О.А.Логачёв, В.В.Ященко

КОДЫ ТИПА РИДА—МАЛЛЕРА НА КОНЕЧНОЙ АБЕЛЕВОЙ ГРУППЕ[1]

Введены коды типа Рида—Маллера с помощью определенных множеств комплекснозначных функций на конечной абелевой группе. В случае элементарной абелевой 2-группы — это обычные двоичные коды Рида—Маллера. Для кодов типа Рида—Маллера доказаны некоторые из алгебраических свойств, хорошо известных для обычных кодов Рида—Маллера.

§1. Исходные определения, обозначения и результаты

Основным объектом для настоящей работы является множество комплекснозначных функций на конечной абелевой группе и коды, построенные с помощью этого множества. В обозначениях и исходных результатах мы будем следовать двум работам: [1] — по абстрактному гармоническому анализу и [2] — по теории кодирования.

Пусть G — конечная абелева группа в мультипликативной записи, порядок G равен n, экспонента G (максимальный порядок элементов из G) равна q, $\mathbf{e}$ — единица G. Пусть T — группа вращений окружности, т.е.

$$T = \{e^{2\pi i x}, \quad 0 \leqslant x < 1\},$$

T_q — подгруппа T, состоящая из корней степени q из единицы. Как обычно, через T^G обозначим множество функций на G со значениями в T. Если зафиксировать некоторую нумерацию элементов G, то множество T^G можно отождествить с множеством T^n и представлять его как множество векторов длины n с координатами из T или, если это удобно, как n-мерный тор (произведение n экземпляров окружности T). T^G является подмножеством линейного пространства $\mathbf{C}^G$ — всех комплекснозначных функций на G. На $\mathbf{C}^G$ обычным образом вводится скалярное произведение

$$(f_1, f_2) = \sum_{x \in G} f_1(x)\overline{f_2(x)},$$

где $\overline{f_2(x)}$ — число, комплексносопряженное к числу $f_2(x)$. Отметим, что если $f \in T^G$, то $(f, f) = n$.

Множество $T_q^G \subset T^G$ функций на G со значениями в T_q является конечной абелевой группой относительно покоординатного умножения функций, порядок T_q^G равен q^n, экспонента — q. Подгруппой группы T_q^G является группа $\widehat{G}$ — группа характеров группы G, т.е. гомоморфизмов $\chi\colon G \to T_q$. Группа $\widehat{G}$ изоморфна группе G, зафиксируем некоторый изоморфизм и будем считать, что все характеры $\chi_\alpha \in \widehat{G}$ занумерованы элементами $\alpha \in G$. Характеры удовлетворяют нескольким соотношениям ортогональности:

$$\sum_{x \in G} \chi_\alpha(x) \;=\; \begin{cases} 0, & \text{если } \alpha \neq \mathbf{e}, \\ n, & \text{если } \alpha = \mathbf{e}, \end{cases}$$

[1]Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 96–01–00931).

$$\sum_{\alpha\in G}\chi_\alpha(x) = \begin{cases} 0, & \text{если } x\neq \mathbf{e},\\ n, & \text{если } x=\mathbf{e},\end{cases}$$

$$(\chi_\alpha,\chi_\beta) = \begin{cases} 0, & \text{если } \alpha\neq\beta,\\ n, & \text{если } \alpha=\beta.\end{cases}$$

Удобно ввести в рассмотрение квадратную матрицу $H(G)$ размера $n\times n$

$$H(G)=\|\chi_\alpha(x)\|.$$

Строка матрицы $H(G)$ с номером $\alpha\in G$ — это вектор значений характера $\chi_\alpha\in\widehat{G}$. В случае, когда G — элементарная абелева 2-группа порядка 2^k, матрица $H(G)$ является хорошо известной в теории кодирования матрицей Адамара [2]. Соотношения ортогональности приводят к следующему матричному равенству:

$$H(G)H^*(G)=nE,$$

где E — единичная матрица размера $n\times n$, $H^*(G)$ — транспонированная и комплексносопряженная к $H(G)$ матрица. Матрица $H(G)$ задает преобразование Фурье функций из $\mathbf{C}^G$

$$\widehat{f}(\alpha)=\sum_{x\in G} f(x)\overline{\chi_\alpha(x)}.$$

Обратное преобразование находится с помощью соотношений ортогональности

$$f(x)=\frac{1}{n}\sum_{\alpha\in G}\widehat{f}(\alpha)\chi_\alpha(x).$$

При этом выполняется равенство Парсеваля

$$\sum_{\alpha\in G}|\widehat{f}(\alpha)|^2=n\sum_{x\in G}|f(x)|^2,$$

которое для функций $f\in T^G$ упрощается

$$\sum_{\alpha\in G}|\widehat{f}(\alpha)|^2=n^2.$$

Приведем некоторые свойства преобразования Фурье, необходимые для дальнейшего. Преобразование Фурье любого характера сосредоточено в одной точке

$$\widehat{\chi}_\beta(\alpha)=\begin{cases} 0, & \text{если } \alpha\neq\beta,\\ n, & \text{если } \alpha=\beta.\end{cases}$$

Обозначим через ${}_\sigma f$, $\sigma\in G$, функцию, полученную сдвигом аргумента функции f

$${}_\sigma f(x)=f(\sigma x).$$

Тогда

$$\left(\widehat{{}_\sigma f}\right)(\alpha)=\chi_\alpha(\sigma)\widehat{f}(\alpha).$$

