Об одном классе ортогональных многочленов, связанных с символами Лежандра

В. М. Сидельников*
(черновик)

1. Введение

Пусть $\mathbf{F}_p$ — конечное простое поле. Мы будем рассматривать следующее m-мерное представление

$$W_A = \{\mathrm{diag}\left(\exp\left(\frac{ka_1 \cdot 2\pi i}{p}\right), \exp\left(\frac{ka_2 \cdot 2\pi i}{p}\right), \ldots, \exp\left(\frac{ka_m \cdot 2\pi i}{p}\right)\right);\ k = 0, \ldots, p-1\}$$

аддитивной группы поля $\mathbf{F}_p$, где $A = \{a_1, \ldots, a_m\} \subset \mathbf{F}_p \setminus \{0\}$.

Рассмотрим конечную группу диагональных $nm \times nm$-матриц $W_A^n = W_A \times \cdots \times W_A = \{\mathrm{diag}(\xi(k_1), \ldots, \xi(k_n)); \xi(k_j) \in W_A\}$, где $\xi(k) = \left(\exp\left(\frac{a_1 k \cdot 2\pi i}{p}\right), \ldots, \exp\left(\frac{a_m k \cdot 2\pi i}{p}\right)\right)$, которая является представлением аддитивной группы пространства $\mathbf{F}_p^n$.

Очевидно, функция $\phi(\alpha) = \mathrm{diag}(\xi(\alpha_1), \ldots, \xi(\alpha_n))$, где $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{F}_p^n$, изоморфно отображает элементарную p-группу $\mathbf{F}_p^n$ в матричную группу W_A^n.

Рассмотрим пространство (конечное множество в C^{nm})

$$X_{A,n} = \{(\xi(\alpha_1), \ldots, \xi(\alpha_n));\ \alpha \in \mathbf{F}_p^n\},$$

содержащее p^n элементов. Это пространство может быть также представлено как орбита $X_{A,n} = \mathbf{a}W_A^n$ группы W_A^n с начальным вектором $\mathbf{a} = (1, \ldots, 1)$ (mn действительных единиц).

Скалярное произведение (α, β) на $\mathbf{F}_p^n$ определим как

$$(\alpha, \beta) = \langle \mathbf{a}\phi(\alpha), \mathbf{a}\phi(\beta) \rangle = \sum_{j=1}^{n} \sum_{s=1}^{m} \exp\left(\frac{(\alpha_j - \beta_j)a_s \cdot 2\pi i}{p}\right), \tag{1}$$

где $\langle \mathbf{a}\phi(\alpha), \mathbf{a}\phi(\beta) \rangle$ — обычное скалярное произведение векторов в C^{nm}.

Метрику $d_A(\alpha, \beta)$ на $\mathbf{F}_p^n$ определим равенством

$$d_A(\alpha, \beta) = \left(\sum_{j=1}^{n} |\xi(\alpha_j) - \xi(\beta_j)|^2\right)^{\frac{1}{2}} = (2nm - 2Re((\alpha, \beta)))^{\frac{1}{2}}, \tag{2}$$

где $Re(x)$ — действительная часть числа x и $|u| = \langle u, u \rangle^{\frac{1}{2}}, u \in C^m$, — норма в C^m.

Отметим, что если $A = \{1, 2, \ldots, p-1\} = \mathbf{F}_p \setminus \{0\}$, то функция $\frac{1}{4}d_A^2$ совпадает с метрикой Хемминга d на $\mathbf{F}_p^n$, ибо, как нетрудно проверить, $Re((\alpha, \beta)) = (p-1)n - 2d(\alpha, \beta)$.

Пусть G — группа автоморфизмов (как pгруппы) пространства $\mathbf{F}_p^n$. Метрика λ на $\mathbf{F}_p^n$ называется G-инвариантной, если $\lambda(\alpha, \beta) = \lambda(g\alpha, g\beta)$ для всех $g \in G$.

Например, метрики Хемминга d и метрика $d_A = 2\sqrt{d}$, $A = \mathbf{F}_p \setminus \{0\}$, являются инвариантными относительно, так называемой, полной мономиальной группы G над полем $\mathbf{F}_p$, элементы которой переставляют координаты векторов из $\mathbf{F}_p^n$ и умножают их на ненулевые элементы поля $\mathbf{F}_p$. Метрика d_A, $A = \{a\}$, где a — произвольный ненулевой элемент поля $\mathbf{F}_p$, инвариантна относительно мономиальной группы $B_{2,p}S_n$ (определение группы $B_{s,p}S_n$ см. ниже), элементы которой переставляют координаты векторов из $\mathbf{F}_p^n$ и умножают их на ± 1.

В общем случае мы рассматриваем метрики d_A, которые инвариантны относительно мономиальной группы $B_{s,p}S_n$, элементы которой переставляют координаты векторов из $\mathbf{F}_p^n$ и умножают их на ненулевые элементы поля $\mathbf{F}_p$, принадлежащие подгруппе $B_{s,p}$ порядка s, $s|p-1$, мультипликативной группы $\mathbf{F}_p^*$ конечного поля $\mathbf{F}_p$. Очевидно, метрика d_A является $B_{s,p}S_n$-инвариантной, если $A = B_{s,p}$.

Работа выполнена при финансовой поддержке РФФИ,№99-01-00941.

