Math-Net.Ru

Общероссийский математический портал

С. В. Конягин, Оценки сумм характеров в конечных полях, *Матем. заметки*, 2010, том 88, выпуск 4, 529–542

DOI: <https://doi.org/10.4213/mzm8852>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.209.52.79

26 апреля 2023 г., 17:10:52

Оценки сумм характеров в конечных полях

С. В. Конягин

Доказаны аналоги оценок Берджеса для сумм характеров по n -мерным сегментам в полях $\mathbb{F}_{p^n}$.

Библиография: 10 названий.

Посвящается светлой памяти Анатолия Алексеевича Карацубы

1. Введение. Пусть p – простое число, n – натуральное число, $\{\omega_1, \dots, \omega_n\}$ – произвольный базис конечного поля $\mathbb{F}_{p^n}$ над полем $\mathbb{F}_p$. Тогда каждый элемент $\xi \in \mathbb{F}_{p^n}$ имеет единственное разложение вида

$$\xi = x_1\omega_1 + \dots + x_n\omega_n, \quad 0 \leq x_i < p.$$

Пусть B – n -мерный параллелепипед с ребрами $H_1, \dots, H_n$:

$$B = \left\{ \sum_{i=1}^n x_i \omega_i : N_i + 1 \leq x_i \leq N_i + H_i, i = 1, \dots, n \right\}, \quad (1)$$

где N_i и H_i – целые числа, удовлетворяющие условиям

$$0 \leq N_i < N_i + H_i < p. \quad (2)$$

Иногда мы будем заменять условие (2) более слабым $0 < H_i \leq p$.

Пусть χ – нетривиальный мультипликативный характер поля $\mathbb{F}_{p^n}$. Возникает вопрос, при каких условиях на B можно получить нетривиальные оценки суммы характеров $\sum_{x \in B} \chi(x)$.

В случае $n = 1$ имеет место классическая теорема Берджеса [1]: для любого $\varepsilon > 0$ найдется такое $\delta > 0$, что для любых $N, H \in \mathbb{Z}$, $H > p^{1/4+\varepsilon}$, и любого нетривиального характера χ справедливо неравенство

$$\left| \sum_{x=N+1}^{N+H} \chi(x) \right| \ll p^{-\delta} H,$$

где константа в $\ll$ может зависеть только от ε . Далее Берджес [2] получил следующий аналог этого результата для $n = 2$. Пусть $k \in \mathbb{Z}$, $k < 0$. Через P_k обозначим

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 08-01-00208) и программы “Ведущие научные школы” (грант № НШ-3233.2008.1).

множество простых чисел p таких, что $(\frac{p}{k}) = -1$. Пусть θ – корень уравнения $\theta^2 - k = 0$ в $\mathbb{F}_{p^2}$. Фиксируем линейно независимые над $\mathbb{F}_p$ вектора

$$(\omega_1^{(1)}, \omega_2^{(1)}) \in \mathbb{F}_p^2 \quad \text{и} \quad (\omega_1^{(2)}, \omega_2^{(2)}) \in \mathbb{F}_p^2.$$

Определим элементы

$$\omega_i = \omega_1^{(i)} + \omega_2^{(i)}\theta \in \mathbb{F}_{p^2}, \quad i = 1, 2.$$

ТЕОРЕМА А [2]. Для любого $\varepsilon > 0$ найдется такое $\delta > 0$, что если $p \in P_k$, $H > p^{1/4+\varepsilon}$, $0 \leq N_i < p - H$, $i = 1, 2$, χ – нетривиальный мультипликативный характер поля $\mathbb{F}_{p^2}$, то

$$\left| \sum_{x_1=N_1+1}^{N_1+H} \sum_{x_2=N_2+1}^{N_2+H} \chi(x_1\omega_1 + x_2\omega_2) \right| \ll (p^{-\delta}H)^2,$$

где константа $v \ll$ зависит от k, ε и $\omega_j^{(i)}$, $i, j = 1, 2$.

Карацуба [3], [4] обобщил теорему А на произвольные конечные поля. Пусть F – неприводимый над $\mathbb{Q}$ унитарный многочлен с целыми коэффициентами, $\theta \in \mathbb{C}$ – корень уравнения $F(\theta) = 0$,

$$\theta^i = \sum_{j=0}^{n-1} d_{i,j} \theta^j, \quad 0 \leq i \leq 2n-2, \quad K = \max_{i,j} |d_{i,j}|.$$

Пусть p – простое число такое, что многочлен F неприводим над $\mathbb{F}_p$, $\omega \in \mathbb{F}_{p^n}$ – корень уравнения $F(\omega) = 0$, $\omega_i = \omega^{i-1}$, $i = 1, \dots, n$, множество B определено соотношением (1), где N_i, H_i удовлетворяют (2), причем $H_1 = \dots = H_n = H$.

ТЕОРЕМА В [4]. Пусть $k \geq n+1$ и

$$p^{1/4+1/(4k)} \leq H \leq p^{1/2+1/(4k)}.$$

Тогда для любого нетривиального мультипликативного характера χ поля $\mathbb{F}_{p^n}$ справедлива оценка

$$\left| \sum_{x \in B} \chi(x) \right| \leq c(H^{1-1/k} p^{1/(4k)+1/(4k^2)})^n (\log p)^\gamma,$$

где $\gamma = (2^{n+1} - 1)/k$, а c зависит только от n и k .

В связи с теоремой В возникает вопрос о возможности получения для сумм характеров нетривиальных оценок, равномерных по базисам $\{\omega_1, \dots, \omega_n\}$. Первый результат в этом направлении получили Дженпорт и Льюис [5].

