Math-Net.Ru

Общероссийский математический портал

Л. А. Бассальго, В. А. Зиновьев, О многочленах над конечным полем четной характеристики с максимальным значением модуля тригонометрической суммы, *Матем. заметки*, 2002, том 72, выпуск 2, 171–177

DOI: <https://doi.org/10.4213/mzm412>

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: 34.227.88.159

26 апреля 2023 г., 15:18:43

УДК 512.6

О МНОГОЧЛЕНАХ НАД КОНЕЧНЫМ ПОЛЕМ ЧЕТНОЙ ХАРАКТЕРИСТИКИ С МАКСИМАЛЬНЫМ ЗНАЧЕНИЕМ МОДУЛЯ ТРИГОНОМЕТРИЧЕСКОЙ СУММЫ

Л. А. Бассальго, В. А. Зиновьев

В статье изучаются тригонометрические суммы в конечных полях F_Q . Известна оценка Вейля таких сумм: $|S(f)| \leq (\deg f - 1)\sqrt{Q}$, где f – многочлен с коэффициентами из $F(Q)$. Построены два класса многочленов f , $(Q, 2) = 2$, для которых $|S(f)|$ принимает максимально возможное значение и, в частности, $|S(f)| = (\deg f - 1)\sqrt{Q}$.

Библиография: 3 названия.

1. Введение. Данная работа является естественным продолжением статьи [1]. Поэтому мы кратко приведем те сведения из нее, которые нам понадобятся. Пусть $q = 2^l$, $Q = q^m = 2^{lm}$, где l, m – целые положительные числа, $m \geq 3$, а $F_2 \subseteq F_q \subset F_Q$ – соответствующие конечные поля. Пусть далее

$$f(x) = a_1x + \dots + a_nx^n, \quad a_i \in F_Q,$$
$$S(f) = \sum_{x \in F_Q} (-1)^{\text{Tr}_Q(f(x))},$$

где $\text{Tr}_Q(x)$ – функция следа,

$$\text{Tr}_Q(x) = x + x^2 + x^{2^2} + \dots + x^{2^{l-1}}, \quad x \in F_Q.$$

Согласно известной оценке Вейля [2] модуль тригонометрической суммы ограничен сверху:

$$|S(f)| \leq (\deg f - 1)\sqrt{Q}.$$

Мы продолжаем начатое в [1] изучение $S(f)$ для многочленов $f(x)$ специального вида

$$f(x) = \sum_{s=0}^{\lfloor m/2 \rfloor} a_s x^{1+q^s}, \quad a_s \in F_Q, \quad (1)$$

Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований, грант № 99-01-00828, и фонда INTAS, грант № 00-738.

где $\text{Tr}_Q(f(x)) \neq \text{const}$ для $x \in F_Q$. Там мы свели исследование тригонометрической суммы многочлена $f(x)$ вида (1) от одной переменной над полем F_{q^m} к исследованию кратной тригонометрической суммы квадратичной формы от m переменных над полем F_q . Известно [2], что модуль кратной тригонометрической суммы квадратичной формы от m переменных вида

$$z_1 z_2 + z_3 z_4 + \dots + z_{2r-1} z_{2r}, \quad r \leq \left\lfloor \frac{m}{2} \right\rfloor, \quad (2)$$

равен q^{m-r} .

В [1] был изучен случай простейшей квадратичной формы $z_1 z_2$ и соответственно были построены два класса многочленов (в зависимости от четности и нечетности m) вида (1) с модулем тригонометрической суммы, равным q^{m-1} . В частности, при четных m на этих многочленах достигается оценка Вейля. В данной работе изучается случай квадратичной формы $z_1 z_2 + z_3 z_4$ и соответственно строятся два новых класса многочленов $f(x)$ вида (1) с $|S(f)| = q^{m-2}$. В частности, при четных m на этих многочленах достигается оценка Вейля (теорема 2).

Все эти построения основаны на легко извлекаемых из работы [1] достаточных условиях на коэффициенты многочлена вида (1), при которых его тригонометрическая сумма равна кратной тригонометрической сумме квадратичной формы (2). Здесь мы выпишем эти условия в явном виде (так как эти условия и их дальнейшее использование слегка различаются в зависимости от четности и нечетности m , то мы сразу разделим последующее изложение на две части и в начале каждой из них приведем эти условия в качестве предложений 1 и 2).

2. Случай $m = 2k$.

