Exact value of module of trigonometric sums over a finite field for the polynomials of special type

L.A. Bassalygo, V.A. Zinoviev
"Uspehi Matematicheskih Nauk", 1997, No. 1, to appear

We described all the polynomials of special type which have the maximal value of the module of the trigonometric sum over finite fields.

Let $q = p^l,\ Q = q^m = p^{lm}$, where p is prime, l, m are positive integers, $m > 1,\ F_p \subseteq F_q \subset F_Q$ be the corresponding finite fields. For

$$f(x) = a_1 x + \cdots + a_n x^n,\ a_i \in F_Q,$$

define

$$S(f) = \sum_{x \in F_Q} exp\{\frac{2\pi i Tr_Q(f(x))}{p}\}, \tag{1}$$

where

$$Tr_Q(x) = x + x^p + x^{p^2} + \cdots + x^{p^{lm-1}},\ x \in F_Q.$$

We need the following presentation of $Tr_Q(x)$:

$$Tr_Q(x) = Tr_q(Tr_{Q \to q}(x)), \tag{2}$$

where

$$Tr_{Q \to q}(x) = x + x^q + \cdots + x^{q^{m-1}},\ x \in F_Q.$$

In this paper we study the values of the module of trigonometric sums for the polynomials of the following special type

$$f(x) = \sum_{s=0}^{\lfloor m/2 \rfloor} a_s x^{1+q^s}, \ a_s \in F_Q \ , \ Tr_Q(f(x)) \neq const \qquad (3)$$

(i.e. we exclude the trivial case when $|S(f)| = Q$). Of course, we might investigate polynomials from larger class

$$f'(x) = \sum_{i,j=0}^{m-1} a_{ij} x^{q^i+q^j},$$

but from the relation $Tr_{Q\to q}(y) = Tr_{Q\to q}(y^q), \ y \in F_Q$, it follows, that for any polynomial $f'(x)$ there is a polynomial $f(x)$ of the type (3), such that

$$Tr_{Q\to q}(f'(x)) \ = \ Tr_{Q\to q}(f(x))$$

and, therefore, $S(f') = S(f)$.

In general the investigation of the trigonometric sums of the polynomials of one variable over the field F_{q^m} reduces to the investigation of the multiple trigonometric sums of the polynomial of m variables over the field F_q. Indeed, let $\Phi(x)$ be an arbitrary polynomial over the field $F_Q, \ Q = q^m$. Fix a basis $\gamma_0, \gamma_1, \ldots, \gamma_{m-1}$ of F_Q over the field F_q , any element $x \in F_Q$ present in the form

$$x = \sum_{s=0}^{m-1} x_s \gamma_s \ \ , \ x_s \in F_q.$$

Define

$$G(x_0, x_1, \ldots, x_{m-1} \ ) = \ Tr_{Q\to q}(\Phi(\sum_{s=0}^{m-1} x_s\gamma_s)) \ . \qquad (4)$$

It is clear, that $G(x_0, \ldots, x_{m-1})$ is a polynomial of m variables over the field F_q. By the definition of the multiple trigonometric sum

$$S_m(G(x_0, \ldots, x_{m-1})) = \sum_{x_0,\ldots,\ x_{m-1} \in \ F_q} exp\{\frac{2\pi i Tr_q(G(x_0, \ldots, x_{m-1}))}{p}\}$$

and using (4), we obtain that

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

For a given polynomial $G(x_0, \ldots, x_{m-1})$ it is possible to find the polynomial $\Phi(x)$ such that the equality (4) holds (see paper [1]). Of course, such reduction helps only in the case, when we can compute the multiple trigonometric sum. One such case - it is quadratic forms [2,3]. In paper [1] we showed, that for any quadratic form $g(x_0, \ldots, x_{m-1})$ the corresponding polynomial $\Phi(x)$ (see (4)) can be chosen in the form (3). On the other hand, it is not difficult to see, that for any polynomial $f(x)$ of the form (3) the corresponding polynomial $G(x_0, \ldots, x_{m-1})$ (see again (4)) is a quadratic form $g(x_0, \ldots, x_{m-1})$. It is known [2, 3], that the module of the trigonometric sum of quadratic forms from m variables over F_q take any value:

$$\begin{array}{ll} q^{r/2}, & \text{where } r = 2m-1,\ 2m-2, ...,\ m, \quad q \text{ odd}, \\ q^{r}, & \text{where } r = m-1,\ m-2, ...,\ \lceil m/2 \rceil, \quad q \text{ even}, \end{array}$$

and do not take any other nonzero ($\neq q^m$) values. Therefore we can tell the same about the module of the trigonometric sums for the polynomials of the form (3). Here we describe all the polynomials of the form (3) with the maximal value of the module of the trigonometric sum, and we give many examples of the polynomials for which the Weyl upper bound is exact.

I. The case of the odd characteristic ($p \geq 3$).

In this case the maximal value of the module of the trigonometric sum for the polynomials (3) is equal to $q^{m-\frac{1}{2}}$ [1] (for odd m this value coincides with the Weyl upper bound). Stepanov [4] gave the examples of such polynomials in the evident form. We describe here all such polynomials.