ТЕОРЕМА С [5]. Для любого $\varepsilon > 0$ найдется такое $\delta > 0$, что если χ – нетривиальный мультипликативный характер поля $\mathbb{F}_{p^n}$, множество B определено соотношением (1), где N_i, H_i удовлетворяют (2), причем $H_1 = \dots = H_n = H > p^{n/(2n+2)+\varepsilon}$, то

$$\left| \sum_{x \in B} \chi(x) \right| \leq (p^{-\delta}H)^n.$$

Отметим, что показатель $n/(2n+2)$ в теореме **C** стремится к $1/2$ при $n \rightarrow \infty$. Теорема **C** была усилена Чанг [6].

ТЕОРЕМА D [6]. Для любого $\varepsilon > 0$ найдется такое $\delta > 0$, что если χ – нетривиальный мультипликативный характер поля $\mathbb{F}_{p^n}$, множество B определено соотношением (1), где N_i, H_i удовлетворяют (2), причем

$$\prod_{i=1}^n H_i > p^{(2/5+\varepsilon)n},$$

то

$$\left| \sum_{x \in B} \chi(x) \right| \ll_n p^{-\varepsilon^2/4} |B|.$$

Более того, Чанг [7] получила нетривиальные оценки сумм характеров в случае $n = 2$, $H_1, H_2 > p^{1/4+\varepsilon}$.

Сформулируем основной результат настоящей работы.

ТЕОРЕМА 1. Если $\varepsilon \in (0, 1/4]$, χ – нетривиальный мультипликативный характер поля $\mathbb{F}_{p^n}$, множество B определено соотношением (1), где N_i, H_i – целые числа, причем

$$p^{1/4+\varepsilon} \leq H_i \leq p, \quad i = 1, \dots, n,$$

то

$$\left| \sum_{x \in B} \chi(x) \right| \ll_{n,\varepsilon} p^{-\varepsilon^2/2} |B|.$$

Для $A \subset \mathbb{F}_{p^n}$ и $k \in \mathbb{N}$ обозначим

$$A^k = \{a_1 \cdots a_k : a_1, \dots, a_k \in A\}.$$

СЛЕДСТВИЕ 1. Для любых $\varepsilon > 0$ и $\kappa > 0$ найдутся натуральное число $k = k(\kappa, \varepsilon)$ и число $s = s(n, \kappa, \varepsilon) > 0$ такие, что если B удовлетворяет условиям теоремы 1, $A \subset B$, $|A| \geq \kappa |B|$, то $|A^k| \geq sp^n$.

Доказательство теоремы 1 основано на следующем утверждении.

ЛЕММА 1. Пусть множество B определено соотношением (1), где $N_i, H_i > 0$ – целые числа, причем $H_1 = \dots = H_n \leq p^{1/2}$. Тогда уравнение

$$x^1 x^2 = x^3 x^4, \quad x^1, x^2, x^3, x^4 \in B, \quad (3)$$

имеет $O_n(|B|^2 \log p)$ решений.

Лемма 1 является аналогом леммы 3 из [4] (доказательство последней использует, однако, ограничения на структуру базиса $\{\omega_1, \dots, \omega_n\}$) и усиливает предложение 1 из [6]. Доказательство этого предложения основано на аддитивной комбинаторике, в то время как лемма 1 доказывается с использованием соображений геометрической теории чисел.

Отметим, что для сумм характеров, построенных по базисам, удовлетворяющих условиям теоремы Карацубы [4], его теорема дает лучшую оценку сумм характеров, чем теорема 1: при фиксированном ε в теореме **B** экспонента в понижающем множителе пропорциональна n , в то время как в теореме 1 она от n не зависит. Это

вызвано тем, что для общих базисов не удастся доказать аналога леммы 5 из [4], в которой для параллелепипедов B с центром в нуле строятся достаточно большие множества A, A' такие, что $aa' \in B$ для любых $a \in A, a' \in A'$.

Лемма 1 будет доказана в п. 2, теорема 1 – в п. 3, следствие 1 – в п. 4. Через $C_1, C_2, \dots$ мы будем обозначать абсолютные положительные константы.

2. Доказательство леммы 1. Обозначим $H = H_1 = \dots = H_n$,

$$Z = \frac{B \setminus \{0\}}{B \setminus \{0\}} = \{z \in \mathbb{F}_{p^n} : \exists x, y \in B \setminus \{0\} \ xz = y\}.$$

Если $x^1, x^2, x^3, x^4 \in B$, $x^1 x^2 = x^3 x^4$ и $(x^1, x^4) \neq (0, 0)$, $(x^2, x^3) \neq (0, 0)$, то для некоторого $z \in Z$ мы имеем $x^1 z = x^3$, $x^4 z = x^2$. Следовательно, количество E решений уравнения (3) может быть оценено следующим образом:

$$E \leq 2|B|^2 + \sum_{z \in Z} f^2(z),$$

где $f(z)$ есть количество решений уравнения $xz = y$, $x, y \in B$. Обозначим

$$B_0 = \{x_1 \omega_1 + \dots + x_n \omega_n : -H \leq x_j \leq H\},$$

$$Z_0 = \frac{B_0 \setminus \{0\}}{B_0 \setminus \{0\}}, \quad f_0(z) = |\{(x, y) \in B_0^2 : xz = y\}|.$$

Заметим, что $f(z) \leq f_0(z)$ и что $f_0(z) = 1$ при $z \in \mathbb{F}_{p^n}^* \setminus Z_0$. Таким образом,

$$\sum_{z \in Z} f^2(z) \leq \sum_{z \in Z_0} f_0^2(z) + |Z \setminus Z_0|.$$

Поскольку $|Z| \leq |B|^2$, мы получаем

$$E \leq 3|B|^2 + \sum_{z \in Z_0} f_0^2(z), \quad (4)$$

и нам достаточно оценить последнюю сумму.

