Math-Net.Ru

Общероссийский математический портал

Л. А. Бассальго, В. А. Зиновьев, О многочленах специального вида над конечным полем с точным значением тригонометрической суммы, *Матем. заметки*, 2007, том 82, выпуск 1, 3–10

DOI: <https://doi.org/10.4213/mzm3747>

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: 54.198.187.58

26 апреля 2023 г., 17:21:42

УДК 512.62

О многочленах специального вида над конечным полем с точным значением тригонометрической суммы

Л. А. Бассалыго, В. А. Зиновьев

Приведена явная конструкция многочленов специального вида над конечным полем, тригонометрическая сумма которых в точности известна.

Библиография: 4 названия.

Пусть $q = p^l$, $Q = q^m = p^{lm}$, где p – простое число, l, m – целые положительные числа, $m \geq 2$, и $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \mathbb{F}_Q$ – соответствующие конечные поля. Пусть далее

$$f(x) = a_1x + \dots + a_nx^n, \quad a_i \in \mathbb{F}_Q,$$
$$S(f) = \sum_{x \in \mathbb{F}_Q} \exp \left\{ \frac{2\pi i \operatorname{Tr}_Q(f(x))}{p} \right\}, \quad (1)$$

где $\operatorname{Tr}_Q(x)$ – функция следа,

$$\operatorname{Tr}_Q(x) = x + x^p + x^{p^2} + \dots + x^{p^{l-1}}, \quad x \in \mathbb{F}_Q.$$

Нам понадобится также представление $\operatorname{Tr}_Q(x)$ в виде

$$\operatorname{Tr}_Q(x) = \operatorname{Tr}_q(\operatorname{Tr}_{Q \rightarrow q}(x)), \quad (2)$$

где

$$\operatorname{Tr}_{Q \rightarrow q}(x) = x + x^q + \dots + x^{q^{m-1}}, \quad x \in \mathbb{F}_Q.$$

В [1] было указано, что нахождение тригонометрической суммы многочлена от одной переменной над полем $\mathbb{F}_{q^m}$ сводится к исследованию кратной тригонометрической суммы многочлена от m переменных над полем $\mathbb{F}_q$. Действительно, пусть $\Phi(x)$ – произвольный многочлен над полем $\mathbb{F}_Q$, $Q = q^m$. Зафиксируем базис $\gamma_0, \gamma_1, \dots, \gamma_{m-1}$ поля $\mathbb{F}_Q$ над полем $\mathbb{F}_q$: любой элемент $x \in \mathbb{F}_Q$ представим в виде

$$x = \sum_{s=0}^{m-1} x_s \gamma_s, \quad x_s \in \mathbb{F}_q. \quad (3)$$

Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований, грант № 06-01-00226.

Положим

$$G_{\Phi}(x_0, x_1, \dots, x_{m-1}) = \text{Tr}_{Q \rightarrow q} \Phi \left(\sum_{s=0}^{m-1} x_s \gamma_s \right). \quad (4)$$

Ясно, что $G_{\Phi}(x_0, \dots, x_{m-1})$ – многочлен от m переменных над полем $\mathbb{F}_q$, т.е. с коэффициентами из поля $\mathbb{F}_q$. По определению кратной тригонометрической суммы

$$S_m(G_{\Phi}(x_0, \dots, x_{m-1})) = \sum_{x_0, \dots, x_{m-1} \in \mathbb{F}_q} \exp \left\{ \frac{2\pi i \text{Tr}_q(G_{\Phi}(x_0, \dots, x_{m-1}))}{p} \right\}$$

и в силу (1), (2), (4) имеем, что

$$S(\Phi(x)) = S_m(G_{\Phi}(x_0, \dots, x_{m-1})).$$

Конечно, такое сведение помогает лишь в том случае, когда мы можем вычислить кратную тригонометрическую сумму. Так как тригонометрическая сумма для некоторых частных случаев квадратичных форм известна [2], [3], то в предыдущих работах [1], [4] мы использовали такой подход для полей четной характеристики и описали некоторые классы многочленов, тригонометрическая сумма которых совпадает с тригонометрическими суммами следующих простейших квадратичных форм от m переменных:

$$z_1 z_2, \quad z_1^2 + z_1 z_2 + a z_2^2, \quad z_1 z_2 + z_3 z_4.$$

Здесь мы используем тот же подход для поля $\mathbb{F}_Q$ произвольной характеристики p ($p \geq 2$) и описываем класс многочленов, сводимых к простейшей форме степени s ($s \leq m$) от m переменных:

$$z_1 z_2 \cdots z_s.$$

Тригонометрическая сумма такой формы известна и легко вычисляется. Действительно, по определению

$$\begin{aligned} S_m(z_1 \cdots z_s) &= \sum_{z_1, \dots, z_m \in \mathbb{F}_q} \exp \left\{ \frac{2\pi i}{p} \text{Tr}(z_1 \cdots z_s) \right\} \\ &= \sum_{z_1, \dots, z_s \in \mathbb{F}_q} \sum_{z_{s+1}, \dots, z_m \in \mathbb{F}_q} \exp \left\{ \frac{2\pi i}{p} \text{Tr}(z_1 \cdots z_s) \right\} \\ &= q^{m-s} \left(\sum_{z_1 \cdots z_{s-1} \neq 0} \sum_{z_s \in \mathbb{F}_q} \exp \left\{ \frac{2\pi i}{p} \text{Tr}(z_1 \cdots z_s) \right\} + \sum_{z_1 \cdots z_{s-1} = 0, z_s \in \mathbb{F}_q} 1 \right) \\ &= q^{m-s} (0 + q^s - q(q-1)^{s-1}) = q^m - q^{m-s+1}(q-1)^{s-1}, \end{aligned}$$

где $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

К такой форме степени s мы будем сводить многочлены $f(x) \in \mathbb{F}_Q[x]$ следующего вида:

$$f(x) = \sum_{0 \leq i_1, \dots, i_s \leq m-1} a_{i_1, \dots, i_s} x^{q^{i_1} + \dots + q^{i_s}}, \quad a_{i_1, \dots, i_s} \in \mathbb{F}_Q. \quad (5)$$

Выпишем многочлен $F(x)$, полученный из $f(x)$ применением функции следа на поле $\mathbb{F}_q$:

$$\begin{aligned} F(x) &= \text{Tr}_{Q \rightarrow q}(f(x)) = \text{Tr}_{Q \rightarrow q} \left(\sum_{0 \leq i_1, \dots, i_s \leq m-1} a_{i_1, \dots, i_s} x^{q^{i_1} + \dots + q^{i_s}} \right) \\ &= \sum_{t=0}^{m-1} \left(\sum_{0 \leq i_1, \dots, i_s \leq m-1} a_{i_1, \dots, i_s}^{q^t} x^{q^{i_1+t} + \dots + q^{i_s+t}} \right) \\ &= \sum_{0 \leq u_1, \dots, u_s \leq m-1} \left(\sum_{t=0}^{m-1} a_{u_1-t, \dots, u_s-t}^{q^t} \right) x^{q^{u_1} + \dots + q^{u_s}}, \end{aligned}$$

где индексы берутся по модулю m .

Прежде всего выясним, когда многочлен $F(x)$ представляется в виде произведения s линейаризованных многочленов $z_i(x) \in \mathbb{F}_q[x]$, линейно независимых над полем $\mathbb{F}_q$:

$$z_i(x) = \sum_{j=0}^{m-1} \alpha_{i,j} x^{q^j}, \quad i = 1, \dots, s. \quad (6)$$

Приравняем оба многочлена $F(x)$ и $z_1(x) \cdots z_s(x)$:

$$\begin{aligned} \prod_{i=1}^s z_i(x) &= \prod_{i=1}^s \left(\sum_{j=0}^{m-1} \alpha_{i,j} x^{q^j} \right) = \sum_{u_1, \dots, u_s} \prod_{i=1}^s \alpha_{i, u_i} x^{q^{u_1} + \dots + q^{u_s}} \\ &= \sum_{u_1, \dots, u_s} \left(\sum_{t=0}^{m-1} a_{u_1-t, \dots, u_s-t}^{q^t} \right) x^{q^{u_1} + \dots + q^{u_s}} = F(x). \end{aligned}$$

Ясно, что для выполнения равенства $F(x) = \prod_{i=1}^s z_i(x)$ достаточно, чтобы для любого набора $u_1, \dots, u_s$ выполнялось равенство

$$\sum_{t=0}^{m-1} a_{u_1-t, \dots, u_s-t}^{q^t} = \prod_{i=1}^s \alpha_{i, u_i}, \quad 0 \leq u_1, u_2, \dots, u_s \leq m-1. \quad (7)$$

Положим

$$A_j(u_1, \dots, u_s) = \sum_{t=0}^{m-1} a_{u_1-j-t, \dots, u_s-j-t}^{q^t}, \quad j = 0, \dots, m-1.$$