For odd q any polynomial (3) can be written as follows:

$$\phi(x) \ = \ a_0 x^2 \ + \ 2 \sum_{s=1}^{\lfloor m/2 \rfloor} a_s x^{1+q^s} \ . \qquad (5)$$

In order to find the coefficients of the corresponding (see (4)) quadratic form $g(x_0, ..., x_{m-1})$

$$g(x_0, ..., x_{m-1}) \ = \ Tr_{Q \to q}(\phi(\sum_{s=0}^{m-1} x_s \gamma_s)) \ = \ \sum_{u,v=0}^{m-1} c_{uv} x_u x_v, \ c_{uv} \ = \ c_{vu} \ ,$$

let's write first $Tr_{Q\to q}(\phi(x))$:

$$Tr_{Q\to q}(\phi(x)) \ = \ \sum_{i,j=0}^{m-1} b_{ij} x^{q^i+q^j} \ ,$$

where

$$\begin{array}{rcl} b_{ii} & = & a_0^{q^i} \ , \quad i = 0, 1, ..., m-1 \ , \\ b_{ij} & = & b_{ji} = \ a_{j-i}^{q^i} \ + \ a_{i-j}^{q^j}, i \neq j \ , \end{array} \qquad (6)$$

where the indices of the coefficients a_s are considered by module m and $a_s = 0$, if $s > \lfloor m/2 \rfloor$). Denote by $B = [b_{ij}]$ a symmetrical matrix of the coefficients b_{ij}. Then a symmetrical matrix of the coefficients $C = [c_{uv}]$ is defined as follows:

$$C \ = \ DBD^T \ ,$$

where

$$D \ = \ [\gamma_i^{q^j}] \ .$$

As D is a nonsingular matrix, the ranks of the matrices of C and B are equal: $rank\ (C) \ = \ rank\ (B)$. As $S(\phi(x)) \ = \ S_m(g(x_0, ..., x_{m-1}))$ and

$$|S_m(g)| \ = \ q^{m-\frac{1}{2}rank(C)} \ ,$$

then the following statement is valid:

Statement 1 *Let $\phi(x)$ be any polynomial of the type (5) and let a matrix B be defined by the relations (6). Then*

$$|S(\phi)| \ = \ q^{m-\frac{1}{2}rank(B)} \ .$$

As we consider only nontrivial case, when $rank\ (B) \neq 0$, then the maximal value of the module of this sum $S(\phi)$ corresponds to the case, when $rank\ (B) = 1$, and, therefore, our problem reduces to description of all the polynomial $\phi(x)$ of the type (5) such that the corresponding matrix B has a rank 1. The cases of odd m and even m we consider separately.

I.a. $m = 2k+1, k \geq 1$.

Theorem 1 *Let*

$$\phi(x) \;=\; a_0 x^2 \;+\; 2\sum_{s=1}^{k} a_s x^{1+q^s} \;.$$

Then

$$|S(\phi)| \;=\; q^{m-\frac{1}{2}}$$

(i.e. the value of $|S(\phi)|$ satisfies Weyl upper bound), if and only if

$$a_s \;=\; a_0^{\frac{q^s+1}{2}} \;,\; s = 1, ..., k \;, \tag{7}$$

where a_0 is an arbitrary nonzero element of F_{q^m}. The number of different such polynomials $\phi(x)$ is equal to $q^m - 1$.

Proof. As for odd m the matrix B looks as (see (6))

$$B \;=\; \begin{bmatrix} a_0 & a_1 & a_2 & ... & a_k & a_k^{q^{k+1}} & ... & a_2^{q^{2k-1}} & a_1^{q^{2k}} \\ a_1 & a_0^q & a_1^q & ... & a_{k-1}^q & a_k^q & ... & a_3^{q^{2k-1}} & a_2^{q^{2k}} \\ . & . & . & ... & . & . & ... & . & . \end{bmatrix},$$

its rank is equal to 1 if and only if the second row is proportional to the first row (any row of B is a cyclic shift of the previous row, where each element is taken to the power q). Therefore, if the second row is proportional to the first one, then the third row is proportional to the second row and so on. It is enough to check, that for given a_0 all the rest coefficients a_s $(s = 1, ..., k)$ are defined uniquely in accordance with (7). Indeed, the relations (7) follow directly from the proportionality of subrowes:

$$\begin{bmatrix} a_0 & a_1 & a_2 & ... & a_{k-1} & a_k \\ a_1 & a_0^q & a_1^q & ... & a_{k-2}^q & a_{k-1}^q \end{bmatrix}$$

(first we find a_1, then a_2 and so on). The coefficient a_1 may take two values

$$a_1 \;=\; \pm a_0^{\frac{q+1}{2}} \;,$$

but all the following coefficients $a_2, a_3, ..., a_k$ for given a_0 and a_1 are defined uniquely. So for given a_0 from the conditions of proportionality of the subrowes we have two solutions:

$$a_s \;=\; a_0^{\frac{q^s+1}{2}} \;,\; s = 1, 2, ..., k \;,$$

and

$$a_s \;=\; (-1)^s a_0^{\frac{q^s+1}{2}} \;,\; s=1,2,...,k\;.$$

But because of the condition that m is odd, all another conditions of proportionality are valid only for the first solution. As a_0 is any nonzero element of F_Q, $Q=q^m$, and all the rest elements $a_s, s=1,...,k$, are defined uniquely for given a_0, the number of different polynomials (5) with maximal module of the trigonometric sum is equal to q^m-1. □

