Glasgow Math. J. **52** (2010) 315–324. © Glasgow Mathematical Journal Trust 2010.
doi:10.1017/S0017089510000017.

ESTIMATION OF SOME EXPONENTIAL SUM BY MEANS OF q-DEGREE

VALÉRIE GILLOT and PHILIPPE LANGEVIN

Institut de Mathématiques de Toulon, Université du Sud Toulon-Var, France
e-mail: {gillot, langevin}@univ-tln.fr

(Received 10 July 2006; accepted 31 August 2009)

Abstract. In this paper, we improve results of Gillot, Kumar and Moreno to estimate some exponential sums by means of q-degrees. The method consists in applying suitable elementary transformations to see an exponential sum over a finite field as an exponential sum over a product of subfields in order to apply Deligne bound. In particular, we obtain new results on the spectral amplitude of some monomials.

1. Introduction. Exponential sums and bounds for them are exploited by coding theorists and communications engineers [**15**]. The minimal distance of dual BCH and other cyclic codes can be evaluated in terms of exponential sums. They are also useful in the study of sequences with small correlations for spread-spectrum and other communication applications. In both cases, the estimation of exponential sums is often a key point for the construction of a good code. In this paper, we focus on the estimation of exponential sums over finite fields for some polynomials. First, we begin introducing the tools and known results about spectral amplitude. Then, we generalise results of Kumar and Moreno [**10**] over spectral amplitude of some monomials in odd characteristics. We define the q-degree and the principle of multivariate point of view to be able to apply the results of Deligne [**4**] for exponential sums over a product of finite fields. Thus, we obtain a bound in terms of q-degree generalising the result of Gillot [**6**].

2. Spectral Amplitude. All along the paper, L denotes an extension of degree m of a finite field K of order q and characteristic p. The Fourier coefficient of a polynomial $f(X) \in L[X]$ at $a \in L$ is by definition equal to the value of the exponential sum:

$$\hat{f}(a) = \sum_{x \in L} \mu_L\big(f(x) + ax\big), \tag{1}$$

where μ_L denotes the canonical additive character of L. The maximal value that can take the absolute value of the Fourier coefficients is often called the *spectral amplitude* of f; we will use the notation $R_L(f) = \max_{a \in L} |\hat{f}(a)|$. A very difficult question coming from coding theory and cryptography consists in finding polynomials having a small spectral amplitude. If the degree, say d, of f is not divisible by p, then the spectral amplitude of f is upper-bounded by the Carlitz-Uchiyama bound:

$$R_L(f) \le (d-1)\sqrt{q^m}. \tag{2}$$

https://doi.org/10.1017/S0017089510000017 Published online by Cambridge University Press

For each $a \in L$, applying Weil theorem to the Artin–Schreier curve $y^p - y = f(x) + ax$ of genus $g = \frac{(p-1)(d-1)}{2}$, there exists $2g$ Weil numbers ω_i of absolute value $\sqrt{q^m}$ such that Fourier coefficient of f at a in a finite extension L_r of degree r of L is given by

$$\sum_{x \in L_r} \mu_{L_r}\big(f(x) + ax\big) = -\sum_{i=1}^{2g} \omega_i^r.$$

It follows that the bound (2) is optimal in the sense that, when $a \in L$ and $f(X) \in L[X]$ are fixed, there exists an infinite sequence of finite extensions $(L_k)_{k \in \mathbb{N}}$ of the field L of increasing degree r_k such that

$$\left|\sum_{x \in L_k} \mu_{L_k}\big(f(x) + ax\big)\right| \sim R_{L_k}(f) \sim (d-1)\sqrt{q^{mr_k}}.$$

