

On divisibility of exponential sums of polynomials of special type over fields of characteristic 2

Leonid Bassalygo, Victor Zinoviev

► **To cite this version:**

Leonid Bassalygo, Victor Zinoviev. On divisibility of exponential sums of polynomials of special type over fields of characteristic 2. WCC 2011 - Workshop on coding and cryptography, Apr 2011, Paris, France. pp.389-396, 2011. <inria-00614453>

HAL Id: inria-00614453

<https://hal.inria.fr/inria-00614453>

Submitted on 11 Aug 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On divisibility of exponential sums of polynomials of special type over fields of characteristic 2 ^{*}

Leonid A. Bassalygo and Victor A. Zinoviev

Institute for Problems of Information Transmission,
Russian Academy of Sciences,
Bol'shoi Karetnyi per. 19, GSP-4,
Moscow, 127994, Russia, bass@iitp.ru, zinov@iitp.ru

Abstract. We study divisibility by eight of exponential sums of several classes of functions over finite fields of characteristic two. For the binary classical Kloosterman sums $K(a)$ over such fields we give a simple recurrent algorithm for finding the largest k , such that 2^k divides the Kloosterman sum $K(a)$. This gives a simple description of zeros of such Kloosterman sums.

Keywords: exponential sum, Kloosterman sum, divisibility by power of two, zero of Kloosterman sum

1. Introduction. Let $\mathbb{F} = \mathbb{F}_{2^m}$ be the field of characteristic 2 of order 2^m , where $m \geq 3$ is an integer. By \mathbb{F}_2 denote the field, consisting of two elements. Set

$$e(x) = (-1)^{Tr(x)}, \quad x \in \mathbb{F},$$

where $Tr(x)$ is the trace function from \mathbb{F} into \mathbb{F}_2 . For an arbitrary polynomial $f(x)$ over \mathbb{F} define its exponential sum $S(f)$,

$$S(f) = \sum_{x \in \mathbb{F}} e(f(x)).$$

Recall that under x^{-i} we understand x^{2^m-1-i} , avoiding by this way a division into 0. The sum

$$K(a) = \sum_{x \in \mathbb{F}} e(x + a/x), \quad a \in \mathbb{F}^*,$$

is called the *Kloosterman sum*.

Given a polynomial $f(x)$ over \mathbb{F} it is a hard mathematical problem to write out the value of its exponential sum $S(f)$ or the module $|S(f)|$. This problem is interesting from several points of view, for example, for the theory of error-correcting codes, for sequences, for solving of equations over finite fields, for

^{*} Supported by the Russian Fundamental Research Foundation, project No. 09 -01 - 00536.

cryptography and etc. In some cases the value $S(f)$ is known (see [1], [2], [8] and references there). From this point of view, the divisibility of $S(f)$ is an interesting important open problem. Recently, the divisibility of $K(a)$ has been considered in several papers. In particular, the divisibility of $K(a)$ modulo 24 has been solved in [4], and the divisibility by 16 has been solved in [9].

In the present paper we use an elementary combinatorial approach to study divisibility by eight of exponential sums of polynomials of special type (such as $a(x^d + x^{-d})$, $ax^d + bx^{-1}$, $a(x + x^{-1})^d$, and etc.). This is considered in the first three sections. In the last section we consider the divisibility of Kloosterman sums $K(a)$ into the maximal power of two, which results in a simple algorithm of finding of zeros of Kloosterman sums. Kloosterman zeros play a significant role in construction of highly nonlinear functions that are used in cryptography, in particular, for construction of *bent functions* (see [5], [6]) and *hyperbent functions* (see [5]).

2. Polynomials of type $a(x^d + x^{-d})$. We start by studying the divisibility by 8 of exponential sums of polynomials $f(x)$ of the type

$$f(x) = a(x^d + x^{-d}), \quad a \in \mathbb{F}^*,$$

where d is any odd integer, $1 \leq d \leq 2^m - 3$. All our proofs of divisibility by eight are based on the following quite evident observation.

