УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА.
СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

2019, Т. 161, кн. 2
С. 292–300

ISSN 2541-7746 (Print)
ISSN 2500-2198 (Online)

УДК 519.7

doi: 10.26907/2541-7746.2019.2.292-300

О СПОСОБАХ ЗАДАНИЯ ПЕРЕСТАНОВОК НА МНОЖЕСТВАХ НАБОРОВ ИЗ ЭЛЕМЕНТОВ КОНЕЧНОГО ПОЛЯ

В.С. Кугураков, А.Ф. Гайнутдинова, В.Т. Дубровин

Казанский (Приволжский) федеральный университет, г. Казань, 420008, Россия

Аннотация

Рассмотрена следующая задача. Пусть $S = S_1 \times S_2 \times \cdots \times S_m$ – декартово произведение подмножеств S_i, являющихся подгруппами мультипликативной группы конечного поля $\mathbb{F}_q$ из q элементов или их расширениями путём добавления нулевого элемента. Отображение $f : S \to S$ множества S в себя может быть задано системой многочленов $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_m]$. Получены необходимые и достаточные условия, при которых отображение $f = \langle f_1, \ldots, f_m \rangle$ является биективным, то есть взаимно однозначным. Затем эта задача обобщена на случай, когда подмножества S_i являются любыми подмножествами в $\mathbb{F}_q$. Полученные результаты могут быть использованы при построении таблиц замен (S-box) и перестановок (P-box) в блочных шифрах, а также при вычислении групп автоморфизмов кодов с исправлением ошибок.

Ключевые слова: криптография, коды с исправлением ошибок, конечные поля, перестановочные многочлены

Любая перестановка на подмножестве элементов конечного поля $\mathbb{F}_q$ порядка q может быть задана некоторым многочленом $f(x) \in \mathbb{F}_q[x]$. Такие многочлены называют перестановочными. Вопросам получения критериев, которым должны удовлетворять перестановочные многочлены, а также смежным вопросам, посвящена обширная литература, подробно освещённая в [1]. Отметим, что перестановочные многочлены используются в комбинаторике и при изучении конечных проективных плоскостей. На их основе могут быть построены отдельные блоки криптографических систем, в частности таблицы замены (S-box) и таблицы перестановок (P-box) в блочных шифрах. Наконец, перестановочные многочлены используются при описании автоморфизмов, которыми может обладать тот или иной линейный или нелинейный код с исправлением аддитивных ошибок [2–6].

В настоящей работе решается следующая задача. Пусть $\mathbb{F}_q$ – конечное поле из q элементов и пусть $S_1, \ldots, S_m$ – его любые (непустые) подмножества, а

$$S = S_1 \times \ldots \times S_m = \{(a_1, \ldots, a_m) \,|\, a_i \in S_i, i = 1, \ldots, m\} \tag{1}$$

– их декартово произведение. Система $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_m]$ многочленов задаёт отображение $\pi : S \to S$ множества S в себя, если $(f_1(a_1, \ldots, a_m), \ldots, f_m(a_1, \ldots, a_m)) \in S$ для любого набора $(a_1, \ldots, a_m) \in S$. Любое отображение π множества S в себя может быть задано таким образом: в качестве искомых многочленов f_i можно взять, например,

$$f_i = \sum_{(a_1,\ldots,a_m)\in S} b_i^{(a_1,\ldots,a_m)} \chi_{a_1}(x_1) \cdots \chi_{a_m}(x_m)$$

где $(b_1^{(a_1,\dots,a_m)},\dots,b_m^{(a_1,\dots,a_m)})$ – образ набора $(a_1,\dots,a_m)\in S$ при отображении π,

$$\chi_a(x)=1-(x-a)^{q-1}=\begin{cases}0, & \text{если } x\in\mathbb{F}_q\backslash\{a\},\\ 1, & \text{если } x=a\end{cases}$$

– характеристическая функция элемента a.

Пусть S – декартово произведение (1). Степенью множества S назовём набор $\deg S=(n_1-1,\dots,n_m-1)$, где $n_i=|S_i|$ – число элементов множества S_i; степенью многочлена $f(x_1,\dots,x_m)$ назовём набор $\deg f=(k_1,\dots,k_m)$, где k_i – степень многочлена f по переменной x_i, $i=1,\dots,m$. Далее запись $(k_1,\dots,k_m)\preccurlyeq(l_1,\dots,l_m)$ означает, что $k_1\le l_1,\dots,k_m\le l_m$.