On an other side, the Parseval relation

$$\sum_{b \in L} |\hat{f}(b)|^2 = q^{2m}, \tag{3}$$

implies that $\sqrt{q^m} \leq R_L(f)$. There exists polynomials of spectral amplitude $\sqrt{q^m}$, they define *generalised bent functions*, see for example [**11**]. For remark that only a very small number of bent functions of monomial form are known, see [**7**]. Moreover, if $p = 2$, then for all $f \in L[X]$ is fixed

$$\max_{b \in L^\times} R_L(bf) \geq \sqrt{2q^m}.$$

This fact proved by Chabaud and Vaudenay [**3**] is remarked as a consequence of Sidel'nikov bound in [**13**]. It is not true in odd characteristic as we will see in the next section. The goal of this paper consists in giving an upper-bound on the spectral amplitude of monomial (i.e. polynomial of the form bx^d with $b \in L^\times$). More precisely, denoting by $S(a, b, d)$ the exponential sum $\sum_{x \in L} \mu_L(bx^d + ax)$, we will present a new upper-bound on

$$\max_{b \in L^\times} R_L(bx^d) = \max_{a \in L} \max_{b \in L^\times} \big|S(a, b, d)\big|.$$

If δ denotes the gcd of d and $q^m - 1$, then by an averaging argument one can easily prove

$$\sqrt{(\delta - 1)q^m} \leq \max_{b \in L^\times} \big|S(0, b, d)\big| \leq \max_{a \in L} \max_{b \in L^\times} \big|S(a, b, d)\big|.$$

Several authors, such as Vinogradov, Davenport and Heilbronn, Hardy and Littlewood, Hua and Vandiver, Akulinicev, Karatsuba and Carlitz, have given general estimations on the magnitude of trigonometric sums involving binomials [**12**]. The exponential sum $S(0, b, d)$ is a *Gauss sum* and

$$\forall b \in L^\times, \qquad \big|S(0, b, d)\big| \leq (\delta - 1)\sqrt{q^m}.$$

https://doi.org/10.1017/S0017089510000017 Published online by Cambridge University Press

In the paper Lachaud [**12**] generalises the inequality of Akulinicev to obtain the bound

$$\forall a \in L, \quad \forall b \in L^{\times}, \qquad \big|S(a, b, d)\big| \leq \frac{q^m}{\sqrt{\delta}}.$$

It is easy to verify that the *fourth power moment method*, used by Karatsuba [**8**] in the case of a prime field, works on the extension fields as well, leading to the estimation

$$\forall b \in L^{\times}, \quad \forall a \in L^{\times}, \qquad \big|S(a, b, d)\big| \leq (d-1)^{\frac{1}{4}} q^{\frac{3}{4}m}$$

3. q-degree. All the previous bounds do not take in consideration an important parameter that we will call the *q-degree*. Before giving a definition, let us analyse a paradigm example to introduce this notion. It is the case where p is odd and $d = 1 + q^r$. The function $Q_b \colon x \mapsto \mathrm{Tr}_{L/K}(bx^d)$ is nothing but a quadratic form whose bi-linear associate form ϕ_b is given by

$$\begin{aligned} \phi_b(x, y) &= Q_b(x + y) - Q_b(x) - Q_b(y) \\ &= \mathrm{Tr}_{L/K}\big(b(x + y)^d - bx^d - by^d\big) \\ &= \mathrm{Tr}_{L/K}\big(bxy^{q^r} + bx^{q^r} y\big). \end{aligned}$$

The general theory of quadratic forms tells us that the spectral amplitude of Q_b takes the form $q^{(m+\kappa(b))/2}$, where $\kappa(b)$ denotes the dimension of the *radical* of the K-space L with respect to the bi-linear form ϕ_b (i.e. the space defined by $V_b = \{x \in L \mid \forall y \in L, \quad \phi_b(x, y) = 0\}$). In this precise case

$$\phi_b(x, y) = \mathrm{Tr}_{L/K}\big((bx + b^{q^r} x^{q^{2r}})y^{q^r}\big),$$

because the bi-linear form $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is non-degenerative, and the kernel of Q_b corresponds to the set of solutions of the linear equation