Theorem 1 yields the idea, that there are the polynomials of type (5) of lower degree for which the Weil bound is exact. Indeed, consider the polynomials for which $a_{r+1}=\cdots=a_{\lfloor m/2\rfloor}=0$. The Weil bound for such polynomials (of degree q^r+1) is equal to $q^{r+k+\frac{1}{2}}$ and this bound is reached if and only if the rank of the corresponding matrix B is equal to $2(k-r)+1$. In Theorem 1 we studied the case when $r=k$ and we even described all such matricess. The general case is quite difficult for solution, but the other extremal case, when $r=1$ (the case $r=0$ is well known, as Gauss sums) we want to describe now, but only for the case, when the coefficients a_0, a_1 are the elements of F_q. For this case the matrix B looks as

$$B \;=\; \begin{bmatrix} a_0 & a_1 & 0 & \cdots & 0 & a_1 \\ a_1 & a_0 & a_1 & \cdots & 0 & 0 \\ 0 & a_1 & a_0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & a_0 & a_1 \\ a_1 & 0 & 0 & \cdots & a_1 & a_0 \end{bmatrix}.$$

The computations show that the rank of this matrix is equal to $2k-1$ if and only if the determinant $\Delta_k=\Delta_k(a_0,a_1)$ of the following matrix of size $k\times k$

$$\begin{bmatrix} a_0 & a_1 & 0 & \cdots & 0 & 0 \\ a_1 & a_0 & a_1 & \cdots & 0 & 0 \\ 0 & a_1 & a_0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & a_0 & a_1 \\ 0 & 0 & 0 & \cdots & a_1 & a_0-a_1 \end{bmatrix} \qquad (8)$$

is equal to zero. As

$$\Delta_k \;=\; a_0\Delta_{k-1} \;-\; a_1^2\Delta_{k-2},\; k\geq 2\;,\; \Delta_0=1,\; \Delta_1=a_0-a_1\;,$$

then

$$\Delta_k(a_0, a_1) \;=\; \sum_{j=0}^{k} (-1)^{\lceil j/2 \rceil} \binom{k - \lceil j/2 \rceil}{\lfloor j/2 \rfloor} a_0^{k-j} a_1^j \;.$$

Therefore the following statement is valid.

Theorem 2 *Let $\phi(x) = a_0 x^2 + 2a_1 x^{1+q}$, where $a_0,\ a_1 \in F_q$ and $a_1 \neq 0$. Then*

$$|S(\phi)| \;=\; q^{k+\frac{3}{2}}$$

(i.e. the Weil bound is reached) if and only if

$$\Delta_k(a_0, a_1) = 0\;.$$

It is easy to see that the equation $\Delta_k(a_0, a_1) = 0$ is not always solvable for $a_0,\ a_1 \in F_q^*$. For example, the equation

$$\Delta_2(a_0, a_1) \;=\; a_0^2 \;-\; a_0 a_1 \;-\; a_1^2 \;=\; 0$$

has no nonzero solutions in the field F_3. However this equation always has a solution, for example, in any even extension of F_3 or in any field of the characteristic 5.

But for the case $k = 1$ the equation $\Delta_1(a_0, a_1) = a_0 - a_1 = 0$ always has a nonzero solution $a_0 = a_1$ in F_q. This example was given by Stepanov[4] (it follows also from Theorem 1). From the remark due to Rodier [5] (that the polynomial, meeting the Weil bound over a finite field is also meeting the Weyl bound over any extension of this field) it follows that a pair $a_0 = a_1$ is a solution of the equation $\Delta_k(a_0, a_1) = 0$ for any k such that 3 divides $2k + 1$ (the another solutions are also possible).

I.b. $m = 2k,\ k \geq 1$

Theorem 3 *Let*

$$\phi(x) \;=\; a_0 x^2 \;+\; 2\sum_{s=1}^{k} a_s x^{1+q^s}\;.$$

Then

$$|S(\phi)| \;=\; q^{m-\frac{1}{2}}\;,$$

if and only if, either

$$a_s \ = \ a_0^{\frac{q^s+1}{2}} \ , \ s \ = \ 1, ..., \ k-1 \ ,$$

where a_0 is an arbitrary quadratic residue of $F_{q^{2k}}$ and a_k is an arbitrary root of the equation

$$a_k \ + \ a_k^{q^k} \ = \ a_0^{\frac{q^k+1}{2}} \ ,$$

or

$$a_s \ = \ (-1)^s a_0^{\frac{q^s+1}{2}} \ , \ s = 1, ..., \ k-1 \ ,$$

where a_0 is an arbitrary quadratic residue of $F_{q^{2k}}$ and a_k is an arbitrary root of the equation

$$a_k \ + \ a_k^{q^k} \ = \ (-1)^k a_0^{\frac{q^k+1}{2}} \ .$$

The number of different such poilynomials is equal to $(q^m - 1)q^{m/2}$.

