

ӨОЖ 512.624
FTAXP 27.17.27

<https://doi.org/10.55452/1998-6688-2024-21-2-170-180>

^{1*}Турусбекова У.К.,

PhD, ORCID ID 0000-0002-0591-2143, e-mail: umut.t@mail.ru

²Алтынбек С.А.,

ORCID ID 0000-0002-8435-7773, e-mail: serik_aa@bk.ru

¹«Esil University» мекемесі, 010000, Астана қ., Қазақстан

²Қазақ технология және бизнес университеті, 010000, Астана қ., Қазақстан

КЕЗ КЕЛГЕН АҚЫРЛЫ ӨРІС АЛМАСТЫРУЛАРЫН ҚҰРУ ӘДІСТЕРІ ЖӘНЕ ОЛАРДЫҢ СЫЗЫҚТЫҚ СИПАТТАМАСЫ

Аңдатпа

Ақырлы өрістегі алмастырулар (биективті түрлендірулер) көптеген қосымшаларға байланысты, соның ішінде, ақпаратты қорғау теориясында белсенді зерттелуде. Алмастырулар көбінесе ақпаратты өңдеу тораптарын құру элементтері ретінде қолданылады. 20-шы ғасырдың ортасында К. Шеннон осындай тораптарда жүзеге асырылатын бейнелеулерге қойылатын басты талаптарды теориялық негіздеді. Қазіргі уақытта биективті түрлендірулерді құруда бұл талаптар GF(2) өрісінде кесте арқылы берілген сызықтық емес бейнелеулердің композициясымен қамтамсыз етіледі. Ұсынылған мақала тұрақты функционалды жүйелердің өлшемін ұлғайту әдістері туралы [1] жұмыс нәтижелерін жалпылайды. Дәлірек айтқанда, жұмыста ақырлы өрісте бастапқы алмастырулардан жаңа алмастырулар құру тәсілдері зерттелген. Құрылған алмастырулар үшін сызықтық сипаттама есептелді. Координаталық функциялармен берілген алмастыруларды құру есебі күрделі. Мақала тақырыбының өзектілігі талап етілетін комбинаторлы-алгебралық қасиеттерге ие үлкен өлшемді кеңістіктерде алмастыру кластарын құрудың жаңа, теориялық негізделген әдістерін іздеу қажеттіліктерімен анықталады. Жұмыста ақырлы өрістер алмастыруларын, кіші өлшемді векторларға әсер ететін, бастапқы алмастырулардан құрудың бірнеше әдістері қарастырылған. Екілік жағдайда, бұл алмастырулардың координаттық функцияларының сызықтық комбинацияларының барлық аффиндік функциялар класына жақындығын сипаттайтын қарастырылып отырған алмастырулардың бейсызықтығын табуға мүмкіндік береді. Ұсынылған мақаланың нәтижелері кез келген ақырлы өріс жағдайында алмастыруларды құру мүмкіндіктерін кеңейтеді.

Тірек сөздер: ақырлы өріс, алмастыру, логикалық функциялар, сызықтық сипаттама, биективті түрлендіру.

Кіріспе

[1] жұмыста бастапқы алмастырулардан ұзындығы артық екілік векторлардың алмастыруларын құру тәсілдері ұсынылған. Ұсынылған жұмыста осындай алмастыруларды q элементтен тұратын кез келген өрісте құру мәселесі зерттеледі. Құрылған бейнелеулер үшін олардың сызықтық сипаттамасы табылды. Екілік жағдайда қарастырылған алмастырулардың сызықтық еместігі көрсетіледі.

Айталық, $P = GF(q)$ – q элементтен тұратын ақырлы өріс болсын. Егер барлық $c \in P$ үшін $|f^{-1}(c)|$ түпбейне қуаты q^{n-1} -ге тең болса, $f: P^n \rightarrow P$ функциясын теңдестірілген деп атаймыз. Егер әрбір $(x_1, \dots, x_n) \in P^n$ үшін $\varphi(x_1, \dots, x_n) = [\varphi_1(x_1, \dots, x_n), \dots, \varphi_n(x_1, \dots, x_n)]$ болса, онда кез келген $\varphi: P^n \rightarrow P^n$ бейнелеуі үшін $\varphi_i: P^n \rightarrow P$ бейнелеулері, $i \in \overline{1, n}$, φ бейнелеуінің координаттық функциялары деп аталады. Бұл жағдайда $\varphi = (\varphi_1, \dots, \varphi_n)$ белгілеуін қолданамыз.

