1 \le X \le t$, then

$$|\sigma(X)| < q^{n/2} \ln t.$$

Proof. We have

$$\sum_{z=1}^{X}\sum_{x=1}^{t}\sum_{a=1}^{t} \chi(\gamma \bullet \Delta_x) \times e_t\big(a(x-z)\big) = \sum_{z=1}^{t}\sum_{x=1}^{t} \chi(\gamma \bullet \Delta_x) \times e_t\big(a(x-z)\big)$$

and therefore

$$t\sum_{x=1}^{X} \chi(\gamma \bullet \Delta_x) = X \sum_{x=1}^{t} \chi(\gamma \bullet \Delta_x) + \sum_{a=1}^{t-1}\sum_{x=1}^{t} \chi(\gamma \bullet \Delta_x) e_t(a \times x) \times \sum_{z=1}^{X} e_t(-a \times z),$$

$$t|\sigma(X)| \le X + q^{n/2}\left|\sum_{a=1}^{t-1}\sum_{z=1}^{X} e_t(-a \times z)\right| < X + q^{n/2}(t \ln t - t).$$

This easily yields $|\sigma(X)| < q^{n/2} \ln t$.

Theorem 1. *Let $X \le t$, $1 \le s < n$, $t > 12$, $1 \le m < t$. Suppose that $\delta^{(1)} = \{\delta_x^{(1)}\}_x, \dots, \delta^{(s)} = \{\delta_x^{(s)}\}_x$ are solutions of equation* (1) *which are linearly independent over the field $\mathbb{F}$, $T_{1X} = T_{1X}(b_1, \dots, b_s; \delta^{(1)}, \dots, \delta^{(s)})$ and $T_{2X} = T_{1X}(b_1, \dots, b_s; m; \delta^{(1)}, \dots, \delta^{(s)})$ are the numbers of solutions in integers of the system of equations of the forms*

$$\delta_x^{(1)} = b_1, \quad \dots, \quad \delta_x^{(s)} = b_s, \qquad 1 \le x \le X,$$

and

$$\delta_x^{(1)} = \delta_{x+m}^{(1)} + b_1, \quad \dots, \quad \delta_x^{(s)} = \delta_{x+m}^{(s)} + b_s, \qquad 1 \le x \le X,$$

respectively. Then

(1) $T_{1X} = T_{1X}(b_1, \dots, b_s; \delta^{(1)}, \dots, \delta^{(s)}) = \dfrac{X}{q^s} + \varepsilon q^{n/2} \ln t$, *where $\varepsilon \in \mathbb{C}$ and $|\varepsilon| < 1$;*

(2) $T_{2X} = T_{1X}(b_1, \dots, b_s; m; \delta^{(1)}, \dots, \delta^{(s)}) = \dfrac{X}{q^s} + \varepsilon q^{n/2} \ln t$, *where $\varepsilon \in \mathbb{C}$ and $|\varepsilon| < 1$.*

Proof. Each of two nonzero solutions of equation (1) is a shift of the other solution. Therefore there exist nonnegative integers $m_1, \dots, m_s$ such that

$$\delta_x^{(1)} = \delta_{x+m_1}, \quad , \dots, \quad \delta_x^{(s)} = \delta_{x+m_s}$$

for all $x \in \mathbb{Z}$. By virtue of Lemma 5, we have

$$T_{1X} = \frac{1}{q^s} \sum_{x=1}^{X} \sum_{c_1, \dots, c_s \in \mathbb{F}} \chi\big(c_1(\delta_{x+m_1} - b_1) + \dots + c_s(\delta_{x+m_s} - b_s)\big),$$

and therefore

$$T_{1X} = \frac{1}{q^s} \sum_{c_1, \dots, c_s \in \mathbb{F}} \chi(-c_1 b_1 - \dots - c_s b_s) \sum_{x=1}^{X} \chi(\gamma_x),$$

where $\gamma_x = c_1 \delta_{x+m_1} + \dots + c_s \delta_{x+m_s}$. Using Lemma 1, we obtain

$$\gamma_x = \Delta_x \bullet (c_1 \times \beta_{m_1} + \dots + c_s \times \beta_{m_s}).$$