Пусть $f_1(x),\dots,f_m(x)\in\mathbb{F}_q[x]$. Обозначим через $I=(f_1(x_1),\dots,f_m(x_m))$ идеал кольца $\mathbb{F}_q[x_1,\dots,x_m]$, порождённый многочленами $f_1,\dots,f_m$ (идеал I образован всевозможными многочленами вида

$$g_1(x_1,\dots,x_m)f_1(x_1)+\dots+g_m(x_1,\dots,x_m)f_m(x_m),\quad g_1,\dots,g_m\in\mathbb{F}_q[x_1,\dots,x_m]).$$

Запись $f\equiv g\pmod I$ (f сравнимо с g по модулю идеала I) означает, что $f-g\in I$. Для множества S вида (1) положим $I_S=(\sigma_1(x_1),\dots,\sigma_m(x_m))$, где $\sigma_i(x)\in\mathbb{F}_q[x]$ – унитарный многочлен, корнями которого являются элементы множества S_i,

$$\sigma_i(x)=\prod_{a\in S_i}(x-a),\quad i=1,\dots,m.$$

Далее будем употреблять векторную запись наборов: $\mathbf{a}=(a_1,\dots,a_m)$ и вместо $f(a_1,\dots,a_m)$ использовать запись $f(\mathbf{a})$.

Лемма 1. *Пусть S – декартово произведение (1) и $I=I_S$. Тогда*

a) Для любого многочлена $f\in\mathbb{F}_q[x_1,\dots,x_m]$ найдётся единственный многочлен $g\in\mathbb{F}_q[x_1,\dots,x_m]$ степени $\deg g\preccurlyeq\deg S$ такой, что $f(\mathbf{a})=g(\mathbf{a})$ для любого набора $\mathbf{a}\in S$. В частности, если $f(\mathbf{a})=0$ для любого набора $\mathbf{a}\in S$, то g – нулевой многочлен.

b) Если f, $g\in\mathbb{F}_q[x_1,\dots,x_m]$, то равенство $f(\mathbf{a})=g(\mathbf{a})$ выполняется для любого $\mathbf{a}\in S$ тогда и только тогда, когда $f\equiv g\pmod I$.

Доказательство. Доказательство леммы 1 приведено, например, в [1, лемма 7.40] для случая $S_1=\dots=S_m=\mathbb{F}_q$, где $I=(x_1^q-x_1,\dots,x_m^q-x_m)$. Оно переносится без принципиальных изменений на более общий случай, когда $S_1,\dots,S_m$ – подмножества в $\mathbb{F}_q$. □

Многочлен g, определённый в п. a) леммы 1, называется результатом приведения многочлена f по модулю идеала I и обозначается через $f \bmod I$. Приведение f к виду $f \bmod I$ может быть выполнено следующим образом: каждый член $x_i^{u_i}$ в мономах многочлена f заменяется на остаток от деления $x_i^{u_i}$ на $\sigma_i(x_i)$, после чего раскрываются скобки и приводятся подобные члены. Из п. b) леммы 1 следует, что если системы многочленов $f_1,\dots,f_m$ и $h_1,\dots,h_m\in\mathbb{F}_q[x_1,\dots,x_m]$ задают соответственно отображения π и ρ множества S в себя, то $\pi=\rho$ тогда и только тогда, когда $f_1\equiv h_1,\dots,f_m\equiv h_m\pmod I$.

Лемма 2. *Система многочленов $f_1,\dots,f_m\in\mathbb{F}_q[x_1,\dots,x_m]$ задаёт отображение множества S в себя тогда и только тогда, когда*

$$\sigma_1(f_1)\equiv 0,\dots,\sigma_m(f_m)\equiv 0\pmod I. \tag{2}$$

Доказательство. Если имеет место (2), то $\sigma_i(f_i(\mathbf{a})) = 0$, и, следовательно, $f_i(\mathbf{a}) \in S_i$ для любого набора $\mathbf{a} \in S$, $i = 1, \ldots, m$, а значит, система многочленов $f_1, \ldots, f_m$ задаёт отображение множества S в себя. Обратно, если $f_i(\mathbf{a}) \in S_i$, то есть $\sigma_i(f_i(\mathbf{a})) = 0$ для любого набора $\mathbf{a} \in S$, то $\sigma_i(f_i) \pmod I$ – нулевой многочлен, $i = 1, \ldots, m$, поэтому имеет место (2). □

