Применение различных способов задания аддитивных характеров конечного поля к изучению свойств дискретных функций

В. Г. Рябов*

Наряду с каноническим способом задания аддитивных характеров конечного поля составного порядка предложен альтернативный способ - на основе векторного представления поля. Для обоих способов найдены множества групп характеров с различной параметризацией и установлены отношения между ними. Получены формулы, связывающие разностные и нелинейные свойства отображений над конечными полями со спектрами Фурье их характеров.

Ключевые слова: конечное поле, характер, векторная функция, разностный спектр, нелинейность, коэффициенты Фурье.

Решается *задача*: определить еще один способ задания аддитивных характеров конечного поля составного порядка, показать его связь с широко применяемым каноническим способом задания, а также продемонстрировать преимущества каждого из способов при исследовании важных с точки зрения приложений на базе ИИ свойств векторных функций над конечными полями с использованием аппарата гармонического анализа.

Пусть $\mathbb{F}_q$ – поле из q элементов, где $q = p^r$, а $(\mathbb{F}_q, +)$ – его аддитивная группа. Простое поле $\mathbb{F}_p$ изоморфно кольцу вычетов $\mathbb{Z}_p$. Характер группы $(\mathbb{F}_p q, +)$ с индексом a задается соотношением $\chi_a(x) = e^{\frac{2\pi i}{p}ax}$. Для полей составного порядка ($r \geqslant 2$) аналогом $\mathbb{Z}_p$ выступает факторкольцо многочленов $\mathbb{F}_p[x]/(g(x))$, где $g(x)$ – неприводимый унитарный многочлен над $\mathbb{F}_p$ степени r, от выбора которого зависит умножение в полях составного порядка $q > 4$. *Канонический характер* определяется как $\chi_1(x) = e^{\frac{2\pi i}{p}Tr(x)}$, где $Tr(x)$ – функция абсолютного следа. Остальные аддитивные характеры имеют вид $\chi_a(x) = \chi_1(ax) = e^{\frac{2\pi i}{p}Tr(ax)}$. В поле составного порядка индексация одних и тех же аддитивных характеров в группе зависит от задания умножения и, соответственно, выбора многочлена $g(x)$. Обозначим через $\mathbf{G}\chi(r, p)$ множество групп канонически заданных характеров с различной параметризацией.

Как и в [2], определим альтернативные аддитивные характеры. Обозначим $\mathbb{F}_q^n$ пространство размерности n над полем $\mathbb{F}_q$. Всякое поле $\mathbb{F}_q$ можно

* *Рябов Владимир Геннадьевич* — канд. физ.-мат. наук, независимый исследователь, e-mail: 4vryabov@gmail.com, ORCID: 0000-0001-6981-4238.

Ryabov Vladimir Gennadievich — cand. phys.-math. scien., independent researcher.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

представить пространством $\mathbb{F}_p^r$. Пусть базис Θ пространства $\mathbb{F}_p^r$ состоит из векторов $\theta_1, \dots \theta_r$. Тогда каждый элемент $a \in \mathbb{F}_q$ однозначно представляется комбинацией $\tilde{a}_1\theta_1 + \dots + \tilde{a}_r\theta_r$, где $\tilde{a}_1, \dots \tilde{a}_r \in \mathbb{F}_p$. Вектор $(\tilde{a}_1, \dots, \tilde{a}_r) \in \mathbb{F}_p^r$ будем называть *проекцией элемента a в базисе Θ*. Для элементов a и b поля $\mathbb{F}_q$ через $\langle a, b\rangle_\Theta$ будем обозначать скалярное произведение их проекций в базисе Θ. Тогда *альтернативный аддитивный характер* поля имеет вид $\psi_a^\Theta(x) = \prod_{j=1}^r \chi_{\tilde{a}_j}(\tilde{x}_j) = e^{\frac{2\pi i}{p}\sum_{j=1}^r \tilde{a}_j\tilde{x}_j} = e^{\frac{2\pi i}{p}\langle a,x\rangle_\Theta}$. В отличие от канонического задания индексация альтернативных характеров не связана с умножением, но зависит от выбора базиса Θ. Невырожденные линейные преобразования пространства $\mathbb{F}_p^r$, сохраняющие скалярное произведение, задают базисы с одинаковой индексацией и образуют ортогональную группу с известным порядком. Тогда мощность множества групп альтернативных характеров с различной параметризацией $\mathbf{G}\psi(r,p)$ определяется как частное от деления числа базисов на порядок ортогональной группы. Определим отношение между множествами групп характеров при каноническом и альтернативном задании.