By virtue of Lemma 2, the vectors $\beta_{m_1}, \beta_{m_2}, \dots, \beta_{m_s}$ are linearly independent over the field $\mathbb{F}$. Therefore

$$T_{1X} = \frac{X}{q^s} + \frac{1}{q^s} \sum\nolimits^*_{c_1, \dots, c_s \in \mathbb{F}} \chi(-c_1 b_1 - \dots - c_s b_s) \sum_{x=1}^{X} \chi(\gamma_x),$$

where $\sum^*$ is the sum over all collections $c_1, c_2, \dots, c_s$ of elements of the field $\mathbb{F}$. From this and from Lemma 8 we get the first assertion of the theorem.

Next we have

$$T_{2X} = \frac{1}{q^s} \sum_{x=1}^{X} \sum_{c_1, \dots, c_s \in \mathbb{F}} \chi\big(c_1(\delta_{x+m_1} - \delta_{x+m_1+m} - b_1) + \dots + c_s(\delta_{x+m_s} - \delta_{x+m_s+m} - b_s)\big).$$

By virtue of Lemmas 1 and 3, for every i, $1 \le i \le s$, we have

$$\delta_{x+m_i} - \delta_{x+m_i+m} = \Delta_x \bullet \big(B^{m_i} \bullet (\beta_0 - \beta_m)\big).$$

It follows from the hypothesis of the theorem that $\beta_0 - \beta_m \ne \theta$, and since the primitive period of the sequence $\{\beta_x\}_{x=-\infty}^{+\infty}$ is equal to $t = q^n - 1$, the relation $\beta_0 - \beta_m = \beta_{m^*}$ holds true for a certain positive integer m^*, $0 \le m^* < t$. Therefore

$$T_{2X} = \frac{1}{q^s} \sum_{c_1,\dots,c_s \in \mathbb{F}} \chi(-c_1 b_1 - \dots - c_s b_s) \sum_{x=1}^{X} \chi(\Delta_0 \bullet \gamma_{c_1,\dots,c_s}),$$

where

$$\gamma_{c_1,\dots,c_s} = c_1 \beta_{m^*+m_1} + \dots + c_s \beta_{m^*+m_s} = B^{m^*} \bullet (c_1 \beta_{m_1} + \dots + c_s \beta_{m_s}).$$

And since the vectors $\beta_{m_1}, \dots, \beta_{m_s}$ are linearly independent over the field $\mathbb{F}$ by virtue of Lemma 2, we have $\gamma_{c_1,\dots,c_s} = \theta$ if and only if $c_1 = \dots = c_s = 0$. Consequently,

$$T_{2X} = \frac{X}{q^s} + \frac{1}{q^s} \sum\nolimits^{*}_{c_1,\dots,c_s \in \mathbb{F}} \chi(-c_1 b_1 - \dots - c_s b_s) \sum_{x=1}^{X} \chi(\Delta_0 \bullet \gamma_{c_1,\dots,c_s}),$$

where the summation in the sum $\sum^*$ is carried out over all nonzero collections of elemnts of the field $\mathbb{F}$. This and Lemma 8 yield the second assertion of the theorem.

We are considering a sequence of rectangular $n \times k$ matrices which satisfies the recurrence equation of the form

$$C \bullet D_{n,k}^{(x)} = D_{n,k}^{(x+1)}, \qquad x \in \mathbb{Z}, \tag{4}$$

where C is a square $n \times n$ matrix and $D_{n,k}^{(0)}$ is a rectangular $n \times k$ matrix. In the sequel we shall use the following notation:

$$C = \begin{Vmatrix} c_{1,1} & \dots & c_{1,n} \\ \vdots & \ddots & \vdots \\ c_{n,1} & \dots & c_{n,n} \end{Vmatrix}, \qquad C^x = \begin{Vmatrix} c_{1,1}^{(x)} & \dots & c_{1,n}^{(x)} \\ \vdots & \ddots & \vdots \\ c_{n,1}^{(x)} & \dots & c_{n,n}^{(x)} \end{Vmatrix}, \qquad D_{n,k}^{(0)} = \begin{Vmatrix} d_{1,1} & \dots & d_{1,k} \\ \vdots & \ddots & \vdots \\ d_{n,1} & \dots & d_{n,k} \end{Vmatrix},$$