$$bx + b^{q^r} x^{q^{2r}} = 0. \tag{4}$$

Assuming $b \neq 0$, the non-zero solutions are also the solutions for the equation $x^{q^{2r}-1} = -b^{1-q^r}$ in the multiplicative group of L. By the Euclidean algorithm, we know that $\gcd(q^{2r} - 1, q^m - 1) = q^{\Delta} - 1$, where $\Delta = \gcd(2r, m)$. If there exists a pair $(x, b) \in L^{\times} \times L^{\times}$ satisfying (4), then $\kappa(b) = \Delta$ and thus

$$\max_{b \in L^{\times}} R_L(bx^d) = q^{\frac{m+\Delta}{2}}.$$

The existence of a solution in (4) is equivalent to the fact that -1 is in the product of two groups $(L^{\times})^{q^{2r}-1}$ of order $\frac{q^m-1}{q^{\Delta}-1}$, and $(L^{\times})^{q^r-1}$ of order $\frac{q^m-1}{q^{\Delta'}-1}$ with $\Delta' = \gcd(r, m)$. This product of cyclic groups has order $\frac{q^m-1}{q^{\Delta}-1} \times \frac{q^{\Delta}-1}{q^{\Delta'}-1}$, which is an odd number if and only if both $\frac{m}{\Delta}$ and $\frac{\Delta}{\Delta'}$ are odd. This case is equivalent to say -1, which is not in the product, and thus, all the quadratic forms Q_b are non-degenerative, we conclude $R_L(bx^d) = q^{\frac{m}{2}}$.

https://doi.org/10.1017/S0017089510000017 Published online by Cambridge University Press

PROPOSITION 3.1. *Let q be odd, and let $d = 1 + q^r$. If the dyadic valuation of r is greater or equal to the dyadic valuation of m, then*

$$\forall b \in L^\times, \quad R_L(bx^d) = q^{\frac{m}{2}}.$$

Otherwise

$$\max_{b \in L^\times} R_L(bx^d) = q^{\frac{m+\Delta}{2}},$$

where $\Delta = \gcd(2r, m)$.

Proof. Indeed, let us write $r = 2^a r'$ and $m = 2^b m'$, where m' and r' are odd integers, so that

$$\Delta = 2^{\min(b,a+1)} \gcd(r', m') \quad \text{and} \quad \Delta' = 2^{\min(b,a)} \gcd(r', m').$$

Whence the dyadic valuation of $\frac{m}{\Delta}$ is equal to $b - \min(b, a + 1)$ and those of $\frac{\Delta}{\Delta'}$ is equal to $\min(b, a + 1) - \min(b, a)$. These valuations are equal to 0 if and only if $a \geq b$. □

The above proposition generalises the result obtained by Kumar and Moreno in the Section II of [**10**]. As there, it could be possible to give a complete description of the Fourier coefficient distribution by means of quadratic Gauss sums.

By definition the q-ary weight of a positive integer $d < q^m$, denoted by $\mathrm{wt}_q(d)$, is equal to sums of the digits $d_0 + d_1 + d_2 + \cdots + d_{m-1}$ of the q-ary expansion of $d = d_0 + d_1 q^1 + d_2 q^2 + \cdots + d_{m-1} q^{m-1}$. The q-degree of a polynomial f is defined as the integer

$$\deg_q(f) = \max_{d \in \mathrm{supp}\,(f)} \{\mathrm{wt}_q(d)\},$$

where $\mathrm{supp}\,(f) = \{i \mid a_i \neq 0\}$ is the support of $f(x) = \sum_i a_i x^i$. As we will see in the next section, the q-degree of f is nothing but the degree of a certain polynomial F in several variables, this is the explanation of the terminology *q-degree* used in the title.