Proof. For even m the matrix B looks as follows (see(6)):

$$B \ = \ \left[\begin{array}{ccccccccc} a_0 & a_1 & a_2 & ... & a_{k-1} & a_k + a_k^{q^k} & a_{k-1}^{q^{k+1}} & ... & a_1^{q^{2k-1}} \\ a_1 & a_0^q & a_1^q & ... & a_{k-2}^q & a_{k-1}^q & a_k^q + a_k^{q^{k+1}} & ... & a_2^{q^{2k-1}} \\ . & . & . & ... & . & . & . & ... & . \end{array} \right] .$$

As in the previous case, its rank is equal to 1 if and only if the second row is proportional to first one. For odd m we defined uniquely the coefficients $a_1, ..., a_k$ through the first a_0. Here we do the same thing: we will choose arbitrary the first coefficient a_0 and find all another from the proportional conditions of the subrows

$$\left[\begin{array}{cccccc} a_0 & a_1 & a_2 & ... & a_{k-1} & a_k + a_k^{q^k} \\ a_1 & a_0^q & a_1^q & ... & a_{k-2}^q & a_{k-1}^q \end{array} \right]$$

The situation is similar to the previous case for all the coefficients $a_1, ..., a_{k-1}$. For the last coefficient a_k we have the following equation:

$$a_k \ + \ a_k^{q^k} \ = \ a_0^{\frac{q^k+1}{2}} \ , \qquad \text{when} \ \ a_1 \ = \ a_0^{\frac{q+1}{2}} \ ,$$

and

$$a_k \ + \ a_k^{q^k} \ = \ (-1)^k a_0^{\frac{q^k+1}{2}} \ , \ \text{when} \ \ a_1 \ = \ -a_0^{\frac{q+1}{2}} \ .$$

It is easy to see that any of these equations has a solution if and only if a_0 is a quadratic residue of $F_{q^{2k}}$, and the number of solutions is equal to q^k. It is easy to check that under such conditions the coefficients $a_0, a_1, ..., a_k$ satisfy all the other conditions of the proportionality. The total number of different solutions $a_0, a_1, ..., a_k$ is equal to

$$\frac{q^{2k}-1}{2} \cdot 2 \cdot q^k$$

(because of a_0 is an arbitrary quadratic residue, a_1 takes exactly two values for given a_0, each a_i , $1 < i < k$, is defined uniquely for given a_0 and a_1, and the element a_k takes exactly q^k values for given a_0 and a_1). □

Remark 1 *Theorem 1 of paper Stepanov [4] is a particular case of Theorems 1 and 2.*

As we see, the Weil bound is not reached for Theorem 3. But as for the previous case we can consider the polynomials of type (5) of lower degree and show that at least for some of such polynomials the Weil bound is reached. First consider the polynomials for which $a_k = 0$. For such polynomials the Weil bound is equal to q^{2k-1}. According to Statement 1 this bound is reached for the polynomials for which the corresponding matrix B has a rank 2. Again considering only the polynomials with the coefficients from the small field F_q it is not difficult to prove the following theorem.

Theorem 4 *Let*

$$\phi(x) \;=\; a_0x^2 + 2\sum_{s=1}^{k-1} a_s x^{1+q^s} \;,$$

where $a_s \in F_q,\;\; s = 0, 1, ..., k-1$. *Then*

$$|S(\phi)| \;=\; q^{2k-1}$$

(i.e. the Weil bound is reached), if and only if

$$a_s = 0 \text{ for } s \equiv k \ (mod\ 2) \text{ and } a_s = a \text{ for } s \equiv k-1 \ (mod\ 2),$$

where a *is an arbitrary nonzero element of* F_q.

Another extremal case, when all the coefficients starting from a_2 are equal to zero. Here we have a theorem similar to Theorem 2. Denote by $\Omega_k(a_0,\ a_1)$ a determinant of the matrix of size $k \times k$ which differs from the matrix (8) only in one element at the lower right corner, where instead of the element $a_0 - a_1$ there is an element a_0. It is not difficult to account, that

$$\Omega_k(a_0,\ a_1) \ = \ \sum_{j=0}^{k} (-1)^j \binom{k-j}{j} a_0^{k-2j} a_1^{2j} \ .$$

Therefore the following result is valid.