УТВЕРЖДЕНИЕ 1. Пусть $F(x) = z_1(x) \cdots z_s(x)$. Тогда для любого набора $u_1, \dots, u_s$, $0 \leq u_1, u_2, \dots, u_s \leq m-1$, и для любого j , $j = 0, \dots, m-1$, имеет место следующее равенство:

$$A_j(u_1, \dots, u_s) = A_0^{q^{-j}}(u_1, \dots, u_s).$$

ДОКАЗАТЕЛЬСТВО. Вводя новый параметр l , $j+t=l$, получаем

$$\begin{aligned} A_j(u_1, \dots, u_s) &= \sum_{t=0}^{m-1} a_{u_1-j-t, \dots, u_s-j-t}^{q^t} = \sum_{l=0}^{m-1} a_{u_1-l, \dots, u_s-l}^{q^{l-j}} \\ &= \left(\sum_{l=0}^{m-1} a_{u_1-l, \dots, u_s-l}^{q^l} \right)^{q^{-j}} = A_0^{q^{-j}}(u_1, \dots, u_s). \end{aligned}$$

Из этого утверждения в силу (7) вытекают следующие условия на коэффициенты α_{i,u_i} многочленов $z_i(x)$:

$$\prod_{i=1}^s \alpha_{i,u_i-j} = \left(\prod_{i=1}^s \alpha_{i,u_i} \right)^{q^{-j}}, \quad j = 1, 2, \dots, m-1. \quad (8)$$

Нетрудно видеть, что m^s соотношений (7) на m^s коэффициентов $a_{u_1, \dots, u_s}$ многочлена $f(x)$ естественным образом разбивают эти коэффициенты на m^{s-1} групп по m коэффициентов в каждой, так что коэффициенты из одной группы и только они входят ровно в m соотношений (7). При этом, если выполнено условие (8), то все m соотношений для коэффициентов одной группы сводятся к одному. Поэтому в дальнейшем положим равным нулю первый индекс u_1 ($u_1 = 0$) всех коэффициентов $a_{u_1, \dots, u_s}$ и получим для любого набора $u_2, \dots, u_s$ следующую систему соотношений, эквивалентную (7):

$$\sum_{t=0}^{m-1} a_{-t, u_2-t, \dots, u_s-t}^q = \alpha_{1,0} \prod_{i=2}^s \alpha_{i,u_i}, \quad 0 \leq u_2, \dots, u_s \leq m-1. \quad (9)$$

Таким образом, условия (8) и (9) являются достаточными для равенства многочленов $F(x)$ и $z_1(x) \cdots z_s(x)$. Перейдем теперь к многочленам от m переменных, используя представление (3). В этом случае многочлен

$$G_F(x_0, x_1, \dots, x_{m-1}) = F\left(\sum_{l=0}^{m-1} x_l \gamma_l\right)$$

является многочленом от m переменных с коэффициентами из поля $\mathbb{F}_q$. Ясно, что

$$G_F(x_0, \dots, x_{m-1}) = z'_1(x_0, \dots, x_{m-1}) \cdots z'_s(x_0, \dots, x_{m-1}),$$

где

$$z'_i(x_0, \dots, x_{m-1}) = z_i\left(\sum_{l=0}^{m-1} x_l \gamma_l\right) = \sum_{j=0}^{m-1} \alpha_{i,j} \left(\sum_{l=0}^{m-1} x_l \gamma_l\right)^{q^j} = \sum_{l=0}^{m-1} x_l \left(\sum_{j=0}^{m-1} \alpha_{i,j} \gamma_l^{q^j}\right).$$

Для того, чтобы тригонометрическая сумма $S_m(G_F(x_0, \dots, x_{m-1}))$ равнялась $S_m(z'_1(x_0, \dots, x_{m-1}) \cdots z'_s(x_0, \dots, x_{m-1}))$, достаточно, чтобы коэффициенты каждой линейной формы $z'_i(x_0, \dots, x_{m-1})$, $i = 1, \dots, s$, принадлежали $\mathbb{F}_q$, т.е., чтобы выполнялось условие

$$\sum_{j=0}^{m-1} \alpha_{i,j} \gamma_l^{q^j} \in \mathbb{F}_q, \quad i = 1, \dots, s, \quad l = 0, \dots, m-1. \quad (10)$$

Напомним, что ранее мы потребовали линейную независимость форм $z_i(x)$ над полем $\mathbb{F}_q$, что эквивалентно линейной независимости форм $z'_i(x_0, x_1, \dots, x_{m-1})$ над $\mathbb{F}_q$. Итак, приведенные выше рассуждения приводят к следующему результату.