Негізгі ережелер

[2] жұмыста φ бейнелеуінің биективтілігінің оның координаттық функциялары терминінде келесі критерийі алынған.

Теорема 1. Айталық, $P = GF(q)$, онда $\varphi = (\varphi_1, \dots, \varphi_n): P^n \rightarrow P^n$ бейнелеуі биективті болуы үшін кез келген $(c_1, \dots, c_n) \in P^n \setminus \{0\}$ үшін $\sum_{i=1}^n c_i \varphi_i$ функциясы теңдестірілген болуы қажетті және жеткілікті.

Алдағы уақытта келесі тұжырым қажет болады.

Лемма 1. Айталық, $P = GF(q)$, $1 \leq m < n$ және $\varphi(x_1, \dots, x_n)$ функциясы мына түрде берілсін:

$$\varphi(x_1, \dots, x_n) = \varphi_1(x_1, \dots, x_m) + \varphi_2(x_{m+1}, \dots, x_n).$$

Егер $\varphi_1(x_1, \dots, x_m)$ немесе $\varphi_2(x_{m+1}, \dots, x_n)$ функцияларының ең болмағанда біреуі теңдестірілген болса, онда $\varphi(x_1, \dots, x_n)$ функциясы теңдестірілген болады.

Дәлелдеу. Айталық, $\varphi(x_1, \dots, x_n)$ функциясы теңдестірілген делік. Онда кез келген $c \in P$ элементі үшін оның толық түпбейнесінің қуаты

$$|\varphi^{-1}(c)| = \sum_{\substack{a, b \in P \\ a+b=c}} |\varphi_1^{-1}(a)| |\varphi_2^{-1}(b)| = \sum_{b \in P} |\varphi_1^{-1}(c-b)| |\varphi_2^{-1}(b)|$$

формуласымен табылады. $\varphi(x_1, \dots, x_m)$ функциясы теңдестірілген болғандықтан, алатынымыз:

$$|\varphi^{-1}(c)| = q^{m-1} \sum_{b \in P} |\varphi_2^{-1}(b)| = q^{m-1} q^{n-m} = q^{n-1}.$$

Айталық, $P = GF(q)$ – кез келген өріс, p – оның сипаттамасы, $\varphi = (\varphi_1, \dots, \varphi_n)$ – кез келген бейнелеу, χ_a , $a \in P \setminus \{0\}$ – P өрісінің аддитивті сипаттамасы болсын, ол келесі теңдікпен анықталады:

$$\chi_a(x) = e^{2\pi i (\text{tr}_p^q(ax)/p)}$$

мұндағы tr_p^q – P өрісінен жай ішкі өріске «із». Әрбір $a = (a_1, \dots, a_n)$, $c = (c_1, \dots, c_n) \in P^n$ векторлары үшін

$$C_a^\varphi(a, c) = \sum_{x \in P^n} \chi_a \left(\sum_{j=1}^n a_j x_j - \sum_{j=1}^n c_j \varphi_j(x) \right)$$

шамасын қарастырайық.

[3] жұмыста көрсетілгендей, φ бейнелеуінің сызықтық сипаттамасы деп келесі шаманы атаймыз:

$$\delta(\varphi) = \max_{a \neq 0} \max_{a \in P^n} \max_{c \in P^n \setminus \{0\}} |C_b^\varphi(a, c)|.$$

Әдебиетке шолу

[1] жұмыс бастапқы алмастырулардан ұзындығы артық екілік векторлардың алмастыруларын құру тәсілдеріне арналған. Жұмыста бейнелеудің биективтілігін оның координаттық функциялары арқылы өрнектеу ұсынылған [2]. [3] мақалада бейнелеудің сызықтық сипат-

[illegible][illegible]
$$(a + nb)\varphi_1(x_1) + \cdots + (a + nb)\varphi_n(x_1) + \\ (b + na)\varphi_1(x_2) + \cdots + (b + na)\varphi_n(x_2).$$
$$\begin{cases} a + nb = 0 \\ b + na = 0; \end{cases}$$

173

$$(e - n^2 e)\varphi_1(x_1) + \cdots + (e - n^2 e)\varphi_n(x_1) + \\ + (-ne + ne)\varphi_1(x_2) + \cdots + (-ne + ne)\varphi_n(x_2).$$