Theorem 5 *Let $\phi(x) = a_0 x^2 + 2a_1 x^{1+q}$, where $a_0,\ a_1 \in F_q$ and $a_1 \neq 0$. Then*

$$|S(\phi)| \ = \ q^{k+1}$$

(i.e. the Weil bound is reached), if and only if

$$\Omega_k(a_0,\ a_1) = 0 \ .$$

Remark 2 *Note that for odd k any pair $a_0 = 0,\ a_1 \neq 0$ is a solution to the equation $\Omega_k(a_0,\ a_1) = 0$.*

Remark 3 *Wolfmann [6] found, in particular, exact value of the trigonometric sum of the monom $a_r x^{1+q^r}$, where r divides k and $a_r \in {F_Q}^*$, and derived the necessary and sufficient conditions in order this sum reaches the Weil bound. This condition might be obtained considering a matrix B, which has a simple enough structure for the case of the monom $a_r x^{1+q^r}$.*

Our final remark concerns to the arbitrary m - even and odd - and gives one more example of the polynomials, for which the Weil bound is exact. Consider the polynomial

$$f_a(x) \ = \ a \sum_{s \le r : s \equiv r \ (mod \ m-2r)} x^{1+q^s} \ , \ a \in F_q^* \ .$$

It is easy to check, that the rank of the matrix B, which corresponds to this polynomial $f_a(x)$, is equal to $m - 2r$, if $m - 2r$ divides m (in this case the matrix B contains exactly $m - 2r$ different rows). Therefore the following result is valid.

Statement 2 *Let $m-2r$ divides m. Then for the polynomial $f_a(x)$ the Weil bound is exact:*

$$|S(f_a)| \;=\; q^{r+\frac{m}{2}} \;.$$

II. The case of the even characteristic ($p = 2$).

In this case the maximal value of the module of the trigonometric sum for the polynomials (3) ie equal to q^{m-1} (see paper [1]). Stepanov [4] gave the examples of such polynomials in evident form for odd m. We give here a wide class of such polynomials for odd and even m both, but we can not state, that we describe all such polynomials (as we have done for odd q), although we conjecture that there are no such another polynomials.

For the case of even q we have no Statement 1, and so we should go by another way. It is well known [2,3], that only two quadratic forms from m variables in the reduced form over F_q have the module of the trigonometric sum equal to q^{m-1}:

$$z_1 z_2 \tag{9}$$

and

$$z_1^2 \;+\; z_1 z_2 \;+\; a z_2^2 \;,\ \text{where } Tr_q(a) \;=\; 1 \;. \tag{10}$$

Therefore our problem is to find the polynomials (3), such that the corresponding quadratic forms (see (4)),

$$g(x_0, x_1, ..., x_{m-1}) \;=\; Tr_{Q\to q}(f(\sum_{s=0}^{m-1} x_s\gamma_s)) \;=\; \sum_{0\le u\le v\le m-1} c_{uv}x_u x_v \tag{11}$$

are reduced to one of given above types. Similarly to sec. I, first write

$$h(x) \;=\; Tr_{Q\to q}(\sum_{s=0}^{k} a_s x^{1+q^s}) \;=\; \sum_{0\le i\le j\le m-1} b_{ij}x^{q^i+q^j} \;. \tag{12}$$

But already here, in order to find the coefficients b_{ij} through a_s, it is more convenient to consider the cases of even and odd m separately.

II.a. $m = 2k + 1,\ k \ge 1$

In this case the coefficients b_{ij} are computed by the following way:

$$b_{ij} \;=\; \begin{cases} a_0^{q^i} \;, & \text{where} \qquad\quad i \;=\; j \;, \\ a_{j-i}^{q^i} \;, & \text{where} \;\; 0 \;\leq\; i \;<\; j \;\leq\; k+i \;, \\ a_{m+i-j}^{q^j} \;, & \text{where} \;\; k+i \;<\; j \;\leq\; m-1 \;. \end{cases} \tag{13}$$

First we consider the case, when the quadratic form (11) might be reduced to the form (9). Let

$$z_1(x) \;=\; \sum_{i=0}^{m-1} \alpha_i x^{q^i} \quad , \quad z_2(x) \;=\; \sum_{j=0}^{m-1} \beta_j x^{q^j} \;, \tag{14}$$

and demand that the following equality is valid:

$$h(x) \;=\; z_1(x) z_2(x) \;. \tag{15}$$

From the relations (12)-(15) we obtain the following system of equalities:

$$\left.\begin{array}{rcll} a_0^{q^i} & = & \alpha_i\beta_i \;, & \text{when} \;\; i = 0, 1, ..., m-1 \;, \\ a_{j-i}^{q^i} & = & \alpha_i\beta_j + \alpha_j\beta_i \;, & \text{when} \;\; 0 \leq i < j \leq k+i \;, \\ a_{m+i-j}^{q^j} & = & \alpha_i\beta_j + \alpha_j\beta_i \;, & \text{when} \;\; k+i < j \leq m-1 \;. \end{array}\right\} \tag{16}$$

Now assume that α_i and β_j satisfy the following condition:

$$\alpha_i \;=\; \alpha_0^{q^i} \;, \quad \beta_j \;=\; \beta_0^{q^j} \;, \; \text{when} \; i, j \;=\; 1, ..., m-1 \;. \tag{17}$$

Under such conditions the system (16) might be written as follows

$$\begin{array}{rcl} a_0 & = & \alpha_0\beta_0 \;, \\ a_s & = & \alpha_0\beta_0^{q^s} + \alpha_0^{q^s}\beta_0 \;, \; s = 1, ..., k \;. \end{array} \tag{18}$$