ПРЕДЛОЖЕНИЕ 1 [1]. Пусть $\{\alpha_i, \beta_i, i = 1, \dots, r\}$ – элементы поля $F_{q^{2k}}$, линейно независимые над F_q . Тогда модуль тригонометрической суммы многочлена $f(x)$ типа (1) с коэффициентами $a_s, s = 0, 1, \dots, k$, удовлетворяющими соотношениям

$$\begin{aligned} a_0 &= \sum_{i=1}^r \alpha_i \beta_i, & a_s &= \sum_{i=1}^r \alpha_i \beta_i^{q^s} + \alpha_i^{q^s} \beta_i, & s &= 1, \dots, k-1, \\ a_k + a_k^{q^k} &= \sum_{i=1}^r \alpha_i \beta_i^{q^k} + \alpha_i^{q^k} \beta_i, \end{aligned}$$

равен q^{m-r} .

Конечно, значение q^{m-r} весьма далеко от оценки Вейля, которая в данном случае выглядит так:

$$|S(f)| \leq (\deg f - 1) \sqrt{Q} \leq q^m, \quad (3)$$

ибо, вообще говоря, степень многочлена $f(x)$ равна $q^k + 1$. Однако если мы сумеем обратить в нуль r последних коэффициентов многочлена $f(x)$, то получим многочлен степени $q^{k-r} + 1$, на котором достигается оценка Вейля. Сразу отметим, что в силу той же оценки это наименьшая возможная степень многочлена $f(x)$. Укажем также естественное ограничение: $k \geq r + 1$, ибо при $k = r$ многочлен $f(x)$ превращается в одночлен $a_0 x^2$, тригонометрическая сумма которого в поле четной характеристики равна 0.

Из предложения 1 вытекает, что возможно обратить в нуль r последних коэффициентов многочлена $f(x)$, если существует линейно независимое над F_q решение системы r уравнений над полем $F_{q^{2k}}$ относительно переменных $\alpha_i, \beta_i, i = 1, \dots, r$:

$$\sum_{i=1}^r (\alpha_i \beta_i^{q^s} + \alpha_i^{q^s} \beta_i) = 0, \quad s = k - r + 1, \dots, k - 1,$$

$$\sum_{i=1}^r (\alpha_i \beta_i^{q^k} + \alpha_i^{q^k} \beta_i) = 0.$$

Если такое решение существует, то соответствующий многочлен $f(x)$ имеет степень $q^{k-r} + 1$ и $|S(f)| = q^{2k-r}$, что совпадает с оценкой Вейля (3). В общем случае (при любых r и $k, k \geq r + 1$) мы не умеем решать эту систему (и даже не умеем доказывать существование соответствующего решения). Однако для первого нетривиального случая ($r = 2$) мы укажем, как получаются все линейно независимые над F_q решения этой системы, правда только в подполе F_{q^k} , а не во всем поле $F_{q^{2k}}$ (отсюда и ограничение $k \geq 4$ в утверждении 1, ибо в подполе F_{q^3} не существует четырех линейно независимых над F_q элементов).

УТВЕРЖДЕНИЕ 1. Пусть $k \geq 4$. Тогда существует линейно независимое над F_q решение $(\alpha_0, \beta_0, \xi_0, \lambda_0)$ следующей системы двух уравнений над полем $F_{q^{2k}}$:

$$\begin{aligned} \alpha_0 \beta_0^{q^k} + \alpha_0^{q^k} \beta_0 + \xi_0 \lambda_0^{q^k} + \xi_0^{q^k} \lambda_0 &= 0, \\ \alpha_0 \beta_0^{q^{k-1}} + \alpha_0^{q^{k-1}} \beta_0 + \xi_0 \lambda_0^{q^{k-1}} + \xi_0^{q^{k-1}} \lambda_0 &= 0. \end{aligned} \quad (4)$$

ДОКАЗАТЕЛЬСТВО. Решение этой системы мы будем искать в подполе F_{q^k} , и, на самом деле, мы найдем все такие решения. Действительно, в этом случае первое уравнение системы (4) выполнено автоматически и, следовательно, задача сводится к решению второго уравнения. Мы же рассмотрим несколько более общее уравнение, частным случаем которого и будет второе уравнение системы (4). Итак, следующая теорема завершает доказательство утверждения 1.

ТЕОРЕМА 1. Пусть e и t — целые числа, где $1 \leq e \leq t, t \geq 4$ и e и t взаимно просты. Тогда существует линейно независимое над F_q решение (x, y, u, v) следующего уравнения в поле F_{q^t} :

$$xy^{q^e} + x^{q^e}y + uv^{q^e} + u^{q^e}v = 0. \quad (5)$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим в поле F_{q^t} уравнение

$$xy^{q^e} + x^{q^e}y = A, \quad A \in F_{q^t}. \quad (6)$$

Обозначим через $\Omega(A)$ множество решений этого уравнения, т.е. множество упорядоченных пар (x, y) , удовлетворяющих (6). Следующие две леммы могут быть непосредственно проверены.