Рассмотрим действие автоморфизмов группы G на аргументы функции f и обозначим через f^w, $w \in \mathrm{Aut}(G)$, полученную при этом функцию

$$f^w(x) = f(x^w),$$

где x^w — образ элемента $x \in G$ при автоморфизме $w \in \mathrm{Aut}(G)$. Обычным образом определяется автоморфизм $\widetilde{w} \in \mathrm{Aut}(G)$, сопряженный к автоморфизму w, так что для любого характера χ_α выполнено

$$\chi_{\alpha^{\widetilde{w}}}(x) = \chi_\alpha^w(x) = \chi_\alpha(x^w).$$

При этом получим равенство

$$\widehat{f}^w(\alpha) = \widehat{f}(\alpha^{\widetilde{w^{-1}}}).$$

Преобразование Фурье произведения двух функций равно свертке преобразований Фурье, которая определяется следующим равенством:

$$(\widehat{f} * \widehat{\varphi})(\alpha) = \frac{1}{n} \sum_{\beta \in G} \widehat{f}(\beta)\widehat{\varphi}(\alpha\beta^{-1}).$$

При этом

$$(\widehat{f\varphi})(\alpha) = (\widehat{f} * \widehat{\varphi})(\alpha).$$

Применив преобразование Фурье к обеим частям тождества

$$f(x)\overline{f(x)} = 1,$$

получим "соотношения ортогональности" для коэффициентов Фурье любой функции $f \in T^G$:

$$\sum_{\alpha \in G} \widehat{f}(\alpha)\overline{\widehat{f}}(\alpha\beta^{-1}) = \begin{cases} 0, & \text{если } \beta \neq \mathbf{e}, \\ n^2, & \text{если } \beta = \mathbf{e}. \end{cases}$$

При этом мы воспользовались легко проверяемым тождеством

$$\widehat{\overline{f}}(\alpha) = \overline{\widehat{f}}(\alpha^{-1}).$$

В теории кодирования [2] изложенные результаты применяются больше всего для случая, когда G — элементарная абелева 2-группа, которую можно считать векторным пространством V_k размерности k над полем из двух элементов, тогда $q = 2$, $n = 2^k$. В этом случае $T_q = \{-1, +1\}$, и рассматриваются функции вида $(-1)^{\varphi(x)}$, где $\varphi(x)$ — некоторая булева функция. Векторы значений булевых функций — это векторы длины 2^k, состоящие из нулей и единиц. Кодом Рида—Маллера $R(r, k)$ называется множество векторов, соответствующих булевым функциям степени нелинейности не более r. С основными свойствами кодов $R(r, k)$ можно познакомиться в [2]; в настоящей работе будут построены коды типа Рида—Маллера для произвольной конечной абелевой группы G и доказаны аналогичные свойства.

Коды $R(r,k)$ входят в различные семейства кодов, построенных с использованием конечных абелевых групп. Поэтому и рассмотренные в настоящей работе коды типа Рида—Маллера при некоторых значениях параметров входят в соответствующие семейства. Укажем работы, в которых изучались такие семейства кодов. (Более подробно вопрос о различных обобщениях кодов Рида—Маллера освещен в [3], а вопрос о соотношении введенных в настоящей работе кодов с этими известными кодами — это предмет отдельного исследования, результаты которого будут отражены в следующей работе авторов.) Вначале подчеркнем, что наш выбор мультипликативной записи группы G диктовался желанием использовать аппарат гармонического анализа в стандартной форме [1]. Чаще в теории кодирования рассматривают абелевы группы в аддитивной записи, она больше приспособлена для изучения метрических свойств. В этом случае и множество функций на G рассматривают также в аддитивной записи и поэтому приходят к Z_qG — групповому кольцу группы G над кольцом Z_q (определение группового кольца см. в [4]).

В [5] введены FG-коды — идеалы групповой алгебры группы G над конечным полем F. Частным случаем FG-кодов являются радикальные коды, определяемые как степени радикала модулярной групповой алгебры. Для радикальных p-кодов в [5] получены точные формулы для кодового расстояния в метрике Хэмминга, а в [6] рассмотрены алгоритмы мажоритарного декодирования при некоторых значениях параметров кода. В [7, 8] для широкого класса абелевых групповых кодов с использованием характеров абелевых групп доказаны тождества Мак-Вильямс для дуальных кодов.

§2. Определение и основные свойства кода $RM_1(G)$

Кодом $RM_1(G)$ типа Рида—Маллера первого порядка на группе G будем называть множество точек n-мерного тора T^G, соответствующих векторам значений характеров группы G и их сдвигов:

$$RM_1(G) = \{f \in T_q^G : \exists \alpha, \sigma \in G, \quad f(x) = \chi_\alpha(\sigma x) \quad \forall x \in G\}.$$

Точки $RM_1(G)$ как функции на G естественно называть аффинными функциями на G; они получаются из характеров (линейных функций) умножением на константу:

$f \in RM_1(G)$ тогда и только тогда, когда $f(x) = f(\mathbf{e})\chi_\alpha(x)$ для некоторого $\alpha \in G$ при всех $x \in G$.

Поэтому очевидно, что

$$|RM_1(G)| = qn.$$

Метрические свойства кодов в настоящей работе рассматриваться не будут, им будет посвящена следующая работа авторов, поэтому здесь мы не указываем конкретную метрику (евклидову, Хэмминга или какую-нибудь еще). Ограничимся лишь указанием некоторых полезных свойств скалярных произведений, они в какой-либо форме необходимы для изучения в дальнейшем метрических свойств кодов типа Рида—Маллера. Из определения кода $RM_1(G)$ и соотношений ортогональности для характеров легко получить для любых $f_1, f_2 \in RM_1(G)$:

$$(f_1, f_2) = \begin{cases} 0, & \text{если } \overline{f_1(\mathbf{e})} f_1 \neq \overline{f_2(\mathbf{e})} f_2, \\ f_1(\mathbf{e})\overline{f_2(\mathbf{e})} n & \text{в противном случае.} \end{cases}$$

Найдем теперь группу автоморфизмов кода $RM_1(G)$. Обозначим через S_G симметрическую группу всех перестановок элементов G. Как и раньше, для любой $f \in T^G$ и любой $\pi \in S_G$ определим функцию $f^\pi \in T^G$ следующим равенством:

$$f^\pi(x) = f(x^\pi),$$

где x^π — образ элемента $x \in G$ при перестановке $\pi \in S_G$. Для любого множества (кода) $K \subset T^G$ группу автоморфизмов $\mathrm{Aut}(K)$ определим следующим равенством:

$$\mathrm{Aut}(K) = \{\pi \in S_G : f^\pi \in K \quad \text{для всех} \quad f \in K\}.$$

Назовем аффинной группой преобразований группы G следующую группу:

$$A(G) = \{\pi \in S_G : x^\pi = \mathbf{e}^\pi x^w, \quad w \in \mathrm{Aut}(G)\}.$$

Т е о р е м а 1. $\mathrm{Aut}(RM_1(G)) = A(G)$.