ТЕОРЕМА 1. Пусть коэффициенты $\alpha_{i,j}$ из (6) таковы, что матрица $\|\alpha_{i,j}\|$ имеет ранг s над $\mathbb{F}_q$ и выполнены условия (8) и (10). Тогда любой многочлен $f(x)$ вида (5), коэффициенты которого удовлетворяют системе соотношений (9), имеет следующую тригонометрическую сумму:

$$S(f) = q^{m-s+1}(q^{s-1} - (q-1)^{s-1}). \quad (11)$$

Для применения теоремы естественно явно указать набор коэффициентов $\alpha_{i,j}$, удовлетворяющих перечисленным в теореме условиям. Положим

$$\alpha_{i,u_i} = (\alpha_{i,0})^{q^{u_i}}, \quad i = 1, \dots, s, \quad (12)$$

где $\alpha_{i,0} \in \mathbb{F}_Q$. Нетрудно проверить, что условия (8) при этом выполняются:

$$\prod_{i=1}^s \alpha_{i,u_i-j} = \prod_{i=1}^s (\alpha_{i,0})^{q^{u_i-j}} = \left(\prod_{i=1}^s (\alpha_{i,0})^{q^{u_i}} \right)^{q^{-j}} = \left(\prod_{i=1}^s \alpha_{i,u_i} \right)^{q^{-j}}.$$

Условия (10) в этом случае также выполняются:

$$\sum_{j=0}^{m-1} \alpha_{i,j} \gamma_l^{q^j} = \sum_{j=0}^{m-1} \alpha_{i,0}^{q^j} \gamma_l^{q^j} = \text{Tr}_{Q \rightarrow q}(\alpha_{i,0} \gamma_l),$$

так как $\text{Tr}_{Q \rightarrow q}(b)$ принадлежит $\mathbb{F}_q$ для любого элемента $b \in \mathbb{F}_Q$.

При выполнении условия (12) линейные формы $z'_i(x_0, \dots, x_{m-1})$, $i = 1, \dots, s$, над $\mathbb{F}_q$ имеют вид

$$z'_i(x_0, \dots, x_{m-1}) = \sum_{l=0}^{m-1} x_l \text{Tr}_{Q \rightarrow q}(\alpha_{i,0} \gamma_l).$$

Поэтому они линейно независимы над $\mathbb{F}_q$ тогда и только тогда, когда элементы $\alpha_{i,0} \in \mathbb{F}_Q$, $i = 1, \dots, s$, линейно независимы над полем $\mathbb{F}_q$, ибо ранг матрицы $\|\text{Tr}_{Q \rightarrow q}(\alpha_{i,0} \gamma_l)\|$, $i = 1, \dots, s$, $l = 0, 1, \dots, m-1$, равен s в этом и только этом случае.

Поэтому имеет место следующий результат, непосредственно вытекающий из теоремы.

СЛЕДСТВИЕ 1. Пусть элементы $\alpha_{1,0}, \dots, \alpha_{s,0}$ поля $\mathbb{F}_Q$ линейно независимы над полем $\mathbb{F}_q$. Тогда любой многочлен $f(x)$, коэффициенты которого удовлетворяют системе соотношений

$$\sum_{t=0}^{m-1} a_{-t, u_2-t, \dots, u_s-t}^{q^t} = \prod_{i=1}^s (\alpha_{i,0})^{q^{u_i}}, \quad \text{где } u_1 = 0, \quad 0 \leq u_2, \dots, u_s \leq m-1, \quad (13)$$

имеет тригонометрическую сумму, определяемую равенством (11).

Недостатком полученных утверждений является то, что многочлен $f(x)$ вида (5) записан не в стандартной форме (подобные члены не приведены). Однако из этих утверждений нетрудно извлечь результаты и для многочленов, приведенных в стандартном виде.

Для примера подробно разберем случай, когда $s = 2$ и m произвольно.