Under the conditions (17) the polynomials $z_1(x)$ and $z_2(x)$ from (14) can be considered as linear forms over F_q of m variables $x_0, ..., x_{m-1}$. Indeed, using the expression x through the basis $\gamma_0, ..., \gamma_{m-1}$, we obtain from (14).

$$z_1(x_0, ..., x_{m-1}) \;=\; \sum_{i=0}^{m-1} \alpha_0^{q^i} (\sum_{s=0}^{m-1} \gamma_s x_s)^{q^i} \;=\; \sum_{s=0}^{m-1} Tr_{Q \to q}(\alpha_0 \gamma_s) x_s \;,$$

and

$$z_2(x_0,...,x_{m-1}) \;=\; \sum_{i=0}^{m-1} \beta_0^{q^i} (\sum_{s=0}^{m-1} \gamma_s x_s)^{q^i} \;=\; \sum_{s=0}^{m-1} Tr_{Q\to q}(\beta_0 \gamma_s) x_s \ ,$$

The linear forms $z_1(x_0,...,x_{m-1})$ and $z_2(x_0,...,x_{m-1})$ are independent over F_q, if and only if the elements α_0 and β_0 of the field F_Q are linearly independent over the field F_q. Therefore, for any such choice α_0 and β_0,

$$\alpha_0,\ \beta_0 \ \in\ F_Q^* \ ,\ \alpha_0 \ \neq\ c\beta_0 \ ,\ c \ \in\ F_q^* \ , \tag{19}$$

and for any choice of the coefficients $a_0, a_1, ..., a_k$ of the polynomial $f(x)$ of the form (3), which satisfy to the relations (18), the corresponding quadratic form (see (11)) is reduced to the form (9):

$$g(x_0,...,x_{m-1}) \;=\; z_1(x_0,...,x_{m-1})\ z_2(x_0,...,x_{m-1}) \ .$$

Now lets value from the below the number of different such polynomials $f(x)$ of the form (3). It is clear that the number of different ordered pairs (α_0, β_0) which satisfy the condition (19) is equal to $(q^m-1)(q^m-q)$. On the other hand, the number of different pairs (α_0, β_0), defining the same pairs of the two first coefficients a_0 and a_1 (see (18)):

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

is not more than $2(q-1)$. Therefore the number of such different polynomials (3) with maximal module of the trigonometric sum q^{m-1} is not less than $(q^m-1)(q^m-q)/2(q-1)$ (in fact, we have an equality, because together with a pair (α_0, β_0) the same set of the coefficients $a_0, a_1, ..., a_k$ are given by (β_0, α_0) and $(c\alpha_0, c^{-1}\beta_0)$, where c is an arbitrary nonzero element of F_q).

Now consider the case when the quadratic form (11) can be reduced to the type (10). Using the same arguments as in the previous case, we obtain that the only difference is that the system of relations (18) now looks as follows

$$\begin{aligned} a_0 \quad &= \quad \alpha_0^2 \ +\ \alpha_0\beta_0 \ +\ a\beta_0^2, \\ a_s \quad &= \quad \alpha_0\beta_0^{q^s} \ +\ \alpha_0^{q^s}\beta_0,\ s=1,\ldots,k \ , \end{aligned} \tag{20}$$

where, of course, the elements α_0, β_0 satisfy to the condition (18). Now lets value from the below the number of different $(k+1)$-tuples $a_0, a_1, \ldots, a_k$, defined by the condition (20). As the number of different pairs (α_0, β_0), defining the same pair of two first coefficients a_0 and a_1 (see (20)):

$$\begin{aligned} a_0 &= \alpha_0^2 + \alpha_0\beta_0 + a\beta_0^2 \ , \\ a_1 &= \alpha_0\beta_0^q + \alpha_0^q\beta_0 \ , \end{aligned}$$

is not more than $2(q+1)$ (by known Bezout theorem) then the number of different such sets is not less than $(q^m - 1)(q^m - q)/2(q+1)$. In fact, it is equal to this number. Indeed, together with a pair (α_0, β_0) the same tuple of the coefficients $a_0, a_1, ..., a_k$ give the pairs $(c_{11}\alpha_0 + c_{12}\beta_0, c_{21}\alpha_0 + c_{22}\beta_0)$, where $c_{ij} \in F_q$ satisfy the following system of the equations:

$$\begin{aligned} c_{11}^2 + c_{11}c_{21} + ac_{21}^2 &= 1 \ , \\ c_{11}c_{22} + c_{12}c_{21} &= 1 \ , \\ c_{12}^2 + c_{12}c_{22} + ac_{22}^2 &= a \ . \end{aligned}$$

The number of different solutions of this system is exactly equal to $2(q+1)$.