Д о к а з а т е л ь с т в о. Включение $A(G) \subseteq \mathrm{Aut}(RM_1(G))$ вытекает из существования сопряженного автоморфизма $\widetilde{w} \in \mathrm{Aut}(G)$, поскольку для любой функции $f \in RM_1(G)$ и любой $\pi \in A(G)$ получаем

$$f^\pi(x) = f(x^\pi) = f(\mathbf{e})\chi_\alpha(x^\pi) = f(\mathbf{e})\chi_\alpha(\mathbf{e}^\pi x^w) = f(\mathbf{e})\chi_\alpha(\mathbf{e}^\pi)\chi_\alpha(x^w) =$$
$$= f(\mathbf{e})\chi_\alpha(\mathbf{e}^\pi)\chi_{\alpha^{\widetilde{w}}}(x) \in RM_1(G).$$

.

Пусть теперь $\pi \in \mathrm{Aut}(RM_1(G))$. Тогда $\chi(x^\pi) \in RM_1(G)$ для любого характера χ, т.е. существует такой характер $\chi^{(\pi)}(x)$, что

$$\chi(x^\pi) = \chi(\mathbf{e}^\pi)\chi^{(\pi)}(x) \qquad \text{для всех} \quad x \in G.$$

Используя это равенство, путем простых преобразований получим при любых $x, y \in G$ равенство

$$\chi((xy)^\pi) = \chi(\mathbf{e}^\pi)\chi^{(\pi)}(xy) = \chi(\mathbf{e}^\pi)\chi^{(\pi)}(x)\chi^{(\pi)}(y) =$$
$$= \overline{\chi(\mathbf{e}^\pi)}\left(\chi(\mathbf{e}^\pi)\chi^{(\pi)}(x)\right)\left(\chi(\mathbf{e}^\pi)\chi^{(\pi)}(y)\right) =$$
$$= \overline{\chi(\mathbf{e}^\pi)}\chi(x^\pi)\chi(y^\pi) = \chi((\mathbf{e}^\pi)^{-1}x^\pi y^\pi).$$

Поскольку это равенство выполнено для любого характера χ, то

$$(xy)^\pi = (\mathbf{e}^\pi)^{-1}x^\pi y^\pi.$$

Это равенство означает, что перестановка $w \in S_G$ задаваемая условием

$$x^w = (\mathbf{e}^\pi)^{-1}x^\pi,$$

является автоморфизмом группы G, и тем самым $\pi \in A(G)$. ▲

Теперь, рассматривая расположение функций $f \in T^G$ относительно $RM_1(G)$, можно воспользоваться теоремой 1 и перейти к эквивалентным (относительно действия $A(G)$) функциям. При этом все множество T^G разбивается на орбиты относительно действия группы $A(G)$, которые мы будем называть аффинными классами по аналогии с соответствующим понятием для булевых функций. Функции из одной орбиты мы будем называть

аффинно эквивалентными (или просто эквивалентными). Такие характеристики функций, которые постоянны на орбите, т.е. которые равны для аффинно эквивалентных функций, мы будем называть аффинными инвариантами.

Большой класс аффинных инвариантов описывается следующим образом. Для фиксированного аффинного класса $K \subset T^G$ и фиксированной функции $f \in T^G$ рассмотрим множество чисел $\{(f,\varphi) \quad \forall \varphi \in K\}$. Назовем мультимножеством $B(f,K)$ множество различных значений (f,φ), $\varphi \in K$ с указанием, сколько раз это значение встречается, когда φ пробегает все K.

Т е о р е м а 2. *Мультимножество $B(f,K)$ является аффинным инвариантом для любого аффинного класса K.*

Д о к а з а т е л ь с т в о. Для любой $\pi \in S_G$ имеем

$$(f^\pi,\varphi) = \sum_{x\in G} f(x^\pi)\overline{\varphi(x)} = \sum_{y\in G} f(y)\overline{\varphi(y^{\pi^{-1}})} = (f,\varphi^{\pi^{-1}}).$$

Таким образом, для аффинно эквивалентных функций f и f^π, $\pi \in A(G)$ множества $\{(f,\varphi)\ \forall\varphi \in K\}$, $\{(f^\pi,\varphi)\ \forall\varphi \in K\}$ отличаются только перестановкой элементов, а это означает, что мультимножества $B(f,K)$ и $B(f^\pi,K)$ совпадают. ▲

Из указанных в § 1 свойств преобразования Фурье видно, что преобразования Фурье аффинно эквивалентных функций связаны простыми соотношениями.