$$D_{n,k}^{(x)} = \begin{Vmatrix} d_{1,1}^{(x)} & \dots & d_{1,k}^{(x)} \\ \vdots & \ddots & \vdots \\ d_{n,1}^{(x)} & \dots & d_{n,k}^{(x)} \end{Vmatrix}, \qquad \Delta_x^{(j)} = \begin{Vmatrix} d_{1,j}^{(x)} \\ \vdots \\ d_{n,j}^{(x)} \end{Vmatrix}, \qquad \Psi_x^{(i)} = \begin{Vmatrix} c_{i,1}^{(x)} & \dots & c_{i,n}^{(x)} \end{Vmatrix},$$

f is the characteristic polynomial of the matrix C.

Theorem 2. *Let* $f = \lambda^n - a_1 \lambda^{n-1} - \dots - a_{n-1}\lambda - a_n$, $\operatorname{ord} f = q^n - 1$, $\operatorname{rang} D_{n,k}^{(0)} = k$. *Then*

(1) *for any pair of integers* (i,j), $1 \le i \le n$, $1 \le j \le k$, *the sequence* $\{d_{i,j}^{(x)}\}_x$ *is a nonzero solution of equation* (1);

(2) *for every* j, $1 \le j \le k$, *the solutions of equation* (1) *of the form*

$$\{d_{1,j}^{(x)}\}_x, \quad \dots, \quad \{d_{n,j}^{(x)}\}_x \tag{5}$$

are linearly independent over the field $\mathbb{F}$;

(3) *for every* i, $1 \le i \le n$, *the solutions of equation* (1) *of the form*

$$\{d_{i,1}^{(x)}\}_x, \quad \dots, \quad \{d_{i,k}^{(x)}\}_x \tag{6}$$

are linearly independent over the field $\mathbb{F}$.

Proof. We have

$$C^n - a_1C^{n-1} - a_2C^{n-2} - \dots - a_{n-1}C - a_nE_n = \square_{n,n},$$

and therefore

$$(C^n - a_1C^{n-1} - \dots - a_{n-1}C - a_nE_n) \bullet D_{n,k}^{(x)} D_{n,k}^{(x+n)} - a_1 D_{n,k}^{(x+n-1)} - \dots - a_n D_{n,k}^{(x)} = \square_{n,k}.$$

Consequently, for any pair of positive integers (i,j), $1 \le i \le n$, $1 \le j \le k$, we have

$$d_{i,j}^{(n+x)} - a_1 d_{i,j}^{(n-1+x)} - \dots - a_n d_{i,j}^{(x)} = 0.$$

Thus, the sequence $\{d_{i,j}^{(x)}\}_x$ is a solution of equation (1). The primitive period of sequence (7) is equal to 1 if it is zero and to t otherwise. It immediately follows from relation (4) that $C \bullet \Delta_x^{(j)} = \Delta_{x+1}^{(j)}$. Therefore $C^x \bullet \Delta_0^{(j)} = \Delta_x^{(j)}$. Note that for any nonzero vector α of the space $\mathbf{V}_n$ we have

$$C^x \bullet \alpha = C^y \bullet \alpha$$

if and only if $x \equiv y \pmod t$. It follows that the vectors of the series $\Delta_0^{(j)}, \Delta_1^{(j)}, \dots, \Delta_{t-1}^{(j)}$, and all columns of the matrix M_j of the form

$$M_j = \begin{Vmatrix} d_{1,j}^{(0)} & d_{1,j}^{(1)} & \dots & d_{1,j}^{(t-1)} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n,j}^{(0)} & d_{n,j}^{(1)} & \dots & d_{n,j}^{(t-1)} \end{Vmatrix}$$

are different. And since their number is equal to the number of nonzero vectors of the space $\mathbf{V}_n$, the rows of the matrix M_j are linearly independent over the field $\mathbb{F}$. Consequently, the solutions of (5) are also linearly independent over the field $\mathbb{F}$. In particular, the solutions $\{c_{1,j}^{(x)}\}_x, \{c_{2,j}^{(x)}\}_x, \dots, \{c_{n,j}^{(x)}\}_x$ are linearly independent over the field $\mathbb{F}$. It is easy to deduce from the relation $\Psi_x^{(i)} * C = \Psi_{x+1}^{(i)}$ that the solutions

