ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.115, 519.113.5, 512.624, 512.552.7

О ЧИСЛЕ ОДНОРОДНЫХ НЕВЫРОЖДЕННЫХ p-ИЧНЫХ ФУНКЦИЙ ЗАДАННОЙ СТЕПЕНИ[1]

М. И. Анохин

Институт проблем информационной безопасности Московского государственного университета имени М. В. Ломоносова, г. Москва, Россия

Пусть p — простое число, $F = \mathrm{GF}(p)$, V_n — n-мерное векторное пространство над F, e — базис пространства V_n. Пусть также $\varphi\colon V_n \to F$. Функция φ называется e-однородной, если $\varphi(x) = \pi_{\varphi,e}(\mathbf{x})$ для всех $x \in V_n$, где $\pi_{\varphi,e}$ — однородный многочлен от n переменных над F, имеющий степень не более $p-1$ по каждой переменной, а $\mathbf{x}$ — набор координат вектора x в базисе e. Функция φ называется невырожденной, если $\deg\varphi \geqslant 1$ и $\deg \partial_v\varphi = (\deg\varphi) - 1$ для любого $v \in V_n \setminus \{0\}$, где $(\partial_v\varphi)(x) = \varphi(x+v) - \varphi(x)$ для всех $v, x \in V_n$. Получена формула для числа $\mathrm{HN}_p(n,d)$ e-однородных невырожденных функций $\varphi\colon V_n \to F$, имеющих степень d (это число не зависит от e), а именно: если $n \geqslant 1$ и $d \in \{1,\dots,n(p-1)\}$, то $\mathrm{HN}_p(n,d) = \sum\limits_{k=0}^{n} (-1)^k p^{\binom{k}{2}+\left\{{n-k \atop d}\right\}_p} \begin{bmatrix} n \\ k \end{bmatrix}_p = \sum\limits_{S\subseteq\{1,\dots,n\}} (-1)^{|S|} p^{\sigma(S)-|S|+\left\{{n-|S| \atop d}\right\}_p}$, где $\left\{{m \atop d}\right\}_p$ — обобщённый биномиальный коэффициент порядка p; $\begin{bmatrix} n \\ k \end{bmatrix}_p$ — биномиальный коэффициент Гаусса; $\sigma(S)$ — сумма всех элементов множества S. Доказано, что $\mathrm{HN}_p(n,d) \geqslant p^{\left\{{n \atop d}\right\}_p} - 1 - (p^n-1)\left(p^{\left\{{n-1 \atop d}\right\}_p} - 1\right)/(p-1)$ для любых $d \geqslant 1$ и $n \geqslant d/(p-1)$. Используя эту оценку, получаем, что если $d \geqslant 3$, то $\mathrm{HN}_p(n,d) \sim p^{\left\{{n \atop d}\right\}_p}$ при $n \to \infty$.

Ключевые слова: *p-ичная функция, однородная функция, невырожденная функция, степень функции, формула обращения Мёбиуса, групповая алгебра, фундаментальный идеал, базис Дженнингса.*

DOI 10.17223/20710410/41/1

ON THE NUMBER OF HOMOGENEOUS NONDEGENERATE p-ARY FUNCTIONS OF THE GIVEN DEGREE

M. I. Anokhin

Information Security Institute, Lomonosov University, Moscow, Russia

E-mail: anokhin@mccme.ru

[1]Работа поддержана грантом РФФИ № 16-01-00226.

Let p be a prime number and $F = \mathrm{GF}(p)$. Suppose V_n is an n-dimensional vector space over F and e is a basis of V_n. Also, let $\varphi\colon V_n \to F$. The function φ is called e-homogeneous if $\varphi(x) = \pi_{\varphi,e}(\mathbf{x})$ for all $x \in V_n$, where $\pi_{\varphi,e}$ is an n-variate homogeneous polynomial over F of degree at most $p-1$ in each variable and $\mathbf{x}$ is the coordinate vector of x with respect to the basis e. The function φ is said to be nondegenerate if $\deg\varphi \geqslant 1$ and $\deg\partial_v\varphi = (\deg\varphi) - 1$ for any $v \in V_n \setminus \{0\}$, where $(\partial_v\varphi)(x) = \varphi(x+v) - \varphi(x)$ for all $v, x \in V_n$. This notion was introduced by O. A. Logachev, A. A. Sal'nikov, and V. V. Yashchenko in the case when $p = 2$. Our main results are as follows. First, we obtain a formula for the number $\mathrm{HN}_p(n,d)$ of e-homogeneous nondegenerate functions $\varphi\colon V_n \to F$ of degree d (this number does not depend on e). Namely, if $n \geqslant 1$ and $d \in \{1,\ldots,n(p-1)\}$, then $\mathrm{HN}_p(n,d) = \sum\limits_{k=0}^{n}(-1)^k p^{\binom{k}{2}+\left\{{n-k \atop d}\right\}_p}\begin{bmatrix} n \\ k \end{bmatrix}_p = \sum\limits_{S\subseteq\{1,\ldots,n\}}(-1)^{|S|}p^{\sigma(S)-|S|+\left\{{n-|S| \atop d}\right\}_p}$, where $\left\{{m \atop d}\right\}_p$ is the generalized binomial coefficient of order p, $\begin{bmatrix} n \\ k \end{bmatrix}_p$ is the Gaussian binomial coefficient, and $\sigma(S)$ is the sum of all elements of S. The proof of this formula is based on the Möbius inversion. Previously, only formulas for $\mathrm{HN}_p(n,2)$ were known; unlike our formula, their forms depend on the parities of p and n. Second, we prove that $\mathrm{HN}_p(n,d) \geqslant p^{\left\{{n \atop d}\right\}_p - 1 - (p^n-1)\left(p^{\left\{{n-1 \atop d}\right\}_p}-1\right)/(p-1)}$ for any $d \geqslant 1$ and $n \geqslant d/(p-1)$. Using this bound, we obtain that if $d \geqslant 3$, then $\mathrm{HN}_p(n,d) \sim p^{\left\{{n \atop d}\right\}_p}$ as $n \to \infty$. For $p = 2$ the last two statements were proved by Yu. V. Kuznetsov. The proofs of our main results use a Jennings basis of the group algebra FG_n, where G_n is an elementary abelian p-group of rank n.