Перейдем к другому описанию кода $RM_1(G)$. Прежде всего подчеркнем, что код $RM_1(G)$ — групповой, т.е. $RM_1(G)$ является подгруппой группы T_q^G. Введем понятие производной функции $f \in T^G$ по направлению $\sigma \in G$, задавая функцию $\frac{df}{d\sigma}(x)$ следующим равенством:

$$\frac{df}{d\sigma}(x) = \overline{f(x)}f(\sigma x) \qquad \forall x \in G.$$

Очевидно, что для любого $\sigma \in G$ оператор дифференцирования $\frac{d}{d\sigma}\colon T^G \to T^G$ является гомоморфизмом группы T^G. Отметим следующие простейшие соотношения для производных:

$$\begin{aligned}
\frac{df}{d\mathbf{e}}(x) &\equiv 1 \quad \forall f \in T^G,\\
\frac{dc}{d\sigma}(x) &\equiv 1 \quad \forall c \in T,\ \forall \sigma \in G,\\
\frac{d\chi}{d\sigma}(x) &= \chi(\sigma) \quad \forall \sigma \in G,\ \forall \chi \in \widehat{G}.
\end{aligned}$$

Для любой функции $f \in T^G$ через $L_f \subseteq G$ обозначим следующее множество:

$$L_f = \left\{\sigma \in G : \quad \frac{df}{d\sigma}(x) \equiv \mathrm{const}\right\}.$$

Л е м м а 1. *Множество L_f для любой $f \in T^G$ является подгруппой группы G.*

Д о к а з а т е л ь с т в о. По определению производной имеем

$$f(\sigma x) = \frac{df}{d\sigma}(x) f(x) \quad \forall \sigma, x \in G.$$

Применяя это равенство, последовательно получаем

$$f(\sigma_1 \sigma_2 x) = \frac{df}{d\sigma_1}(\sigma_2 x) f(\sigma_2 x) = \frac{df}{d\sigma_1}(\sigma_2 x) \frac{df}{d\sigma_2}(x) f(x),$$

и поэтому

$$\frac{df}{d(\sigma_1 \sigma_2)}(x) = \frac{df}{d\sigma_1}(\sigma_2 x) \frac{df}{d\sigma_2}(x) \quad \forall \sigma_1, \sigma_2, x \in G.$$

Если теперь $\sigma_1, \sigma_2 \in L_f$, то, очевидно, и $\sigma_1 \sigma_2 \in L_f$. Включение $\mathbf{e} \in L_f$ вытекает из простейших свойств производной. ▲

Подгруппу L_f будем называть группой линейности функции f. Оказывается, свойство максимальности группы линейности является характеристическим свойством для $RM_1(G)$.

Т е о р е м а 3. $RM_1(G) = \{f \in T_q^G : \quad L_f = G\}$.

Д о к а з а т е л ь с т в о. Из определения $RM_1(G)$ и простейших свойств производной легко получить, что если $f \in RM_1(G)$, то $L_f = G$.

Пусть теперь $L_f = G$. Это значит, что при всех $x, \sigma \in G$ выполнено равенство

$$\frac{df}{d\sigma}(x) = \frac{df}{d\sigma}(\mathbf{e}) = \overline{f(\mathbf{e})} f(\sigma).$$

Подставляя это в определение производной, получим при всех $x, \sigma \in G$

$$f(\sigma x) = \overline{f(\mathbf{e})} f(\sigma) f(x)$$

и тем самым

$$\overline{f(\mathbf{e})} f(\sigma x) = (\overline{f(\mathbf{e})} f(\sigma))(\overline{f(\mathbf{e})} f(x)).$$

Это равенство означает, что $\overline{f(\mathbf{e})} f(x)$ — характер группы G, и поэтому $f \in RM_1(G)$. ▲

В общей ситуации, когда группа L_f нетривиальна, т.е. $L_f \neq G$, $L_f \neq \mathbf{e}$, функцию f можно разложить по группе L_f в следующем смысле. Пусть группа G представлена в виде прямого произведения $G = U \times V$. Будем говорить, что $f \in T^G$ разложима по группе U с выделением характера или что от функции f отщепляется характер группы U, если для всех $u \in U$, $v \in V$ выполнено равенство

$$f(u, v) = \chi(u) \psi(v)$$

с некоторым характером χ группы U и функцией $\psi \in T^V$.

Т е о р е м а 4. *Пусть $G = U \times V$. От функции $f \in T^G$ отщепляется характер группы U в том и только в том случае, когда U — подгруппа группы L_f.*

Д о к а з а т е л ь с т в о. Пусть от f отщепляется характер группы U; найдем производную f по направлению $\sigma \in U$:

$$\frac{df}{d\sigma}(u, v) = \overline{f}(u, v) f(\sigma u, v) = \overline{\chi}(u) \overline{\psi}(v) \chi(\sigma u) \psi(v) = \chi(\sigma).$$

Поэтому $\sigma \in L_f$ для любого $\sigma \in U$, и тем самым $U < L_f$.

Пусть теперь $U < L_f$. Покажем, что функция $\overline{f}(\mathbf{e},\mathbf{e})f(\sigma,\mathbf{e})$, $\sigma \in L_f$ является характером группы L_f, а значит и группы U. По определению L_f при любом $\sigma \in L_f$ имеем

$$f\big((\sigma,\mathbf{e})(z,\mathbf{e})\big) = \overline{f}(\mathbf{e},\mathbf{e})f(\sigma,\mathbf{e})f(z,\mathbf{e}),$$

и поэтому

$$\overline{f}(\mathbf{e},\mathbf{e})f\big((\sigma,\mathbf{e})(z,\mathbf{e})\big) = \big(\overline{f}(\mathbf{e},\mathbf{e})f(\sigma,\mathbf{e})\big)\big(\overline{f}(\mathbf{e},\mathbf{e})f(z,e)\big),$$

т.е. $\overline{f}(\mathbf{e},\mathbf{e})f(\sigma,\mathbf{e})$ — характер L_f. Положим для любых $u \in U, v \in V$

$$\begin{aligned}\overline{f}(\mathbf{e},\mathbf{e})f(u,\mathbf{e}) &= \chi(u),\\ f(\mathbf{e},v) &= \psi(v).\end{aligned}$$

Тогда получаем

$$f(u,v) = f\big((u,\mathbf{e})(\mathbf{e},v)\big) = \overline{f}(\mathbf{e},\mathbf{e})f(u,\mathbf{e})f(\mathbf{e},v) = \chi(u)\psi(v). \quad \blacktriangle$$