It is easy to show that choosing another element $a' \neq a,\ a' \in F_q,\ Tr_q(a') = 1$, for the quadratic form (10), we obtain the same sequence of the coefficients $(a_0, a_1, ..., a_k)$, as for the element a. Indeed, consider two systems of the equtions with two variables:

$$\begin{aligned} x^2 + xy + ay^2 &= a_0 \ , \\ xy^{q^s} + x^{q^s}y &= a_s, \ s = 1, ..., k \ , \end{aligned} \tag{21}$$

and

$$\begin{aligned} u^2 + uv + a'v^2 &= a_0 \ , \\ uv^{q^s} + u^{q^s}v &= a_s, \ s = 1, ..., k \ . \end{aligned} \tag{22}$$

Let (x, y) be a solution to the system (21). Then $u = b_1x + a^{1/2}y,\ v = a^{-1/2}x$ is a solution to the system (22), where the element $b_1 \in F_q$ is a root of the equation

$$b_1^2 + b_1a^{-1/2} + a'a^{-1} = 1$$

(and this last equation always has a solution, because $Tr_q(a + a') = 0$). On the other hand, even the sets of the pairs (a_0, a_1) of two first coefficients, defined by the quadratic form (9) and by the quadratic form (10) with fixed a, do not intersect. In order to see it, it is enough to show that two systems of the equtions

$$\begin{aligned} uv &= a_0 \\ uv^q + u^qv &= a_1 \end{aligned} \tag{23}$$

and

$$\begin{aligned} x^2 + xy + ay^2 &= a_0 \\ xy^q + x^q y &= a_1 \end{aligned} \tag{24}$$

do not have simultaneously solutions in the field F_Q for fixed $a_0, a_1 \in F_Q^*$. Indeed, if (x, y) is a solution to (24), then the system (23) does not have a solution. Suppose, in contrary, that the system (23) has a solution also. Consider the system of equations which is equivalent to (23):

$$\begin{array}{ccc} uv & = & a_0 \\ v^{q-1} + u^{q-1} & = & a_1/a_0. \end{array}$$

If this system is solvable, then the following quadratic equation ($z = v^{q-1}$) is also solvable in F_Q:

$$z^2 \ + \ \frac{a_1}{a_0} z \ + \ a_0^{q-1} \ = \ 0.$$

But this quadratic equation has a solution in F_Q if and only if

$$Tr_Q\left(\frac{a_0^{q-1}}{(a_1/a_0)^2}\right) = 0. \tag{25}$$

Taking into account the condition (24), the condition (25) is equivalent to the following one:

$$Tr_Q\left(\frac{(x^{2q} + x^q y^q + ay^{2q})(x^2 + xy + ay^2)}{x^2 y^{2q} + x^{2q} y^2}\right) \ = \ Tr_Q(a) \ +$$

$$+ \ Tr_Q\left(\frac{x^{2q+2} + x^{2q+1} y + x^{q+2} y^q + x^{q+1} y^{q+1}}{x^2 y^{2q} + x^{2q} y^2}\right) \ = \ Tr_Q(a) \ = \ Tr_q(a) \ = \ 0 \ ,$$

that contradicts to the condition (10) (at the last step we used that $a \in F_q$, where q is a power 2, and that m is odd). Therefore the total number of different polynomials (3) with maximal module of the trigonometric sum q^{m-1} is not less than

$$(q^m - 1)(q^m - q)\left(\frac{1}{2(q-1)} + \frac{1}{2(q+1)}\right) \ = \ \frac{(q^m - 1)(q^{m-1} - 1)q^2}{q^2 - 1} \ .$$

So we obtain the following result.

Theorem 6 *Let*

$$f(x) \;=\; \sum_{s=0}^{k} a_s x^{1+q^s} \;,\; m = 2k+1 \;.$$

If the coefficients a_s satisfy to the conditions (18) or (20), where $Tr_q(a) = 1,\; a \in F_q$, and α_0, β_0 satisfy to (19), then

$$|S(f)| \;=\; q^{m-1} \;.$$

The number of such distinct polynomials is equal to

$$\frac{(q^m-1)(q^{m-1}-1)q^2}{q^2-1} \;.$$

Remark 4 *Theorem 4 of paper Stepanov [4] is a particular case of Theorem 6.*

II.b. $m = 2k,\; k \geq 1.$

For this case the coefficients b_{ij} in (12) are calculated as follows:

$$b_{ij} \;=\; \begin{cases} a_0^{q^i} \;, & \text{when} \quad i \;=\; j \;, \\ a_{j-i}^{q^i} \;, & \text{when} \quad 0 \;\leq\; i \;<\; j \;<\; k+i \;, \\ a_k^{q^i} \;+\; a_k^{q^j} \;, & \text{when} \quad j \;=\; k+i \;, \\ a_{m+i-j}^{q^j} \;, & \text{when} \quad k+i \;<\; j \;\leq\; m-1. \end{cases} \tag{26}$$