ЛЕММА 1. Пусть $(x_0, y_0) \in \Omega(A)$. Тогда x_0 и y_0 линейно зависимы над F_q , если и только если $A = 0$.

ЛЕММА 2. Пусть $(x_0, y_0) \in \Omega(A)$, $A \neq 0$, и $a, b, c, d \in F_q$. Тогда $(ax_0 + by_0, cx_0 + dy_0) \in \Omega(A)$, если и только если $ad + bc = 1$.

Обе эти леммы используются при доказательстве леммы 3.

ЛЕММА 3. Пусть $(x_0, y_0) \in \Omega(A)$ и $(u_0, ax_0 + by_0) \in \Omega(A)$, где $A \neq 0$ и $a, b \in F_q$. Тогда u_0, x_0, y_0 линейно зависимы над F_q .

ДОКАЗАТЕЛЬСТВО. Пусть $c, d \in F_q$ таковы, что $ad + bc = 1$. Тогда по лемме 2 пара $(cx_0 + dy_0, ax_0 + by_0) \in \Omega(A)$. Следовательно,

$$(cx_0 + dy_0)(ax_0^{q^e} + by_0^{q^e}) + (cx_0^{q^e} + dy_0^{q^e})(ax_0 + by_0) = A.$$

С другой стороны, по условию леммы

$$u_0(ax_0^{q^e} + by_0^{q^e}) + u_0^{q^e}(ax_0 + by_0) = A.$$

Складывая эти два равенства, получаем, что

$$(u_0 + cx_0 + dy_0)(ax_0 + by_0)^{q^e} + (u_0 + cx_0 + dy_0)^{q^e}(ax_0 + by_0) = 0,$$

и поэтому по лемме 1 элементы $u_0 + cx_0 + dy_0$ и $ax_0 + by_0$ линейно зависимы над F_q .

Обозначим через

$$\begin{aligned} \Omega_{(x_0, y_0)}(A) = \{ (u_0, v_0) \in \Omega(A) : u_0 = ax_0 + by_0, v_0 = cx_0 + dy_0, \\ a, b, c, d \in F_q, ad + bc = 1 \}. \end{aligned} \quad (7)$$

ЛЕММА 4. Пусть $(x_0, y_0) \in \Omega(A)$ и $(u_0, v_0) \in \Omega(A)$, но $(u_0, v_0) \notin \Omega_{(x_0, y_0)}(A)$, где $A \neq 0$. Тогда элементы x_0, y_0, u_0, v_0 линейно независимы над F_q .

ДОКАЗАТЕЛЬСТВО. Предположим, что элементы x_0, y_0, u_0, v_0 линейно зависимы. Без ограничения общности можно считать, что $v_0 = a'x_0 + b'y_0 + c'u_0$, $a', b', c' \in F_q$ и $(a', b', c') \neq (0, 0, 0)$. Так как $(u_0, v_0) \in \Omega(A)$, то

$$\begin{aligned} u_0v_0^{q^e} + u_0^{q^e}v_0 &= u_0(a'x_0 + b'y_0 + c'u_0)^{q^e} + u_0^{q^e}(a'x_0 + b'y_0 + c'u_0) \\ &= u_0(a'x_0 + b'y_0)^{q^e} + u_0^{q^e}(a'x_0 + b'y_0) = A. \end{aligned}$$

Но это означает, что $(u_0, a'x_0 + b'y_0) \in \Omega(A)$, и по лемме 3 элементы u_0, x_0, y_0 линейно зависимы над F_q . Следовательно, и элементы v_0, x_0, y_0 также линейно зависимы над F_q и согласно лемме 2 пара $(u_0, v_0) \in \Omega_{(x_0, y_0)}(A)$, что противоречит условию леммы.