P^{n+t} жиынын биективті түрлендіруді P^n жиынын биективті түрлендіру арқылы құру әдісін ұсынайық. Ол үшін $x_1 = (x_1, \dots, x_{n+t}) \in P^{n+t}$, $x_1 = (x_1, \dots, x_n) \in P^n$ белгілеулерін енгізейік.

$$\left\{ \begin{array}{l} \Phi_1(x) = \varphi_1(x_1); \\ \dots\dots\dots \\ \Phi_n(x) = \varphi_n(x_1); \\ \Phi_{n+1}(x) = \varphi_{i_1}(x_1) + \tau_1(x_{n+1}); \\ \dots\dots\dots \\ \Phi_{n+t}(x) = \varphi_{i_t}(x_1) + \tau_t(x_{n+t}) \end{array} \right. \quad (3)$$

Дәлелдеу. φ бейнелеуі биективті болмаса, Φ бейнелеуі де биективті болмайтынын көру қиын емес. Айталық, φ – биективті делік. Коэффициенттері P өрісінен алынған координаттық функциялардың келесі сызықтық комбинациясын қарастырайық:

$$\begin{aligned}
& a_1\Phi_1(x) + \cdots + a_n\Phi_n(x) + b_1\Phi_{n+t}(x) + \cdots + b_t\Phi_{n+t}(x) = \\
& a_1\varphi_1(x) + \cdots + a_n\varphi_n(x) + b_i[\varphi_{i_1}(x_1) + \tau_1(x_{n+t})] + \\
& + \cdots + b_t[\varphi_{i_t}(x_1) + \tau_t(x_{n+t})] = a_1\varphi_1(x_1) + \cdots + \\
& + (a_{i_1} + b_1)\varphi_{i_1}(x_1) + \cdots + (a_{i_t} + b_t)\varphi_{i_t}(x_1) + \cdots + \\
& + a_n\varphi_n(x_1) + b_1\tau_1(x_{n+t}) + \cdots + b_t\tau_t(x_{n+t})
\end{aligned} \tag{4}$$

174

$$\left\{ \begin{array}{l} a_1 = 0; \\ \dots \dots \dots \\ a_{i_1} + b_1 = 0; \\ \dots \dots \dots \\ a_{i_t} + b_t = 0; \\ \dots \dots \dots \\ a_n = 0; \\ b_1 = 0; \\ \dots \dots \dots \\ b_t = 0 \end{array} \right.$$

жағдайын қарастыру қалды. Бұл жағдайда $a_1 = \dots = a_n = 0$ және Φ_i , $i = \overline{1, n+t}$ координаттық функциялардың сызықтық комбинациясы тривиалды болады.

Нәтижелер мен талқылау

(1) ереже бойынша құрылған ψ түрлендіруінің сызықтық сипаттамасының φ бейнелеуінің сызықтық сипаттамасымен байланысын табайық.

Теорема 4. Айталық, $n \in N$, $n^2 \not\equiv 1 \pmod{p}$, $\varphi = (\varphi_1, \dots, \varphi_n): P^n \rightarrow P^n$ – кез келген бейнелеу және $\psi = (\psi_1, \dots, \psi_{2n}): P^{2n} \rightarrow P^{2n}$ – (1) ереже бойынша құрылған бейнелеу болсын. Онда

$$\delta(\psi) = \delta(\varphi)q^n. \quad (5)$$

Дәлелдеу.
$$C_\delta^\psi(a, c) = \sum_{x \in P^n} \chi_b \left(\sum_{j=1}^{2n} a_j x_j - \sum_{j=1}^{2n} c_j \psi_j(x) \right)$$

өрнегін қарастырайық. Келесі теңдіктер орын алады:

$$C_\delta^\psi(a, c) = \sum_{x \in P^n} \chi_b \left(\sum_{j=1}^{2n} a_j x_j - \sum_{j=1}^{2n} c_j \psi_j(x) \right) = \sum_{x \in P^{2n}} \chi_b \left(\sum_{j=1}^n a_j x_j - \sum_{j=1}^n c_j \psi_j(x) + \sum_{j=n+1}^{2n} a_j x_j - \sum_{j=n+1}^{2n} c_j \psi_j(x) \right).$$