Далее рассматриваются перестановки (взаимно однозначные отображения) на множестве $S^{(m,\,k)}$. Множество $S^{(m,\,k)}$, определяемое ниже, является частным случаем множества (1). Пусть $n \mid q-1$. Обозначим через E_n множество корней n-ой степени из единицы поля $\mathbb{F}_q$ и положим $E_n^0 = E_n \cup \{0\}$, где E_n – подгруппа мультипликативной группы $\mathbb{F}_q^*$ поля $\mathbb{F}_q$. Если $n = p^s - 1$, $q = p^r$ и $s \mid r$, где p – характеристика поля $\mathbb{F}_q$, то E_n^0 – подполе поля $\mathbb{F}_q$.) Пусть $m \geq 1$, $m \geq k \geq 0$; $n_1, \ldots, n_m \in \mathbb{N}$ – любые (не обязательно различные) делители числа $q-1$. Положим

$$S^{(m,\,k)} = E_{n_1} \times \ldots \times E_{n_k} \times E^0_{n_{k+1}} \times \ldots E^0_{n_m}, \tag{3}$$

подразумевая при этом, что $S^{(0,\,m)} = E^0_{n_1} \times \ldots \times E^0_{n_m}$ и $S^{(m,\,0)} = E_{n_1} \times \ldots \times E_{n_m}$ для крайних случаев, когда $k = 0$ и $k = m$.

Лемма 3. *Пусть B^s – множество всех двоичных наборов длины s; $a_1, \ldots, a_s$ – любые числа. Тогда выполняется*

$$A_s \stackrel{\text{def}}{=} \sum_{(d_1,\ldots,d_s)\in B^s} (-1)^{d_1+\cdots+d_s} \prod_{i=1}^{s} (a_i + 1 - d_i) = 1.$$

Доказательство. По индукции имеем $A_s = 1$; $A_{s+1} = A_s(a_{s+1}+1) - A_s a_{s+1}$, $s = 1, 2, \ldots$, откуда следует доказательство леммы. □

Лемма 4. *Пусть $S = S^{(m,\,k)}$, $g \in \mathbb{F}_q[x_1, \ldots, x_m]$ – любой многочлен степени $\deg g \preccurlyeq \deg S$. Тогда*

$$\sum_{\mathbf{a}\in S} g(\mathbf{a}) = \left(\prod_{i=1}^{k} n_i\right) \sum_{(u_1,\ldots,u_m)\in U} g_{u_1,\ldots,u_m} \prod_{i=k+1}^{m} (n_i + 1 - \frac{u_i}{n_i}), \tag{4}$$

где $g_{u_1,\ldots,u_m}$ – коэффициент многочлена g при $x_1^{u_1} \ldots x_m^{u_m}$, $U = U^{(m,\,k)}$ – множество всех целочисленных наборов $(u_1, \ldots, u_m)$ таких, что $u_i = 0$ для $i = 1, \ldots, k$ и $u_i = 0$ или $u_i = n_i$ для $i = k+1, \ldots, m$. (Здесь и ниже, по определению, $\prod_{i=1}^{0} = \prod_{i=m+1}^{m} = 1$ и $U^{(m,\,m)}$ – множества из одного нулевого набора.)

Доказательство. Ограничимся случаем $m > k > 0$ (случаи $k = 0$ и $k = m$ принципиальных изменений не требуют). Так как

$$g = \sum_{(u_1,\ldots,u_m)\in U'} g_{u_1,\ldots,u_m} x_1^{u_1} \ldots x_m^{u_m},$$

где U' – множество всех целочисленных наборов $(u_1, \ldots, u_m)$ таких, что $0 \leq u_i \leq \leq n_i - 1$ для $i = 1, \ldots, k$ и $0 \leq u_i \leq n_i$ для $i = k+1, \ldots, m$, то искомая сумма равна

$$\sum_{(u_1,\ldots,u_m)\in U'} g_{u_1,\ldots,u_m} \left(\prod_{i=1}^{k} \sum_{a_i\in E_{n_i}} a_i^{u_i}\right) \left(\prod_{i=k+1}^{m} \sum_{a_i\in E^0_{n_i}} a_i^{u_i}\right). \tag{5}$$

Используя формулы

$$\sum_{a\in E_n} a^u = \begin{cases} 0, & \text{если } u = 1,2,\dots,n-1, \\ n, & \text{если } u = 0 \text{ и } u = n, \end{cases}$$

$$\sum_{a\in E_n^0} a^u = \begin{cases} 0, & \text{если } u = 1,2,\dots,n-1, \\ n+1-u/n, & \text{если } u = 0 \text{ и } u = n, \end{cases}$$