Запишем многочлен (5) в стандартном виде:

$$f(x) = \sum_{i_1=0}^{m-1} a_{i_1, i_1} x^{2q^{i_1}} + \sum_{0 \leq i_1 < i_2 \leq m-1} (a_{i_1, i_2} + a_{i_2, i_1}) x^{q^{i_1} + q^{i_2}}. \quad (14)$$

Тогда соотношения (13) принимают вид

$$\sum_{t=0}^{m-1} a_{-t, u_2-t}^{q^t} = \alpha_0 \beta_0^{q^{i_2}}, \quad i_2 = 0, 1, \dots, m-1, \quad (15)$$

где $\alpha_0 = \alpha_{1,0}$ и $\beta_0 = \alpha_{2,0}$ (еще раз напомним, что индексы берутся по модулю m). Таким образом, m^2 коэффициентов $f(x)$ должны удовлетворять m соотношениям (15). Тем самым, имеется богатый выбор для коэффициентов многочлена $f(x)$, тригонометрическая сумма которого в точности известна. Постараемся сейчас выбрать эти коэффициенты таким образом, чтобы степень многочлена $f(x)$ вида (14) была минимально возможной.

Заметим, что при $i_2 = 0$ первое соотношение (15) имеет вид

$$a_{0,0} + a_{-1,-1}^q + \dots + a_{-(m-1),-(m-1)}^{q^{m-1}} = \alpha_0 \beta_0.$$

Положим в этом соотношении все коэффициенты, кроме $a_{0,0}$, равными нулю, а $a_{0,0} = \alpha_0 \beta_0$. Заметим, что для каждого $i_2 \neq 0$ коэффициенты a_{0,i_2} и $a_{-i_2,0}$ входят в одно соотношение (напомним, что каждый коэффициент $f(x)$ входит ровно в одно соотношение (15)).

Начиная с этого места, удобнее рассматривать случаи четного и нечетного m раздельно.

Случай $m = 2k + 1$. Пусть $1 \leq i_2 \leq k$. Тогда в соотношении, включающем a_{0,i_2} , положим все остальные коэффициенты равными нулю, а $a_{0,i_2} = \alpha_0 \beta_0^{q^{i_2}}$. Пусть теперь $k + 1 \leq i_2 \leq 2k$. В соотношении, включающем a_{0,i_2} , положим все коэффициенты равными нулю, а $a_{-i_2,0} = \alpha_0^{q^{-i_2}} \beta_0$. Тогда $a_{-i_2,0}^{q^{i_2}} = \alpha_0 \beta_0^{q^{i_2}}$ и, следовательно, соответствующее соотношение (15) выполнено.

Таким образом, для $m = 2k + 1$ ($k \geq 1$) получаем следующее

УТВЕРЖДЕНИЕ 2. Пусть

$$f(x) = \alpha_0 \beta_0 x^2 + \sum_{i_2=1}^k (\alpha_0 \beta_0^{q^{i_2}} + \alpha_0^{q^{-i_2}} \beta_0) x^{1+q^{i_2}},$$

где α_0, β_0 – произвольные элементы поля $\mathbb{F}_{q^m}^*$. Тогда

1) если α_0, β_0 линейно независимы над $\mathbb{F}_q$, то

$$S(f) = S_m(z_1 z_2) = q^{m-1};$$

2) если $\beta_0 = c \alpha_0$, $c \in \mathbb{F}_q^*$, то

$$S(f) = S_m(c z_1^2) = q^{m-1} \cdot S(c z^2).$$

Случай $m = 2k$. Для всех $i_2 = 0, \dots, k - 1$ (соответственно $i_2 = k + 1, \dots, 2k - 1$) ситуация та же, что и для нечетного m , т.е. мы выбираем такие же коэффициенты $a_{0,i_2} = \alpha_0 \beta_0^{q^{i_2}}$ (соответственно $a_{-i_2,0} = \alpha_0^{q^{-i_2}} \beta_0$), а все остальные коэффициенты в соответствующих соотношениях (15) полагаем равными нулю. При $i_2 = k$ положим все остальные коэффициенты равными нулю, а $a_{0,k}$ и $a_{k,0}$ выберем так, чтобы выполнялось равенство $a_{0,k} + a_{k,0}^{q^k} = \alpha_0 \beta_0^{q^k}$. Отсюда следует, что выполняется и равенство $a_{k,0} + a_{0,k}^{q^k} = \alpha_0^{q^k} \beta_0$. Складывая эти равенства, получаем, что коэффициент многочлена при x^{1+q^k} , равный $a_{0,k} + a_{k,0}$, должен удовлетворять следующему уравнению:

$$(a_{0,k} + a_{k,0}) + (a_{0,k} + a_{k,0})^{q^k} = \alpha_0 \beta_0^{q^k} + \alpha_0^{q^k} \beta_0.$$

Пусть a_k – произвольный корень уравнения

$$a_k + a_k^{q^k} = \alpha_0 \beta_0^{q^k} + \alpha_0^{q^k} \beta_0. \quad (16)$$