(1) ережеден және аддитивті сипаттама қасиеттерінен алатынымыз

$$\begin{aligned} & \chi_b \left(\sum_{j=1}^n a_j x_j - \sum_{j=1}^n c_j \psi_j(x) + \sum_{j=n+1}^{2n} a_j x_j - \sum_{j=n+1}^{2n} c_j \psi_j(x) \right) = \\ & \chi_b \left(\sum_{j=1}^n a_j x_j - \sum_{j=1}^n c_j \psi_j(x) \right) \chi_b \left(\sum_{j=n+1}^{2n} a_j x_j - \sum_{j=n+1}^{2n} c_j \psi_j(x) \right) = \end{aligned}$$

$$= \chi_b \left(\sum_{j=1}^n a_j x_j - \sum_{j=1}^n c_j \psi_j(x) - \varphi_{n+1}(x_2) \sum_{j=1}^n c_j \right) \times \\ \times \chi_b \left(\sum_{j=n+1}^{2n} a_j x_j - \sum_{j=n+1}^{2n} c_j \varphi_{j-n}(x_2) - \varphi_{n+1}(x_1) \sum_{j=n+1}^{2n} c_j \right).$$

Айталық,

$$\text{онда} \quad r_1 = \sum_{j=n+1}^{2n} c_j, \quad r_2 = \sum_{j=1}^n c_j,$$

$$\chi_b \left(\sum_{j=1}^n a_j x_j - \sum_{j=1}^n c_j \psi_j(x) + \sum_{j=n+1}^{2n} a_j x_j - \sum_{j=n+1}^{2n} c_j \psi_j(x) \right) = \\ = \chi_b \left(\sum_{j=1}^n a_j x_j - \sum_{j=1}^n d_j \varphi_j(x_1) \right) \chi_b \left(\sum_{j=n+1}^{2n} a_j x_j - \sum_{j=n+1}^{2n} d_j \varphi_{j-n}(x_2) \right),$$

мұндағы кез келген $j \in \overline{1, n}$ үшін $d_j = c_j + r_1$ және $j \in \overline{n+1, 2n}$ үшін $d_j = c_j + r_2$.

Осылайша, алатынымыз

$$C_b^\psi(a, c) = C_b^\varphi(a_1, d_1) C_b^\varphi(a_2, d_2),$$

мұндағы $a = (a_1, a_2)$; $d = (d_1, d_2)$. Егер c барлық нөл емес векторлардың мәндерін жүгіріп өтсе, онда d_1 және d_2 мәндері де $\mathbb{R}^n$ өрісіндегі барлық нөл емес векторлар арқылы өтетінін ескерейік. Бұл жағдайда $d_1 \neq 0$ немесе $d_2 \neq 0$. Шынымен, егер $d_1 = d_2 = 0$ болса, онда $c = (-r_1, \dots, -r_1, -r_2, \dots, -r_2)$, $r_1 = -nr_2$, $r_2 = -nr_1$, демек, $r_2 \neq 0$, $r_2 = n^2 r_2$, бұлай болуы мүмкін емес. Сонымен қатар $c = (e, \dots, e, -ne, \dots, -ne)$, және $a_2 = 0$

$$C_b^\varphi(a, c) = C_b^\varphi(a_1, d_1) C_b^\varphi(0, 0) = C_b^\varphi(a_1, d_1) q^n.$$

Бұдан $\delta(\psi) = \delta(\varphi) q^n$ аламыз.

Салдар 1. Айталық, 4-теорема шартында $q = 2$ болсын, онда (1) ереже бойынша құрылған ψ бейнелеуінің сызықтық еместігі

$$NL(\psi) = 2^n NL(\varphi)$$

шартын қанағаттандырады.

Дәлелдеу. Келесі теңдіктерді [4] және 3-теореманы қолдану жеткілікті.

$$NL(\psi) = 2^{2n-1} - \frac{1}{2} \delta(\psi); \\ NL(\varphi) = 2^{2n-1} - \frac{1}{2} \delta(\varphi)$$

$NL(\psi)$ шамасы ψ бейнелеуінің координаттық функцияларының барлық тривиальды емес сызықтық комбинациялары мәндерінің бағандарынан $2n$ айнымалылы барлық аффиндік логикалық функциялары мәндерінің бағандарына дейінгі ең қысқа Хэмминг қашықтығына тең екенін айта кетейік.

1-кестеде $GF(2^{2n})$ өрісінде (1) ереже бойынша құрылған алмастырулардың сызықтық еместігінің максималды мүмкін мәндері көрсетілген, $n \in \{4, 6\}$.