4. Multivariate point of view. The principle of the multivariate method detailed in [**6, 10**], applied to a single-variable polynomial $f(X) \in L[X]$, consists in transforming the exponential sum

$$S(f, L) = \sum_{x \in L} \mu_L\big(f(x)\big) \tag{5}$$

in an exponential involving several variables. This is done by choosing an arbitrary basis $\{\beta_1, \beta_2, \ldots, \beta_m\}$ of L over K.

$$\begin{aligned} S(f, L) &= \sum_{x_1, x_2, \ldots, x_m \in K} \mu_L\big(f(x_1\beta_1 + \cdots + x_m\beta_m)\big) \\ &= \sum_{x_1, x_2, \ldots, x_m \in K} \mu_K\big(F(x_1, x_2, \ldots, x_m)\big) \\ &= S(F, K^m), \end{aligned}$$

https://doi.org/10.1017/S0017089510000017 Published online by Cambridge University Press

where μ_K is the canonical additive character of K and F is the multivariate polynomial associate to f. The polynomial F is obtained by reduction modulo the ideal $I = (X_1^q - X_1, \dots, X_m^q - X_m)$ of the partial development of the trace operator

$$F(x_1, \dots, x_m) = \mathrm{Tr}_{L/K}\big(f(x_1\beta_1 + \dots + x_m\beta_m)\big) \mod I. \tag{6}$$

We use the Deligne bound, stated in [**4**], to evaluate $S(F, K^m)$.

THEOREM 4.1. *Let Q be a polynomial in n variables with degree d over K. Let Q_d be the homogeneous part of degree d of Q. Let $\psi : K \to \mathbb{C}^*$ be a non-trivial additive character over K. Assume that*

(i) *d is prime to the characteristic of K;*

(ii) *the homogeneous part Q_d defines a smooth hypersurface H_0 in $\mathbb{P}^{n-1}(\overline{K})$.*

Then

$$\left| \sum_{x_1,\dots,x_n \in K} \psi(Q(x_1, \dots, x_n)) \right| \leq (d-1)^n q^{n/2}. \tag{7}$$

In most of the cases the homogeneous part of higher degree of F rises from the exponents with greatest q-ary weight in the support of f. Of course, the degree of F is nothing but the q-degree of the polynomial f. In order to study the singularities of the hypersurface defined by F, we substitute $x_1\beta_1^{q^{i-1}} + \dots + x_m\beta_m^{q^{i-1}}$ by y_i in F to obtain an other multivariate polynomial

$$\phi(y_1, \dots, y_m) = F(x_1, \dots, x_m). \tag{8}$$

According to

$$\frac{\partial F}{\partial x_j}(x_1, \dots, x_m) = \sum_{i=1}^{m} \frac{\partial \phi}{\partial y_i}(y_1, \dots, y_m) \times \frac{\partial y_i}{\partial x_j} \tag{9}$$

and noting that the previous transformation is invertible, explicitly $x_i = \lambda_i y_1 + \lambda_i^q y_2 + \dots + \lambda_i^{q^{m-1}} y_m$, where $(\lambda_i)_{1 \leq i \leq m}$ is the trace-dual basis of $(\beta_i)_{1 \leq i \leq m}$ (i.e. $\mathrm{Tr}_{L/K}(\beta_i \lambda_j) = \delta_{ij}$ (the Kronecker symbol), the study of singularities of F is reduced to those of ϕ.

In [**6**], a bound for $S(f, L)$ in terms of the q-ary weight for specific cases of degree of f is given, let us state this result with our notations in the following theorem:

THEOREM 4.2. *Let f be a one-variable polynomial defined over L, such that $f(x) = bx^d + g(x)$, where d is the only exponent in the support of f with q-ary weight equal to* $\deg_q(f)$. *Assume that $d = 1 + d_r q^r$ with $(p, d_r) \neq 1$, then*

$$|S(f, L)| \leq \big(\mathrm{wt}_q(d) - 1\big)^m q^{m/2}.$$

Proof. See [**6**]. □

5. A new exponential sum bound. In this section, the study of singularities of $\phi(y_1, \dots, y_m)$ lead us to the characterisation of the exponents for which the multivariate method applies, generalising Theorem 4.2.

https://doi.org/10.1017/S0017089510000017 Published online by Cambridge University Press

LEMMA 5.1. *Let ϕ be the transformed polynomial associated to a monomial $f(x) = bx^d$. If d has more than two digits in its q-ary expansion or if $d = d_k q^k + d_l q^l$ with $d_k \neq 1$ and $d_l \neq 1$, then ϕ is singular.*