Keywords: *p-ary function, homogeneous function, nondegenerate function, degree of a function, Möbius inversion formula, group algebra, augmentation ideal, Jennings basis.*

1. Определения, обозначения и необходимые факты

Фиксируем простое число p и обозначим через F поле из p элементов. В настоящей работе все объекты и понятия линейной алгебры рассматриваются над основным полем F. Для произвольного множества X через F^X обозначается множество всех функций из X в F. Это множество является векторным пространством относительно поточечных операций сложения и умножения на элементы из F. Если S — какая-либо система векторов произвольного векторного пространства, то $\langle S\rangle$ обозначает линейную оболочку этой системы. Пусть также n — произвольное целое неотрицательное число и V_n — n-мерное векторное пространство (над полем F). Элементы множества F^{V_n} естественно назвать *p-ичными функциями*.

Выберем какой-либо базис $e = (e_1,\ldots,e_n)$ пространства V_n. Иногда будем выбирать этот базис некоторым специальным образом. Пусть также $\varphi \in F^{V_n}$. Тогда хорошо известно, что существует единственный многочлен $\pi_{\varphi,e} = \pi_{\varphi,e}(t) \in F[t_1,\ldots,t_n]$ (зависящий от φ и e), который имеет степень не более $p-1$ по каждой переменной и удовлетворяет равенству

$$\varphi(x_1e_1 + \ldots + x_ne_n) = \pi_{\varphi,e}(x_1,\ldots,x_n)$$

для любых $x_1,\ldots,x_n \in F$. Другими словами, если x — произвольный вектор из V_n и $\mathbf{x}$ — набор координат этого вектора в базисе e, то $\varphi(x) = \pi_{\varphi,e}(\mathbf{x})$. Функция $\varphi \mapsto \pi_{\varphi,e}$

($\varphi \in F^{V_n}$) является изоморфизмом векторного пространства F^{V_n} на векторное пространство всех многочленов из $F[t_1, \ldots, t_n]$, имеющих степень не более $p-1$ по каждой переменной.

Напомним, что *производной* функции φ по направлению $v \in V_n$ называется функция $\partial_v\varphi \in F^{V_n}$, определённая равенством $(\partial_v\varphi)(x) = \varphi(x+v)-\varphi(x)$ для каждого $x \in V_n$. *Степенью* функции φ, обозначаемой $\deg\varphi$, называется степень многочлена $\pi_{\varphi,e}$. Считаем, что степень нулевого многочлена (а следовательно, и степень нулевой функции из F^{V_n}) равна -1. Определённая таким образом степень функции φ не зависит от выбора базиса e, так как она совпадает с наименьшим целым числом $d \geqslant -1$, для которого $\partial_{v_1} \ldots \partial_{v_{d+1}}\varphi = 0$ при всех $v_1, \ldots, v_{d+1} \in V_n$ [1, свойство B7]. Очевидно, что $-1 \leqslant \deg\varphi \leqslant n(p-1)$ и что если $\deg\varphi \geqslant 0$, то $\deg\partial_v\varphi \leqslant \deg\varphi - 1$ для любого $v \in V_n$. Кроме того, если $d \in \{-1, \ldots, n(p-1)\}$, то множество $\mathrm{RM}_d = \{\psi \in F^{V_n} : \deg\psi \leqslant d\}$ является подпространством пространства F^{V_n}. Обозначение RM_d связано с тем, что именно так можно определить p-ичный код Рида—Маллера порядка d и длины p^n.

Функция φ называется *e-однородной*, если $\pi_{\varphi,e}$ является однородным многочленом (к которым относится и нулевой многочлен). Очевидно, что всякая e-однородная функция степени не более $p-1$ будет также e'-однородной для любого базиса e' пространства V_n. Поэтому можно говорить просто об однородных функциях степени не более $p-1$. Однако в общем случае однородность функции φ зависит от выбора базиса e. Например, пусть $n = 2$ и функция $\psi \in F^{V_2}$ такова, что $\pi_{\psi,e} = t_1^{p-1}t_2$. Тогда если $e' = (e_1 + e_2, e_2)$, то $\pi_{\psi,e'} = t_1 + t_1^{p-1}t_2$. Таким образом, функция ψ e-однородна, но не e'-однородна.

Замечание 1. Очевидно, что функция φ представима единственным образом в виде $\varphi_{(0,e)} + \ldots + \varphi_{(d,e)}$, где $d = \deg\varphi$, а $\varphi_{(i,e)}$ — либо e-однородная функция степени i из F^{V_n}, либо нулевая функция из F^{V_n} ($i \in \{0, \ldots, d\}$), причём если $d \geqslant 0$, то $\varphi_{(d,e)} \neq 0$. Функция $\varphi_{(i,e)}$ называется *i-й e-однородной компонентой* функции φ.