Кесте 1 – $GF(2^{2n})$ өрісінде (1) ереже бойынша құрылған алмастырулардың максималды сызықтық еместігі

n	$NL(\varphi)$	$NL(\psi)$
4	4	64
6	24	1536

(3) ереже бойынша құрылған Φ түрлендіруінің сызықтық сипаттамасын қарастырайық.

Теорема 5. Айталық, $\varphi = (\varphi_1, \dots, \varphi_n): P^n \rightarrow P^n$ – кез келген бейнелеу, $\varphi = (x_1, \dots, x_n): P^n \rightarrow P, i \in \overline{1, n}, 1 \leq i_1 < \dots < i_t \leq n, \tau_j - P$ жиынында алмастыру, $j \in \overline{1, t}$ және $\Phi = (\Phi_1, \dots, \Phi_{n+t}): P^{n+t} \rightarrow P^{n+t}$ бейнелеуі (3) ереже бойынша құрылған болсын. Онда Φ бейнелеуінің сызықтық сипаттамасы үшін

$$\delta(\Phi) = \max\{\delta(\varphi)q^t, q^{n+t-1}m\}$$

қатынасы орындалады, мұндағы

$$m = \max_{s \in \overline{1, t}} \delta(\tau_s).$$

$$\begin{aligned} C_b^\Phi(a, c) &= \sum_{x \in P^{n+t}} \chi_b \left(\sum_{j=1}^n a_j x_j - \sum_{j=1}^n c_j \Phi_j(x) + \sum_{j=n+1}^{n+1} a_j x_j - \sum_{j=n+1}^{n+1} c_j \Phi_j(x) \right) = \\ &= \sum_{x \in P^{n+t}} \chi_b \left(\sum_{j=1}^n a_j x_j - \sum_{j=1}^n c_j \varphi_j(x_1) + \right. \\ &\quad \left. \sum_{j=n+1}^{n+1} c_j \varphi_{j-n}(x_1) \right) \sum_{(x_{n+1}, \dots, x_{n+t}) \in P^t} \chi_b \left(\sum_{j=n+1}^{n+1} c_j \tau_{j-n}(x_j) \right) \\ &= \sum_{j=1}^n c_j \varphi_j(x_1) + \sum_{j=n+1}^{n+1} c_j \varphi_{j-n}(x_1) \end{aligned}$$

қосындысын қарастырайық. Ол үшін мынадай теңдіктер орындалады:

$$\begin{aligned} S &= c_1 \varphi_1(x_1) + \dots + c_{i_1} \varphi_{i_1}(x_1) + \dots + c_n \varphi_n(x_1) + \\ &\quad + c_{n+1} \varphi_{i_1}(x_1) + \dots + c_{n+t} \varphi_{i_t}(x_1) = \end{aligned}$$

$$\begin{aligned} &= d_1 \varphi_1(x_1) + \dots + d_{i_1} \varphi_{i_1}(x_1) + \dots + d_{i_t} \varphi_{i_t}(x_1) + d_n \varphi_n(x_1), \\ \text{мұндағы } (d_1, \dots, d_{i_1}, \dots, d_{i_t}, \dots, d_n) &= (c_1, \dots, c_{i_1} + c_{n+1}, \dots, c_{i_t} + c_{n+t}, \dots, c_n). \end{aligned}$$

Онда

$$C_b^\Phi(a, c) = \sum_{x_1 \in P^n} \chi_b \left(\sum_{j=1}^n a_j x_j - \sum_{j=1}^n c_j \varphi_j(x_1) \right) \prod_{j=1}^t \sum_{x_{n+j} \in P} \chi_b (a_{n+j} x_{n+j} - c_{n+j} \tau(x_{n+j})) =$$

$$C_b^\Phi(a_1, d) \prod_{j=1}^t C_b^{\tau_j}(a_{n+j}, c_{n+j}).$$

$c \in P^{n+t} \setminus \{0\}$ элементін еркін таңдаймыз. Егер $d \neq 0$ болса, онда

$$\max_{a \in P^{n+t}} \max_{c: d \neq 0} |C_b^\Phi(a, c)| \leq \delta(\varphi) q^t.$$

Егер $d \neq 0$ болса, онда $c = (0, \dots, -b, \dots, 0, \dots, b, \dots, 0)$ векторларын қарастыра отырып, мұндағы $b \neq 0$, $(-b)$ i_s -ші орында, ал b $n+s$ -ші орында тұрады, $s=1, \dots, t$, алатынымыз

$$\max_{a \in P^{n+t}} \max_{c: d \neq 0} |C_b^\Phi(a, c)| \leq \delta(\tau_s) q^{n+t-1}.$$

Бұдан

$$\delta(\Phi) = \max\{\delta(\varphi) q^t, q^{n+t-1} m\}.$$

Салдар 2. Айталық, 5-теорема шартында $q = 2$ болсын, онда $NL(\Phi) = 0$.