В работе в явном виде выписаны полное семейство $P_{s,n}, |P_{s,n}| = \binom{n+1}{s}$, ортогональных многочленов от $\frac{p-1}{s}$ переменных на конечном s-мерном дискретном интервале $I_{s,n}$, которые определяются мономиальной группой $B_{s,p}S_n$. В частном случае $s = p-1$ многочлены из $P_{p-1,n}$ совпадают с многочленами Кравчука [1]. Интервал $I_{s,n}$ является симплексом с целочисленными координатами, состоящим из $|I_{s,n}| = \binom{n+1}{s}$ $(s+1)$-мерных векторов $\mathbf{t} = (t_0, \dots, t_s)$ с неотрицательными целыми координатами такими, что $t_0 + \dots + t_s = n$.

Эти многочлены обладают многими замечательными свойствами. В частности, если $s|k$, то каждый многочлен из P_s является взвешенной суммой с положительными коэффициентами многочленов из P_k. В частности, каждый многочлен Кравчука (многочлен из $P_{p-1,n}$) является суммой многочленов из $P_{s,n}$ при любом s. Кроме того, многочлены из $P_{s,n}$ играют ту же роль что и многочлены Кравчука в соотношениях типа МакВильямс для линейных кодов в $\mathbf{F}_p^n$ с неХемминговой метрикой d_A (см. [3]).

2. Основные определения

Пусть $f(\mathbf{x}), g(\mathbf{x}) \in C[\mathbf{x}], \mathbf{x} = (x_1, \dots, x_n)$, — многочлены от n переменных. Скалярное произведение $\langle f(\mathbf{x}), g(\mathbf{x})\rangle$ в $C[\mathbf{x}]$ многочленов $f(\mathbf{x}), g(\mathbf{x})$ определим соотношением

$$\langle f(\mathbf{x}), g(\mathbf{x})\rangle = p^{-n} \sum_{\alpha \in \mathbf{F}_p^n} f(\tau(\alpha))\overline{g(\tau(\alpha))}. \tag{3}$$

Очевидно,

$$\langle f(\mathbf{x}), g(\mathbf{x})\rangle = \frac{1}{m} p^{-n} \sum_{\alpha \in \mathbf{F}_p^n} \sum_{j=1}^{m} f(\tau(a_j\alpha))\overline{g(\tau(a_j\alpha))} = \frac{1}{m} p^{-n} \sum_{\mathbf{x} \in X^{(n)}} \sigma_A(f(\mathbf{x}), g(\mathbf{x})), \tag{4}$$

где

$$\tau(\alpha) = \left(\exp\left(\frac{\alpha_1 \cdot 2\pi i}{p}\right), \dots, \exp\left(\frac{\alpha_n \cdot 2\pi i}{p}\right)\right), \tag{5}$$

$$X^{(n)} = \{\left(\exp\left(\frac{\alpha_1 \cdot 2\pi i}{p}\right), \dots, \exp\left(\frac{\alpha_n \cdot 2\pi i}{p}\right)\right);\ \alpha \in \mathbf{F}_p^n\} \tag{6}$$

и

$$\sigma_A(f(\mathbf{x}), g(\mathbf{x})) = \sum_{j=1}^{m} f(x_1^{a_j}, \dots, x_n^{a_j})\overline{g(x_1^{a_j}, \dots, x_n^{a_j})}. \tag{7}$$

Положим

$$\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n},\ \alpha \in \mathbf{F}_p^n,\ \mathbf{x} \in X^{(n)},\ \mathbf{x}^\alpha \in C[\mathbf{x}]. \tag{8}$$

Как легко видеть,

$$\langle \mathbf{x}^\alpha, \mathbf{x}^\beta\rangle = \begin{cases} 1, & \text{если } \alpha = \beta, \\ 0, & \text{если } \alpha \neq \beta \end{cases}. \tag{9}$$

Отсюда следует, что если $D \subset \mathbf{F}_p^n$ и

$$\pi_D(\mathbf{x}) = |D|^{-\frac{1}{2}} \sum_{\alpha \in D} \mathbf{x}^\alpha, \tag{10}$$

то

$$\langle \pi_D(\mathbf{x}), \pi_{D'}(\mathbf{x})\rangle = |D|^{-\frac{1}{2}} |D'|^{-\frac{1}{2}} |D \cap D'|, \tag{11}$$

в частности,

$$\langle \pi_D(\mathbf{x}), \pi_{D'}(\mathbf{x})\rangle = \begin{cases} 1, & \text{если } D = D', \\ 0, & \text{если } D \cap D' = \emptyset. \end{cases} \tag{12}$$

3. Ортогональные многочлены

Пусть G группа, элементами g которой являются преобразованиями пространства $\mathbf{F}_p^n$ в себя, и пусть $\mathbf{F}_p^n = \cup_{j=0}^h F_j$ — разбиение $\mathbf{F}_p^n$ на классы эквивалентности по группе G. Классы F_j будем обозначать через $F_{[\alpha]}$, где α — произвольный представитель класса F_j. Таким образом, $F_{[\alpha]} = F_{[\alpha']}$, если найдется $g \in G$ такое, что $g\alpha = \alpha'$, и $F_{[\alpha]} \neq F_{[\alpha']}$, если такого g не найдется.

Элемент $g \in G$ индуцирует отображение $\tilde{g}$ множества $X^{(n)}$ в себя следующим образом

$$\tilde{g}\mathbf{x} = \tilde{g}\tau(\alpha) = \tau(\alpha'), \tag{13}$$

где $\mathbf{x} = \tau(\alpha)$ и $\alpha' = g\alpha$. Таким образом, преобразования $\tilde{g}$ образуют группу $\tilde{G}$ пространства $X^{(n)}$, которая изоморфна G. Классы эквивалентности элементов из $X^{(n)}$ по группе $\tilde{G}$ будем обозначать через $X_{[\beta]}$, где $\tau(\beta)$, $\tau(\beta) \in X^{(n)}$, — представитель соответствующего класса смежности.