Предположим, что $\deg\varphi \geqslant 1$ (это возможно, если и только если $n \geqslant 1$). Тогда полагаем

$$L(\varphi) = \{v \in V_n : \deg\partial_v\varphi \leqslant \deg\varphi - 2\}.$$

Легко видеть, что $L(\varphi)$ является собственным подпространством пространства V_n. Можно также сказать, что $L(\varphi)$ — группа инерции смежного класса $\varphi + \mathrm{RM}_{(\deg\varphi)-2}$ в группе сдвигов пространства V_n, если отождествить сдвиг $x \mapsto x + v$ на вектор $v \in V_n$ с самим этим вектором. Очевидно, что RM_d для любого $d \in \{-1, \ldots, n(p-1)\}$ замкнуто относительно сдвигов аргумента функции. Будем пользоваться тем, что если $\varphi' \in \varphi + \mathrm{RM}_{(\deg\varphi)-1}$, то $L(\varphi') = L(\varphi)$. Функция φ называется *невырожденной*, если $L(\varphi) = \{0\}$, или, что эквивалентно, $\deg\partial_v\varphi = \deg\varphi - 1$ для любого $v \in V_n \setminus \{0\}$. Понятие невырожденной функции введено в [2] в случае, когда $p = 2$ (см. также [3, определение 3.5.2]). Основной смысл этого понятия состоит в следующей теореме (в случае $p = 2$ см. [2, теорема 3] или [3, теорема 3.5.3]):

Теорема 1. Пусть $\varphi \in F^{V_n}$, причём $\deg\varphi = d \geqslant 1$. Предположим, что $L(\varphi) = \langle e_{m+1}, \ldots, e_n\rangle$ для некоторого $m \in \{1, \ldots, n\}$. Тогда существуют функции $\varphi' \in F^{V_n}$ и $\psi \in F^{V_n/L(\varphi)}$, удовлетворяющие следующим условиям:

1) $\deg\varphi' \leqslant d - 1$;
2) ψ имеет степень d, $(e_1 + L(\varphi), \ldots, e_m + L(\varphi))$-однородна и невырождена;
3) $\varphi(x) = \varphi'(x) + \psi(x + L(\varphi))$ для всех $x \in V_n$.

Теорема 1 может быть легко доказана по схеме, описанной в [2] и [3, разд. 3.5] (хотя в обоих этих источниках подробное доказательство не приводится), а именно: пусть

$\varphi_{(d,e)}$ — d-я e-однородная компонента функции φ (см. замечание 1). Непосредственно проверяется, что многочлен $\pi_{\varphi_{(d,e)},e}$ не зависит от переменных $t_{m+1},\dots,t_n$. Следовательно, существует функция $\psi \in F^{V_n/L(\varphi)}$, такая, что $\varphi_{(d,e)}(x) = \psi(x + L(\varphi))$ для всех $x \in V_n$. Из равенства

$$\pi_{\psi,(e_1+L(\varphi),\dots,e_m+L(\varphi))}(t_1,\dots,t_m) = \pi_{\varphi_{(d,e)},e}(t_1,\dots,t_m)$$

вытекает п. 2 теоремы 1. Поэтому $\varphi' = \varphi - \varphi_{(d,e)}$ и ψ удовлетворяют условиям этой теоремы.

Пусть $d \in \{1,\dots,n(p-1)\}$ (и, следовательно, $n \geqslant 1$). В связи с теоремой 1 представляет интерес нахождение числа e-однородных невырожденных функций из F^{V_n}, имеющих степень d. Это число будем обозначать через $\mathrm{HN}_p(n,d)$.

Замечание 2. Пусть $\alpha \in (\mathrm{RM}_d/\mathrm{RM}_{d-1}) \setminus \{0\}$, где $d \in \{1,\dots,n(p-1)\}$. Определим $L(\alpha)$ как $L(\chi)$ для произвольной функции χ из смежного класса α; корректность этого определения очевидна. Из замечания 1 следует, что в смежном классе α содержится ровно одна e-однородная функция, а именно d-я e-однородная компонента произвольной функции из этого смежного класса. Это показывает, что

$$\mathrm{HN}_p(n,d) = |\{\alpha \in (\mathrm{RM}_d/\mathrm{RM}_{d-1}) \setminus \{0\} : L(\alpha) = \{0\}\}|.$$

В частности, $\mathrm{HN}_p(n,d)$ не зависит от выбора базиса e.

Легко видеть, что

$$\mathrm{HN}_p(n,1) = \begin{cases} p-1, & \text{если } n = 1, \\ 0, & \text{если } n \geqslant 2. \end{cases} \tag{1}$$

Приведём теперь формулы для $\mathrm{HN}_p(n,2)$. Пусть φ — e-однородная функция степени 2 из F^{V_n}. Тогда существует единственная ненулевая матрица $A_{\varphi,e}$ размера $n \times n$ над F с нулями под главной диагональю (а при $p = 2$ и на главной диагонали), такая, что $\pi_{\varphi,e} = tA_{\varphi,e}t^{\mathrm{T}}$. Здесь и далее $t = (t_1,\dots,t_n)$ — набор переменных, а верхний индекс «$^{\mathrm{T}}$» обозначает транспонирование. Непосредственно проверяется, что $\pi_{\partial_v\varphi,e} = \mathbf{v}(A_{\varphi,e} + A_{\varphi,e}^{\mathrm{T}})t^{\mathrm{T}} + \mathbf{v}A_{\varphi,e}\mathbf{v}^{\mathrm{T}}$ для любого $v \in V_n$, где $\mathbf{v}$ — набор координат вектора v в базисе e. Поэтому функция φ невырождена тогда и только тогда, когда матрица $A_{\varphi,e} + A_{\varphi,e}^{\mathrm{T}}$ невырождена. Отметим, что $A_{\varphi,e} + A_{\varphi,e}^{\mathrm{T}}$ является матрицей симметричной билинейной формы $(x,y) \mapsto \varphi(x+y) - \varphi(x) - \varphi(y)$ $(x,y \in V_n)$, ассоциированной с φ как квадратичной формой, в базисе e. Это показывает, что функция φ невырождена в смысле настоящей работы тогда и только тогда, когда она невырождена как квадратичная форма (т. е. ассоциированная с ней билинейная форма невырождена).