$$\{c_{1,j}^{(x)}\}_x, \quad \{c_{2,j}^{(x)}\}_x, \quad \dots, \quad \{c_{n,j}^{(x)}\}_x \tag{7}$$

are also linearly independent over the field $\mathbb{F}$. It remains to prove that the solutions of (6) are linearly independent over the field $\mathbb{F}$. If this is not the fact, then there exist elements $u_1, u-2, \dots, u_k$, not all of which are zero, such that

$$u_1 d_{i,1}^{(x)} + u_2 d_{i,2}^{(x)} + \dots + u_k d_{i,k}^{(x)} = 0$$

for all $x \in \mathbb{Z}$. Noting that $C^x \bullet D_{n,k}^{(0)} = D_{n,k}^{(x)}$, we obtain

$$c_{i,1}^{(x)} d_{1,j} + \dots + c_{i,n}^{(x)} d_{n,j} = d_{i,j}^{(x)}$$

for all $x \in \mathbb{Z}$. Therefore, for every integer x, we have

$$u_1(c_{i,1}^{(x)} d_{1,1} + \dots + c_{i,n}^{(x)} d_{n,1}) + u_2(c_{i,1}^{(x)} d_{1,2} + \dots + c_{i,n}^{(x)} d_{n,2}) + \dots + u_k(c_{i,1}^{(x)} d_{1,k} + \dots + c_{i,n}^{(x)} d_{n,k})$$
$$= c_{i,1}^{(x)}(u_1 d_{1,1} + u_2 d_{1,2} + \dots + u_k d_{1,k}) + \dots + c_{i,n}^{(x)}(u_1 d_{n,1} + u_2 d_{n,2} + \dots + u_k d_{n,k}) = 0.$$

Since the solutions of (7) are linearly independent over the field $\mathbb{F}$, we obtain

$$u_1 d_{1,1} + u_2 d_{1,2} + \dots + u_k d_{1,k} = 0,$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$u_1 d_{n,1} + u_2 d_{n,2} + \dots + u_k d_{n,k} = 0,$$

and this is impossible.

ACKNOWLEDGMENTS

This work was supported by the Russian Foundation for Fundamental Research (project no. 96-01-00767).

REFERENCES

1. Vinogradov, I. M., *Osnovy teorii chisel* (Foundations of Number Theory), 9th ed., Moscow: Nauka, 1981.
2. Korobov, N. M., Distribution of Nonresidues and Primitive Roots in Recurrent Series, *Dokl. Akad. Nauk SSSR*, 1953, vol. 88, no. 4, pp. 603–606.
3. Lidl, R. and Niderreider, H., *Finite Fields, Encycl. Math. Appl.*, 1983, vol. 20, Massachusets: Eddison Wesley.
4. Nechaev, V. I., Group of Nonsingular Matrices over a Finite Field and Recurrent Sequences, *Dokl. Akad. Nauk SSSR*, 1963, vol. 152, no. 2, pp. 275–277.
5. Nechaev, V. I., An Unimprovable Estimate of Trigonometric Sums for Recurrent Functions with Nonconstant Coefficients, *Dokl. Akad. Nauk SSSR*, 1964, vol. 154, no. 3, pp. 520–522.
6. Nechaev, V. I., Trigonometric Sums for Recurrent Sequences, *Dokl. Akad. Nauk SSSR*, 1972, vol. 206, no. 4, pp. 811–814.
7. Nechaev, V. I., Trigonometric Sums for Elements of a Finite Field, *Mat. Zametki*, 1972, vol. 11, no. 5, pp. 597–607.
8. Laksov, D., Linear Recurring Sequences over Finite Fields, *Math. Scand.*, 1965, vol. 16, pp. 181–196.
9. Lidl, R. and Niderreiter, H., *Introduction to Finite Fields and Their Applications*, Cambridge (London), 1985.
10. Zierler, N., Linear Recurring Sequences, *J. Soc. Indust. Appl. Math.*, 1959, vol. 7, pp. 31–48.

Translated by I. Aleksandrova