Дәлелдеу. $s=1, \dots, t$ үшін $\delta(\tau_s) = 2$ екенін ескеру жеткілікті.

Қорытынды

Жұмыста баяндалған нәтижелер кіші өлшемді векторларға әсер ететін бастапқы биективті түрлендірулер негізінде құрылған биективті түрлендірулердің екі класын сипаттауға мүмкіндік береді. Құрылған алмастырулардың сызықтық сипаттамаларын есептеу формулалары алынды. Екілік жағдайда бұл қарастырылып отырған бейнелеулердің сызықтық еместігін анықтауға мүмкіндік берді.

Қаржыландыру туралы ақпарат

Зерттеу жұмысы Қазақстан Республикасы Ғылым және жоғары білім министрлігінің қолдауымен АР19677733 «Ғылыми мәтіндерді параллельді талдаудың зияткерлік үлестірілген жүйесін әзірлеу» жобасы шеңберінде орындалды. Авторлар зерттеу жұмысына көрсетілген қолдау үшін алғыстарын білдіреді.

ӘДЕБИЕТТЕР

- 1 Никонов В.Г., Саранцев А.В. Методы компактной реализации биективных отображений, заданных регулярными системами однотипных булевых функций // Вестник Российского университета дружбы народов. Серия: Прикладная и компьютерная математика. – 2003. – Т. 2. – № 1. – С. 94–105.
- 2 Лидл Р., Нидеррайтер Г. Конечные поля. – М.: Мир, 1988. – 822 с.
- 3 Бугров А.Д. Кусочно-аффинные подстановки конечных полей // Прикладная дискретная математика. – 2015. – № 4 (30). – С. 5–23.
- 4 Логачев О.А., Сальников А.А., Яценко В.В. Булевы функции в теории кодирования и криптологии. – М.: Изд-во МЦНМО, 2012. – 584 с.
- 5 Abornev A.V. Recursively-generated permutations of a binary space // Математические основы криптографии. – 2014. – Т. 5. – № 2. – С. 7–20.
- 6 Рожков М.И. Биективные отображения, порождаемые фильтрующим генератором // Прикладная дискретная математика. – 2014. – Т. 1. – № 23. – С. 27–39.
- 7 Blondeau C., Nyberg K. Perfect Nonlinear Functions and Cryptography // Finite Fields Appl. – 2015. – Т. 32. – С. 120–147.
- 8 Li C.H. The finite primitive permutation groups containing an abelian regular subgroup // Proc. London Math. Soc., MR MR2005881 (2004i:20003) – 87. – 2003. – С. 725–747.

REFERENCES

- 1 Nikonov V.G. and Sarantsev A.V. (2003). Metody kompaktnoy realizatsii biyektivnykh otobrazheniy, zadannykh regul'yarnymi sistemami odnotipnykh bulevykh funktsiy, Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Prikladnaya i komp'yuternaya matematika, vol. 2, no. 1, pp. 94–105 [in Russian].
- 2 Lidl R. and Niderrayter G. (1988) Konechnyye polya, Moscow, 822 p. [in Russian].
- 3 Bugrov A.D. (2015) Kusochno-affinnyye podstanovki konechnykh poley, Prikladnaya diskretnaya matematika, no. 4 (30), pp. 5–23 [in Russian].
- 4 Logachev O.A., Sal'nikov A.A. and Yashchenko V.V. (2004) Bulevy funktsii v teorii kodirovaniya i kriptologii, Moscow, 584 p. [in Russian].
- 5 Abornev A.V. (2014) Recursively-generated permutations of a binary space, Matematicheskiye osnovy kriptografii, vol. 5, no. 2, pp. 7–20.
- 6 Rozhkov M.I. (2014) Biyektivnyye otobrazheniya, porozhdayemye fil'truyushchim generatorom, Prikladnaya diskretnaya matematika, no. 1(23), pp. 27–39 [in Russian].
- 7 Blondeau C. and Nyberg K. (2015) Perfect Nonlinear Functions and Cryptography, Finite Fields Appl, no. 32, pp. 120–147.
- 8 Li C.H. (2003) The finite primitive permutation groups containing an abelian regular subgroup, Proc. London Math. Soc., MR MR2005881 (2004i:20003) – 87, pp. 725–747.