Для фиксированного $z \in Z_0$ определим решетку Γ в $\mathbb{Z}^{2n}$:

$$\Gamma = \Gamma_z = \left\{ (x_1, \dots, x_n, y_1, \dots, y_n) \in \mathbb{Z}^{2n} : z \sum_{i=1}^n x_i \omega_i = \sum_{i=1}^n y_i \omega_i \right\}.$$

При фиксированных $x_1, \dots, x_n \in \mathbb{Z}$ условие $(x_1, \dots, x_n, y_1, \dots, y_n) \in \Gamma$ определяет вычет каждого из чисел $y_1, \dots, y_n$ по модулю p . Поэтому количество точек решетки Γ в большом кубе можно оценить асимптотически при $M \rightarrow \infty$:

$$|\{(x_1, \dots, y_n) \in \Gamma : |x_i| \leq M, |y_i| \leq M, i = 1, \dots, n\}| = \frac{(2M)^{2n}}{p^n} (1 + o(1)).$$

Следовательно,

$$\text{mes}(\mathbb{R}^{2n}/\Gamma) = p^n. \quad (5)$$

Определим куб $D \subset \mathbb{R}^{2n}$:

$$D = \{(x_1, \dots, y_n) \in \mathbb{R}^{2n} : |x_i| \leq H, |y_i| \leq H, i = 1, \dots, n\}.$$

Заметим, что

$$f_0(z) = |D \cap \Gamma_z|. \quad (6)$$

Напомним, что i -м *последовательным минимумом*

$$\lambda_i = \lambda_i(z) = \lambda_i(D, \Gamma_z)$$

множества D относительно решетки Γ_z называется минимальное число λ такое, что множество λD содержит i линейно независимых векторов решетки Γ_z , $i = 1, \dots, 2n$. Очевидно, $\lambda_1(z) \leq \dots \leq \lambda_{2n}(z)$ и при этом $z \in Z_0$ в том и только том случае, когда $\lambda_1(z) \leq 1$. Вторая теорема Минковского (см. [8; теорема 3.30]) утверждает, что

$$\frac{2^{2n}}{(2n)!} \leq \frac{\lambda_1 \cdots \lambda_{2n}}{\text{mes}(\mathbb{R}^{2n}/\Gamma)}.$$

Отсюда, учитывая (5), получаем

$$\lambda_1 \cdots \lambda_{2n} \geq \frac{p^{n4n}}{(2n)! H^{2n}}. \quad (7)$$

Известно, что для количества $f_0(z)$ точек решетки Γ_z в D справедливо неравенство

$$f_0(z) \leq (2n)^{C_1 n} \prod_{i=1}^{2n} \max\left(1, \frac{1}{\lambda_i}\right) \quad (8)$$

(см. [8; упражнение 3.5.6]).

Определим полярную решетку $\Gamma^* = \Gamma_z^*$ как множество векторов $(u_1, \dots, u_{2n}) \in \mathbb{R}^{2n}$ таких, что

$$\sum_{i=1}^n u_i x_i + \sum_{i=1}^n u_{n+i} y_i \in \mathbb{Z}$$

для всех $(x_1, \dots, x_n, y_1, \dots, y_n) \in \Gamma$. Заметим, что $\Gamma_z^* \subset p^{-1}\mathbb{Z}^{2n}$, поскольку $p\mathbb{Z}^{2n} \subset \Gamma_z$. Пусть $\lambda_1^* = \lambda_1^*(z)$ обозначает первый последовательный минимум решетки Γ_z^* относительно полярного множества

$$D^* = \left\{ (u_1, \dots, u_{2n}) : \sum_{i=1}^{2n} |u_i| \leq \frac{1}{H} \right\}.$$

В силу [9]

$$\lambda_{2n} \lambda_1^* \leq C_2 n (1 + \log n)^{1/2}. \quad (9)$$

Обозначим $\nu = \nu(z) = \min(\lambda_1 H, p\lambda_1^*/H)$, $s = \max\{j : \lambda_j \leq 1\}$. Если $z \in Z_0$, то $\lambda_1 \leq 1$ и s корректно определено.

В случае $s \leq n$ мы имеем

$$\prod_{i=1}^{2n} \max\left(1, \frac{1}{\lambda_i}\right) = \prod_{i=1}^s (\lambda_i)^{-1} \leq (\lambda_1)^{-n} \leq \nu^{-n} H^n.$$

Если же $s > n$, то в силу (7) и (9)

$$\begin{aligned} \prod_{i=1}^{2n} \max\left(1, \frac{1}{\lambda_i}\right) &= \prod_{i=1}^s (\lambda_i)^{-1} \leq \prod_{i=1}^{2n} (\lambda_i)^{-1} \lambda_{2n}^{2n-s} \ll_n \prod_{i=1}^{2n} (\lambda_i)^{-1} (\lambda_1^*)^{s-2n} \\ &\ll_n \frac{H^{2n}}{p^n} \frac{p^{2n-s}}{H^{2n-s} \nu^{2n-s}} = \nu^{-n} H^n \left(\frac{H\nu}{p}\right)^{s-n}. \end{aligned}$$

Но

$$\frac{H\nu}{p} \leq \frac{H^2 \lambda_1}{p} \leq \frac{H^2}{p} \leq 1,$$

и в обоих случаях мы имеем

$$\prod_{j=1}^{2n} \max\left(1, \frac{1}{\lambda_j}\right) \ll_n \nu^{-n} H^n.$$

Далее, используя (8), мы получаем

$$f_0(z) \ll_n \nu(z)^{-n} H^n. \quad (10)$$

Обозначим $J := [\log_2 H] + 1$ и разобьем множество Z_0 на подмножества Z_j , $j = 1, \dots, J$, где

$$Z_j = \{z \in Z_0 : 2^{j-1} \leq \nu(z) < 2^j\}.$$

Далее, $Z_j \subset Z_j^1 \cup Z_j^2$, где

$$Z_j^1 = \{z \in Z_0 : \lambda_1(z)H < 2^j\}, \quad Z_j^2 = \{z \in Z_0 : p\lambda_1^*(z)/H < 2^j\}.$$