Proof. For a monomial $f(x) = bx^d$ of degree $d = d_0 + d_1 q + \cdots + d_{m-1} q^{m-1}$, we have

$$F(x_1, \ldots, x_m) = \sum_{k=1}^{m} b^{q^{k-1}} \left(x_1 \beta_1^{q^{k-1}} + \cdots + x_m \beta_m^{q^{k-1}} \right)^d,$$

$$\phi(y_1, \ldots, y_m) = \sum_{k=1}^{m} b^{q^{k-1}} y_k^{d_0} y_{k+1}^{d_1} \ldots y_{k+m-1}^{d_{m-1}},$$

where the indexes are calculated by modulo m. In both cases $(1 : 0 \ldots : 0)$ is a singular point of ϕ. □

LEMMA 5.2. *Let ϕ be the transformed polynomial of $f(x) = bx^d$. Assume that r and m are co-prime, $d = d_0 + d_r q^r$ with $d_0 = 1$ or $d_r = 1$. Then all the components of singularity of ϕ are different from zero.*

Proof. For $d = d_0 + d_r q^r$, from now let $d_0 = 1$ (the result remains true for the symmetric case $d_r = 1$) to obtain $\phi(y_1, \ldots, y_m) = \sum_{i=1}^{m} b^{q^{i-1}} y_i y_{i+r}^{d_r}$ and

$$\frac{\partial \phi}{\partial y_j}(y_1, \ldots, y_m) = b^{q^{j-1}} y_{j+r}^{d_r} + d_r b^{q^{j-1-r}} y_{j-r} y_j^{d_r - 1}.$$

Assume that P is a singularity of ϕ with $y_j = 0$. Replacing y_j by 0 in the partial derivative $\frac{\partial \phi}{\partial y_j}(P)$, we obtain $y_{j+r} = 0$. Now replacing y_{j+r} by 0 in the partial derivative $\frac{\partial \phi}{\partial y_{j+r}}(P)$, we obtain $y_{j+2r} = 0$. While reiterating the method, we obtain that the components of P are null for the positions $\{j, j+r, j+2r, j+3r, \ldots, j+kr\}$. For $(m, r) = 1$, the smallest k such that $kr = 0 \mod m$, is m, thus P has m components equal to zero. A contradiction is obtained and a singularity of ϕ cannot have a component equal to zero. □

LEMMA 5.3. *For an integer d of the form $d = d_0 + d_r q^r$ and for any $b \in L^\times$, we have*

$$\mathrm{Tr}_{L/K}(bx^d) = 0$$

for any $x \in L$ if and only if $r = m/2$, $d_0 = d_r$ and $\mathrm{Tr}_{L/\mathbb{F}_{q^r}}(b) = 0$.

Proof. See [**6**]. □

THEOREM 5.1. *Let $f(x) = bx^d + g(x) \in L[x]$ be a polynomial such that for any $b \in L^\times$ the q-degree of f only depends on the term bx^d that is $\deg_q(f) = \mathrm{wt}_q(d) > \deg_q(g)$. If*

(i) *the q-ary expansion of d has only two digits $d = d_0 + d_r q^r$ with $d_0 = 1$ or $d_r = 1$, where r is any integer coprime to m, and*

(ii) $d_0^m \neq (-1)^m d_r^m \mod p$,

then

$$|S(f, L)| \leq \left(\mathrm{wt}_q(d) - 1 \right)^m q^{m/2}.$$

https://doi.org/10.1017/S0017089510000017 Published online by Cambridge University Press

Proof. Let $F(x_1,\ldots,x_m)$ be the transformed (6) polynomial of $f(x)=bx^d+g(x)$. If $d=d_0+d_rq^r$ and $(m,r)=1$, then, according to Lemma 5.3, the term $\mathrm{Tr}_{L/K}(bx^d)$ is not equal to zero. In the particular case $m=2$, the assumption (5.1) of the theorem also gives $\mathrm{Tr}_{L/K}(bx^d)\neq 0$. In both cases, the homogeneous part of higher degree of the transformed polynomial F, say F_d, only depends on the term bx^d, since the q-degree of f is $\mathrm{wt}_q(d)$, its degree is $\mathrm{wt}_q(d)=d_0+d_r$.