^{1*}Турусбекова У.К.,

PhD, ORCID ID 0000-0002-0591-2143, e-mail: umut.t@mail.ru

²Алтынбек С.А.,

ORCID ID 0000-0002-8435-7773, e-mail: serik_aa@bk.ru

¹Учреждение «Esil University», 010000, г. Астана, Казахстан

²Казахский университет технологии и бизнеса, 010000, г. Астана, Казахстан,

МЕТОДЫ ПОСТРОЕНИЯ ПОДСТАНОВОК ПРОИЗВОЛЬНОГО КОНЕЧНОГО ПОЛЯ И ИХ ЛИНЕЙНАЯ ХАРАКТЕРИСТИКА

Аннотация

Подстановки в конечном поле (биективные преобразования) активно изучаются во многих приложениях, в том числе и в теории защиты информации. Подстановки часто используются в качестве элементов для построения узлов обработки информации. В середине XX века К. Шеннон теоретически обосновал основные требования к отображениям, осуществляемым на таких узлах. В настоящее время при построении биективных преобразований эти требования обеспечиваются композицией нелинейных представлений, заданных таблицей в поле $GF(2)$. Представленная статья обобщает результаты работы [1] о методах увеличения размерности стационарных функциональных систем. Именно в данной работе исследованы подходы к построению новых подстановок из исходных подстановок в конечном поле. Для построенных подстановок вычислена линейная характеристика. Задача построения подстановок, заданных координатными функциями, является сложной. Актуальность темы статьи определяется необходимостью поиска новых, теоретически обоснованных методов построения классов подстановок в многомерных пространствах, обладающих требуемыми комбинаторно-алгебраическими свойствами. В работе рассмотрено несколько методов построения подстановок конечных полей из исходных подстановок, действующих на векторы меньшей размерности. В бинарном случае это позволяет найти нелинейность рассматриваемых подстановок, характеризующих сродство линейных комбинаций координатных функций подстановок ко всему классу аффинных функций. Результаты представленной работы несколько расширяют возможности построения подстановок для произвольного конечного поля.

Ключевые слова: конечное поле, подстановка, логические функции, линейная характеристика, биективное преобразование.

^{1*}**Turusbekova U.K.,**

PhD, ORCID ID: 0000-0002-0591-2143, e-mail: umut.t@mail.ru

²**Altynbek S.A.,**

ORCID ID: 0000-0002-8435-7773, e-mail: serik_aa@bk.ru

¹Institution «Esil University», 010000, Astana, Kazakhstan²Kazakh University of Technology and Business, 010000, Astana, Kazakhstan**METHODS FOR CONSTRUCTING PERMUTATIONS
OF AN ARBITRARY FINITE FIELD AND THEIR
LINEAR CHARACTERISTICS****Abstract**

Permutations in a finite field (bijective transformations) are actively studied in many applications, including in information security theory. Permutations are often used as elements for building information processing nodes. In the middle of the 20th century, K. Shannon theoretically justified the basic requirements for mapping performed on such nodes. Currently, when constructing bijective transformations, these requirements are provided by the composition of nonlinear representations given by the table in the field $GF(2)$. The presented paper summarizes the results of work [1] on methods for increasing the dimension of stationary functional systems. Namely, in this paper, approaches to the construction of new permutations from the initial permutations in the finite field are investigated. The linear characteristic is calculated for the constructed permutations. The problem of constructing permutations given by coordinate functions is difficult. The relevance of the topic of the paper is determined by the need to search for new theoretically sound methods for constructing s permutation classes in multidimensional spaces with the required combinatorial-algebraic properties. The paper considers several methods for constructing substitutions of finite fields from initial permutations acting on vectors of smaller dimension. In the binary case, this allows us to find the nonlinearity of the substitutions under consideration, characterizing the proximity of linear combinations of coordinate functions of permutations to the entire class of affine functions. The results of the presented work somewhat expand the possibilities of constructing permutations for an arbitrary finite field.

Key words: finite field, permutation, Boolean functions, linear characteristic, bijective transformation.