получаем, что для произвольного набора $(u_1,\dots,u_m)\in U$ произведение внутренних сумм в (5) равно

$$n_1\dots n_k \prod_{i=k+1}^{m}\left(n_i+1-\frac{u_i}{n_i}\right),$$

а для любого набора $(u_1,\dots,u_m)\notin U$ оно равно 0, то есть имеет место (4). □

Лемма 5. *Пусть* $a,\ x\in E_n$; $b,\ y\in E_n^0$. *Тогда*

$$\chi'_n(a,\ x) \stackrel{\text{def}}{=} \frac{1}{n}\sum_{i=0}^{n-1}\left(\frac{x}{a}\right)^i = \begin{cases} 1, & \textit{если } x = a, \\ 0, & \textit{если } x \neq a; \end{cases}$$

$$\chi''_n(b,\ y) \stackrel{\text{def}}{=} \left(\frac{n+1}{n}b^n - 1\right)y^n + \frac{b^n}{n}\sum_{i=1}^{n-1} b^{n-i}y^i + (1-b^n) = \begin{cases} 1, & \textit{если } y = b, \\ 0, & \textit{если } y \neq b. \end{cases}$$

Доказательство. Доказательство вполне элементарно и осуществляется разбором случаев. □

Теорема 1. [1, теорема 7.41] *Пусть* p *– характеристика поля* $\mathbb{F}_q$. *Система многочленов* $f_1,\ \dots,\ f_m\in\mathbb{F}_q[x_1,\ \dots,\ x_m]$ *задаёт перестановку на множестве* $S=\mathbb{F}_q^m$ *тогда и только тогда, когда выполнены следующие два условия:*

a) $g^{(q-1,\dots,q-1)}\neq 0$;

b) $g^{(t_1,\dots,t_m)}=0$ *для любого набора* $(t_1,\dots,t_m)\in T$,

где $g^{(t_1,\dots,t_m)}$ *– коэффициент при* $x_1^{q-1}\dots x_m^{q-1}$ *в многочлене* $f_1^{t_1}\dots f_m^{t_m} \bmod (x_1^q - x_1,\dots,x_m^q-x_m)$, *а* T *– множество всех целочисленных наборов* $(t_1,\dots,t_m)\neq (0,\dots,0)$ *таких, что* $0\le t_i\le q-1$ *для* $1\le t_i\le m$ *и хотя бы одно* t_i *не сравнимо с* 0 *по модулю* p.

Следующее утверждение обобщает теорему 1 на случай произвольного множества S вида (3).

Теорема 2. *Система многочленов* $f_1,\dots,f_m\in\mathbb{F}_q[x_1,\dots,x_m]$ *задаёт перестановку на множестве* $S=S^{(m,\ k)}$ *тогда и только тогда, когда выполнены следующие два условия:*

a)

$$(f_i^{n_i}-1) \bmod I = 0 \quad \textit{для} \quad i=1,\dots,k;$$

$$(f_i^{n_i+1}-f_i) \bmod I = 0 \quad \textit{для} \quad i=k+1,\dots,m,$$

где $I=(x_1^{n_1}-1,\dots,x_k^{n_k}-1,\ x_{k+1}^{n_{k+1}+1}-x_{k+1},\dots,x_{m+1}^{n_{m+1}+1}-x_{m+1})$;

b) $B_{t_1,\dots,t_m} = \begin{cases} 0, & \textit{если} \quad (t_1,\dots,t_m)\in T\backslash U, \\ \displaystyle\prod_{i=k+1}^{m}\left(n_i+1-\frac{u_i}{n_i}\right), & \textit{если} \quad (t_1,\dots,t_m)\in U^*, \end{cases}$

где

$$B_{t_1,\dots,t_m} \stackrel{\text{def}}{=} \sum_{(u_1,\dots,u_m)\in U} g_{u_1,\dots,u_m}^{(t_1,\dots,t_m)} \prod_{i=k+1}^{m} \left(n_i + 1 - \frac{u_i}{n_i}\right);$$

$g_{u_1,\dots,u_m}^{(t_1,\dots,t_m)}$ – *коэффициент при* $x_1^{u_1}\dots x_m^{u_m}$ *в многочлене* $f_1^{t_1}\dots f_m^{t_m} \bmod I$*;* $T = T^{(m,\,k)}$ – *множество целочисленных наборов* $(t_1,\dots,t_m)$ *таких, что* $0 \le t_i \le n_i - 1$ *для* $1 \le i \le k$ *и* $0 \le t_i \le n_i$ *для* $k+1 \le i \le m$*;* $U = U^{(m,\,k)}$ – *множество, определённое в лемме* 4*,* $U^* = U\backslash\{(0,\dots,0)\}$.