Proposition 1 . *Let $\mathbf{b} = (b_1, \dots, b_k, b_{k+1}, \dots, b_{2k})$ be a binary sequence of even length $2k$, and let $\mathbf{b}_{inv} = (b_{2k}, \dots, b_{k+1}, b_k, \dots, b_1)$ be the inverse sequence. Then the Hamming distance*

$$d(\mathbf{b}, \mathbf{b}_{inv}) \equiv \begin{cases} 0 \pmod{4}, & \text{if } \text{wt}(\mathbf{b}) \text{ even,} \\ 2 \pmod{4}, & \text{if } \text{wt}(\mathbf{b}) \text{ odd,} \end{cases}$$

where $\text{wt}(\mathbf{b})$ is the Hamming weight of \mathbf{b} (i.e. the number of ones in the sequence \mathbf{b}).

Let β be a primitive element of \mathbb{F} . For a given $a \in \mathbb{F}^*$ and an odd integer d , $1 \leq d \leq 2^m - 3$, define a binary vector of length 2^m :

$$\mathbf{T}(ax^d) = (\text{Tr}(0), \text{Tr}(a), \text{Tr}(a\beta^d), \text{Tr}(a\beta^{2d}), \dots, \text{Tr}(a\beta^{(2^m-2)d})).$$

In the similar way define the vector $\mathbf{T}(ax^{-d})$ of the same length. Denote

$$\mathbf{T}_1(ax^d) = (\text{Tr}(a\beta^d), \text{Tr}(a\beta^{2d}), \dots, \text{Tr}(a\beta^{(2^{m-1}-1)d}))$$

and

$$\mathbf{T}_2(ax^d) = (\text{Tr}(a\beta^{2^{m-1}d}), \text{Tr}(a\beta^{(2^{m-1}+1)d}), \dots, \text{Tr}(a\beta^{(2^m-2)d})).$$

Similarly define also the vectors $\mathbf{T}_1(ax^{-d})$ and $\mathbf{T}_2(ax^{-d})$. Note that the vector $(\mathbf{T}_1(ax^{-d}), \mathbf{T}_2(ax^{-d}))$ of length $2^m - 2$ is an inversion of the vector

$$(\mathbf{T}_1(ax^d), \mathbf{T}_2(ax^d)).$$

Since

$$\sum_{x \in \mathbb{F}} \text{Tr}(a x^d) = \text{Tr} \left(\sum_{i=0}^{2^m-2} a \beta^{i d} \right) = \text{Tr} \left(a \frac{\beta^{d(2^m-1)} - 1}{\beta - 1} \right) = 0,$$

the weight of the vector $(\mathbf{T}_1(a x^d), \mathbf{T}_2(a x^d))$ is even, if $\text{Tr}(a) = 0$. The same property is valid for the vector $(\mathbf{T}_1(a x^{-d}), \mathbf{T}_2(a x^{-d}))$. But if $\text{Tr}(a) = 1$, then the corresponding weights are odd. Therefore, according to Proposition 1 we obtain that

$$d(\mathbf{T}(a x^d), \mathbf{T}(a x^{-d})) \equiv \begin{cases} 0 & (\text{mod } 4), \text{ if } \text{Tr}(a) = 0, \\ 2 & (\text{mod } 4), \text{ if } \text{Tr}(a) = 1. \end{cases}$$

Since

$$S(a(x^d + x^{-d})) = 2^m - 2 d(\mathbf{T}(a x^d), \mathbf{T}(a x^{-d})),$$

the following result holds.

Statement 1 . Let $a \in \mathbb{F}^*$, and d be any odd integer, $1 \leq d \leq 2^m - 3$. Then

$$S(a(x^d + x^{-d})) \equiv \begin{cases} 0 & (\text{mod } 8), \text{ if } \text{Tr}(a) = 0, \\ 4 & (\text{mod } 8), \text{ if } \text{Tr}(a) = 1. \end{cases}$$

The proof given above is quite elementary. Remark, that this result was known for $d = 1$ and, therefore, for any d which is relatively prime to $2^m - 1$ (see [7], where two proofs of this result are given: the first one based on finding of the number of solutions of some system of equations over \mathbb{F} , and the second one, suggested by P. Charpin, based on Melas codes).