Из леммы 4 следует, что множество $\Omega(A)$ разбивается на непересекающиеся подмножества $\Omega_{(x_0, y_0)}(A)$. Взяв для любого $A \in F_{q^t}^*$ две любые пары элементов (x_0, y_0) и (u_0, v_0) из $\Omega(A)$ таких, что

$$\Omega_{(x_0, y_0)}(A) \cap \Omega_{(u_0, v_0)}(A) = \emptyset,$$

мы получим линейно независимое над F_q решение (x_0, y_0, u_0, v_0) уравнения (5), и каждое такое решение получается указанным способом. Для завершения доказательства теоремы 1 нам осталось оценить снизу число различных линейно независимых над F_q решений уравнения (5). Так как с учетом леммы 1 любая пара (x, y) элементов поля F_{q^t} , линейно независимых над F_q , является решением уравнения (6) для некоторого ненулевого значения A , а число таких пар равно $(q^t - 1)(q^t - q)$, то

$$\sum_{A \in F_{q^t}^*} |\Omega(A)| = (q^t - 1)(q^t - q). \quad (8)$$

С другой стороны, из (7) следует, что для любых $A \in F_{q^t}^*$ и $(x_0, y_0) \in \Omega(A)$

$$|\Omega_{(x_0, y_0)}(A)| = |\{(a, b, c, d) \in (F_q)^4 : ad + bc = 1\}| = q^3 - q. \quad (9)$$

Из равенств (8) и (9) вытекает, что число $\omega(t)$ различных линейно независимых над F_q решений уравнения (5) равно

$$\omega(t) = \sum_{A \in F_{q^t}^*} |\Omega(A)| (|\Omega(A)| - (q^3 - q)).$$

Отсюда и из равенства (8) вытекает, что

$$\omega(t) \geq (q^t - 1)(q^t - q)(q^t - q^3), \quad (10)$$

что и завершает доказательство теоремы 1, так как при $t \geq 4$ правая часть неравенства (10) больше нуля.

ЗАМЕЧАНИЕ 1. Из доказательства теоремы 1 ясно, что при $t = k$ и $e = k - 1$ мы не только указываем способ получения всех линейно независимых решений $(\alpha_0, \beta_0, \xi_0, \lambda_0)$ системы (4) в подполе F_{q^k} , но и можем оценить снизу число различных многочленов $f(x)$ вида (1) степени $q^{k-2} + 1$, удовлетворяющих границе Вейля. В самом деле, правая часть неравенства (10) оценивает снизу число линейно независимых над F_q различных упорядоченных четверок $(\alpha_0, \beta_0, \xi_0, \lambda_0)$, порождающих наши многочлены $f(x)$. Конечно, некоторые из этих четверок порождают один и тот же многочлен, но число таких четверок возможно оценить сверху.

Пусть коэффициенты a_s , $s = 0, 1, \dots, k$, многочлена $f(x)$ фиксированы. Число четверок $(\alpha_0, \beta_0, \xi_0, \lambda_0)$, порождающих этот многочлен, заведомо не превосходит числа различных решений следующей системы двух уравнений над F_{q^k} относительно неизвестных $\alpha_0, \beta_0, \xi_0, \lambda_0$:

$$\begin{aligned} a_0 &= \alpha_0 \beta_0 + \xi_0 \lambda_0, \\ a_1 &= \alpha_0 \beta_0^q + \alpha_0^q \beta_0 + \xi_0 \lambda_0^q + \xi_0^q \lambda_0. \end{aligned}$$

При заданных (a_0, a_1, a_2, a_3) число упорядоченных линейно независимых над F_q четверок $(\alpha_0, \beta_0, \xi_0, \lambda_0)$, удовлетворяющих этой системе, заведомо не превосходит

$$2(q - 1)(q^k - 1)(q^k - q)$$

(пара (ξ_0, λ_0) может быть выбрана $(q^k - 1)(q^k - q)$ способами; при этом число пар (α_0, β_0) , удовлетворяющих системе при фиксированных (ξ_0, λ_0) , не превосходит $2(q - 1)$).

Отсюда и из оценки (10) при $t = k$ и $e = k - 1$ следует, что число искомым различных многочленов $f(x)$ не меньше, чем

$$\mu(k) \stackrel{\text{def}}{=} \frac{1}{2} \cdot \frac{(q^k - q^3)}{(q - 1)}. \quad (11)$$

Итак, из предложения 1, утверждения 1 и замечания 1 вытекает основной результат этого пункта.

ТЕОРЕМА 2. Пусть k — целое число, $k \geq 4$. Тогда существует, по крайней мере, $\mu(k)$ различных многочленов $f(x)$ вида (1) степени $q^{k-2} + 1$ над полем $F_{q^{2k}}$, модуль тригонометрической суммы которых достигает оценки Вейля $|S(f)| = q^{2k-2}$.

ЗАМЕЧАНИЕ 2. Хотя при $k = 3$ наш метод не проходит, но в этом случае многочлен $f(x)$ превращается в двучлен

$$f(x) = a_0 x^2 + a_1 x^{q+1},$$

а про такие двучлены известно [3], что на них (при $a_0 = 0$ и $a_1 = 1$) достигается граница Вейля.