Доказательство. *Необходимость условий* a*) и* b). Пусть система многочленов $f_1,\dots,f_m$ индуцирует перестановку на множестве S. Необходимость условия a) очевидна ввиду леммы 5. Пусть $(t_1,\dots,t_m) \in T$ – любой набор и пусть

$$g = f_1^{t_1}\dots f_m^{t_m} \bmod I = \sum_{(u_1,\dots,u_m)\in T} g_{u_1,\dots,u_m}^{(t_1,\dots,t_m)} x_1^{u_1}\dots x_m^{u_m}.$$

Если набор $\mathbf{a}$ пробегает S, то и набор $(f_1(\mathbf{a}),\dots,f_m(\mathbf{a}))$ также пробегает S. Поэтому

$$\sum_{\mathbf{a}\in S} g(\mathbf{a}) = \sum_{\mathbf{a}\in S} f_1^{t_1}(\mathbf{a})\cdots f_m^{t_m}(\mathbf{a}) = \sum_{(a_1,\dots,a_m)\in S} a_1^{t_1}\cdots a_m^{t_m} =$$

$$= \sum_{a_1\in E_{n_1}} a_1^{t_1}\cdots \sum_{a_k\in E_{n_k}} a_k^{t_k} \times \sum_{a_{k+1}\in E^0_{n_{k+1}}} a_{k+1}^{t_{k+1}}\cdots \sum_{a_m\in E^0_{n_m}} a_m^{t_m} =$$

$$= \begin{cases} 0, & \text{если } (t_1,\dots,t_m) \in T\backslash U, \\ n_1\dots n_k \prod_{i=k+1}^{m}\left(n_i + 1 - \dfrac{u_i}{n_i}\right), & \text{если } (t_1,\cdots,t_m) \in U^*. \end{cases}$$

С другой стороны, согласно лемме 4,

$$\sum_{\mathbf{a}\in S} g(\mathbf{a}) = n_1\cdots n_k B_{t_1,\dots,t_m}.$$

Сравнивая полученные выражения, приходим к необходимости условия b).

Достаточность условий a*) и* b). Обозначим через $N(\mathbf{b})$, где $\mathbf{b} = (b_1,\dots,b_m) \in S$; число решений системы уравнений $f_1(\mathbf{a}) = b_1,\dots,f_m(\mathbf{a}) = b_m$ относительно $\mathbf{a} = (a_1,\dots,a_m) \in S$. Многочлены $f_1,\dots,f_m$ задают перестановку на множестве S, если $N = N(\mathbf{b}) > 0$ для любого $\mathbf{b}\in S$. Покажем, что $N > 0$. Для этого достаточно показать, что $N \ne 0$, рассматривая N как элемент поля $\mathbb{F}_q$.

Ввиду леммы 2, условие a) гарантирует, что многочлены $f_1,\dots,f_m$ задают отображение множества S в себя, то есть $f_i(\mathbf{a}) \in E_{n_i}$, $1 \le i \le k$, и $f_i(\mathbf{a}) \in E^0_{n_i}$, $k+1 \le i \le m$ любого набора $\mathbf{a}\in S$. Используя введённые в лемме 5 функции χ'_n и χ''_n, получаем (где для краткости пишем f_i вместо $f_i(\mathbf{a})$):

$$N = \sum_{\mathbf{a}\in S}\prod_{i=1}^{k} \chi'_{n_i}(b_i, f_i) \prod_{i=k+1}^{m} \chi''_{n_i}(b_i,\ f_i) =$$

$$= \frac{1}{A_k}\sum_{\mathbf{a}\in S}\left(\prod_{i=1}^{k}\sum_{j=0}^{n_i-1}\left(\frac{f_i}{b_i}\right)^j\right)\prod_{i=k+1}^{m}\Big(\Big(\frac{n_i+1}{n_i}b_i^{n_i} - 1\Big)f_i^{n_i} +$$

$$+ b_i^{n_i}\sum_{j=1}^{n_i-1} b_i^{n_i-j} f_i^j\,(1 - b_i^{n_i})\Big) = \frac{1}{A_k}\left(\sum\nolimits_1 + \sum\nolimits_2\right),$$