Если $z \in Z_j^1$, то найдется ненулевой вектор $v = (v_1, \dots, v_{2n}) \in \Gamma_z$ такой, что $\max_i |v_i| < 2^j$. Вектор v определяет z , ибо

$$z = \sum_{i=n+1}^{2n} v_i \omega_{i-n} \left(\sum_{i=1}^n v_i \omega_i \right)^{-1}.$$

(Случай, когда векторы $\sum_{i=n+1}^{2n} v_i \omega_{i-n}$ и $\sum_{i=1}^n v_i \omega_i$ являются нулевыми в $\mathbb{F}_{p^n}$ невозможен, поскольку $\max_i |v_i| < 2^j < p$). Поэтому $|Z_j^1| < (2^{j+1})^{2n}$. Аналогично, для $z \in Z_j^2$ найдется ненулевой вектор $u = (u_1, \dots, u_{2n}) \in p\Gamma_z^*$ такой, что $\sum_i |u_i| < 2^j$. Вектор u определяет z . Действительно, предположим противное. Тогда найдутся различные z' и z'' такие, что $u \in p\Gamma_{z'}^*$ и $u \in p\Gamma_{z''}^*$. Возьмем произвольный элемент $x \in \mathbb{F}_{p^n}$, и пусть

$$y' = xz' = \sum_{i=1}^n y'_i \omega_i, \quad y'' = xz'' = \sum_{i=1}^n y''_i \omega_i.$$

Мы имеем

$$\sum_{i=1}^n y_i u_{i+n} \equiv 0 \pmod{p}, \quad (11)$$

где $y_i = y'_i - y''_i$. Так как для любого $y \in \mathbb{F}_{p^n}$ и $x = y(z' - z'')^{-1}$ справедливо равенство $xz' - xz'' = y$, то сравнение (11) имеет место для всех $(y_1, \dots, y_n) \in \mathbb{Z}^n$.

Отсюда вытекает, что $u_{n+1} \equiv \dots \equiv u_{2n} \equiv 0 \pmod{p}$, и поскольку $\max_i |u_i| < 2^J < p$, то

$$u_{n+1} = \dots = u_{2n} = 0.$$

Из последнего равенства следует, что

$$\forall (x_1, \dots, x_n) \in \mathbb{Z}^n \quad \sum_{i=1}^n x_i u_i \equiv 0 \pmod{p},$$

откуда $u_1 = \dots = u_{2n} = 0$, что противоречит выбору u . Итак, вектор u определяет z , откуда вытекает, что $|Z_j^2| < (2^{j+1})^{2n}$.

Соединяя вышеприведенные оценки, мы получаем

$$\begin{aligned} |Z_j| &\leq |Z_j^1| + |Z_j^2| < 2^{2n+1} 2^{2jn}, \\ \sum_{z \in Z_j} f_0(z)^2 &\ll_n (2^{j-1})^{-2n} H^{2n} |Z_j| \ll_n H^{2n}, \\ \sum_{z \in Z_0} f_0(z)^2 &\leq \sum_{j=1}^J \sum_{z \in Z_j} f_0(z)^2 \ll_n H^{2n} \log p. \end{aligned}$$

Применение (4) завершает доказательство леммы.

ЗАМЕЧАНИЕ 1. Величину O_n в лемме 1 можно взять в виде $(2n)^{C_3 n}$.

3. Доказательство теоремы 1. Для натурального числа $H \leq p/2$ и мультипликативного характера χ поля $\mathbb{F}_{p^n}$ обозначим

$$\Delta(H, \chi) = \max_B \left| \sum_{x \in B} \chi(x) \right| |B|^{-1},$$

где максимум берется по параллелепипедам вида (1) таким, что

$$H \leq H_i \leq 2H, \quad i = 1, \dots, n. \quad (12)$$

Иногда для фиксированного характера χ мы будем писать $\Delta(H)$ вместо $\Delta(H, \chi)$. Отметим, что если ребра параллелепипеда B удовлетворяют более слабому ограничению, чем (12), а именно,

$$H \leq H_i \leq p, \quad i = 1, \dots, n,$$

то его можно разбить на параллелепипеды, ребра которых удовлетворяют условию (12). Поэтому

$$\left| \sum_{x \in B} \chi(x) \right| \leq \Delta(H, \chi) |B|,$$

и для доказательства теоремы 1 нам достаточно убедиться в том, что при $0 < \varepsilon \leq 1/2$

$$\Delta([p^{1/4+\varepsilon}], \chi) \ll_n p^{-\varepsilon^2/2}. \quad (13)$$

ЛЕММА 2. Пусть множество B определено соотношением (1), где $N_i, H_i > 0$ – целые числа, удовлетворяющие (12). Пусть $H, \tilde{H}$ – натуральные числа, $\tilde{H} \leq H/2$ и элемент $u = \sum_{i=1}^n u_i \omega_i$ удовлетворяет условию

$$1 \leq u_i \leq \tilde{H}, \quad i = 1, \dots, n.$$

Пусть также χ – мультипликативный характер поля $\mathbb{F}_{p^n}$. Тогда

$$\left| \sum_{x \in B} \chi(x) - \sum_{x \in B} \chi(x+u) \right| \leq 6n\Delta(\tilde{H}, \chi)|B| \frac{\tilde{H}}{H}.$$