It is easy to see that the sum $S(a(x^d + x^{-d}))$ depends on the value of the greatest common divisor $h = (d, 2^m - 1)$ of numbers d and $2^m - 1$. In particular, h divides $S(a(x^d + x^{-d})) - 1$. Indeed, denoting $2^m - 1 = hu$, we obtain

$$\begin{aligned} S(a(x^d + x^{-d})) &= 1 + \sum_{i=0}^{2^m-2} e(a(\beta^{i d} + \beta^{-i d})) \\ &= 1 + \sum_{i=0}^{2^m-2} e(a \beta^{i d}) e(a \beta^{-i d}) \\ &= 1 + \sum_{j=0}^{u-1} \sum_{s=0}^{h-1} e(a(\beta^{(j+s u) d}) e(a \beta^{-(j+s u) d}) \\ &= 1 + \sum_{j=0}^{u-1} e(a \beta^{j d}) e(a \beta^{-j d}) \sum_{s=0}^{h-1} e(a \beta^{s u d}) e(a \beta^{-s u d}) \\ &= 1 + h \sum_{j=0}^{u-1} e(a \beta^{j d}) e(a \beta^{-j d}) \\ &= 1 + h \sum_{j=0}^{u-1} e(a(\beta^{j d} + \beta^{-j d})). \end{aligned}$$

From the last expression and Statement 1 we have the following

Statement 2 . Let d be any odd integer, $1 \leq d \leq 2^m - 3$, and $h = (d, 2^m - 1)$. For any elements $a_1, a_2 \in \mathbb{F}^*$ the following congruence is valid:

$$S(a_1(x^d + x^{-d})) - S(a_2(x^d + x^{-d})) \equiv \begin{cases} 0 & (\text{mod } 4h), \text{ if } \text{Tr}(a_1) \neq \text{Tr}(a_2), \\ 0 & (\text{mod } 8h), \text{ if } \text{Tr}(a_1) = \text{Tr}(a_2), . \end{cases}$$

From the proof of Statement 1 also follows clearly the following more general

Statement 3 . Let $a_1, \dots, a_t \in \mathbb{F}^*$ and d_1, \dots, d_t be any odd numbers, $1 \leq d_i \leq 2^m - 3$, $i = 1, \dots, t$. Then

$$S\left(\sum_{i=1}^t a_i(x^{d_i} + x^{-d_i})\right) \equiv \begin{cases} 0 & (\text{mod } 8), \text{ if } \text{Tr}\left(\sum_{i=1}^t a_i\right) = 0, \\ 4 & (\text{mod } 8), \text{ if } \text{Tr}\left(\sum_{i=1}^t a_i\right) = 1. \end{cases}$$

3. Polynomials of type $a(x + x^{-1})^d$. Now consider polynomials $f(x) = a(x + x^{-1})^d$, where

$$d = \sum_{j=0}^{\ell} 2^{d_j}$$

is any odd number, $3 \leq d \leq 2^m - 3$,

$$m > d_\ell > d_{\ell-1} > \dots > d_0 = 0$$

and $\ell \geq 1$. Clearly

$$\begin{aligned} f(x) &= a(x + x^{-1})^{\sum_{j=0}^{\ell} 2^{d_j}} \\ &= a \prod_{j=0}^{\ell} (x^{2^{d_j}} + x^{-2^{d_j}}) \\ &= \sum_k a(x^k + x^{-k}), \end{aligned}$$

where summing is taken over all k of the type

$$k = 2^{d_\ell} \pm 2^{d_{\ell-1}} \pm \dots \pm 1$$

(i.e. the value k takes 2^ℓ different values). Since $\text{Tr}(\sum_k a) = 0$ (indeed, the sum consists of even number of monoms), then according to Statement 3 (taking into account, that $a_i = a$ for all $i = 1, \dots, 2^\ell$) we obtain the following result.

Statement 4 . Let $a \in \mathbb{F}^*$ and d be any odd number, $3 \leq d \leq 2^m - 3$. Then

$$S(a(x + x^{-1})^d) \equiv 0 \pmod{8}.$$

From Statement 3 also follows more general result.