On the other hand, we can associate to F_d, the polynomial ϕ, as in (8). Lemma 5.1 gives us the restriction on the case where the exponent d has only two digits in its q-ary expansion. Note that $d_kq^k+d_rq^r=q^k(d_k+d_rq^{r-k})$, after the reduction in (9), we just have to study integers of the form $d_0+d_rq^r$, with $d_0=1$ or $d_r=1$.

The homogeneous polynomial F_d satisfies the condition (i) of Deligne theorem since the second assumption implies that $\mathrm{wt}_q(d)$ is prime to the field characteristic p. Using the simple form of $d=d_0+d_rq^r$,

$$\phi(y_1,\ldots,y_m)=\sum_{k=1}^{m}b^{q^{k-1}}y_k^{d_0}y_{k+r}^{d_r}.$$

Since the degree of the homogeneous form of ϕ is prime to the characteristic of L, the singularities of ϕ correspond exactly to the non-zero solutions of partial derivative system

$$\frac{\partial\phi}{\partial y_i}(y_1,\ldots,y_m)=0,\qquad \forall i,\quad 1\leq i\leq m. \tag{10}$$

According to Lemma 5.2, we may assume that for all i, $y_i\neq 0$. Multiplying the ith equation by y_i, we obtain a new system

$$y_i\frac{\partial\phi}{\partial y_i}(y_1,\ldots,y_m)=d_0b^{q^{i-1}}y_i^{d_0}y_{i+r}^{d_r}+d_rb^{q^{i-r-1}}y_{i-r}^{d_0}y_i^{d_r}=0,$$
$$\forall i,\quad 1\leq i\leq m. \tag{11}$$

Changing $y_i^{d_0}y_{i+r}^{d_r}$ by z_i, we obtain

$$y_i\frac{\partial\phi}{\partial y_i}(y_1,\ldots,y_m)=d_0b^{q^{i-1}}z_i+d_rb^{q^{i-r-1}}z_{i-r}=0,$$
$$\forall i,\quad 1\leq i\leq m. \tag{12}$$

The matrix of this system is

$$(b^{q^{j-1}}d_{i-j})_{1\leq i,j\leq m}\text{ with }d_{i-j}=\begin{cases}d_0 & \text{if } i=j,\\ d_r & \text{if } i-j=r,\\ 0 & \text{otherwise.}\end{cases}$$

Up to the norm factor $\prod_{j=1}^{m}b^{q^{j-1}}$, the determinant of the previous matrix is

$$\prod_{\zeta^m=1}(d_0+d_r\zeta^r).$$

If $(-d_0/d_r)$ is not a m-th root of unity modulo p, the system (12) has only one solution $(0,\ldots,0)$. According to Lemma 5.2 this solution is not admissible since the singularity

https://doi.org/10.1017/S0017089510000017 Published online by Cambridge University Press

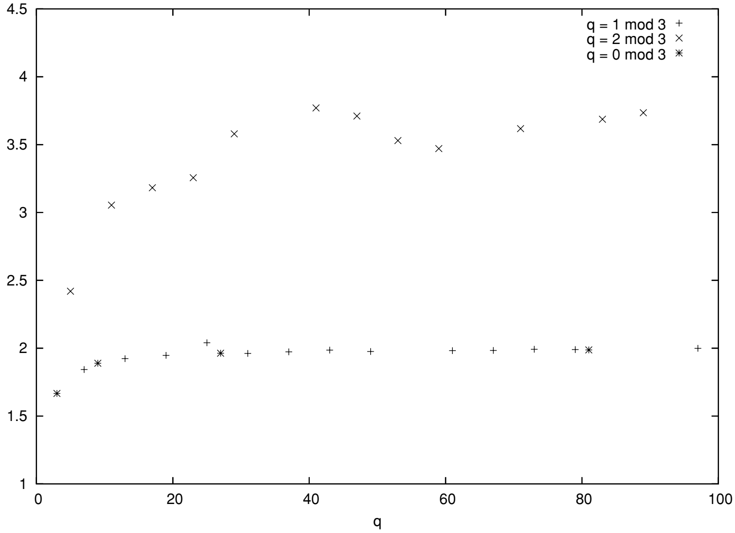

Figure 1. The value of $\frac{1}{q}\max_{b\in L^\times} R_L(bx^d)$, where L has order q^2 and $q \leq 100$.