ДОКАЗАТЕЛЬСТВО. Сумма характеров $\sum_{x \in B} \chi(x+u)$ может быть получена из суммы $\sum_{x \in B} \chi(x)$ путем прибавления и вычитания нескольких сумм по параллелепипедам. Для $j = 1, \dots, n$ обозначим

$$B_j = \left\{ \sum_{i=1}^n x_i \omega_i \right\},$$

где

$$\begin{aligned} N_i + u_i + 1 &\leq x_i \leq N_i + H_i, & i = 1, \dots, j-1, \\ N_j + 1 &\leq x_j \leq N_j + u_j, \\ N_i + 1 &\leq x_i \leq N_i + H_i, & i = j+1, \dots, n. \end{aligned}$$

Аналогично, положим

$$B'_j = \left\{ \sum_{i=1}^n x_i \omega_i \right\},$$

где

$$\begin{aligned} N_i + u_i + 1 &\leq x_i \leq N_i + H_i, & i = 1, \dots, j-1, \\ N_j + H_j + 1 &\leq x_j \leq N_j + H_j + u_j, \\ N_i + u_j + 1 &\leq x_i \leq N_i + H_i + u_j, & i = j+1, \dots, n. \end{aligned}$$

Тогда

$$\sum_{x \in B} \chi(x) - \sum_{x \in B} \chi(x+u) = \bigcup_{j=1}^n \sum_{x \in B_j} \chi(x) - \bigcup_{j=1}^n \sum_{x \in B'_j} \chi(x). \quad (14)$$

Далее, для $j = 1, \dots, n$ параллелепипед B_j может быть представлен в виде разности параллелепипедов: $B_j = B_j^1 \setminus B_j^2$, где при определении B_j^1 и B_j^2 промежутки изменения компонент x_i при $i \neq j$ такие же, как у B_j , а x_j удовлетворяют условиям $N_j + 1 \leq x_j \leq N_j + u_j + \tilde{H}$ для B_j^1 и $N_j + u_j + 1 \leq x_j \leq N_j + u_j + \tilde{H}$ для B_j^2 . Мы имеем

$$\sum_{x \in B_j} \chi(x) = \sum_{x \in B_j^1} \chi(x) - \sum_{x \in B_j^2} \chi(x).$$

Все ребра параллелепипедов B_j^1 и B_j^2 не меньше $\tilde{H}$. Следовательно,

$$\begin{aligned} \left| \sum_{x \in B_j} \chi(x) \right| &\leq \Delta(\tilde{H}, \chi)(u_j + \tilde{H}) \prod_{i=1}^{j-1} (H_i - u_i) \prod_{i=j+1}^n H_i \\ &\leq \Delta(\tilde{H}, \chi) 2\tilde{H} \prod_{i \neq j} H_i \leq \Delta(\tilde{H}, \chi) |B| \frac{2\tilde{H}}{H}. \end{aligned}$$

Аналогично,

$$\left| \sum_{x \in B_j^1} \chi(x) \right| \leq \Delta(\tilde{H}, \chi) |B| \frac{\tilde{H}}{H}.$$

Значит,

$$\left| \sum_{x \in B_j} \chi(x) \right| \leq \left| \sum_{x \in B_j^1} \chi(x) \right| + \left| \sum_{x \in B_j^2} \chi(x) \right| \leq \Delta(\tilde{H}, \chi) |B| \frac{3\tilde{H}}{H}. \quad (15)$$

Аналогично,

$$\left| \sum_{x \in B'_j} \chi(x) \right| \leq \Delta(\tilde{H}, \chi) |B| \frac{3\tilde{H}}{H}. \quad (16)$$

В силу равенства (14) и неравенств (15) и (16)

$$\left| \sum_{x \in B} \chi(x) - \sum_{x \in B} \chi(x+u) \right| \leq \sum_{j=1}^n \left| \sum_{x \in B_j} \chi(x) \right| + \sum_{j=1}^n \left| \sum_{x \in B'_j} \chi(x) \right| \leq 6n\Delta(\tilde{H}, \chi) |B| \frac{\tilde{H}}{H},$$

что и требовалось доказать.

Далее нам потребуется версия Шмидта оценки Вейля для сумм характеров.

ТЕОРЕМА Е [10; теорема 2C', с. 43]. Пусть χ – мультипликативный характер порядка $d > 1$ поля $\mathbb{F}_{p^n}$. Предположим, что многочлен $f \in \mathbb{F}_{p^n}[x]$ имеет m различных корней и что f не является d -й степенью. Тогда

$$\left| \sum_{x \in \mathbb{F}_{p^n}} \chi(f(x)) \right| \leq (m-1)p^{n/2}.$$

Следующая лемма, основанная на хорошо известной восходящей к Берджесу технике (см., например, [1], [4], [6]), устанавливает оценку сумм характеров с помощью теоремы Е и леммы 1.