Statement 5 . Let $a_1, \dots, a_t \in \mathbb{F}^*$, d_1, \dots, d_t be any odd numbers, $3 \leq d_i \leq 2^m - 3$. Then

$$S\left(\sum_{j=1}^t a_j (x + x^{-1})^{d_j}\right) \equiv 0 \pmod{8}.$$

Remark 1 . Clearly Statement 5 is still satisfied, if we change $x + x^{-1}$ by $x^r + x^{-r}$, where r is any integer, $3 \leq r \leq 2^m - 3$.

4. Polynomials of type $ax^d + bx^{-1}$. Consider now polynomials $f(x) = ax^d + bx^{-1}$, where $a, b \in \mathbb{F}$, $a \neq 0$, and d is any odd number, $1 \leq d \leq 2^m - 3$. First prove the following statement.

Proposition 2 . Let $c \in \mathbb{F}^*$. Then

$$S(cx^d + x^{-1}) + S(cx^d) = S(c(x + x^{-1})^d).$$

Proof. The following chain of equalities takes place:

$$\begin{aligned} & S(cx^d + x^{-1}) + S(cx^d) \\ &= \sum_{\text{Tr}(x^{-1})=0} e(cx^d + x^{-1}) + \sum_{\text{Tr}(x^{-1})=1} e(cx^d + x^{-1}) \\ &+ \sum_{\text{Tr}(x^{-1})=0} e(cx^d) + \sum_{\text{Tr}(x^{-1})=1} e(cx^d) \\ &= \sum_{\text{Tr}(x^{-1})=0} e(cx^d + x^{-1}) + \sum_{\text{Tr}(x^{-1})=0} e(cx^d) \\ &= 2 \times \sum_{x \in \mathbb{F}: \text{Tr}(x^{-1})=0} e(cx^d). \end{aligned}$$

Since the equation

$$y + \frac{1}{y} = x, \quad x \in \mathbb{F} \tag{1}$$

has two distinct zeros y_1, y_2 in the field \mathbb{F} , if and only if $\text{Tr}(x^{-1}) = 0$ (see [8]) and the number of the elements $x \in \mathbb{F}$, such that $\text{Tr}(x^{-1}) = 0$, is equal to 2^{m-1} , then the solutions y_1, y_2 of the equation (1), for all such x , run over the all field \mathbb{F} . Therefore,

$$2 \times \sum_{x \in \mathbb{F}: \text{Tr}(x^{-1})=0} e(cx^d) = \sum_{y \in \mathbb{F}} e\left(c\left(y + \frac{1}{y}\right)^d\right) = S\left(c\left(x + x^{-1}\right)^d\right). \quad \triangle$$

From Proposition 2 and Statement 4 the following statement follows.

Statement 6 . Let $a, b \in \mathbb{F}^*$ and d be any odd integer, $3 \leq d \leq 2^m - 3$. Then

$$S(ax^d + bx^{-1}) \equiv 0 \pmod{8},$$

if and only if

$$S(ax^d) \equiv 0 \pmod{8}.$$

Proof. Since

$$S(ax^d + bx^{-1}) = S(cx^d + x^{-1}).$$

where $c = ab^d$, and $S(cx^d) = S(ax^d)$, then, according to Proposition 2,

$$S(ax^d + bx^{-1}) = S(c(x + x^{-1})^d) - S(ax^d).$$

Now to complete the proof it is enough to use Statement 4. □

Recall that if d and $2^m - 1$ are relatively prime, then $S(ax^d) = 0$ for any element a from \mathbb{F} .

Corollary 1 . *Let $a, b \in \mathbb{F}^*$ and d be any odd integer, such that $3 \leq d \leq 2^m - 3$. If d and $2^m - 1$ are mutually prime, then*

$$S(ax^d + bx^{-1}) \equiv 0 \pmod{8}.$$

Corollary 2 . *Since $S(ax^3) \equiv 0 \pmod{8}$ for even $m \geq 6$ (see [2]), then*

$$S(ax^3 + bx^{-1}) \equiv 0 \pmod{8}, \quad a, b \in \mathbb{F}^*,$$

for even $m \geq 6$.