где

$$\sum\nolimits_1 = \sum_{\mathbf{a}\in S} f_1^0 \cdots f_k^0 \prod_{i=k+1}^{m} \left(\left(\frac{n_i+1}{n_i} b_i^{n_i} - 1 \right) f_i^{n_i} + (1 - b_i^{n_i}) \right),$$

$$\sum\nolimits_2 = \sum_{\mathbf{a}\in S} \sum_{(t_1,\ldots,t_m)\in T\setminus U} d_{t_1,\ldots,t_m} f_1^{t_1} \cdots f_m^{t_m} \quad \text{при некоторых} \quad d_{t_1\ldots t_m} \in \mathbb{F}_q.$$

Вторая сумма в силу леммы 4 и условия b) равна нулю. Действительно,

$$\sum\nolimits_2 = \sum_{(t_1,\ldots,t_m)\in T\setminus U} d_{t_1,\ldots,t_m} \sum_{\mathbf{a}\in S} f_1^{t_1} \ldots f_m^{t_m} =$$

$$= \sum_{(t_1,\ldots,t_m)\in T\setminus U} d_{t_1,\ldots,t_m} A_k \sum_{(u_1,\ldots,u_m)\in U} g_{u_1,\ldots,u_m}^{(t_1,\ldots,t_m)} \prod_{i=k+1}^{m} \left(n_i + 1 - \frac{u_i}{n_i} \right) =$$

$$= \sum_{(t_1,\ldots,t_m)\in T\setminus U} d_{t_1,\ldots,t_m} A_k B_{t_1,\ldots,t_m} = 0.$$

Поэтому

$$N = \frac{1}{A_k} \sum\nolimits_1 = \frac{1}{A_k} \sum_{\mathbf{a}\in S} f_1^0 \cdots f_m^0 \prod_{\substack{k+1 \le i \le m \\ b_i \neq 0}} \frac{f_i^{n_i}}{n_i} \prod_{\substack{k+1 \le i \le m \\ b_i = 0}} (1 - f_i^{n_i}).$$

Вводя при необходимости новую индексацию, можно считать, что $b_i \neq 0$ при $k+1 \le i \le l$ и $b_i = 0$ при $l+1 \le i \le m$. Обозначая символом Σ' суммирование по всем двоичным наборам $(d_{l+1}, \ldots, d_m)$, получаем

$$N = \frac{1}{A_k} \sum\nolimits_1 = \frac{1}{A_k} \sum_{\mathbf{a}\in S} f_1^0 \ldots f_m^0 \prod_{i=k+1}^{l} \frac{f_i^{n_i}}{n_i} \sum\nolimits' (-1)^{d_{l+1}+\cdots+d_m} \prod_{i=l+1}^{m} f_i^{d_i n_i}$$

$$= \frac{1}{A_k n_{k+1} \ldots n_l} \sum\nolimits' (-1)^{d_{l+1}+\cdots+d_m} \sum_{\mathbf{a}\in S} \prod_{i=1}^{m} f_i^{t_i},$$

где $(t_1, \ldots, t_m) = (0, \ldots, 0, n_{k+1}, \ldots, n_l, d_{l+1} n_{l+1}, \ldots, d_m n_m)$.

Наконец, учитывая леммы 3 и 4 и условие b), получаем

$$N = \frac{1}{A_k n_{k+1} \ldots n_l} \sum\nolimits' (-1)^{d_{l+1}+\cdots+d_m} A_k n_{k+1} \ldots n_l \times$$

$$\times \sum_{(u_1,\ldots,u_m)\in U} g_{u_1,\ldots,u_m}^{(t_1,\ldots,t_m)} \prod_{i=l+1}^{m} (n_i + 1 - d_i)$$

$$= \sum\nolimits' (-1)^{d_{l+1}+\cdots+d_m} \prod_{i=l+1}^{m} (n_i + 1 - d_i) = 1 \neq 0.$$

□

Отметим некоторые частные случаи теоремы 2.

А. Случай $S = E_{n_1} \times \ldots \times E_{n_m}$ (т.е. $m = k \ge 1$). Условие b) сводится к следующему: $g^{(t_1,\ldots,t_m)} = 0$ для любого набора $(t_1, \ldots, t_m) \in T\setminus U$, где $g^{(t_1,\ldots,t_m)}$ – свободный член многочлена $f_1^{t_1} \ldots f_m^{t_m} \bmod (x_1^{n_1} - 1, \ldots, x_m^{n_m} - 1)$.

B. Случай $S = E_n^0$ (то есть $m = 1,\ k = 0$). Условие b) сводится к следующему:

$$ng_0^{(t)} + (n+1)g_n^{(t)} = \begin{cases} 0, & \text{если} \quad t = 1, \ldots,\ n-1, \\ n, & \text{если} \quad t = n, \end{cases}$$

где $g_0^{(t)}$ – свободный член, а $g_n^{(t)}$ – коэффициент при x^n многочлена $f^t \bmod (x^{n+1} - x)$.