The same arguments, as in sec. II.a, with the condition (26) instead of (13), give us the following two systems of relations between the coefficients $a_0, ..., a_k$ and the parameters $\alpha_0,\; \beta_0$, which are similar to (18) and (20):

$$\begin{aligned} a_0 \quad &= \quad \alpha_0\beta_0 \;, \\ a_s \quad &= \quad \alpha_0\beta_0^{q^s} \;+\; \alpha_0^{q^s}\beta_0 \;,\; s = 1, ..., k-1 \;, \\ a_k \;+\; a_k^{q^k} \quad &= \quad \alpha_0\beta_0^{q^k} + \alpha_0^{q^k}\beta_0 \;, \end{aligned} \tag{27}$$

and

$$\begin{aligned} a_0 \quad &= \quad \alpha_0^2 \;+\; \alpha_0\beta_0 \;+\; a\beta_0^2 \;, \\ a_s \quad &= \quad \alpha_0\beta_0^{q^s} \;+\; \alpha_0^{q^s}\beta_0 \;,\; s = 1, ..., k-1 \;, \\ a_k \;+\; a_k^{q^k} \quad &= \quad \alpha_0\beta_0^{q^k} \;+\; \alpha_0^{q^k}\beta_0 \;. \end{aligned} \tag{28}$$

The systems (27) and (28) differ from the similar systems (18) and (20) only by the last relation, which connect a_k with $\alpha_0,\ \beta_0$. Therefore, for each pair of the parameters $(\alpha_0,\ \beta_0)$ there is not one $(k+1)$-tuple $a_0,...,a_k$, but there are q^k such $(k+1)$-tuples $a_0,...,a_{k-1},a_k$, which differ from each only by the last coefficient a_k. Indeed, for fixed $\alpha_0,\ \beta_0$ the equation to a_k

$$a_k\ +\ a_k^{q^k}\ =\ \alpha_0\beta_0^{q^k}\ +\ \alpha_0^{q^k}\beta_0$$

has exactly q^k different solutions in the field F_Q . Therefore the total number of different tuples of the coefficients $a_0,a_1,...,a_k$ for even $m=2k$ is $q^{m/2}$ times more than for the odd m. With the only this exception, the cases of even m and odd m are absolutely similar. So we proved the following result.

Theorem 7 *Let*

$$f(x)\ =\ \sum_{s=0}^{k} a_s x^{1+q^s},\quad m=2k\ .$$

If the coefficients a_s satisfy to (27) or (28), where $Tr_q(a)=1$, $a\in\ F_q$, and α_0,β_0 satisfy to (19), then

$$|S(f)|\ =\ q^{m-1}\ .$$

The number of different such polynomials is equal to

$$\frac{(q^m-1)(q^{m-1}-1)q^{m/2}q^2}{q^2-1}\ .$$

For $k\geq 2$ there are always the elements $\alpha_0,\ \beta_0$ such that $a_k=0$. It is easy to see that this is the case when $\alpha_0/\beta_0\in F_{q^k}$. For such polynomials the Weil bound is exact. Therefore the following result is valid.

Corollary 1 *Among the polynomials mentioned in Theorem 7, for $k\geq 2$ there are polynomials of degree $q^{k-1}+1$ (i.e. the polynomials with $a_k=0$). for which the Weil bound is exact.*

From this corollary, in particular, the following equality follows:

$$S(q^k+1,\ q^{2k+1})\ =\ q^{2k+\frac{1}{2}}, \tag{29}$$

where $k \geq 1$ and q is an even power of 2, which in [1] we could prove only for odd q; here $S(d, Q) = max|S(f)|$, where the maximum is taken among all the polynomials over F_Q of degree $\leq d$ such that $Tr_Q(f(x)) \neq const$ for $x \in F_Q$. In particular, for $q = 4$ and $k = 1$ this equality has been obtained by Levenshtein [7]. We still believe [1], that when q is an odd power of 2, the equality (29) is not valid.

Conjecture 1 *Let $q = 2^l$, where l is odd. Then*

$$S(q^k + 1,\ q^{2k+1}) \ = \ q^{2k}.$$

A stimulus to writing of this paper was the discussion of our talk at the seminar of the number theory of Karatsuba A.A. of the Moscow State University. The authors thank all the participants of this seminar.

References.

1. *Bassalygo L.A., Zinoviev V.A., Litsyn S.N.*, *A lower bound of complete trigonometric sums in terms of multiple sums*, "Doklady AN USSR", 1988, Vol. 300, No. 5, 1033 - 1036.

2. *Lidl R., Niederreiter H.*, *Finite Fields, Encyclopedia of Mathematics and its Applications*, Vol. 20, Cambridge University Press, Cambridge, 1983.

3. *Malyshev A.V.*, On presentation of integers by positive quadratic forms, "Proceedings of the Steklov Institute of Mathematics in the Academy of Sciences of the USSR", 1962. Vol. 65.

4. *Stepanov S.A.*, On lower bounds of character sums over finite fields, "Diskretnaya Matematika", 1991, Vol. 3, No. 2, 77 - 86.

5. *Rodier F.*, *Estimation asymptotique de la distance minimale du dual des codes BCH et polynomes de Dickson*, "Discrete Mathematics", 1996, Vol. 149, 205-221.

6. *Wolfmann J.*, *The number of points on certain algebraic curves over finite fields*, "Communications in Algebra", 1989, Vol.17, No. 2, 2055-2060.

7. *Levenshtein V.I.*, Bounds for packings of metric spaces and some its applications, "Problemy Kibernetiki", 1983, Vol. 40, 43 - 110.