Из этих рассуждений следует, что функция $\varphi \mapsto A_{\varphi,e} + A_{\varphi,e}^{\mathrm{T}}$ инъективно отображает множество всех e-однородных невырожденных функций степени 2 из F^{V_n} на множество всех невырожденных симметричных матриц размера $n \times n$ над F (а при $p = 2$, кроме того, имеющих на главной диагонали лишь нули). Поэтому $\mathrm{HN}_p(n,2)$ равно числу таких матриц, которое давно известно. Это число можно найти, используя классификацию невырожденных симметричных (при $p \neq 2$) и симплектических (при $p = 2$) билинейных форм над F и формулы для порядков линейных групп, сохраняющих эти формы. Однако удобнее воспользоваться формулами, приведёнными в теоремах 2 и 3 работы [4]. Таким образом, если q — нечётное простое число и m — целое положительное число, то

$$\begin{aligned} &\mathrm{HN}_q(2m-1,2) = q^{m^2-m}\prod_{i=0}^{m-1}(q^{2i+1}-1), \quad \mathrm{HN}_q(2m,2) = q^{m^2+m}\prod_{i=0}^{m-1}(q^{2i+1}-1),\\ &\mathrm{HN}_2(2m-1,2) = 0, \qquad\qquad\qquad\quad \mathrm{HN}_2(2m,2) = 2^{m^2-m}\prod_{i=0}^{m-1}(2^{2i+1}-1). \end{aligned} \tag{2}$$

2. Формулировки основных результатов

Одним из основных результатов настоящей работы является формула для $\mathrm{HN}_p(n,d)$ (см. теорему 2 ниже). Эта формула доказывается с помощью формулы обращения Мёбиуса. В отличие от формул (2) для $\mathrm{HN}_p(n,2)$, вид нашей формулы не зависит ни от чётности p, ни от чётности n. Введём некоторые обозначения. Пусть m — целое неотрицательное число. Положим

$$J_m = \{(j_1,\dots,j_m) : j_1,\dots,j_m \in \{0,\dots,p-1\}\}. \tag{3}$$

Для каждого $j \in J_m$ обозначим через $\sigma(j)$ сумму всех элементов набора j. Тогда для произвольного целого числа k *обобщённый биномиальный коэффициент* $\left\{{m \atop k}\right\}_p$ *порядка* p определяется как $|\{j \in J_m : \sigma(j) = k\}|$. Отметим, что при $k \geqslant 0$ $\left\{{m \atop k}\right\}_p$ — это число способов размещения k одинаковых предметов в m ячейках, в каждой из которых число предметов не может превосходить $p-1$ [5, разд. 1.3]. Если $k \leqslant -1$, то $\left\{{m \atop k}\right\}_p = 0$. Очевидно, что функция $(j_1,\dots,j_m) \mapsto (p-1-j_1,\dots,p-1-j_m)$ инъективно отображает множество $\{j \in J_m : \sigma(j) = k\}$ на множество $\{j \in J_m : \sigma(j) = m(p-1)-k\}$. Поэтому

$$\left\{{m \atop m(p-1)-k}\right\}_p = \left\{{m \atop k}\right\}_p \tag{4}$$

для любого целого числа k (см. также формулу (1.14) из [5]).

Кроме того, для произвольного $k \in \{0,\dots,n\}$ через $\begin{bmatrix} n \\ k \end{bmatrix}_p$ будем обозначать число k-мерных подпространств пространства V_n (*биномиальный коэффициент Гаусса*, или *квантовый биномиальный коэффициент*). Известно, что

$$\begin{bmatrix} n \\ k \end{bmatrix}_p = \prod_{i=1}^{k}\frac{p^{n-i+1}-1}{p^i-1} = \frac{\prod_{i=1}^{n}(p^i-1)}{\prod_{i=1}^{k}(p^i-1)\prod_{i=1}^{n-k}(p^i-1)} \tag{5}$$

(см. пример 2.64 и подразд. C разд. 1 гл. III (в частности, формулы (3.11) и (3.12) из [6], а также формулу (6.4) из [7] и формулы (1.5), (1.6) из [5]).

Теорема 2. Пусть $n \geqslant 1$ и $d \in \{1,\dots,n(p-1)\}$. Тогда

$$\mathrm{HN}_p(n,d) = \sum_{k=0}^{n}(-1)^k p^{\binom{k}{2}+\left\{{n-k \atop d}\right\}_p}\begin{bmatrix} n \\ k \end{bmatrix}_p = \sum_{S\subseteq\{1,\dots,n\}}(-1)^{|S|}p^{\sigma(S)-|S|+\left\{{n-|S| \atop d}\right\}_p}, \tag{6}$$

где $\sigma(S)$ — сумма всех элементов множества $S \subseteq \{1,\dots,n\}$.

Формула (6) имеет не очень простой вид. Поэтому представляет интерес вопрос об асимптотике $\mathrm{HN}_p(n,d)$ при фиксированных p и d и при $n\to\infty$. Случай, когда $d=1$, тривиален ввиду формулы (1). Рассмотрим теперь случай, когда $d=2$. Пусть, как и в формулах (2), q — нечётное простое число и m — целое положительное число. Нам потребуется понятие *квантового символа Похгаммера*: если $0<a,b<1$, то

$$(a;b)_m=\prod_{i=0}^{m-1}(1-ab^i)\quad\text{и}\quad(a;b)_\infty=\lim_{m\to\infty}(a;b)_m=\prod_{i=0}^{\infty}(1-ab^i).$$

Легко видеть, что бесконечное произведение в определении $(a;b)_\infty$ сходится, причём $0<(a;b)_\infty<1$. В частности,

$$(1/p;1/p^2)_m=\prod_{i=0}^{m-1}\left(1-\frac{1}{p^{2i+1}}\right)\quad\text{и}\quad(1/p;1/p^2)_\infty=\prod_{i=0}^{\infty}\left(1-\frac{1}{p^{2i+1}}\right).$$

Из известного равенства $\sum\limits_{i=0}^{m-1}(2i+1)=m^2$ следует, что $\prod\limits_{i=0}^{m-1}(p^{2i+1}-1)=p^{m^2}(1/p;1/p^2)_m$. Используя последнее равенство и формулы (2), получаем

$$\mathrm{HN}_q(2m-1,2)=q^{\binom{2m}{2}}(1/q;1/q^2)_m,\quad \mathrm{HN}_q(2m,2)=q^{\binom{2m+1}{2}}(1/q;1/q^2)_m,$$
$$\mathrm{HN}_2(2m,2)=2^{\binom{2m}{2}}(1/2;1/4)_m.$$