Одним из следствий теоремы 4 является необходимый признак нетривиальности группы L_f — наличие какого-то количества нулей среди коэффициентов Фурье функции f. Это связано с тем, что преобразование Фурье любого характера имеет только одно ненулевое значение. Как и в теореме 4, пусть $G = U \times V$, где $U = L_f$. Обозначим через $\chi_f(u) = \chi_{(a_0,\mathbf{e})}(u)$ характер группы L_f, построенный в теореме 4:

$$\chi_f(u) = \chi_{(a_0,\mathbf{e})}(u) = \overline{f}(\mathbf{e},\mathbf{e})f(u,\mathbf{e}).$$

Л е м м а 2. *При описанных обозначениях для всех $(\alpha,\beta) \in G$, $\alpha \neq \alpha_0$ выполнено равенство*

$$\widehat{f}(\alpha,\beta) = 0$$

Д о к а з а т е л ь с т в о. Воспользовавшись разложимостью функции f, преобразуем формулу для преобразования Фурье:

$$\begin{aligned}\widehat{f}(\alpha,\beta) = \sum_{(u,v)\in G} f(u,v)\overline{\chi}_{(\alpha,\beta)}(u,v) = \sum_{(u,v)\in G} \chi_f(u)\psi(v)\overline{\chi}_{(\alpha,\beta)}(u,v) =\\ = \sum_{v\in V} \psi(v)\overline{\chi}_{(\mathbf{e},\beta)}(\mathbf{e},v) \sum_{u\in U} \chi_f(u)\overline{\chi}_{(\alpha,\mathbf{e})}(u,\mathbf{e}).\end{aligned}$$

Из-за соотношений ортогональности для характеров внутренняя сумма в условиях леммы 2 равна нулю. $\blacktriangle$

Возвращаясь теперь к аффинным классам, естественно выяснить, как связаны группы линейности для аффинно эквивалентных функций.

Т е о р е м а 5. *Пусть $\pi \in A(G)$ имеет вид*

$$x^\pi = \mathbf{e}^\pi x^w, \quad w \in Aut(G).$$

Тогда для любой функции $f \in T^G$ выполнено

$$L_{f^\pi} = (L_f)^w,$$

где

$$(L_f)^w = \{z \in G : z = \sigma^w, \sigma \in L_f\}.$$

Д о к а з а т е л ь с т в о. Для любых $x, \sigma \in G$ имеем

$$(\sigma x)^\pi = \mathbf{e}^\pi (\sigma x)^w = \mathbf{e}^\pi \sigma^w x^w = \sigma^w x^\pi.$$

Теперь легко преобразовать формулу для производной

$$\frac{df^\pi}{d\sigma}(x) = \overline{f^\pi(x)} f^\pi(\sigma x) = \overline{f(x^\pi)} f\big((\sigma x)^\pi\big) = \overline{f(x^\pi)} f(\sigma^w x^\pi) = \frac{df}{d\sigma^w}(x^\pi).$$

Таким образом,

$$\frac{df^\pi}{d\sigma} = \left(\frac{df}{d\sigma^w}\right)^\pi.$$

Это равенство делает утверждение теоремы 5 очевидным. ▲

При использовании аппарата производных и работе со скалярным произведением функций из T^G оказывается полезным одно тождество, которое доказывается с помощью простых преобразований

$$\sum_{\sigma\in G}\left(\frac{df_1}{d\sigma}, \frac{df_2}{d\sigma}\right) = \sum_{\sigma\in G}\sum_{x\in G} \overline{f_1(x)} f_1(\sigma x) f_2(x) \overline{f_2(\sigma x)} =$$
$$= \sum_{x\in G} \overline{f_1(x)} f_2(x) \sum_{\sigma\in G} f_1(\sigma x)\overline{f_2(\sigma x)} = (f_1, f_2)\overline{(f_1, f_2)} = |(f_1, f_2)|^2.$$

Тем самым доказана

Л е м м а 3. *Для любых $f_1, f_2 \in T^G$ выполнено тождество*

$$\sum_{\sigma\in G}\left(\frac{df_1}{d\sigma}, \frac{df_2}{d\sigma}\right) = |(f_1, f_2)|^2.$$

§3. Коды $RM_r(G)$

Коды $RM_r(G)$ типа Рида—Маллера порядка r на группе G будем определять рекуррентным способом. Положим

$$RM_{-1}(G) = \{f \in T_q^G : f(x) \equiv 1\},$$
$$RM_0(G) = \{f \in T_q^G : f(x) \equiv \text{const}\}.$$

Тогда утверждение теоремы 3 можно записать следующим образом:

$$RM_1(G) = \{f \in T_q^G : \frac{df}{d\sigma} \in RM_0(G), \forall \sigma \in G\}.$$

Теперь для $r = 2, 3, \ldots$ положим по определению

$$RM_r(G) = \{f \in T_q^G : \frac{df}{d\sigma} \in RM_{r-1}(G), \forall \sigma \in G\}.$$

Ясно, что в силу конечности T_q^G, начиная с некоторого N, будут выполнены равенства

$$RM_{r+1}(G) = RM_r(G), \quad r = N, N+1, \ldots$$

При этом для некоторых групп может оказаться, что $RM_N(G) = T_q^G$, а для некоторых групп в множестве T_q^G содержатся функции, не принадлежащие ни одному коду типа Рида—Маллера.

Для изучения свойств кодов $RM_r(G)$ удобно рассмотреть более общую конструкцию. Множество функций $\Phi \subseteq T_q^G$ назовем A_0-группой, если выполнены следующие свойства:

1. Φ является подгруппой группы T_q^G;

2. Φ замкнуто относительно действия аффинной группы преобразований, т.е. если $f \in \Phi$, то $f^\pi \in \Phi$ для всех $\pi \in A(G)$;

3. Φ замкнуто относительно "сужений" или, другими словами, "фиксаций части переменных".