Пусть $\pi_D(\mathbf{x}) \; =\in \; C[\mathbf{x}]$ — многочлен, определенный в (10). Через $\pi(\mathbf{x})_D^G$ будем обозначать G-инвариантный многочлен $\pi(\mathbf{x})_D^G = \frac{1}{|G|}\sum_{g\in G}\left(\frac{1}{|D|}\sum_{\alpha\in D}\mathbf{x}^{g\alpha}\right)$. В частностном случае $\pi(\mathbf{x})_D^G = \mathbf{x}^\alpha$ будем использовать обозначение

$$(\mathbf{x}^\alpha)^G = \pi_{[\alpha]}^G(\mathbf{x}) = \frac{1}{|F_{[\alpha]}|}\sum_{\gamma\in F_{[\alpha]}}\mathbf{x}^\gamma = \frac{1}{|G|}\sum_{g\in G}\mathbf{x}^{g\alpha'} \tag{14}$$

где α' — произвольный представитель класса $F_{[\alpha]}$. Индекс G у $\pi_{[\alpha]}^G(\mathbf{x})$ будем иногда опускать.

Очевидно,

$$\frac{1}{|G|}\sum_{g\in G}\mathbf{x}^{g\alpha} = \frac{1}{|\tilde{G}|}\sum_{\tilde{g}\in\tilde{G}}(\tilde{g}\mathbf{x})^\alpha, \tag{15}$$

поэтому классы $X_{[\beta]} = \{\tilde{g}\mathbf{x};\ \tilde{g} \in G\} \subset X^{(n)} = \{\left(\exp\left(\frac{\alpha_1\cdot 2\pi i}{p}\right), \dots, \exp\left(\frac{\alpha_n\cdot 2\pi i}{p}\right)\right);\ \alpha \in \mathbf{F}_p^n\}$ являются множествами, на которых многочлен $\pi_{[\alpha]}(\mathbf{x})$ принимает постоянное значение $b_{[\beta]}$.

Лемма 1. *Предположим, что существует автоморфизм $\sigma: g \to g'$ группы G, для которого выполнено $\langle g\alpha, \beta\rangle = \langle \alpha, \sigma(g)\beta\rangle$ для всех $g \in G$, $\alpha, \beta \in \mathbf{F}_p^n$, где $\langle\alpha,\beta\rangle = \sum_{j=1}^n \alpha_j\beta_j$ — скалярное произведение в $\mathbf{F}_p^n$. Тогда*

$$\pi_{[\alpha]}(\tau(\beta)) = \pi_{[\beta]}(\tau(\alpha)). \tag{16}$$

Доказательство. Значение монома $\mathbf{x}^{g\alpha}$ в точке $\mathbf{x} = \tau(\beta)$ равно $\tau(\beta)^{g\alpha} = \exp\left(\frac{\langle g\alpha,\beta\rangle\cdot 2\pi i}{p}\right)$. Из условия леммы вытекает, что $\exp\left(\frac{\langle g\alpha,\beta\rangle\cdot 2\pi i}{p}\right) = \exp\left(\frac{\langle \alpha,\sigma(g)\beta\rangle\cdot 2\pi i}{p}\right) = \tau(\alpha)^{\sigma(g)\beta}$, т.е. $\tau(\beta)^{g\alpha} = \tau(\alpha)^{\sigma(g)\beta}$. Отсюда и из последнего соотношения в (14) следует утверждение леммы.

Лемма 2. *Пусть H — нормальная подгруппа группы G. Тогда*

$$\pi_{[\alpha]}(\mathbf{x})^G = |G|^{-1}\sum_{j=1}^k |H|\pi_{[\alpha]}(\mathbf{x}^{h_j})^H, \tag{17}$$

где h_j, $j = 1, \dots, k$, $k = \frac{|G|}{|H|}$, определяются условием $G = \cup_{j=1}^k Hh_j$ — разложением G на правые смежные классы по подгруппе H.

Далее в качестве G будем рассматривать мономиальные матричные группы, элементы которых переставляют координаты векторов из $\mathbf{F}_p^n$ и умножают их на ненулевые элементы поля $\mathbf{F}_p$. Таким образом, каждая матрица $g \in G$ имеет в каждом столбце и каждой строке точно один ненулевой элемент поля $\mathbf{F}_p$.

Сначала рассмотрим частный случай, а именно, симметрическую группу S_n, элементы которой переставляют координаты векторов из $\mathbf{F}_p^n$. Эта группа является самой "маленькой" среди рассатриваемых далее мономиальных групп. Классами эквивалентностями F_j для рассматриваемой группы S_n являются множества, образованными векторами, которые имеют одинаковую композицию $\mathbf{w} = (w_1, \dots, w_{p-1})$, $w_0 + \cdots + w_{p-1} = n$, т.е. $F_j = F_{\mathbf{w}} = \{\alpha; w_k(\alpha) = w_k,\ k = 0, \dots p-1\}$, где $w_k(\alpha)$ — число координат у вектора α равных k. Отметим, что классы эквивалентности F_j группы S_n являются самыми "мелким" среди рассматривемых ниже.