C. Случай н.о.д.$(n_i + 1, p) = p$ для $i = k+1, \ldots, m$ $(m > k)$, где p – характеристика поля $\mathbb{F}_q$ (к этому случаю относятся, например, множества $S = \mathbb{F}_p^m$, $\mathbb{F}_q^m$, $E_n \times \mathbb{F}_p^{n-1}$, $E_n \times \mathbb{F}_q^{n-1}$). Условие b) сводится к следующему:

$$g^{(t_1,\ldots,t_m)} = \begin{cases} 0, & \text{если} \quad (t_1, \ldots, t_m) \in T \backslash \{\mathbf{0}, \tau_0\}, \\ 1, & \text{если} \quad (t_1, \ldots, t_m) = \tau_0, \end{cases}$$

где $g^{(t_1,\ldots,t_m)}$ – коэффициент при $x_{k+1}^{n_{k+1}} \ldots x_m^{n_m}$ многочлена $f_1^{t_1} \ldots f_m^{t_m} \bmod I$, а $\tau_0 = (0, \ldots, 0, n_{k+1}, \ldots, n_m)$.

D. Случай н.о.д.$(n_i + 1, p) = p$ для $i = k+2, \ldots, m$. Условие b) сводится к следующему:

$$B_{t_1,\ldots,t_m} = \begin{cases} 0, & \text{если} \quad (t_1, \ldots, t_m) \in T \backslash \{\mathbf{0}, \tau_0, \tau_1\}, \\ n_{k+1} + 1, & \text{если} \quad (t_1, \ldots, t_m) = \tau_0 \ \text{ или } \ \tau_1, \end{cases}$$

где

$$B_{t_1,\ldots,t_m} = n_{k+1} g^{(t_1,\ldots,t_m)} + (n_{k+1} + 1) f^{(t_1,\ldots,t_m)};$$

$g^{(t_1,\ldots,t_m)}$ и $f^{(t_1,\ldots,t_m)}$ – коэффициенты многочлена $f_1^{t_1} \ldots f_m^{t_m} \bmod I$ соответственно при $x_{k+1}^{n_{k+1}} \ldots x_m^{n_m}$ и $x_{k+2}^{n_{k+2}} \ldots x_m^{n_m}$; τ_0 – набор, определённый в случае C, $\tau_1 = (0, \ldots, 0, 0, n_{k+2}, \ldots, n_m)$.

Замечание. Теорема 1 и лемма 2 позволяют указать необходимые и достаточные условия, которым должна удовлетворять система многочленов $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_m]$, задающая перестановку ρ на множестве $S = S_1 \times \ldots \times S_m$, где $S_1, \ldots, S_m$ – любые (непустые) подмножества поля $\mathbb{F}_q$. Перестановка ρ может быть продолжена (разными способами) до перестановки τ на множестве $\mathbb{F}_q^m$. Перестановка τ задается, как и в теореме 1, некоторой системой многочленов $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_m]$, которые должны удовлетворять условиям a) и b) этой теоремы. Однако, чтобы обеспечить замкнутость действия τ на множестве S, необходимо и достаточно, чтобы выполнялась система сравнений (2).

Литература

1. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1, 2. – М.: Мир, 1988.

2. *Сущевский Д.Г., Панченко О.В., Кугураков В.С.* Современные криптосистемы и их особенности // Вестн. Казан. технол. ун-та. – 2015. – Т. 18, № 11. – С. 194–198.

3. *Кугураков В.С., Кирпичников А.П., Сущевский Д.Г.* О генерации псевдослучайных PIN-кодов криптографическим методом // Вестн. Казан. технол. ун-та. – 2015. – Т. 18, № 17. – С. 190–193.

4. *Kugurakov V., Gainutdinova A.* On the full monomial automorphism groups of Reed–Solomon codes and their MDS-extensions // Lobachevskii J. Math. – 2016. – V. 37, No 6. – P. 650–669. – doi: 10.1134/S1995080216060160.

5. *Kugurakov V.S., Gainutdinova A., Anisimova T.* On calculation of monomial automorphisms of linear cyclic codes // Lobachevskii J. Math. – 2018. – V. 39, No 7. – P. 1024–1038. – doi: 10.1134/S1995080218070168.

6. *Кугураков В.С.* О симметрии одного класса кодов // Вероятностные методы и кибернетика. – 1993. – Вып. 25. – С. 91–99.