Следовательно,

$$\mathrm{HN}_q(n,2)\sim q^{\binom{n+1}{2}}(1/q;1/q^2)_\infty\quad\text{и}\quad\mathrm{HN}_2(2m,2)\sim 2^{\binom{2m}{2}}(1/2;1/4)_\infty \tag{7}$$

при $n\to\infty$ и $m\to\infty$ соответственно. Здесь и далее $\sim$ обозначает асимптотическую эквивалентность функций при стремлении к ∞ некоторого указанного целого неотрицательного аргумента этих функций; при этом все остальные аргументы и параметры функций, если они есть, предполагаются фиксированными.

Перейдём к случаю, когда $d\geqslant 3$.

Теорема 3. Пусть $d\geqslant 1$ и $n\geqslant d/(p-1)$. Тогда

$$\mathrm{HN}_p(n,d)\geqslant p^{\left\{{n\atop d}\right\}_p}-1-\frac{p^n-1}{p-1}\left(p^{\left\{{n-1\atop d}\right\}_p}-1\right). \tag{8}$$

Кроме того,

$$d\geqslant 3\implies \mathrm{HN}_p(n,d)\sim p^{\left\{{n\atop d}\right\}_p}\text{ при }n\to\infty. \tag{9}$$

В случае $p=2$ теорема 3 доказана Ю. В. Кузнецовым в [8]. Доказательство теоремы 3 проводится по той же схеме, что и доказательство её частного случая в [8].

Пусть $d\in\{-1,\dots,n(p-1)\}$. Обозначим через $\mathrm{H}_p(n,d)$ число e-однородных функций из F^{V_n}, имеющих степень d (как мы увидим ниже, это число не зависит от выбора базиса e). Легко видеть, что множество, состоящее из нулевой функции из F^{V_n} и всех e-однородных функций степени d из F^{V_n}, является $\left\{{n\atop d}\right\}_p$-мерным подпространством пространства F^{V_n}. Следовательно,

$$\mathrm{H}_p(n,d)=\begin{cases}1, & \text{если } d=-1,\\ p^{\left\{{n\atop d}\right\}_p}-1, & \text{если } d\geqslant 0.\end{cases} \tag{10}$$

В частности, $\mathrm{H}_p(n,0)=p-1$.

Предположим теперь, что $d \geqslant 1$. Тогда легко видеть, что $\left\{ {n \atop d} \right\}_p \to +\infty$ при $n \to \infty$, так как $\left\{ {n \atop d} \right\}_p \geqslant \binom{n}{d} \sim n^d/d!$ при $n \to \infty$. Поэтому

$$d \geqslant 1 \implies \mathrm{H}_p(n,d) \sim p^{\left\{ {n \atop d} \right\}_p} \text{ при } n \to \infty \tag{11}$$

ввиду формулы (10). Это вместе с некоторыми приведёнными выше формулами позволяет найти предел доли невырожденных функций среди e-однородных функций степени d из F^{V_n} (т. е. предел $\mathrm{HN}_p(n,d)/\mathrm{H}_p(n,d)$) при $n \to \infty$, если он существует, а именно: при $d = 2$ и $p = 2$ этого предела не существует, так как $\mathrm{HN}_2(2m-1,2)/\mathrm{H}_2(2m-1,2) = 0$ при всех $m \geqslant 2$ (см. (2) и (10)) и $\mathrm{HN}_2(2m,2)/\mathrm{H}_2(2m,2) \to (1/2;1/4)_\infty > 0$ при $m \to \infty$ ввиду (7), (11) и очевидного равенства $\left\{ {n \atop 2} \right\}_2 = \binom{n}{2}$. Во всех остальных случаях вышеупомянутый предел указан в формуле

$$\lim_{n\to\infty} \frac{\mathrm{HN}_p(n,d)}{\mathrm{H}_p(n,d)} = \begin{cases} 0, & \text{если } d = 1, \\ (1/p;1/p^2)_\infty, & \text{если } d = 2 \text{ и } p \neq 2, \\ 1, & \text{если } d \geqslant 3, \end{cases}$$

которая следует из формул (1), (7), (9) и (11), а также из того, что $\left\{ {n \atop 2} \right\}_p = \binom{n+1}{2}$ при $p \neq 2$.

3. Переход к групповой алгебре элементарной абелевой p-группы над F

С этого момента вместо векторного пространства V_n (в котором умножение на произвольный элемент основного поля F выражается через сложение) будем иметь дело с элементарной абелевой p-группой G_n ранга n. Для этой группы мы используем мультипликативную запись. Разумеется, группа G_n изоморфна аддитивной группе векторного пространства V_n. Поэтому переход от V_n к G_n представляет собой лишь смену обозначений. В частности, все понятия и объекты, определённые в п. 1 и относящиеся к F^{V_n} (например, производная функции, степень функции, пространства RM_d и $L(\varphi)$), имеют естественные аналоги, относящиеся к F^{G_n}. Эти аналоги будут называться и обозначаться так же, как и исходные понятия и объекты. Подпространствам пространства V_n соответствуют подгруппы группы G_n, а размерностям этих подпространств — ранги соответствующих подгрупп.

Множество F^{G_n} является унитарным модулем над групповой алгеброй FG_n, в котором действие FG_n продолжает по линейности действие группы G_n сдвигами аргумента, а именно

$$\left(\left(\sum_{g \in G_n} f_g g \right) \varphi \right)(x) = \sum_{g \in G_n} f_g \varphi(xg)$$

для любых $f_g \in F$ ($g \in G_n$), $\varphi \in F^{G_n}$ и $x \in G_n$. Такой подход используется в [9] (там рассматривается несколько другое действие, однако его отличие от действия настоящей работы не принципиально).