of ϕ cannot have a null component. Thus, under the conditions of the theorem, the solution of (10) is trivial and ϕ is always smooth. Theorem 4.1 can be applied to the polynomial F of degree $\mathrm{wt}_q(d) = d_0 + d_r$ to obtain the bound in terms of the q-degree of f:

$$|S(f, L)| = |S(F, K^m)| \leq \big(d_0 + d_r - 1\big)^m q^{m/2}.$$

□

6. Numerical results and final remarks. If we apply Theorem 5.1 in the case of q-degree equal to 2, we recovered the theorem given Kumar and Moreno [**10**], but this is also a consequence of Proposition 3.1. In particular, the bound is optimal.

In order to check the interest of the bound given in Theorem 5.1 in the case q-degree equals to 3, we computed the true spectral amplitude of all the monomials bx^d over a quadratic extension for the finite field of odd order $q \leq 100$ with degree $d = 2 + q$. Note that $(d, q^2 - 1) = 1$ or 3 according to $q \equiv 2 \mod 3$ or $q \equiv 1 \mod 3$, in particular $S(0, b, d) \leq 2q$. For a such d, the conditions of the main theorem are fulfilled if and only if $(p, 3) = 1$, and in that case our bound claims

$$\frac{1}{q}\max_{b\in L^\times} R_L(bx^d) \leq 4. \tag{13}$$

The values are plotted in the graphic of Figure 1.. The numerical experiments show that the bound seems very good for all $q \equiv 2 \mod 3$ but two times too large in the case $q \not\equiv 2 \mod 3$. This last point is a probable consequence of the cancellation of Weil numbers. It is interesting to note that these exponential sums can be described by means of the norm $\mathrm{N}_{L/K}$ from L onto K,

$$\sum_{x\in L} \mu_L(ax + bx\mathrm{N}_{L/K}(x)). \tag{14}$$

https://doi.org/10.1017/S0017089510000017 Published online by Cambridge University Press

As it has been pointed out by Katz, one can use a trick of Deligne [**5**] (4.5 of Sommes trig.) to reduce to the split case in which L is no longer the quadratic extension of K, rather it is the product $K \times K$, with trace function $(x, y) \mapsto x + y$, and the norm $(x, y) \mapsto N((x, y)) = xy$. In an appropriate extension field E the sum (14) becomes

$$\sum_{x,y \in E} \mu_E(a(x+y) + b(x+y)xy),$$

and again Deligne's theorem applies as soon as $p \neq 3$ to show that the sum depends on four Weil numbers. Using a remark by Blache, one can avoid Deligne result to estimate the above sum, in the case $[L : K] = 2$, as follows. Let N be an non-quadratic residue of K, and let $\omega \in L$ such that $\omega^2 = N$. Using the basis $\{1, \omega\}$ to decompose $a = u + \omega v$, $b = s + \omega t$ and the elements of L as $x + \omega y$, we have

$$\mathrm{Tr}_{L/K}((u + \omega v)(x + \omega y)) = 2ux - 2Nvy,$$
$$\mathrm{Tr}_{L/K}((s + \omega t)(x + \omega y)^{q+2}) = 2(sx - Nty)(x^2 - Ny^2).$$

In particular, denoting by ψ the composition of the character μ_K by the multiplication by 2,

$$\begin{aligned} S(a, 1, q+2) &= \sum_{x,y \in K} \psi(ux - vNy + x^3 - Nxy^2) \\ &= \sum_{x \in K} \psi(x^3 + ux) \sum_{y \in K} \psi(-vNy - Nxy^2). \end{aligned}$$