Под "фиксацией части переменных" понимается следующая операция: пусть группа G представлена в виде прямого произведения $G = U \times V$; тогда из функции $f(u, v) \in \Phi$ путем фиксации части переменных получаются функции $f_{[u_0]}(u, v) = f(u_0, v)\ \forall u_0 \in U$ и $f_{[v_0]}(u, v) = f(u, v_0)\ \forall v_0 \in V$.

Легко видеть, что множества $RM_{-1}(G)$, $RM_0(G)$, $RM_1(G)$ являются A_0-группами. Определим теперь оператор J, действующий на множествах функций, с помощью следующего равенства:

$$J\Phi = \{f \in T_q^G : \frac{df}{d\sigma} \in \Phi\ \forall \sigma \in G\}.$$

Этот оператор описывает рекуррентный переход в определении кодов типа Рида—Маллера, поскольку теперь можно записать:

$$RM_r(G) = JRM_{r-1}(G), r = 0, 1, 2, \ldots .$$

Легко видеть, что для A_0-групп выполнено включение $\Phi \subseteq J\Phi$.

Т е о р е м а 6. *Оператор J переводит A_0-группу в A_0-группу.*

Д о к а з а т е л ь с т в о. Пусть Φ — A_0-группа, проверим свойства A_0-группы для $J\Phi$.

1. Пусть $f_1, f_2 \in J\Phi$, т.е. $\frac{df_1}{d\sigma}, \frac{df_2}{d\sigma} \in \Phi$ для всех $\sigma \in G$. Тогда

$$\frac{d(f_1 f_2)}{d\sigma} = \frac{df_1}{d\sigma}\frac{df_2}{d\sigma} \in \Phi$$

для всех $\sigma \in G$ и тем самым $f_1 f_2 \in J\Phi$.

2. Пусть $f \in J\Phi$ и $\pi \in A(G)$, причем

$$x^\pi = \mathbf{e}^\pi x^w, w \in \mathrm{Aut}(G)\ \forall x \in G.$$

В § 2 при доказательстве теоремы 5 получено тождество

$$\frac{df^\pi}{d\sigma} = \left(\frac{df}{d\sigma^w}\right)^\pi.$$

Поскольку $\frac{df}{d\sigma^w} \in \Phi$ и Φ — A_0-группа, то $\left(\frac{df}{d\sigma^w}\right)^\pi \in \Phi$, и тем самым $\forall \sigma \in G\ \ \frac{df^\pi}{d\sigma} \in \Phi$, т. е. $f^\pi \in J\Phi$.

3. Это свойство выполнено для $J\Phi$ в силу следующего очевидного соображения: операции "взятия производной" и "фиксации части переменных" для любой функции коммутируют.

Тем самым для $J\Phi$ выполнены все три свойства A_0-группы. ▲

С л е д с т в и е 1. *Коды* $RM_r(G), r = 1, 2, 3, \ldots$ *являются* A_0*-группами для всех* r.

Замечание. Для A_0-группы Φ в определении $J\Phi$ требование

а) $\frac{df}{d\sigma} \in \Phi$ для всех $\sigma \in G$

можно заменить требованием

б) $\frac{df}{d\sigma} \in \Phi$ для всех σ из некоторого базиса G.

Действительно, в § 2 уже использовалось тождество

$$\frac{df}{d(\sigma_1\sigma_2)}(x) = \frac{df}{d\sigma_1}(\sigma_2 x)\frac{df}{d\sigma_2}(x).$$

Поэтому, если Φ — A_0-группа и $\frac{df}{d\sigma_1}$, $\frac{df}{d\sigma_2} \in \Phi$, то и $\frac{df}{d(\sigma_1\sigma_2)} \in \Phi$. Значит, из б) следует а).

Запишем теперь определение кода $RM_{r-1}(G)$ в следующем более удобном виде:

$$RM_{r-1}(G) = J^{r-1}RM_0(G) = J^r RM_{-1}(G),$$

или в развернутой форме:

$$RM_{r-1}(G) = \left\{ f \in T_q^G : \frac{d}{d\sigma_1}\frac{d}{d\sigma_2}\ldots\frac{d}{d\sigma_r}f \equiv 1 \text{ для всех } \sigma_1, \ldots, \sigma_r \in G \right\}.$$

Отсюда видно, что для дальнейшего изучения кодов $RM_r(G)$ необходимо рассмотреть полугруппу операторов на T_q^G, порожденную операторами дифференцирования. Здесь оказывается полезной следующая более общая конструкция.

Рассмотрим Z_qG — групповое кольцо группы G над кольцом Z_q (см. [4, с. 329]). Элементами Z_qG являются всевозможные формальные суммы вида $\sum_{\sigma\in G}\lambda_\sigma\sigma$, где $\lambda_\sigma \in Z_q$, $\sigma \in G$, и произведение в Z_qG вычисляется по обычным правилам умножения многочленов с последующим приведением подобных членов. Определим действие Z_qG на функциях из T_q^G следующим образом. Если $a \in Z_qG$, $a = \sum\lambda_\sigma\sigma$, то

$$\big(af\big)(x) = \prod_{\sigma\in G}\big(f(\sigma x)\big)^{\lambda_{\sigma^{-1}}}.$$

Очевидно, что при таком определении оператор a является гомоморфизмом группы T_q^G, а умножению операторов соответствует умножение в кольце Z_qG. Рассмотренные ранее операторы сдвига и дифференцирования вкладываются в эту конструкцию, поскольку очевидно:

$$\begin{aligned} {}_\sigma f(x) &= \big(\sigma^{-1}f\big)(x), \\ \frac{d}{d\sigma}f(x) &= \big((\sigma^{-1}-1)f\big)(x), \end{aligned}$$

где 1 — единица кольца Z_qG. Подчеркнем, что здесь мы воспользовались тождеством

$$\overline{f(x)} = \big(f(x)\big)^{-1} \;\forall f \in T_q^G.$$

Такой подход значительно упрощает вычисления с операторами дифференцирования и позволяет легко получать различные тождества для производных, используя соотношения в кольце Z_qG. Приведем несколько простейших примеров.