Обозначим через Δ фундаментальный идеал групповой алгебры FG_n, т. е. идеал этой алгебры, порождённый множеством $\{g - 1 : g \in G_n \setminus \{1\}\}$ (легко видеть, что

это множество является также базисом Δ как векторного пространства). Другими словами,

$$\sum_{g\in G_n} f_g g \in \Delta \iff \sum_{g\in G_n} f_g = 0,$$

где $f_g \in F$ $(g \in G_n)$ (см. также теорему 1.2 из [10] или п. (а) леммы 3.1.7 из [11]). Идеал Δ совпадает с радикалом Джекобсона (или, что в данном случае эквивалентно, с наибольшим нильпотентным идеалом) алгебры FG_n (см. теорему 1.2 из [10] или п. (а) теоремы 3.1.9 из [11]). Для целого положительного числа k через Δ^k обозначим k-ю степень идеала Δ; полагаем $\Delta^0 = FG_n$. Известно, что $\Delta^{n(p-1)} \neq \{0\}$, но $\Delta^{n(p-1)+1} = \{0\}$ (см. теоремы 6.2 (или 6.5) и 3.7 из [10], определение и теорему 3.3.12 из [11], а также [12, разд. 1]). Отметим, что производная произвольной функции $\varphi \in F^{G_n}$ по любому направлению $g \in G_n$ может быть записана как $(g-1)\varphi$. Поэтому

$$\mathrm{RM}_d = \{\varphi \in F^{G_n} : \Delta^{d+1}\varphi = \{0\}\} \tag{12}$$

для каждого $d \in \{-1, \ldots, n(p-1)\}$. Из этого, в частности, следует, что RM_d является подмодулем FG_n-модуля F^{G_n}.

Пусть $b = (b_1, \ldots, b_n)$ — базис элементарной абелевой p-группы G_n. Для каждого $j = (j_1, \ldots, j_n) \in J_n$ положим

$$\eta_j(b) = (b_1 - 1)^{j_1} \ldots (b_n - 1)^{j_n}.$$

Здесь множество J_n определено в (3). Напомним также, что если $j \in J_n$, то $\sigma(j)$ — это сумма всех элементов набора j. Тогда для любого целого неотрицательного числа k система $(\eta_j(b) \,|\, j \in J_n,\ \sigma(j) \geqslant k)$ является базисом векторного пространства Δ^k (см. теорему 3.2 из [10], определение и теорему 3.3.12 из [11] или [12, разд. 1]). Этот базис называется *базисом Дженнингса*. В частности,

$$\dim(\Delta^k/\Delta^{k+1}) = \binom{n}{k}_p, \tag{13}$$

так как $(\eta_j(b) + \Delta^{k+1} \,|\, j \in J_n,\ \sigma(j) = k)$ — базис векторного пространства Δ^k/Δ^{k+1} (см. теорему 3.6 из [10], цитируемую в [13] как теорема 3). Очевидно также, что

$$\eta_j(b)\eta_{j'}(b) = \begin{cases} \eta_{j+j'}(b), & \text{если } j + j' \in J_n, \\ 0 & \text{в противном случае} \end{cases} \tag{14}$$

для произвольных $j, j' \in J_n$, где $j + j'$ вычисляется поэлементно. Здесь мы воспользовались тем, что $(g-1)^p = g^p - 1 = 0$ для любого $g \in G_n$.

Легко видеть, что функция

$$\varphi \mapsto \sum_{g\in G_n} \varphi(g)g^{-1} \quad (\varphi \in F^{G_n}) \tag{15}$$

является изоморфизмом F^{G_n} на FG_n как FG_n-модулей. Пусть $d \in \{-1, \ldots, n(p-1)\}$. Тогда ввиду равенства (12) RM_d отображается при изоморфизме (15) на аннулятор идеала Δ^{d+1} в FG_n. Известно, что этот аннулятор совпадает с $\Delta^{n(p-1)-d}$ (основная теорема из [13] или [11, теоремы 4.2.2, 3.2.2]). Этим объясняется то, что в определении и теореме 3.3.12 из [11] $\Delta^{n(p-1)-d}$ называется обобщённым кодом Рида — Маллера порядка d и длины p^n. Следовательно, если $d \in \{1, \ldots, n(p-1)\}$, то

$$\mathrm{HN}_p(n, d) = |\{\alpha \in (\Delta^{n(p-1)-d}/\Delta^{n(p-1)-d+1}) \setminus \{0\} : L(\alpha) = \{1\}\}| \tag{16}$$

ввиду замечания 2. Здесь

$$L(\xi + \Delta^{n(p-1)-d+1}) = L(\xi) = \{g \in G_n : (g-1)\xi \in \Delta^{n(p-1)-d+2}\}$$

для произвольного $\xi \in \Delta^{n(p-1)-d} \setminus \Delta^{n(p-1)-d+1}$; корректность определения очевидна.

Пусть $d \in \{1, \ldots, n(p-1)\}$ и H — подгруппа группы G_n. Положим

$$\gamma_d(H) = |\{\alpha \in (\Delta^{n(p-1)-d}/\Delta^{n(p-1)-d+1}) \setminus \{0\} : L(\alpha) = H\}|,$$
$$\Gamma_d(H) = |\{\alpha \in (\Delta^{n(p-1)-d}/\Delta^{n(p-1)-d+1}) \setminus \{0\} : L(\alpha) \supseteq H\}|.$$