Поступила в редакцию
11.03.19

Кугураков Владимир Сергеевич, кандидат физико-математических наук, доцент кафедры теоретической кибернетики

Казанский (Приволжский) федеральный университет
ул. Кремлевская, д. 18, г. Казань, 420008, Россия
E-mail: *Vladimir.Kugurakov@kpfu.ru*

Гайнутдинова Аида Фаритовна, кандидат физико-математических наук, доцент кафедры теоретической кибернетики

Казанский (Приволжский) федеральный университет
ул. Кремлевская, д. 18, г. Казань, 420008, Россия
E-mail: *aida.ksu@gmail.com*

Дубровин Вячеслав Тимофеевич, кандидат физико-математических наук, доцент кафедры математической статистики

Казанский (Приволжский) федеральный университет
ул. Кремлевская, д. 18, г. Казань, 420008, Россия
E-mail: *Vyacheslav.Dubrovin@kpfu.ru*

ISSN 2541-7746 (Print)
ISSN 2500-2198 (Online)

**UCHENYE ZAPISKI KAZANSKOGO UNIVERSITETA.
SERIYA FIZIKO-MATEMATICHESKIE NAUKI
(Proceedings of Kazan University. Physics and Mathematics Series)**

2019, vol. 161, no. 2, pp. 292–300

doi: 10.26907/2541-7746.2019.2.292-300

About Permutations on the Sets of Tuples from Elements of the Finite Field

V.S. Kugurakov, A.F. Gainutdinova**, V.T. Dubrovin****

Kazan Federal University, Kazan, 420008 Russia
E-mail: **Vladimir.Kugurakov@kpfu.ru*, ***aida.ksu@gmail.com*,
****Vyacheslav.Dubrovin@kpfu.ru*

Received March 11, 2019

Abstract

The following problem was considered: let $S = S_1 \times S_2 \times \ldots \times S_m$ be the Cartesian product of subsets S_i that are subgroups of the multiplicative group of a finite field $\mathbb{F}_q$ of q elements or their extensions by adding a zero element; a map $f : S \to S$ of S into itself can be specified by a system of polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_m]$. Necessary and sufficient conditions, for

which the map $f = \langle f_1, \ldots, f_m \rangle$ is bijective, were obtained. Then this problem was generalized to the case when the subsets S_i are any subsets of $\mathbb{F}_q$. The obtained results can be used to construct S-boxes and P-boxes in block ciphers and to calculate automorphism groups of error-correcting codes.

Keywords: cryptography, error-correcting codes, finite fields, permutation polynomials

References

1. Lidl R., Niederreiter H. *Finite Fields*. Addison Wesley, 1983. 755 p.
2. Sushchevskii D.G., Panchenko O.V., Kugurakov V.S. Modern cryptosystems and their features. *Vestn. Kazan. Tekhnol. Univ.*, 2015, vol. 18, no. 11, pp. 194–198. (In Russian)
3. Kugurakov V.S., Kirpichnikov A.P., Suchshevskii D.G. On pseudo-random PIN code generation using the cryptographic method. *Vestn. Kazan. Tekhnol. Univ.*, 2015, vol. 18, no. 17, pp. 190–193. (In Russian)
4. Kugurakov V., Gainutdinova A. On the full monomial automorphism groups of Reed–Solomon codes and their MDS-extensions. *Lobachevskii J. Math.*, 2016, vol. 37, no. 6, pp. 650–669. doi: 10.1134/S1995080216060160.
5. Kugurakov V.S., Gainutdinova A., Anisimova T. On calculation of monomial automorphisms of linear cyclic codes. *Lobachevskii J. Math.*, 2018, vol. 39, no. 7, pp. 1024–1038. doi: 10.1134/S1995080218070168.
6. Kugurakov V.S. On the symmetry of one class of codes. *Veroyatn. Metody Kibern.*, 1993, no. 25, pp. 91–99. (In Russian)

⟨ ***Для цитирования*:** *Кугураков В.С., Гайнутдинова А.Ф., Дубровин В.Т.* О способах задания перестановок на множествах наборов из элементов конечного поля // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. – 2019. – Т. 161, кн. 2. – С. 292–300. – doi: 10.26907/2541-7746.2019.2.292-300. ⟩

⟨ ***For citation*:** Kugurakov V.S., Gainutdinova A.F., Dubrovin V.T. About permutations on the sets of tuples from elements of the finite field. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2019, vol. 161, no. 2, pp. 292–300. doi: 10.26907/2541-7746.2019.2.292-300. (In Russian) ⟩