Ранее неоднократно использовалось тождество для производных

$$\frac{df}{d(\sigma_1\sigma_2)}(x) = \frac{df}{d\sigma_1}(\sigma_2 x)\frac{df}{d\sigma_2}(x).$$

Теперь видно, что оно является следствием такого тождества в Z_qG:

$$\sigma_1\sigma_2 - 1 = \sigma_2(\sigma_1 - 1) + (\sigma_2 - 1).$$

Пусть теперь $\sigma \in G$ имеет порядок t, тогда

$$\sum_{i=0}^{t-1} \sigma^i(\sigma - 1) = (\sigma - 1)\sum_{i=0}^{t-1} \sigma^i = \sigma^t - 1 = 0.$$

Поэтому для любой функции $f \in T_q^G$ получаем тождество

$$\prod_{i=0}^{t-1} \frac{df}{d\sigma}(\sigma^i x) \equiv 1.$$

Полезно отметить, что последнее тождество является характеристическим для функций, являющихся производными других функций.

Л е м м а 4. *Функцию $\varphi \in T_q^G$ можно представить в виде производной некоторой функции $f \in T_q^G$ по некоторому направлению $\sigma \in G$, $\sigma^t = \mathbf{e}$, в том и только в том случае, если*

$$\prod_{i=0}^{t-1} \varphi(\sigma^i x) \equiv 1 \text{ при всех } x \in G.$$

Д о к а з а т е л ь с т в о. Необходимость очевидна из предыдущего.

Для доказательства достаточности рассмотрим дифференциальное уравнение

$$\frac{df}{d\sigma}(x) = \varphi(x) \quad \forall x \in G$$

относительно неизвестной функции $f \in T_q^G$. Разложим G на смежные классы по циклической группе $\langle\sigma\rangle$ и зафиксируем какую-нибудь полную систему представителей смежных классов — $y_1, y_2, \ldots, y_k \in G$, $n = kt$. Тогда очевидно, что дифференциальное уравнение эквивалентно совокупности k подсистем (из t уравнений каждая) от непересекающихся множеств неизвестных значений $f(x)$ $\forall x \in G$, причем j-ая подсистема ($j = 1, 2, \ldots, k$) имеет вид:

$$\begin{aligned}
\overline{f(y_j)}f(\sigma y_j) &= \varphi(y_j),\\
\overline{f(\sigma y_j)}f(\sigma^2 y_j) &= \varphi(\sigma y_j),\\
\cdots &\quad \cdots\\
\overline{f(\sigma^{t-1} y_j)}f(y_j) &= \varphi(\sigma^{t-1} y_j).
\end{aligned}$$

Условия леммы 4 — это в точности необходимые и достаточные условия разрешимости этих систем. При этом общее решение задается следующим равенством

$$f(\sigma^{i+1}y_j) = f(y_j)\varphi(\sigma^i y_j)\varphi(\sigma^{i-1}y_j)\dots\varphi(y_j), \quad j = 1,\dots,k,\ i = 0,\dots,t-2,$$

причем k начальных значений $f(y_j), j = 1,\dots,k$ можно выбирать произвольным образом. ▲

Возвращаясь к кодам типа Рида—Маллера, записываем теперь определение $RM_{r-1}(G)$ в виде

$$RM_{r-1}(G) = \{f \in T_q^G : \prod_{i=1}^{r}(\sigma_i^{-1} - 1)f \equiv 1 \text{ для всех } \sigma_1,\dots,\sigma_r \in G\}.$$

Через $G(\sigma_1,\dots,\sigma_r) \in Z_qG$ обозначим следующий элемент группового кольца:

$$G(\sigma_1,\dots,\sigma_r) = \prod_{i=1}^{r}(\sigma_i^{-1} - 1) = \sum_{\sigma\in G}\lambda_\sigma\sigma.$$

При так определенных параметрах λ_σ получаем, что функция f принадлежит $RM_{r-1}(G)$ тогда и только тогда, когда для f выполнены следующие соотношения (в теории кодирования такие соотношения принято называть проверками):

$$\prod_{\sigma\in G}(f(\sigma x))^{\lambda_{\sigma^{-1}}} \equiv 1\ \forall x \in G,$$

для всех наборов λ_σ, $\sigma \in G$, которые соответствуют элементам $G(\sigma_1,\dots,\sigma_r)\ \forall\sigma_1,\dots,\sigma_r \in G$.

Теперь уже очевидно, что равенство

$$RM_N(G) = T_q^G$$

выполнено для некоторого N в том и только в том случае, если в групповом кольце Z_qG выполнено тождество

$$G(\sigma_1,\dots,\sigma_N) = 0 \text{ для всех } \sigma_1,\dots,\sigma_N \in G.$$

В силу коммутативности кольца Z_qG такое N существует тогда и только тогда, когда каждый элемент вида $\sigma - 1$, $\sigma \in G$, является нильпотентным элементом кольца Z_qG.

Л е м м а 5. *Любой элемент $\sigma - 1$, $\sigma \in G$, является нильпотентным элементом кольца Z_qG в том и только в том случае, когда число q имеет вид p^s, p — простое, s — натуральное.*

Д о к а з а т е л ь с т в о. Пусть для некоторого N в Z_qG выполнено тождество

$$(\sigma - 1)^N = 0 \quad \forall\sigma \in G,$$

и пусть p — некоторый простой делитель q. При некотором натуральном s выполнено $N \leqslant p^s$ и поэтому

$$(\sigma - 1)^{p^s} = 0 \quad \forall\sigma \in G.$$

Последнее тождество выполнено в Z_qG, а поэтому и в Z_pG. Но в Z_pG выполнено также

$$(\sigma-1)^p=\sigma^p-1\quad\forall\sigma\in G.$$

Из этих двух тождеств следует, что $\sigma^{p^s}=\mathbf{e}$ для всех σ в группе G и поэтому $q=p^{s_1}, s_1\leqslant s$.