3. Случай $m = 2k + 1$.

ПРЕДЛОЖЕНИЕ 2 [1]. Пусть $\alpha_i, \beta_i, i = 1, \dots, r$, — элементы поля $F_{q^{2k+1}}$, линейно независимые над F_q . Тогда модуль тригонометрической суммы многочлена $f(x)$ вида (1) с коэффициентами $a_s, s = 0, 1, \dots, k$, удовлетворяющими соотношениям

$$\begin{aligned} a_0 &= \sum_{i=1}^r \alpha_i \beta_i, \\ a_s &= \sum_{i=1}^r \alpha_i \beta_i^{q^s} + \alpha_i^{q^s} \beta_i, \quad s = 1, \dots, k, \end{aligned}$$

равен q^{m-r} .

Все дальнейшее изложение весьма близко к изложению п. 2, расходясь с ним лишь в некоторых частностях, которые мы и отметим.

Прежде всего, заметим, что здесь мы можем попытаться обратить в нуль лишь $r - 1$ последних коэффициентов многочлена $f(x)$ и получить многочлен степени $q^{k-r+1} + 1$, на котором достигается не оценка Вейля, равная в этом случае $q^{m-r+1/2}$, а максимальное значение модуля тригонометрической суммы многочленов вида (1), равное q^{m-r} (так как модуль кратной тригонометрической суммы от m переменных над полем четной характеристики F_q принимает лишь значения q^t , где t — целое число [2]).

Из предложения 2 вытекает, что возможно обратить в нуль $r - 1$ последних коэффициентов многочлена $f(x)$, если существует линейно независимое над F_q решение системы $r - 1$ уравнений над полем $F_{q^{2k+1}}$ относительно переменных $\alpha_i, \beta_i, i = 1, \dots, r$:

$$\sum_{i=1}^r (\alpha_i \beta_i^{q^s} + \alpha_i^{q^s} \beta_i) = 0, \quad s = k - r + 2, \dots, k.$$

Если такое решение существует, то соответствующий многочлен $f(x)$ имеет степень $q^{k-r+1} + 1$ и $|S(f)| = q^{2k+1-r}$.

В общем случае (при любых r и k , $k \geq r$) мы не умеем решать эту систему (и даже не умеем доказывать существование соответствующего решения), однако для первого нетривиального случая ($r = 2$), когда система превращается в одно уравнение, мы можем указать, как получаются все линейно независимые над F_q решения этого уравнения в поле $F_{q^{2k+1}}$. Действительно, мы это уже проделали в теореме 1, частным случаем которой при $t = 2k + 1$ и $e = k$ является следующее утверждение.

УТВЕРЖДЕНИЕ 2. Пусть $k \geq 2$. Тогда существует линейно независимое над F_q решение $(\alpha_0, \beta_0, \xi_0, \lambda_0)$ следующего уравнения в поле $F_{q^{2k+1}}$:

$$\alpha_0 \beta_0^{q^k} + \alpha_0^{q^k} \beta_0 + \xi_0 \lambda_0^{q^k} + \xi_0^{q^k} \lambda_0 = 0.$$

ЗАМЕЧАНИЕ 3. Совершенно аналогично замечанию 1 можно показать, что число различных многочленов вида (1) степени $q^{k-1} + 1$ с максимальным значением модуля тригонометрической суммы не меньше, чем

$$\nu(k) \stackrel{\text{def}}{=} \frac{1}{2} \cdot \frac{(q^{2k+1} - q^3)}{(q - 1)}. \quad (12)$$

Итак, из предложения 2, утверждения 2 и замечания 3 вытекает основной результат данного пункта.

ТЕОРЕМА 3. Пусть k – целое число, $k \geq 2$. Тогда существует, по крайней мере, $\nu(k)$ различных многочленов $f(x)$ вида (1) степени $q^{k-1} + 1$ над полем $F_{q^{2k+1}}$, модуль тригонометрической суммы которых достигает максимально возможного значения, равного $|S(f)| = q^{2k-1}$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Бассальго Л. А., Зиновьев В. А. Многочлены специального вида над конечным полем с максимальным модулем тригонометрической суммы // УМН. 1997. Т. 52. № 2. С. 31–44.
- [2] Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.
- [3] Moreno O., Moreno C. J. The MacWilliams–Sloane conjecture on the tightness of the Carlitz–Uchiyama bound and the weights of duals of BCH codes // IEEE Trans. Information Theory. 1994. V. 40. № 6. P. 1894–1907.

Институт проблем передачи информации РАН
E-mail: bass@iitp.ru

Поступило
27.11.2001