В свою очередь классами эквивалентностями $X_{\mathbf{v}} \subset X^{(n)}$, $\mathbf{v} = (v_1, \dots, v_{p-1}, v_1 + \cdots + v_{p-1} = n, v_j \geq 0$, являются множества $X_{\mathbf{v}} = \{\mathbf{x}; v_k(\mathbf{x}) = v_k,\ k = 0, \dots p-1\}$, где $v_k(\mathbf{x})$ — число координат вектора $\mathbf{x}$

равных $\exp\left(\frac{k\cdot 2\pi i}{p}\right)$. Наборы $\mathbf{w}(\alpha)=(w_0(\alpha),\dots,w_{p-1}(\alpha))$, $\mathbf{v}(\mathbf{x})=(v_0(\mathbf{x}),\dots,v_{p-1}(\mathbf{x}))$ назовем маркировками соответствующих векторов.

В рассматриваемом случае $G=S_n$ многочлены $\pi_j(\mathbf{x})$ будем индексировать маркировками $\mathbf{w}=(w_0,\dots,w_{p-1})$ и у них удобно измениить нормирующий множитель. Таким образом, мы далее рассматриваем многочлены

$$\pi_{\mathbf{w}}(\mathbf{x})=\binom{n}{\mathbf{w}}^{-\frac{1}{2}}\sum_{w(\alpha)=\mathbf{w}}\mathbf{x}^{\alpha}, \tag{18}$$

где $\binom{n}{\mathbf{w}}=\frac{n!}{w_0!\cdots w_{p-1}!}$ число векторов α с фиксированной маркировкой $\mathbf{w}$.

Следующей группой, которую мы рассмотрим, является полная мономиальная группа $F_p^*S_n$. Эта группа образована всевозможными матрицами, которая имеет в каждом столбце и строке по одному ненулевому элементу из $\mathbf{F}_p^*$. Очевидно, $|F_p^*S_n|=(p-1)^n\cdot n!$.

Классами эквивалентностями $F_w\subset F_p^n$ по группе $F_p^*S_n$, очевидно, являются множества векторов $J_w=\cup_{w_1+\cdots+w_{p-1}=w}F_{\mathbf{w}}$ фиксированного веса w, $w=0,1,\dots,n$. Соответствующие группе $F_p^*S_n$ многочлены $\pi_j(\mathbf{x})$, которые мы обозначаем через $\kappa_w(\mathbf{x})$, имеют вид

$$\kappa_w(\mathbf{x})=\left((p-1)^w\binom{n}{w}\right)^{-\frac{1}{2}}\sum_{wt(\alpha)=w}\mathbf{x}^{\alpha}, \tag{19}$$

где $wt(\alpha)$ — обычный вес вектора α и $(p-1)^w\binom{n}{w}$ — число векторов α веса w.

Как будет видно из дальнейшего, многочлены $\kappa_w(\mathbf{x})$, по существу, являются широко известными многочленами Кравчука (см. [1]).

Отметим, что многочлен $\kappa_w(\mathbf{x})$ является суммой некотрых многочленов $\pi_{\mathbf{w}}(\mathbf{x})$ с положительными коэффициентами. Действительно, S_n — подгруппа группы $F_p^*S_n$ и поэтому $J_w=\cup_{w_1+\cdots+w_{p-1}=w}F_{\mathbf{w}}$. Следовательно,

$$\kappa_w(\mathbf{x})=\left(\binom{n}{w}(p-1)^w\right)^{-1/2}\sum_{w_1+\cdots+w_{p-1}=w}\binom{n}{\mathbf{w}}^{1/2}\pi_{\mathbf{w}}(\mathbf{x}). \tag{20}$$

Мы обозначаем через $B_{s,p}$, $s|p-1$, подгруппу мультипликативной группы F_p^* поля F_p порядка s, т.е. $B_{s,p}=\{x^{\frac{p-1}{s}},\ x\in\mathbf{F}_p^*\}$.

Мономиальная группа $B_{s,p}S_n$ состоит из всех матриц размера $n\times n$, которые имеют в каждом столбце и строке однин ненулевой элемент, принадлежащий группе $B_{s,p}$. Очевидно, $|B_{s,p}S_n|=s^n\cdot n!$, $B_{1,p}S_n=S_n$ и $B_{p-1,p}S_n=S_n=\mathbf{F}^*S_n$.

Будем обозначать через T_r, $r=1,\dots,s$, подмножество $\mathbf{F}_p$, состоящее из чисел j, для которых $\chi(j)=\exp\left(\frac{2\pi i\cdot\mathrm{ind}(j)}{s}\right)=\exp\left(\frac{2\pi ir)}{s}\right)$, где $\chi(x)$ — примитивный s-значный характер группы $\mathbf{F}_p^*$, $s|p-1$, и $\mathrm{ind}(j)$ — индекс элемента j, $j\neq 0$, по какаму-либо первообразному корню группы $\mathbf{F}_p^*$. Положим $T_0=\{0\}$.

Положим $\mathbf{u}(\alpha)=(u_0(\alpha),u_1(\alpha),\dots,u_s(\alpha))$, где $u_r(\alpha)$ — число координат в векторе α, принадлежащих классу T_r, и $S_{\mathbf{u}}=\{\alpha;\mathbf{u}(\alpha)=\mathbf{u}\}$. Соответственно, положим $\mathbf{t}(\mathbf{x})=(t_0(\mathbf{x}),t_1(\mathbf{x}),\dots,t_s(\mathbf{x}))$, где $t_r(\mathbf{x})$ — число координат $x_j=exp\left(\frac{2\pi i\beta_j}{p}\right)$ в векторе $\mathbf{x}$, у которых $\beta_j\in T_r$.