ЛЕММА 3. Пусть $r, H, \tilde{H}$ – натуральные числа,

$$G := [p^{n/(2r)}] \leq \tilde{H} \leq \frac{H}{2}, \quad H \leq p^{1/2}.$$

Пусть также χ – нетривиальный мультипликативный характер поля $\mathbb{F}_{p^n}$. Тогда имеет место неравенство

$$\Delta(H, \chi) \leq 6n\Delta(\tilde{H}) \frac{\tilde{H}}{H} + O_{n,r}((\log p)^{1/(2r)} (H\tilde{H}G^{-1}p^{-1/2})^{-n/(2r)}).$$

ДОКАЗАТЕЛЬСТВО. Положим $I = [1, G] \cap \mathbb{Z}$, $H_0 = [\tilde{H}/G]$

$$B'_0 = \left\{ \sum_{i=1}^n x_i \omega_i : 1 \leq x_i \leq H_0, i = 1, \dots, n \right\}.$$

Заметим, что всякий элемент $x = yz$, $y \in B'_0$, $z \in I$, представим в виде

$$x = \sum_{i=1}^n x_i \omega_i : \quad 1 \leq x_i \leq \tilde{H}, \quad i = 1, \dots, n.$$

Применяя лемму 2, мы получаем, что для любых $y \in B'_0$, $z \in I$ справедливо неравенство

$$\left| \sum_{x \in B} \chi(x + yz) - \sum_{x \in B} \chi(x) \right| \leq 6n\Delta(\tilde{H}, \chi) |B| \frac{\tilde{H}}{H}.$$

Следовательно,

$$\left| \sum_{x \in B} \chi(x) - \frac{1}{|B'_0|G} \sum_{x \in B, y \in B'_0, z \in I} \chi(x + yz) \right| \leq 6n\Delta(\tilde{H}, \chi) |B| \frac{\tilde{H}}{H}. \quad (17)$$

Далее,

$$\begin{aligned} \left| \sum_{x \in B, y \in B'_0, z \in I} \chi(x + yz) \right| &\leq \sum_{x \in B, y \in B'_0} \left| \sum_{z \in I} \chi(x + yz) \right| \\ &= \sum_{x \in B, y \in B'_0} \left| \sum_{z \in I} \chi(xy^{-1} + z) \right| = \sum_{u \in \mathbb{F}_{p^n}} w(u) \left| \sum_{z \in I} \chi(u + z) \right|, \end{aligned}$$

где

$$w(u) = \left| \left\{ (x, y) \in B \times B'_0 : \frac{x}{y} = u \right\} \right|.$$

Дважды применяя неравенство Гёльдера, мы получаем

$$\begin{aligned} \left| \sum_{x \in B, y \in B'_0, z \in I} \chi(x + yz) \right| &\leq \left(\sum_{u \in \mathbb{F}_{p^n}} w(u) \right)^{1-1/r} \left(\sum_{u \in \mathbb{F}_{p^n}} w(u)^2 \right)^{1/(2r)} \left(\sum_{u \in \mathbb{F}_{p^n}} \left| \sum_{z \in I} \chi(u + z) \right|^2 \right)^{1/(2r)}. \quad (18) \end{aligned}$$

Очевидно,

$$\sum_{u \in \mathbb{F}_{p^n}} w(u) = |B| |B'_0|. \quad (19)$$

Для оценки $\sum_{u \in \mathbb{F}_{p^n}} w(u)^2$ введем следующее обозначение: если $A \subset \mathbb{F}_{p^n}$, то через $E(A)$ обозначим количество решений уравнения

$$x^1 x^2 = x^3 x^4, \quad x^1, x^2, x^3, x^4 \in A.$$

Положим также $B^* = B \setminus \{0\}$. Мы имеем

$$\begin{aligned} &\sum_{u \in \mathbb{F}_{p^n}} w(u)^2 \\ &= w(0)^2 + \sum_{u \in \mathbb{F}_{p^n}^*} w(u)^2 \\ &= w(0)^2 + \sum_{\nu \in \mathbb{F}_{p^n}^*} |\{(x_1, x_2, y_1, y_2) \in B^* \times B^* \times B'_0 \times B'_0 : x_1 y_2 = x_2 y_1\}| \\ &\leq |B'_0|^2 + \sum_{\nu \in \mathbb{F}_{p^n}^*} \left| \left\{ (x_1, x_2) \in B^* \times B^* : \frac{x_1}{x_2} = \nu \right\} \right| \left| \left\{ (y_1, y_2) \in B'_0 \times B'_0 : \frac{y_1}{y_2} = \nu \right\} \right| \\ &\leq |B'_0|^2 + E(B, B)^{1/2} E(B'_0, B'_0)^{1/2}. \end{aligned}$$

Применяя лемму 1 и учитывая, что $|B'_0| \leq |B|$, мы получаем

$$\sum_{u \in \mathbb{F}_{p^n}} w(u)^2 \ll_n |B| |B'_0| \log p. \quad (20)$$

Далее мы воспользуемся оценкой последней суммы в (18), полученной в [6]; для полноты мы воспроизводим приведенный там вывод этой оценки. Обозначим $q = p^n$. Мы имеем

$$\sum_{u \in \mathbb{F}_{p^n}} \left| \sum_{z \in I} \chi(u+z) \right|^{2r} = \sum_{z_1, \dots, z_{2r} \in I} \left| \sum_{u \in \mathbb{F}_q} \chi((u+z_1) \cdots (u+z_r)(u+z_{r+1})^{q-2} \cdots (u+z_{2r})^{q-2}) \right|.$$

К тем $z_1, \dots, z_{2r}$, для которых по крайней мере один из этих элементов встречается ровно один раз, можно применить теорему E, согласно которой

$$\left| \sum_{u \in \mathbb{F}_q} \chi((u+z_1) \cdots (u+z_r)(u+z_{r+1})^{q-2} \cdots (u+z_{2r})^{q-2}) \right| < 2rp^{n/2}.$$

Сумма по тем $z_1, \dots, z_{2r}$, в которых каждый элемент встречается по крайней мере дважды, оценивается произведением p^n на количество таких наборов $(z_1, \dots, z_{2r})$. Поскольку все элементы $z_1, \dots, z_{2r}$ принадлежат некоторому подмножеству множества I , содержащего $\min(r, G)$ элементов, а при фиксировании такого подмножества для каждого из этих элементов имеется не более r возможностей выбора, то количество наборов $(z_1, \dots, z_{2r})$ не превосходит $G^r r^{2r}$. Следовательно,

$$\begin{aligned} \sum_{u \in \mathbb{F}_{p^n}} \left| \sum_{z \in I} \chi(u+z) \right|^{2r} &\leq G^r r^{2r} p^n + 2rG^{2r} p^{n/2}, \\ \left(\sum_{u \in \mathbb{F}_{p^n}} \left| \sum_{z \in I} \chi(u+z) \right|^{2r} \right)^{1/(2r)} &\leq rG^{1/2} p^{n/(2r)} + 2Gp^{n/(4r)}. \end{aligned}$$