Теорема 1. *Для полей порядка q, где $q = p^r$ и $r \geqslant 2$, в случаях четного q или нечетных q и r имеем включение $\boldsymbol{G}\chi(r,p) \subset \boldsymbol{G}\psi(r,p)$, а в случае нечетного q и четного r – соотношение $\boldsymbol{G}\chi(r,p) \cap \boldsymbol{G}\psi(r,p) = \varnothing$.*

При доказательстве Теоремы 1 использовались результаты [4] о существовании *самодуального базиса* относительно абсолютного следа. Теорема 1 позволяет для большинства составных полей найти канонически заданные характеры через альтернативные в самодуальном базисе.

На основе заданных канонически характеров поля $\mathbb{F}_q$ можно определить характеры векторного пространства $\mathbb{F}_q^n$ следующим образом: $\chi_{\boldsymbol{a}}(\boldsymbol{x}) = e^{\frac{2\pi i}{p}Tr\left(\langle \boldsymbol{a},\boldsymbol{x}\rangle\right)}$, где $\boldsymbol{a} = (a_1, \dots a_n)$, $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$, а $\langle \boldsymbol{a}, \boldsymbol{x}\rangle$ – скалярное произведение в $\mathbb{F}_q^n$. В случае альтернативных характеров имеем $\psi_{\boldsymbol{a}}^\Theta(\boldsymbol{x}) = e^{\frac{2\pi i}{p}\sum_{t=1}^n \langle a_t,x_t\rangle_\Theta}$. Каждое из множеств $\{\chi_{\boldsymbol{a}}(\boldsymbol{x}) \mid \boldsymbol{a} \in \mathbf{F}_q^n\}$ и $\{\psi_{\boldsymbol{a}}^\Theta(\boldsymbol{x}) \mid \boldsymbol{a} \in \mathbf{F}_q^n\}$ образует мультипликативную группу характеров пространства $\mathbf{F}_q^n$, изоморфную $(\mathbf{F}_q^n, +)$, и является ортонормированным базисом пространства комплекснозначных отображений пространства $\mathbf{F}_q^n$.

Обозначим через $P_q^{n,m}$ множество отображений $\mathbf{F}_q^n$ в $\mathbf{F}_q^m$. Будем также называть их *векторными функциями*. Пусть $\phi_{\boldsymbol{b}}$ – аддитивный характер пространства $\mathbb{F}_q^m$, заданный любым из двух способов. Тогда по аналогии с [2, 3] назовем *характером векторной функции* $F \in P_q^{n,m}$ комплекснозначную композицию характера $\phi_{\boldsymbol{b}}$ и самого отображения F вида $\phi_{\boldsymbol{b}}(F(\boldsymbol{x}))$. Разложение $\phi_{\boldsymbol{b}}(F(\boldsymbol{x}))$ в ряд Фурье по базису $\{\phi_{\boldsymbol{a}}(\boldsymbol{x}) \mid \boldsymbol{a} \in \mathbf{F}_q^n\}$ имеет вид $\phi_{\boldsymbol{b}}(F(\boldsymbol{x})) = \sum_{\boldsymbol{a}\in\mathbb{F}_q^n} c_{\boldsymbol{b}}^F(\boldsymbol{a})\phi_{\boldsymbol{a}}(\boldsymbol{x})$, где $c_{\boldsymbol{b}}^F(\boldsymbol{a}) =$