Нетрудно видеть, что система уравнений

$$\begin{aligned} a_{k,0} + a_{0,k}^{q^k} &= \alpha_0^{q^k} \beta_0, \\ a_{0,k} + a_{k,0} &= a_k \end{aligned}$$

относительно неизвестных $a_{0,k}$ и $a_{k,0}$ имеет решение в поле $\mathbb{F}_{q^{2k}}$. Достаточно проверить, что уравнение

$$a_{k,0}^{q^k} - a_{k,0} = \alpha_0 \beta_0^{q^k} - a_k$$

имеет такое решение. Хорошо известно [2], что для этого необходимо и достаточно, чтобы

$$\mathrm{Tr}_{q^{2k} \rightarrow q^k}(\alpha_0 \beta_0^{q^k} - a_k) = 0,$$

что эквивалентно (16).

Итак имеет место следующее

УТВЕРЖДЕНИЕ 3. Пусть

$$f(x) = \alpha_0 \beta_0 x^2 + \sum_{i_2=1}^{k-1} (\alpha_0 \beta_0^{q^{i_2}} + \alpha_0^{q^{i_2}} \beta_0) x^{1+q^{i_2}} + a_k x^{1+q^k},$$

где α_0, β_0 – произвольные элементы поля $\mathbb{F}_{q^{2k}}^*$, а a_k – произвольный корень уравнения (16). Тогда

1) если α_0, β_0 линейно независимы над $\mathbb{F}_q$, то

$$S(f) = S_m(z_1 z_2) = q^{m-1};$$

2) если $\beta_0 = c \alpha_0$, $c \in \mathbb{F}_q^*$, то

$$S(f) = S_m(c z_1^2) = q^{m-1} \cdot S(c z^2).$$

Покажем теперь, что всегда можно выбрать элементы $\alpha_0, \beta_0 \in F_{q^m}^*$ так, чтобы коэффициент $a_k = 0$, т.е., чтобы выполнялось равенство

$$\alpha_0 \beta_0^{q^k} + \alpha_0^{q^k} \beta_0 = 0. \quad (17)$$

Действительно, все корни уравнения $z^{q^k} + z = 0$ лежат в поле $\mathbb{F}_{q^{2k}}$, ибо многочлен $z^{q^k} + z$ делит многочлен $z^{q^{2k}} - z$ (так как многочлен $z^k + 1$ делит многочлен $z^{2k} - 1$; см. [2; лемма 3.59]). Следовательно, при $k \geq 2$ и при $k = 1$ и $p \neq 2$ всегда существует решение $\alpha_0, \beta_0 \in \mathbb{F}_{q^m}^*$ уравнения (17) такое, что $\alpha_0/\beta_0 \notin \mathbb{F}_q$. Тем самым, получаем следующее

УТВЕРЖДЕНИЕ 4. Многочлен

$$f(x) = \alpha_0 \beta_0 x^2 + \sum_{i_2=1}^{k-1} (\alpha_0 \beta_0^{q^{i_2}} + \alpha_0^{q^{i_2}} \beta_0) x^{1+q^{i_2}},$$

где α_0, β_0 – произвольные элементы поля $\mathbb{F}_{q^{2k}}^*$, удовлетворяющие равенству (17) и линейно независимые над $\mathbb{F}_q$, имеет тригонометрическую сумму, модуль которой (равный q^{m-1}) достигает границы Вейля.

Заметим, что для четной характеристики утверждения 2–4 фактически содержались в [1; теоремы 6, 7 и следствие 1].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Л. А. Бассалыго, В. А. Зиновьев, “Многочлены специального вида над конечным полем с максимальным модулем тригонометрической суммы”, *УМН*, **52**:2 (1997), 31–44.
- [2] Р. Лидл, Г. Нидеррайтер, *Конечные поля*, Мир, М., 1988.
- [3] А. В. Малышев, *О представлении целых чисел положительными квадратичными формами*, Тр. МИАН, **65**, Наука, М., 1962.
- [4] Л. А. Бассалыго, В. А. Зиновьев, “О многочленах над конечным полем четной характеристики с максимальным значением модуля тригонометрической суммы”, *Матем. заметки*, **72**:2 (2002), 171–177.

Л. А. Бассалыго

Институт проблем передачи информации РАН

E-mail: bass@iitp.ru

Поступило

07.11.2006

В. А. Зиновьев

Институт проблем передачи информации РАН

E-mail: zinov@iitp.ru