В виду определения G

$$\left(\sum_{u \in \mathbb{F}_{p^n}} \left| \sum_{z \in I} \chi(u+z) \right|^{2r} \right)^{1/(2r)} \leq (2r+2)Gp^{n/(4r)}. \quad (21)$$

Подставляя (19)–(21) в (18), мы получаем

$$\begin{aligned} \left| \sum_{x \in B, y \in B'_0, z \in I} \chi(x+yz) \right| &\ll_{n,r} (|B| |B'_0|)^{1-1/(2r)} (\log p)^{1/(2r)} Gp^{n/(4r)} \\ &= (\log p)^{1/(2r)} |B| |B'_0| |G| (|B| |B'_0|)^{-1/(2r)} p^{n/(4r)} \\ &= (\log p)^{1/(2r)} |B| |B'_0| |G| \left(H \left[\frac{\tilde{H}}{G} \right] p^{-1/2} \right)^{-n/(2r)} \\ &\leq 2(\log p)^{1/(2r)} |B| |B'_0| |G| (H \tilde{H} G^{-1} p^{-1/2})^{n/(2r)}. \end{aligned}$$

Из последнего неравенства и (17) следует, что

$$\left| \sum_{x \in B} \chi(x) \right| \leq 6n\Delta(\tilde{H}, \chi) |B| \frac{\tilde{H}}{H} + O_{n,r}((\log p)^{1/(2r)} |B| (H \tilde{H} G^{-1} p^{-1/2})^{n/(2r)}).$$

В силу произвольности выбора B отсюда вытекает утверждение леммы. Лемма 3 доказана.

При использовании леммы 3 мы будем считать, что

$$r \geq 2n. \quad (22)$$

Введем параметр α , удовлетворяющий условиям

$$0 < \alpha \leq \frac{1}{(12n)^2}. \quad (23)$$

Пусть также

$$0 < \varepsilon \leq \frac{1}{2}, \quad H = [p^{1/4+\varepsilon}]. \quad (24)$$

Мы полагаем

$$H_i = [\alpha^i H], \quad i \geq 0.$$

Пусть I – наибольшее целое i такое, что $H_i \geq G$, где G задано леммой 3. Поскольку $H \geq G$ в силу (22) и (24), то I определено корректно.

Применяя лемму 3 к H_i и H_{i+1} , мы можем последовательно оценить $\Delta(H_i)$ через $\Delta(H_{i+1})$, $i = 0, \dots, I-1$:

$$\Delta(H_i) \leq 6n\Delta(H_{i+1})\frac{H_{i+1}}{H_i} + O_{n,r}((\log p)^{1/(2r)}(H_i H_{i+1} G^{-1} p^{-1/2})^{-n/(2r)}).$$

Следовательно,

$$\begin{aligned} \Delta(H_i) &\leq (6n)^I \Delta(H_I) \frac{H_I}{H} \\ &+ (\log p)^{1/(2r)} (G^{-1} p^{-1/2})^{-n/(2r)} \sum_{i=0}^{I-1} O_{n,r} \left((6n)^i \frac{H_i}{H} (H_i H_{i+1})^{-n/(2r)} \right). \end{aligned} \quad (25)$$

Далее,

$$\begin{aligned} (6n)^I \Delta(H_I) \frac{H_I}{H} &\leq (6n)^{\log H / (-\log \alpha)} \frac{H_I}{H} \\ &\leq (6n)^{\log p / (-2 \log \alpha)} \alpha^{-1} \frac{G}{H} = p^{\log(6n) / (-2 \log \alpha)} \alpha^{-1} \frac{G}{H}. \end{aligned} \quad (26)$$

Учитывая (22) и (23), мы получаем

$$\begin{aligned} &\sum_{i=0}^{I-1} (6n)^i \frac{H_i}{H} (H_i H_{i+1})^{-n/(2r)} \\ &\leq \sum_{i=0}^{I-1} (6n)^i \alpha^i \left(\frac{H^2 \alpha^{2i+1}}{4} \right)^{-n/(2r)} \leq 2H^{-n/r} \alpha^{-n/(2r)} \sum_{i=0}^{I-1} (6n)^i \alpha^{i(1-n/r)} \\ &\leq 2H^{-n/r} \alpha^{-n/(2r)} \sum_{i=0}^{I-1} (6n)^i \alpha^{i/2} \leq 2H^{-n/r} \alpha^{-n/(2r)} \sum_{i=0}^{I-1} 2^{-i} \leq 4H^{-n/r} \alpha^{-n/(2r)}. \end{aligned} \quad (27)$$

Подставляя (26) и (27) в (25), мы находим

$$\begin{aligned} \Delta(H) &\leq p^{\log(6n)/(-2\log\alpha)} \alpha^{-1} \frac{G}{H} + O_{n,r}((\log p)^{1/(2r)} (G^{-1} p^{-1/2})^{-n/(2r)} H^{-n/r} \alpha^{-n/(2r)}) \\ &\leq 2p^{\log(6n)/(-2\log\alpha)} \alpha^{-1} p^{n/(2r)-1/4-\varepsilon} + O_{n,r}((\log p)^{1/(2r)} \alpha^{-1} p^{-(n/r)(\varepsilon-n/(4r))}). \end{aligned} \quad (28)$$