$\frac{1}{q^n}\sum_{\boldsymbol{x}\in\mathbf{F}_q^n}\phi_{\boldsymbol{b}}(F(\boldsymbol{x}))\overline{\phi_{\boldsymbol{a}}(\boldsymbol{x})}$. В случае канонического и альтернативного задания коэффициенты имеют вид $c_{\boldsymbol{b}}^F(\boldsymbol{a})=\frac{1}{q^n}\sum_{\boldsymbol{x}\in\mathbf{F}_q^n}e^{\frac{2\pi i}{p}Tr\left(\langle\boldsymbol{b},F(\boldsymbol{x})\rangle-\langle\boldsymbol{a},\boldsymbol{x}\rangle\right)}$ и $c_{\boldsymbol{b}}^{F,\Theta}(\boldsymbol{a})=\frac{1}{q^n}\sum_{\boldsymbol{x}\in\mathbf{F}_q^n}e^{\frac{2\pi i}{p}\left(\sum_{s=1}^m\langle b_s,f_s(\boldsymbol{x})\rangle_\Theta-\sum_{t=1}^n\langle a_t,x_t\rangle_\Theta\right)}$, где $(f_1,\ldots,f_m)$ – набор координатных функций отображения F.

Разностным спектром векторной функции $F\in P_q^{n,m}$ называется множество значений $\delta_{\boldsymbol{v}}^F(\boldsymbol{u})=|\{\boldsymbol{x}\in\mathbf{F}_q^n\mid F(\boldsymbol{x}+\boldsymbol{u})-F(\boldsymbol{x})=\boldsymbol{v}\}|$ для всевозможных $\boldsymbol{u}\in\mathbf{F}_q^n$ и $\boldsymbol{v}\in\mathbf{F}_q^m$. Поскольку этот спектр не зависит от операции умножения, воспользуемся альтернативными характерами.

Теорема 2. *Пусть $F\in P_q^{n,m}$, Θ – базис $\mathbb{F}_p^r$. Тогда для $\forall\boldsymbol{u}\in\mathbf{F}_q^n$ и $\forall\boldsymbol{v}\in\mathbf{F}_q^m$*

$$\delta_{\boldsymbol{v}}^F(\boldsymbol{u})=q^{n-m}\sum_{\boldsymbol{b}\in\mathbf{F}_q^m}\sum_{\boldsymbol{a}\in\mathbf{F}_q^n}|c_{\boldsymbol{b}}^{F,\Theta}(\boldsymbol{a})|^2\;e^{\frac{2\pi i}{p}\left(\sum_{s=1}^m\langle b_s,v_s\rangle_\Theta-\sum_{t=1}^n\langle a_t,u_t\rangle_\Theta\right)},$$

а для $\forall\boldsymbol{a}\in\mathbf{F}_q^n$ и $\forall\boldsymbol{b}\in\mathbf{F}_q^m$ имеем[1]

$$|c_{\boldsymbol{b}}^{F,\Theta}(\boldsymbol{a})|^2=\frac{1}{q^{2n}}\sum_{\boldsymbol{v}\in\mathbf{F}_q^m}\sum_{\boldsymbol{u}\in\mathbf{F}_q^n}\delta_{\boldsymbol{v}}^F(\boldsymbol{u})\;e^{-\frac{2\pi i}{p}\left(\sum_{s=1}^m\langle b_s,v_s\rangle_\Theta-\sum_{t=1}^n\langle a_t,u_t\rangle_\Theta\right)}.$$

Обозначим через $\mathbf{M}_q^{m,n}$ множество матриц $m\times n$ над $\mathbf{F}_q$. Всякое аффинное отображение $A\in P_q^{n,m}$ может быть представлено в виде $\boldsymbol{a}_0+\mathbf{A}\boldsymbol{x}$, где $\boldsymbol{a}_0=(a_{1,0},\ldots,a_{m,0})^T\in\mathbf{F}_q^m$, $\mathbf{A}\in\mathbf{M}_q^{m,n}$, а $\boldsymbol{x}=(x_1,\ldots,x_n)^T\in\mathbf{F}_q^n$. Пусть A соответствует матрица $[\boldsymbol{a}_0,\mathbf{A}]\in\mathbf{M}_q^{m,n+1}$, полученная добавлением $\boldsymbol{a}_0$ левым столбцом к $\mathbf{A}$. Для отображений F и G из $P_q^{n,m}$ обозначим через $C(F,G)$ число аргументов с одинаковыми значениями. Тогда под *спектром нелинейности* векторной функции $F\in P_q^{n,m}$ будем понимать множество значений вида $\mathfrak{d}_{[\boldsymbol{a}_0,\mathbf{A}]}^F=\frac{C(F,A)}{q^n}-\frac{1}{q^m}$ для всех аффинных отображений $A\in P_q^{n,m}$, где матрица $[\boldsymbol{a}_0,\mathbf{A}]$ отвечает A. Он зависит от умножения, и здесь используем канонически заданные характеры.