Вычислим $\Gamma_d(H)$. Выберем базис $b = (b_1, \ldots, b_n)$ элементарной абелевой p-группы G_n так, чтобы $b_{m+1}, \ldots, b_n$ порождали подгруппу H ($m \in \{0, \ldots, n\}$). Пусть $\xi \in \Delta^{n(p-1)-d} \setminus \Delta^{n(p-1)-d+1}$ и $\alpha = \xi + \Delta^{n(p-1)-d+1}$. Так как $L(\alpha)$ является подгруппой группы G_n, включение $L(\alpha) \supseteq H$ выполняется тогда и только тогда, когда $(b_i - 1)\xi \in \Delta^{n(p-1)-d+2}$ для всех $i \in \{m+1, \ldots, n\}$. Непосредственно проверяется (с использованием равенства (14)), что последнее условие имеет место, если и только если $\xi \in U + \Delta^{n(p-1)-d+1}$, где

$$U = \langle\{\eta_j(b) : j = (j_1, \ldots, j_m, p-1, \ldots, p-1) \in J_n,\ j_1 + \ldots + j_m = m(p-1) - d\}\rangle.$$

Сумма U и $\Delta^{n(p-1)-d+1}$ прямая, поэтому отсюда следует, что $\Gamma_d(H) = |U| - 1$. Кроме того, $\dim U = \left\{ {m \atop m(p-1)-d} \right\}_p = \left\{ {m \atop d} \right\}_p$ (см. формулу (4)). Таким образом,

$$\Gamma_d(H) = p^{\left\{ {n - \operatorname{rank} H \atop d} \right\}_p} - 1. \tag{17}$$

4. Доказательства теорем 2 и 3

Через $\mathfrak{S}(G_n)$ будем обозначать частично упорядоченное по включению множество всех подгрупп группы G_n.

Доказательство теоремы 2. Пусть $n \geqslant 1$ и $d \in \{1, \ldots, n(p-1)\}$. Очевидно, что

$$\Gamma_d(X) = \sum_{Y \in \mathfrak{S}(G_n) \,|\, Y \supseteq X} \gamma_d(Y)$$

для любого $X \in \mathfrak{S}(G_n)$. Поэтому ввиду формулы (16) и формулы обращения Мёбиуса [6, утверждение 4.18, п. (ii)] получаем равенство

$$\mathrm{HN}_p(n, d) = \gamma_d(\{1\}) = \sum_{X \in \mathfrak{S}(G_n)} \mu(\{1\}, X)\Gamma_d(X), \tag{18}$$

где μ — функция Мёбиуса [6, подраздел B раздела 1 главы IV] частично упорядоченного множества $\mathfrak{S}(G_n)$. Известно, что

$$\mu(\{1\}, X) = (-1)^{\operatorname{rank} X} p^{\binom{\operatorname{rank} X}{2}} \tag{19}$$

для каждого $X \in \mathfrak{S}(G_n)$ [6, предложение 4.20, п. (iii)]. Следовательно,

$$\mathrm{HN}_p(n, d) = \sum_{k=0}^{n} (-1)^k p^{\binom{k}{2}} \left(p^{\left\{ {n-k \atop d} \right\}_p} - 1\right) \begin{bmatrix} n \\ k \end{bmatrix}_p \tag{20}$$

согласно формулам (17)–(19). Кроме того,

$$\sum_{k=0}^{n} (-1)^k p^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_p = \sum_{X \in \mathfrak{S}(G_n)} \mu(\{1\}, X) = 0 \tag{21}$$

ввиду (19) и [6, предложение 4.6] (напомним, что $n \geqslant 1$). Первое равенство в (6) непосредственно вытекает из равенств (20) и (21), второе следует из того, что

$$\begin{bmatrix} n \\ k \end{bmatrix}_p = \sum_{S \subseteq \{1,\ldots,n\} \,|\, |S|=k} p^{\sigma(S)-\binom{k+1}{2}}$$

для любого $k \in \{0,\ldots,n\}$, где $\sigma(S)$ — сумма всех элементов множества $S \subseteq \{1,\ldots,n\}$ [7, теорема 6.1]. При доказательстве второго равенства в (6) используется также очевидное свойство $\binom{k+1}{2} = \binom{k}{2} + k$. ■

Доказательство теоремы 3. Пусть $d \geqslant 1$ и $n \geqslant d/(p-1)$. Пусть также $\alpha \in (\Delta^{n(p-1)-d}/\Delta^{n(p-1)-d+1}) \setminus \{0\}$, причём $L(\alpha) \neq \{1\}$. Тогда $L(\alpha)$ содержит некоторую подгруппу ранга 1. Используя это замечание, а также формулы (4), (13), (16), (17) и (5), получаем

$$\begin{aligned} p^{\left\{{n \atop d}\right\}_p} - 1 - \mathrm{HN}_p(n,d) &= p^{\left\{{n \atop n(p-1)-d}\right\}_p} - 1 - \mathrm{HN}_p(n,d) = |(\Delta^{n(p-1)-d}/\Delta^{n(p-1)-d+1}) \setminus \{0\}| - \\ &- |\{\alpha \in (\Delta^{n(p-1)-d}/\Delta^{n(p-1)-d+1}) \setminus \{0\} \,|\, L(\alpha) = \{1\}\}| \leqslant \\ \leqslant \sum_{H \in \mathfrak{S}(G_n) \,|\, \operatorname{rank} H = 1} \Gamma_d(H) &= \begin{bmatrix} n \\ 1 \end{bmatrix}_p \left(p^{\left\{{n-1 \atop d}\right\}_p} - 1\right) = \frac{p^n - 1}{p-1}\left(p^{\left\{{n-1 \atop d}\right\}_p} - 1\right), \end{aligned}$$

откуда непосредственно следует неравенство (8).