Using a classical result on character sum with quadratic argument (see [**14**] Theorem 5.33), we can express the inner sum in terms of a quadratic Gauss sum $G_K(\psi, \nu)$ involving the quadratic character of K

$$= G_K(\nu, \psi)\nu(-N) \sum_{x \in K^\times} \psi(x^3 + ux + \frac{Nv^2}{4x})\nu(x) + q\delta_0(v).$$

Since the last hybrid sum is a sum of 3 or 4 Weil's numbers, according to whether $v = 0$ or not, we get the previous estimation (13). All the other sums $S(a, b, d)$ are estimated in a similar way.

Numerically, the case $q \equiv 0 \mod 3$ and $q \equiv 1 \mod 3$ seem very similar, and it will be nice to know when and how to avoid the technical hypothesis (ii) of Theorem 5.1 to obtain a more general bound independent of the characteristic of p. Similar transformations using the works of Adolphson and Sperber [**1**] are probably a way to get answers, but we reserve this approach for future researches.

ACKNOWLEDGEMENTS. The authors would like to thank Regis Blache, Nicolas Katz and Igor Shparlinsky for their useful comments and suggestions while preparing the manuscript.

REFERENCES

1. A. Adolphson and S. Sperber, Exponential sums and Newton polyhedra: Cohomology and estimates, *Ann. of Maths.* **130** (1989), 367–406.

https://doi.org/10.1017/S0017089510000017 Published online by Cambridge University Press

2. N. M. Akulinicev, Estimates for rational trigonometric sums of a special type, *Soviet Math. Dokl.* **6** (1965), 480–482.

3. F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, *Eurocrypt 94* **950** (1994), 356–365.

4. P. Deligne, La conjecture de Weil I, *Publ. Math. IHES* **43** (1974), 273–308.

5. P. Deligne, Cohomologie étale des schémas. *Lecture notes in mathematics 569* (Springer Verlag, Berlin, 1977); *Publ. Math. IHES*, **43** (1974), 273–308.

6. V. Gillot, Bounds for exponential sums over finite fields. *Finite Fields Appl.* **1** (1995), 421–436.

7. T. Helleseth and A. Kholosha, Monomial and quadratic bent functions over finite fields of odd characteristic, to appear in *IEEE*.

8. A. A. Karatsuba, On estimates of complete trigonometric sums, *Sov. Math. Dokl.* **7** (1966), 133–139.

9. N. M. Katz, Sommes exponentielles, Cours à Orsay, automne 1979, in *Astérisque*, vol. 79 (Société Mathématique de France, Paris, 1980), 209.

10. P. V. Kumar and O. Moreno, Polyphase sequences with periodic correlation properties better than binary sequences, *IEEE IT Trans.* **37** (1991), 603–616.

11. P. V. Kumar, R. A. Scholtz and L. R. Welch, Generalized bent functions and their properties, *J. Comb. Theory (A)* **40** (1985), 90–107.

12. G. Lachaud, Exponential sums as discrete Fourier transform with invariant phase functions, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC)* **673**(1993), 231–242.

13. Ph. Langevinand P. Véron, On the non-linearity of power functions. *Des. Codes Cryptogr.* **37**(1) (2005), 31–43.

14. R. Lidl and H. Niederreiter, *Finite fields*, vol. 20 of *encyclopedia of mathematics and its applications* (Addison-Wesley, Indianapolis, IN, 1983).

15. K. G. Paterson, Applications of exponential sums in communications theory. Cryptography and coding, in *LNCS vol. 1746* (Walker M., Editor), (Springer-Verlag, Berlin, 1999), 1–24.

16. P. Roquette, Exponential sums: The estimate of Hasse-Davenport-Weil. Available online: http://www.ma.utexas.edu/users/voloch/expsums.html.

17. V. M. Sidel'Nikov, On the mutual correlation of sequences, *Soviet Math. Dokl.* **12** (1971), 197–201.

https://doi.org/10.1017/S0017089510000017 Published online by Cambridge University Press