Теорема 3. *Пусть $F\in P_q^{n,m}$. Тогда для $\forall[\boldsymbol{a}_0,\boldsymbol{A}]\in\boldsymbol{M}_q^{m,n+1}$ имеем*

$$\mathfrak{d}_{[\boldsymbol{a}_0,\boldsymbol{A}]}^F=\frac{1}{q^m}\sum_{\boldsymbol{b}\in\mathbf{F}_q^m\setminus\{\boldsymbol{0}\}}c_{\boldsymbol{b}}^F(\boldsymbol{b}\boldsymbol{A})\;e^{-\frac{2\pi i}{p}Tr(\langle\boldsymbol{b},\boldsymbol{a}_0\rangle)},$$

а для $\forall\boldsymbol{b}\in\mathbf{F}_q^m\setminus\{\boldsymbol{0}\}$ и $\forall\boldsymbol{a}\in\mathbf{F}_q^n$ справедливо равенство

$$c_{\boldsymbol{b}}^F(\boldsymbol{a})=\sum_{\boldsymbol{a}_0\in\mathbf{F}_q^m}\mathfrak{d}_{[\boldsymbol{a}_0,\boldsymbol{A}_{\boldsymbol{b},\boldsymbol{a}}]}^F\;e^{\frac{2\pi i}{p}Tr(\langle\boldsymbol{b},\boldsymbol{a}_0\rangle)},$$

где матрица $\boldsymbol{A}_{\boldsymbol{b},\boldsymbol{a}}\in\boldsymbol{M}_q^{m,n}$ выбирается так, что $\boldsymbol{b}\boldsymbol{A}_{\boldsymbol{b},\boldsymbol{a}}=\boldsymbol{a}$.

[1] Для скалярной функции аналогичное равенство было представлено в [1].

Список литературы

[1] А. С. Амбросимов, "Свойства бент-функций q-значной логики над конечными полями", *Дискретная математика*, **6**:3 (1994), 50–60.

[2] В. Г. Рябов, "Нелинейность векторных функций над конечными полями", *Дискретная математика*, **36**:2 (2024), 50–70. DOI: 10.4213/dm1822.

[3] В. И. Солодовников, "Бент-функции из конечной абелевой группы в конечную абелеву группу", *Дискретная математика*, **14**:1 (2002), 99–113. DOI: 10.4213/dm234.

[4] G. Seroussi, A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields", *SIAM Jour. on Comp.*, **9**:4 (1980), 758–767. DOI: 10.1137/0209059.

Статья поступила 9 ноября 2026 г.

Application of various methods for defining additive characters of a finite field to the study of the properties of discrete functions

V. G. Ryabov

In addition to the canonical method of defining additive characters of a finite field of composite order via the absolute trace function, an alternative approach is proposed, based on the vector-space representation of the field. For both methods, sets of character groups with distinct parameterizations are identified, and the relationships between them are established. Formulas are derived that link the differential and nonlinear properties of mappings over finite fields to the Fourier spectra of their characters.

Keywords: finite field, character, vectorial function, difference spectrum, nonlinearity, Fourier coefficients.

References

[1] A. S. Ambrosimov, "Properties of bent functions of q-valued logic over finite fields", *Diskretnaya Matematika*, **6**:3 (1994), 50–60 (in Russian).

[2] V. G. Ryabov, "Nonlinearity of vectorial functions over finite fields", *Diskretnaya Matematika*, **36**:2 (2024), 50–70 (in Russian).

[3] V. I. Solodovnikov, "Bent functions from a finite abelian group into a finite abelian group", *Diskretnaya Matematika*, **14**:1 (2002), 99–113 (in Russian).

[4] G. Seroussi, A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields", *SIAM Jour. on Comp.*, **9**:4 (1980), 758–767.

Received on November 9, 2026