Очевидно, каждый класс $S_{\mathbf{u}}$ содержит $\left(\frac{p-1}{s}\right)^{n-u_0}\binom{n}{\mathbf{u}}$ элементов и является объединением нескольких классов $F_{\mathbf{w}}$. Всего имеется $\binom{n+1}{s}$ различных классов $S_{\mathbf{u}}$.

Рассмотрим многочлен

$$\delta_{\mathbf{u}}^{(s)}(\mathbf{x})=\left(\left(\frac{p-1}{s}\right)^{n-u_0}\binom{n}{\mathbf{u}}\right)^{-\frac{1}{2}}\sum_{\mathbf{u}(\alpha)=\mathbf{u}}\mathbf{x}^{\alpha}. \tag{21}$$

В том случае, когда $-1\in B_{s,p}$, многочлен $\delta_{\mathbf{u}}^{(s)}(\mathbf{x})$ принимает только действительные значения, ибо в этом случае вместе с мономом $\mathbf{x}^{\alpha}$ в сумму $\sum_{\mathbf{u}(\alpha)=\mathbf{u}}\mathbf{x}^{\alpha}$ входит и моном $\mathbf{x}^{-\alpha}=\overline{\mathbf{x}^{\alpha}}$.

Очевидно, значение многочлена $\delta_{\mathbf{u}}^{(s)}(\mathbf{x})$ зависит только от маркировки $\mathbf{t}(\mathbf{x})=\mathbf{t}$ вектора $\mathbf{x}$, т.е. $\delta_{\mathbf{u}}^{(s)}(\mathbf{x})=\Delta_{\mathbf{u}}^{(s)}(\mathbf{t})$, $\mathbf{t}=\mathbf{t}(\mathbf{x})$.

Отметим, что для мономиальной группы $B_{s,p}S_n$ условие леммы 1 всегда выполнено. Действительно, любой ее элемент можно представить в виде $g = SD$, где S — подстановочная матрица, а D — диагональная матрица с элементами из группы $B_{s,p}$. Требуемый автоморфизм σ имеет вид $\sigma : SD \to DS^{-1}$. Таким образом, вместе с леммой 1 справедлива

Лемма 2. *Если $G = B_{s,p}S_n$, то*

$$\pi_{[\alpha]}(\tau(\beta)) = \left(\left(\frac{p-1}{s}\right)^{n-u_0}\binom{n}{\mathbf{u}}\right)^{-\frac{1}{2}}\delta_{\mathbf{u}}^{(s)}(\tau(\beta)) =$$

$$= \left(\left(\frac{p-1}{s}\right)^{n-u_0}\binom{n}{\mathbf{u}}\right)^{-\frac{1}{2}}\Delta_{\mathbf{u}}^{(s)}(\mathbf{t}) = \left(\left(\frac{p-1}{s}\right)^{n-t_0}\binom{n}{\mathbf{t}}\right)^{-\frac{1}{2}}\Delta_{\mathbf{t}}^{(s)}(\mathbf{u}) = \pi_{[\beta]}(\tau(\alpha)), \tag{22}$$

где $\mathbf{u} = \mathbf{u}(\alpha)$, $\mathbf{t} = \mathbf{t}(\tau(\beta))$.

Особо выделим случай $s = \frac{p-1}{2}$ (группу, образованную ненулевыми квадратичными вычетами (resque) поля $\mathbf{F}_p$), а именно, группу $B_{(p-1)/2,p}S_n$, которую обозначим через U_pS_n.

Пусть $\mathbf{r} = (r_0, r_+, r_-)$, $r_j \geq 0$, $r_0 + r_+ + r_- = n$, $R_{\mathbf{r}} = \{\alpha; \mathbf{r}(\alpha) = \mathbf{r}\}$, где $\mathbf{r}(\alpha) = (r_0(\alpha), r_+(\alpha), r_-(\alpha))$ и $r_0(\alpha)$ — число нулевых координат у α, а $r_+(\alpha)(r_-(\alpha))$ — число координат у α, значениями которых являются ненулевые квадратичные вычеты (квадратичные невычеты). Очевидно,$|R_{\mathbf{r}}| = \left(\frac{p-1}{2}\right)^{r_+ + r_-}\binom{n}{\mathbf{r}} = \left(\frac{p-1}{2}\right)^{n-r_0}\binom{n}{\mathbf{r}}$ — число векторов α с композицией $\mathbf{r}$.

Классами эквивалентностями $F_j \subset \mathbf{F}_p^n$ по группе U_pS_n, очевидно, являются множества $R_{\mathbf{r}}$. Всего имеется $\sum_{r_0=0}^{n}(n+1-r_0) = \binom{n+1}{2}$ различных классов $R_{\mathbf{r}}$.

Положим

$$\rho_{\mathbf{r}}(\mathbf{x}) = \left(\left(\frac{p-1}{2}\right)^{r_+ + r_-}\binom{n}{\mathbf{r}}\right)^{-\frac{1}{2}}\sum_{\alpha \in R_{\mathbf{r}}}\mathbf{x}^{\alpha}, \tag{23}$$

Очевидно, многочлен $\rho_{\mathbf{r}}(\mathbf{x})$ является суммой некоторых многочленов $\pi_{\mathbf{w}}(\mathbf{x})$.