Для завершения доказательства теоремы 1 мы специфицируем параметры r и α . Положим

$$r = \left\lceil \frac{n}{2\varepsilon} \right\rceil + 1, \quad \alpha = (6n)^3.$$

Легко видеть, что условия (22) и (23) выполнены. Так как

$$\frac{4\varepsilon}{3} \leq \frac{n}{r} \leq 2\varepsilon,$$

то

$$\frac{n}{r} \left(\varepsilon - \frac{n}{4r} \right) \geq \frac{8}{9} \varepsilon^2,$$

откуда

$$(\log p)^{1/(2r)} \alpha^{-1} p^{-(n/r)(\varepsilon-n/(4r))} \ll_{n,\varepsilon} p^{-\varepsilon^2/2}.$$

Далее,

$$p^{\log(6n)/(-2\log\alpha)} \alpha^{-1} p^{n/(2r)-1/4-\varepsilon} \ll p^{1/6} p^{-1/4} = p^{-1/12} \leq p^{-\varepsilon^2/2}.$$

Таким образом, из неравенства (28) вытекает справедливость неравенства (13), и теорема 1 доказана.

ЗАМЕЧАНИЕ 2. Выражение $\ll_{n,\varepsilon}$ в теореме 1 можно заменить на $C_4 n^{C_5}/\varepsilon$.

4. Доказательство следствия 1. Мы следуем аргументам [6; следствие 5]. Для $D \subset B$, $k \in \mathbb{N}$ и $z \in \mathbb{F}_{p^n}$ через $f_{k,D}(z)$ обозначим количество решений уравнения

$$x_1 \cdots x_k = z: \quad x_1, \dots, x_k \in D^* := D \setminus \{0\}.$$

Без ограничения общности можно считать, что $\varepsilon \leq 1/4$. Кроме того, можно считать, что p достаточно велико: $p \geq p(n, \varepsilon)$, так как для малых p утверждение следствия вытекает из тривиальной оценки $|A^k| \geq 1$. В частности, мы полагаем, что $\kappa p^{n/4} \geq 1$, и тогда

$$|A^*| \geq \frac{\kappa}{2} |B|. \quad (29)$$

Для $z \in \mathbb{F}_{p^n}^*$ мы имеем

$$f_{k,B}(z) = \frac{1}{p^n - 1} \sum_{\chi} \chi(z) \left(\sum_{x \in B} \bar{\chi}(x) \right)^k,$$

где χ пробегает множество мультипликативных характеров поля $\mathbb{F}_{p^n}$. В силу теоремы 1 для достаточно большого p и любого нетривиального характера χ справедливо неравенство

$$\left| \sum_{x \in B} \bar{\chi}(x) \right| \leq p^{-\varepsilon^2/3} |B|.$$

Поэтому при $k \geq 3n/\varepsilon^2$, обозначая через χ_0 главный характер, мы имеем

$$\begin{aligned} f_{k,B}(z) &\leq \frac{1}{p^n - 1} |B|^k + \frac{1}{p^n - 1} \sum_{\chi \neq \chi_0} (p^{-\varepsilon^2/3} |B|)^k \\ &\leq \frac{1}{p^n - 1} |B|^k + \frac{p^n - 2}{p^n - 1} |B|^k p^{-\varepsilon^2 k/3} \leq \frac{2}{p^n - 1} |B|^k. \end{aligned}$$

Далее,

$$|A^*|^k = \sum_z f_{k,B}(z) \leq |B|^k \max_z f_{k,B}(z) \leq |B|^k \frac{2}{p^n - 1} |B|^k,$$

откуда и из (29) следует, что

$$|B^k| \geq |A^*|^k |B|^{-k} \frac{p^n - 1}{2} \geq \frac{(p^n - 1) \kappa^k}{2^{k+1}} \geq \frac{p^n \kappa^k}{2^{k+2}},$$

что и требовалось доказать.

Автор благодарит О. Н. Германа, Х. Монтгомери и М.-Ч. Чанг за полезные обсуждения и М. З. Гараева, указавшего автору на ряд неточностей в первоначальной версии работы.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] D. A. Burgess, “On character sums and primitive roots”, *Proc. London Math. Soc.* (3), **12** (1962), 179–192.
- [2] D. A. Burgess, “Character sums and primitive roots in finite fields”, *Proc. Lond. Math. Soc.* (3), **17** (1967), 11–25.
- [3] А. А. Карацуба, “Суммы характеров и первообразные корни в конечных полях”, *ДАН СССР*, **180**:6 (1968), 1287–1289.
- [4] А. А. Карацуба, “Об оценках сумм характеров”, *Изв. АН СССР. Сер. матем.*, **34**:1 (1970), 20–30.
- [5] H. Davenport, D. J. Lewis, “Character sums and primitive roots in finite fields”, *Rend. Circ. Mat. Palermo* (2), **12**:2 (1963), 129–136.
- [6] M.-Ch. Chang, “On a question of Davenport and Lewis and new character sum bounds in finite fields”, *Duke Math. J.*, **145**:3 (2008), 409–442.
- [7] M.-Ch. Chang, *Burgess inequality in $\mathbb{F}_{p^2}$* , Preprint, 2009.
- [8] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge Univ. Press, Cambridge, 2006.
- [9] W. Banaszczyk, “Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$ ”, *Discrete Comput. Geom.*, **13**:2 (1995), 217–231.
- [10] W. M. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Math., **536**, Springer-Verlag, Berlin, 1976.

С. В. Конягин

Математический институт им. В. А. Стеклова РАН

E-mail: konyagin23@gmail.com

Поступило

18.08.2009

Исправленный вариант

21.10.2009