Предположим теперь, что $d \geqslant 3$. Из (8) и (10) вытекает, что

$$1 - \frac{1}{p^{\left\{{n \atop d}\right\}_p}} - \frac{(p^n-1)(p^{\left\{{n-1 \atop d}\right\}_p} - 1)}{(p-1)p^{\left\{{n \atop d}\right\}_p}} \leqslant \frac{\mathrm{HN}_p(n,d)}{p^{\left\{{n \atop d}\right\}_p}} \leqslant 1. \tag{22}$$

Мы уже видели при доказательстве формулы (11), что $\left\{{n \atop d}\right\}_p \to +\infty$ при $n \to \infty$. Поэтому

$$\frac{1}{p^{\left\{{n \atop d}\right\}_p}} \to 0 \text{ при } n \to \infty. \tag{23}$$

Кроме того, непосредственно проверяется, что

$$\left\{{n \atop d}\right\}_p - \left\{{n-1 \atop d}\right\}_p = \sum_{i=1}^{p-1} \left\{{n-1 \atop d-i}\right\}_p \geqslant \left\{{n-1 \atop d-1}\right\}_p \geqslant \binom{n-1}{d-1}$$

(см. также [5, формула (1.13)]). Поэтому $\left\{{n \atop d}\right\}_p - \left\{{n-1 \atop d}\right\}_p - n \to +\infty$ при $n \to \infty$, так как $\binom{n-1}{d-1} - n \sim n^{d-1}/(d-1)!$ при $n \to \infty$ (напомним, что $d-1 \geqslant 2$). Следовательно,

$$\frac{(p^n-1)(p^{\left\{{n-1 \atop d}\right\}_p} - 1)}{p^{\left\{{n \atop d}\right\}_p}} \sim \frac{1}{p^{\left\{{n \atop d}\right\}_p - \left\{{n-1 \atop d}\right\}_p - n}} \to 0 \text{ при } n \to \infty. \tag{24}$$

Из (22)–(24) вытекает теперь, что $\mathrm{HN}_p(n,d)/p^{\left\{{n \atop d}\right\}_p} \to 1$ при $n \to \infty$. Таким образом, $\mathrm{HN}_p(n,d) \sim p^{\left\{{n \atop d}\right\}_p}$ при $n \to \infty$. ■

Автор благодарит анонимного рецензента, отзыв которого побудил автора к существенной переработке первоначальной версии настоящей работы.

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная математика. 2010. № 2(8). С. 22–33.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Невырожденная нормальная форма булевых функций // Доклады РАН. 2000. Т. 373. № 2. С. 164–167.
3. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: ЛЕНАНД, 2015.
4. *MacWilliams J.* Orthogonal matrices over finite fields // Amer. Math. Monthly. 1969. V. 76. No. 2. P. 152–164.
5. *Бондаренко Б. А.* Обобщенные треугольники и пирамиды Паскаля, их фракталы, графы и приложения. Ташкент: Фан, 1990.
6. *Айгнер М.* Комбинаторная теория. М.: Мир, 1982.
7. *Кац В. Г., Чен П.* Квантовый анализ. М.: МЦНМО, 2005.
8. *Кузнецов Ю. В.* О числе невырожденных булевых форм // Труды лаборатории МГУ по математическим проблемам криптографии. 2000. С. 78–80.
9. *Анохин М. И.* О некоторых множествах групповых функций // Матем. заметки. 2003. Т. 74. № 1. С. 3–11.
10. *Jennings S. A.* The structure of the group ring of a p-group over a modular field // Trans. Amer. Math. Soc. 1941. V. 50. No. 1. P. 175–185.
11. *Циммерман К.-Х.* Методы теории модулярных представлений в алгебраической теории кодирования. М.: МЦНМО, 2011.
12. *Берман С. Д.* К теории групповых кодов // Кибернетика. 1967. № 1. С. 31–39.
13. *Hill E. T.* The annihilator of radical powers in the modular group ring of a p-group // Proc. Amer. Math. Soc. 1970. V. 25. No. 4. P. 811–815.

REFERENCES

1. *Cheremushkin A. V.* Additivnyy podkhod k opredeleniyu stepeni nelineynosti diskretnoy funktsii [An additive approach to defining the degree of nonlinearity of a discrete function]. Prikladnaya Diskretnaya Matematika, 2010, no. 2(8), pp. 22–33. (in Russian)
2. *Logachev O. A., Sal'nikov A. A., and Yashchenko V. V.* Nevyrozhdennaya normalnaya forma bulevykh funktsiy [The nondegenerate normal form of Boolean functions]. Doklady RAN, 2000, vol. 373, no. 2, pp. 164–167. (in Russian)
3. *Logachev O. A., Sal'nikov A. A., Smyshlyaev S. V., and Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, LENAND Publ., 2015. (in Russian)
4. *MacWilliams J.* Orthogonal matrices over finite fields. Amer. Math. Monthly, 1969, vol. 76, no. 2, pp. 152–164.
5. *Bondarenko B. A.* Generalized Pascal triangles and pyramids, their fractals, graphs, and applications. Santa Clara, CA, The Fibonacci Association, 1993.
6. *Aigner M.* Combinatorial Theory. Berlin et al., Springer Verlag, 1979.
7. *Kac V. and Cheung P.* Quantum Calculus. New York et al., Springer Verlag, 2002.
8. *Kuznetsov Yu. V.* O chisle nevyrozhdennykh bulevykh form [On the number of nondegenerate Boolean forms]. Trudy laboratorii MGU po matematicheskim problemam kriptografii, 2000, pp. 78–80. (in Russian)
9. *Anokhin M. I.* O nekotorykh mnozhestvakh gruppovykh funktsiy [On some sets of group functions]. Matem. Zametki, 2003, vol. 74, no. 1, pp. 3–11. (in Russian)
10. *Jennings S. A.* The structure of the group ring of a p-group over a modular field. Trans. Amer. Math. Soc., 1941, vol. 50, no. 1, pp. 175–185.

11. *Zimmermann K.-H.* Beiträge zur algebraischen Codierungstheorie mittels modularer Darstellungstheorie. Bayreuther mathematische Schriften, Heft 48, 1994. (in German)
12. *Berman S. D.* K teorii gruppovykh kodov [On the theory of group codes]. Kibernetika, 1967, no. 1, pp. 31–39. (in Russian)
13. *Hill E. T.* The annihilator of radical powers in the modular group ring of a p-group. Proc. Amer. Math. Soc., 1970, vol. 25, no. 4, pp. 811–815.