Как следует из (15) значение многочлена $\delta_{\mathbf{u}}^{(s)}(\mathbf{x})$, $\mathbf{x} \in X^n$, определяется только маркировкой $\mathbf{t}(\mathbf{x})$ вектора $\mathbf{x}$. Таким образом, $\delta_{\mathbf{u}}^{(s)}(\mathbf{x}) = \Delta_{\mathbf{u}}^{(s)}(\mathbf{t})$, $\mathbf{t} = \mathbf{t}(\mathbf{x}) = (t_0, \ldots, t_s)$ и скалярное произведение $\langle \delta_{\mathbf{u}}^{(s)}(\mathbf{x}), \delta_{\mathbf{u}'}^{(s)}(\mathbf{x})\rangle$ можно представить в виде

$$\langle \delta_{\mathbf{u}}^{(s)}(\mathbf{x}), \delta_{\mathbf{u}'}^{(s)}(\mathbf{x})\rangle = p^{-n}\binom{n}{\mathbf{u}}^{-1}\sum_{\mathbf{t}}\binom{n}{\mathbf{t}}\Delta_{\mathbf{u}}^{(s)}(\mathbf{t})\overline{\Delta_{\mathbf{u}'}^{(s)}(\mathbf{t})} = \begin{cases} 1, & \text{если } \mathbf{u} = \mathbf{u}', \\ 0, & \text{если } \mathbf{u} \neq \mathbf{u}' \end{cases}. \tag{24}$$

Достаточно просто в случае $s = p-1$ найти явный вид многочлена $\Delta_{\mathbf{u}}^{(p-1)}(\mathbf{t}) = \pi_{\mathbf{w}}(\mathbf{x})$ как функции от маркировки $\mathbf{v}$ вектора $\mathbf{x}$ (см. (18)). Для этого заметим, что, с одной сторны, значение многочлена $\mathbf{x}^{\alpha}, \alpha \in \mathbf{F}_p$, в точке $\tau(\beta)$ равно $\tau(\beta)^{\alpha} = \exp\left(\frac{2\pi i\cdot\langle\alpha,\beta\rangle}{p}\right)$, где $\langle\alpha,\beta\rangle = \sum_{j=1}^{n}\alpha_j\beta_j$ — скалярное произведение в $\mathbf{F}_p^n$. С другой сторны это же значение равно $\tau(\beta)^{\alpha} = \exp\left(\frac{2\pi i\cdot\sum_{j,k=0}^{p-1}jkw_{j,k}}{p}\right)$, где $w_{j,k}$ — число координат у векторов α, β, для которых выполнены соотношения $\alpha_v = j$, $\beta_v = k$ $v = 1, \ldots, n$. Последнее равенство и будем использовать далее.

Отсюда следует, что

$$\Delta_{\mathbf{w}}^{(p-1)}(\mathbf{v}) = \binom{n}{\mathbf{w}}^{-\frac{1}{2}}\sum_{\mathbf{w}^0+\cdots+\mathbf{w}^{p-1}=\mathbf{w}}\binom{v_0}{\mathbf{w}^{(0)}}\binom{v_1}{\mathbf{w}^{(1)}}\cdots\binom{v_{p-1}}{\mathbf{w}^{(p-1)}}\exp\left(\frac{2\pi i\sum_{j=0,k=0}^{p-1}jkw_{j,s}}{p}\right), \tag{25}$$

где $\mathbf{w}^{(j)} = (w_{j,0}, \ldots, w_{j,p-1})$, $w_{j,0} + \cdots + w_{j,p-1} = v_j$, $w_{j,k} \geq 0$.

Как видно из (25), многочлен $\Delta_{\mathbf{w}}^{(p-1)}(\mathbf{v})$ от $p-1$ переменных $v_1, \ldots, v_{p-1}$, принимающих целочисленные значения в области (симплексе) $\mathbf{v}$; $v_0 + v_1 + \cdots + v_{p-1} = n$, $v_j \geq 0$, имеет степень равную $\sum_{j=1}^{p-1}w_j$.

Выражения, аналогичные (25), имеют место и для многочленов $\delta_{\mathbf{u}}^{(s)}(\mathbf{x})$. Они будут рассмотрены в §4.

4. Частные случаи

Рассмотрим некоторые частные случаи выбора множества A и соответствующих многочленов $f_w(v)$.

4.1. Случай 1. G **— полная мономиальная группа,** $s = p-1$. . Этот случай соответствует пространству Хемминга.

Достаточно просто найти явный вид многочлена $K_w(\mathbf{t}) = \Delta^{(p-1)}_{n-w,w}(n-v,v) = \kappa_w(\mathbf{x})$ как функции от маркировки $\mathbf{t} = (n-v,v)$ вектора $\mathbf{x}$ (см. (19)).

Как легко видеть из (25) при $vt(\mathbf{x}) = v$ имеет место соотношение

$$\kappa_w(\mathbf{x}) = K_w(v) = \left((p-1)^w\binom{n}{w}\right)^{-\frac{1}{2}}\sum_{j=0}^{n}\binom{v}{j}\binom{n-v}{w-j}(-1)^j(p-1)^{w-j}. \tag{26}$$

Многочлен $K_w(v)$ является обычным многочленом Кравчука. Соотношение (24) имеет вид

$$\langle\kappa_w(\mathbf{x}),\kappa_{w'}(\mathbf{x})\rangle = p^{-n}\binom{n}{w}^{-1}\sum_{v=0}^{n}\binom{n}{v}K_w(v)K_{w'}(v) = \begin{cases}1, & \text{если } w = w',\\ 0, & \text{если } w \neq w'\end{cases}. \tag{27}$$