Пусть теперь $q=p^s$. Известно (следует из теоремы Лукаса), что биномиальные коэффициенты $\binom{p^s}{k}$, $1\leqslant k<p^s$, делятся на p. Поэтому получаем

$$(\sigma-1)^{p^s}=pQ(\sigma)\quad\forall\sigma\in G$$

с некоторым многочленом $Q(\sigma)$. Перемножая несколько раз, получим нужное тождество в Z_qG:

$$(\sigma-1)^{sp^s}=p^sQ^s(\sigma)=0.\quad\blacktriangle$$

С л е д с т в и е 2. *Любая функция из T_q^G принадлежит некоторому коду типа Рида—Маллера в том и только в том случае, когда q имеет вид p^s, p — простое, s — натуральное.*

Если q не удовлетворяет условиям следствия 2, то среди функций из T_q^G могут быть и неподвижные точки операторов дифференцирования $\frac{d}{d\sigma}$.

Л е м м а 6. *Пусть порядок элемента $\sigma_0\in G$ равен t, t — делитель q. Дифференциальное уравнение*

$$\frac{df}{d\sigma_0}(x)=f(x)\quad\forall x\in G$$

имеет нетривиальное решение $f\in T_q^G$ тогда и только тогда, когда числа q и 2^t-1 имеют общий нетривиальный делитель.

Д о к а з а т е л ь с т в о. Воспользовавшись рассуждениями леммы 4, легко получить, что утверждение леммы 6 выполнено тогда и только тогда, когда выполнены тождества:

$$f(x)f(\sigma_0x)\dots f(\sigma_0^{t-1}x)\equiv 1,$$
$$f(\sigma_0^ix)\equiv\big(f(x)\big)^{2^i},\ i=1,\dots,t-1.$$

Подставляя второе равенство в первое, получаем

$$\big(f(x)\big)^{2^t-1}\equiv 1.$$

Поскольку значения $f(x)$ лежат в T_q, последнее равенство возможно для нетривиальных значений $f(x)$ тогда и только тогда, когда числа q и 2^t-1 имеют общий нетривиальный делитель. $\blacktriangle$

Примеры чисел q, t, удовлетворяющих условиям леммы 6, можно построить с помощью теоремы Эйлера. Пусть m — произвольное нечетное число. Положим $t=\varphi(m)$ (φ — функция Эйлера), $q=$ Н.О.К.(t,m). Тогда q делится на t и m, а по теореме Эйлера 2^t-1 также делится на m.

Возвратимся опять к A_0-группам и получению для них свойств, аналогичных свойствам кода $RM_1(G)$, доказанным в § 2. Пусть Φ — A_0-группа. Для любой функции $f\in T^G$ через $L_f^\Phi\subseteq G$ обозначим следующее множество:

$$L_f^\Phi=\Big\{\sigma\in G:\frac{df}{d\sigma}\in\Phi\Big\}.$$

При этом $L_f^{RM_0(G)} = L_f$ — группа линейности функции f, рассмотренная в § 2. Практически повторяя рассуждения леммы 1 и при этом используя тот факт, что Φ — A_0-группа, легко доказать следующее утверждение.

Л е м м а 7. *Множество L_f^Φ для любой $f \in T^G$ и любой A_0-группы Φ является подгруппой группы G.*

Очевидно также, что, если $\Phi_1 \subseteq \Phi_2$, то для любой $f \in T^G$ выполнено включение подгрупп

$$L_f^{\Phi_1} < L_f^{\Phi_2}.$$

Обратившись теперь к определению оператора J, замечаем, что для любой A_0-группы Φ

$$J\Phi = \left\{ f \in T_q^G : L_f^\Phi = G \right\}.$$

При $\Phi = RM_0(G)$ это равенство является содержанием теоремы 3.

Аналогично теореме 5 получаем следующее утверждение.

Т е о р е м а 7. *Пусть $\pi \in A(G)$ имеет вид*

$$x^\pi = \mathbf{e}^\pi x^w, \quad w \in Aut(G).$$

Тогда для любой функции $f \in T^G$ и любой A_0-группы Φ выполнено

$$L_{f^\pi}^\Phi = (L_f^\Phi)^w,$$

где

$$(L_f^\Phi)^w = \{ z \in G : z = \sigma^w, \quad \sigma \in L_f^\Phi \}.$$

Список литературы

1. *Хьюитт Э., Росс К.* Абстрактный гармонический анализ. Т. 1, 2. М.: Мир, 1975.

2. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.

3. *Зиновьев В.А.* Алгебраическая теория блочных кодов, исправляющих независимые ошибки // Итоги науки и техники. М.: ВИНИТИ, 1976. С. 189-234.

4. *Общая алгебра.* Т. 1. М.: Наука, 1990.

5. *Берман С.Д.* К теории групповых кодов // Кибернетика. 1967. N 1. С. 31–39.

6. *Грушко И.И.* О мажоритарном декодировании обобщенных кодов Рида—Маллера // Пробл. передачи информ. 1990. Т. 26. N 3. С. 12–20.

7. *Дельсарт Ф.* Алгебраический подход к схемам отношений теории кодирования. М.: Мир, 1976.

8. *Зиновьев В.А., Эриксон Т.* О фурье-инвариантных разбиениях конечных абелевых групп и тождестве Мак-Вильямс для групповых кодов // Пробл. передачи информ. 1996. Т. 32. N 1. С. 137–143.