4.2. Случай 2. $G = B_{s,p}S_n$, $s|p-1$. Легко вычислить, что при $\mathbf{t}(\mathbf{x}) = \mathbf{t} = (t_0,\dots,t_{p-1})$, $\mathbf{x} = (x_1,\dots,x_n) \in X^{(n)}$, выполнено

$$\delta^{(s)}_{\mathbf{u}}(\mathbf{x}) = \Delta^{(s)}_{\mathbf{u}}(\mathbf{t}) = \left(\binom{n}{\mathbf{u}}\left(\frac{p-1}{s}\right)^{u_1+\dots+u_s}\right)^{-\frac{1}{2}}\sum_{\mathbf{u}^{(0)}+\dots+\mathbf{u}^{(p-1)}=\mathbf{u}}\ \sum_{\mathbf{u}^{(0)}(\alpha)=\mathbf{u}^{(0)}}\cdots\sum_{\mathbf{u}^{(p-1)}(\alpha)=\mathbf{u}^{(p-1)}}\mathbf{x}^{\alpha} =$$

$$\left(\binom{n}{\mathbf{u}}\left(\frac{p-1}{s}\right)^{u_1+\dots+u_s}\right)^{-\frac{1}{2}}\sum_{\mathbf{u}^{(0)}+\dots+\mathbf{u}^{(p-1)}=\mathbf{u}}\ \prod_{l=0}^{p-1}\binom{t_l}{\mathbf{u}^{(l)}}\prod_{k=1}^{p-1}\varphi^{u_{l,k}}(lk), \tag{28}$$

где

i. $\mathbf{u}^{(l)}(\alpha) = (u_{l,0}(\alpha),\dots,u_{l,p-1}(\alpha))$ и $u_{l,k}(\alpha)$ — число значений j, для которых выполнено $x_j = \exp\left(\frac{2\pi i h}{p}\right)$, $h \in T_l$, $\alpha_j \in T_k$,

ii. суммирование в сумме $\sum_{\mathbf{u}^{(l)}(\alpha,)=\mathbf{u}^{(l)}}$ производится по всем α, для которых $\mathbf{u}^{(l)}(\alpha,) = \mathbf{u}^{(l)}$. Отметим, что число слагаемых этой суммы равно $\binom{t_l}{\mathbf{u}^{(l)}}$.

iii. $\varphi^{(s)}(j) = \frac{1}{s}\sum_{x\in\mathbf{F}_p^*}\exp\left(\frac{2\pi i j x^{\frac{p-1}{s}}}{p}\right) = \frac{1}{s}\sum_{x\in\mathbf{F}_p^*}(1+\chi(x)+\dots+\chi^{s-1}(x))\exp\left(\frac{2\pi i j x}{p}\right) = \frac{1}{s}\sum_{a=0}^{s-1}\tau_j(\chi^a)$, $j \neq 0$, и $\tau_j(\chi^a) = \sum_{x\in\mathbf{F}_p}\chi^a(x)exp\left(\frac{2\pi i j x}{p}\right)$ — гауссова сумма, и $\varphi^{(s)}(0) = \frac{p-1}{s}$,

iv. $C_{\mathbf{u}} = \binom{n}{\mathbf{u}}\left(\frac{p-1}{s}\right)^{u_1+\dots+u_s}$ — число векторов α, для которых $\mathbf{u}(\alpha) = \mathbf{u}$.

Очевидно, $\tau_j(\chi^a) = \chi^a(j^{-1})\tau_1(\chi^a)$ и, следовательно, $\phi_j = \phi_{j'}$, если $\chi(j) = \chi(j')$.

Получим иное по сравнению с (28) выражение для $\Delta^{(s)}_{\mathbf{u}}(\mathbf{t})$. Для этого будем использовать очевидное соотношение $B_{s,p}S_n = D_{s,p,n}\cdot S_n = \dot{S}_n\cdot D_{s,p,n}$, где $D_{s,p,n} = \{\mathrm{diag(b_1,\dots,b_n); b_j \in B_{s,p}}\} = \mathrm{B^n_{s,p}}$. В этом случае

$$(C_{\mathbf{u}})^{-\frac{1}{2}}\Delta^{(s)}_{\mathbf{u}}(\mathbf{t}) = \pi_{[\alpha]}(\mathbf{x}) = \frac{1}{s^n\cdot n!}\sum_{g\in B_{s,p}S_n}\exp\left(\frac{2\pi i\langle\gamma,g\alpha\rangle}{p}\right) =$$

$$\frac{1}{s^n\cdot n!}\sum_{h\in S_n}\sum_{g'\in D_{s,p,n}}\exp\left(\frac{2\pi i\langle\gamma,hg'\alpha\rangle}{p}\right) =$$

$$\frac{1}{s^n\cdot n!}\sum_{h\in S_n}\prod_{j=1}^{n}\varphi^{(s)}(\gamma_j\alpha_j^{(h)})) = \frac{1}{s^n\cdot n!}\sum_{h\in S_n}\prod_{j=1}^{n}\left(\varphi^{(s)}(j)\right)^{t(\gamma,\alpha^{(h)})} =$$

$$\frac{1}{s^n\cdot n!}\sum_{\mathbf{n}}^{s}N_{\mathbf{n}}(\mathbf{t},\mathbf{u})\prod_{j=1}^{s}\left(\varphi^{(s)}(j)\right)^{n_j(\mathbf{t},\mathbf{u})}, \tag{29}$$

где

i. $h\alpha = (\alpha_1^{(h)},\dots,\alpha_n^{(h)})$, $\mathbf{x} = \tau(\gamma)$,

ii. $N_{\mathbf{n}}(\mathbf{x},\mathbf{u}) = N_{\mathbf{n}}(\mathbf{t},\mathbf{u})$, число элементов h группы S_n, для которых $\mathbf{n}(\mathbf{x},h\alpha) = \mathbf{n}$, $\mathbf{n} = (n_0,\dots,n_s)$, $n_0+\dots+n_s$, $n_j \geq 0$,

iii. $\mathbf{n}(\mathbf{x},h\alpha) = (n_0(\mathbf{x},h\alpha),\dots,n_0(\mathbf{x},h\alpha))$ и $n_j(\mathbf{x},h\alpha)$ число координат k, $k=1,\dots,n$, для которых $\gamma_k\alpha_k^{(h)} \in T_j$, $j=0,\dots,s$.

Нетрудно увидеть, что соотношение (29) эквивалентно соотношению (28).

Рассмотрим случай $s=\frac{p-1}{2}$. Как известно, [2]

$$\varphi_m^{(\frac{p-1}{2})} = \frac{1}{2}\begin{cases} -1+\epsilon_p\left(\frac{m}{p}\right)\sqrt{p}, & \text{если } m\neq 0,\\ p-1, & \text{если } m=0,\end{cases} \tag{30}$$

где $\left(\frac{m}{p}\right)$ есть символ Лежандра и $\epsilon_p = \begin{cases}1, & \text{если } p=4t+1,\\ i, & \text{если } p=4t+3.\end{cases}$.

В рассматривемом случае соотношение (28) имеет вид

$$\delta_{\mathbf{u}}^{((p-1)/2)}(\mathbf{t}) = \rho_{\mathbf{r}}(\mathbf{t}) =$$

$$= \left(\left(\frac{p-1}{2}\right)^{r_+ + r_-}\binom{n}{\mathbf{r}}\right)^{-\frac{1}{2}} \sum_{\mathbf{r}^{(0)}+\mathbf{r}^{(+)}+\mathbf{r}^{(-)}=\mathbf{r}} \binom{t_0}{\mathbf{r}^{(0)}}\binom{t_+}{\mathbf{r}^{(+)}}\binom{t_-}{\mathbf{r}^{(-)}} \varphi_+^{r_{+,+}+r_{-,-}}\varphi_-^{r_{-,+}+r_{+,-}}\left(\frac{p-1}{2}\right)^{r_{0,+}+r_{0,-}}, \tag{31}$$

где $\mathbf{r}=(r_0,r_+,r_-)$, $\mathbf{t}=(t_0,t_+,t_-)$. Напомним, что $t_c(\mathbf{x})$, $c\in\{0,+,-\}$, — число координат $x_j = \exp\left(\frac{2\pi i k_j}{p}\right)$ в векторе $\mathbf{x}$, у которых $k_j \in T_c$, где $T_0=\{0\}, T_+$ (T_-) — множество всех ненулевых квадратичных вычетов (невычетов), соответственно, $\varphi_+ = -1+\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\exp\left(\frac{2\pi i\cdot x}{p}\right) = \varphi_1^{((p-1)/2)}$, и $\varphi_- = -1-\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\exp\left(\frac{2\pi i\cdot x}{p}\right) = \varphi_\iota^{((p-1)/2)}$, где ι — квадратичный невычет.

4.3. Случай 3. $A=A_s=\{x^2,\, x\in\mathbf{F}_p^*\}$, $s|p-1$. Этот случай отличается от предыдущего тем, что мы в качестве ортогональных рассматриваем многочлены

$$\lambda_{\mathbf{r}}(\mathbf{x}) = \left(\left(2\frac{p-1}{2}\right)^{r_+ + r_-}\binom{n}{\mathbf{r}}\right)^{-\frac{1}{2}}\sum_{\alpha\in R_{\mathbf{r}}}(\mathbf{x}^\alpha+\mathbf{x}^{-\alpha}) =$$

$$\left(\left(2\frac{p-1}{2}\right)^{r_+ + r_-}\binom{n}{\mathbf{r}}\right)^{-\frac{1}{2}}\sum_{\alpha\in R_{\mathbf{r}}} Re(\mathbf{x}^\alpha) = Re(\tau_{\mathbf{r}}(\mathbf{x})), \tag{32}$$

которые, очевидно, принимают только действительные значения. Если $p=4t+1$, т.е. если $\left(\frac{-1}{p}\right)=1$, то этот случай не отличается от уже рассмотренного в п.2.1, ибо $\lambda_{\mathbf{r}}(\mathbf{x}) = \rho_{\mathbf{r}}(\mathbf{x})$. Мы далее будем рассматриваит только случай $p=4t+3$. Этот случай отличается от уже рассмотренного в п.2.1 в виду того, что $\lambda_{\mathbf{r}}(\mathbf{x}) = \frac{1}{\sqrt{2}}(\rho_{\mathbf{r}}(\mathbf{x})+\rho_{\mathbf{r}'}(\mathbf{x}))$, где $r=(r_0,r_+,r_-)$ и $r'=(r_0,r_-,r_+)$.

Литература

[1] F.J. Mac Williams, N.J.A. Sloane, The theory of error-correcting codes. Am.-N.Y.-Oxford. 1979.

[2] R. Lindl and H. Niederreiter, Finite Fields, Encyclopedia Mathematics and its Applications, V 20, Cambridge, U.C.: Cambridge Univ. Press, 1984.

[3] V.M. Sidel'nikov, MacWillams-type identities for linear p-ary codes in Non-Hamming spaces

[4] V.M. Sidel'nikov, Extending McWilliams Identity to the Noncommutative Groups. Case Study of Spherical Orbit Codes, Отослано в J. Of Algebraic Combinatorics.