This result was known (see [3]).

5. Kloosterman sums. Now consider Kloosterman sums $K(a)$. Here we study the divisibility of such sums by the maximal possible number of the type 2^k (i.e. 2^k divides $K(a)$, but 2^{k+1} does not divide $K(a)$).

We are going to formulate a simple recurrent algorithm for finding the largest k , such that 2^k divides the Kloosterman sum $K(a)$. Before it, recall Lemma 7.4 in [10].

Lemma A [10]. *Let polynomials $g_i = g_i(x)$ over \mathbb{F} be defined by the following recurrent construction:*

$$\begin{aligned} g_0 &= x, \\ g_1 &= x + b_1, \quad \text{where } b_1^4 = a^2, \\ \dots & \quad \dots \quad \dots \end{aligned}$$

$$g_i = g_{i-1}^2 + b_i x \prod_{j=1}^{i-1} (g_j)^2, \quad \text{where } b_i^{2^{i+1}} = a^2 \text{ for } i \geq 2. \tag{2}$$

Then the all zeros of the polynomial g_{k-1} gives the x -th coordinates of the points of order 2^k of the elliptic curve $E(a)$ over \mathbb{F} , defined by the following equation:

$$y^2 + xy = x^3 + a^2. \tag{3}$$

Now recall the following result due to Lisonek P. (see reference in [9]), which we formulate only for $p = 2$.

Theorem B [9]). Let $a \in \mathbb{F}^*$, and let $0 \leq k \leq m$. Then $2^k | K(a)$ if and only if there exists a point of order 2^k on $E(a)$, where the curve $E(a)$ is defined by (3).

For a given element $a \in \mathbb{F}^*$, define now the sequence x_1, x_2, \dots, x_k of elements of the field \mathbb{F} by the following recurrent expression:

$$\left. \begin{aligned} x_1 &= 0, \\ x_{i+1}^2 + \sqrt{x_i} x_{i+1} + a &= 0, \quad i = 1, \dots, k-1. \end{aligned} \right\} \quad (4)$$

The following one of the main results follows from Lemma A and Theorem B.

Theorem 1 . Let a be any element of \mathbb{F}^* and let a sequence of elements x_1, x_2, \dots, x_k be constructed in accordance with recurrent relation (4). Let k be the smallest natural number, such that $\text{Tr}(x_k) = 1$. Then the Kloosterman sum $K(a)$ is divisible by 2^k and is not divisible by 2^{k+1} .

It is interesting to find a direct proof of Theorem 1, which does not use a transition to the number of rational points of the elliptic curve $E(a)$.

Corollary 3 [7]. Since $x_2 = \sqrt{a}$, then $K(a)$ is divisible by 4, but not divisible by 8, if $\text{Tr}(a) = 1$.

Corollary 4 [7], [9]. Let $\text{Tr}(a) = 0$. Then a can be presented as $a = z^8 + z^{16}$. In this case $x_3 = z^6 + z^8$. If $\text{Tr}(z) \neq \text{Tr}(z^3)$, then $K(a)$ is divisible by 8, but not divisible by 16.

Corollary 5 [9]. Under conditions of the Corollary 4 above, if $\text{Tr}(z) = \text{Tr}(z^3)$, then $K(a)$ is divisible by 16.

Recall (see [5] and references there) that the function $f_{a,r}(x)$,

$$f_{a,r}(x) = \text{Tr} \left(a x^{r(2^{m/2}-1)} \right), \quad a \in \mathbb{F}^*,$$

for even m and natural r , such that r and $2^{m/2} + 1$ are mutually prime, is bent, if and only if $K(a) = 0$, and the function $f_a(x)$

$$f_a(x) = \text{Tr} \left(a x^{2^m-1} \right), \quad a \in \mathbb{F}^*,$$

is hyperbent, if and only if $K(a) = 0$.

Theorem 1 implies the following simple necessary and sufficient condition for an element a to be a zero of the Kloosterman sum $K(a)$, i.e. in order to have $K(a) = 0$.

Theorem 2 . Let a be any element of \mathbb{F}^* and let a sequence u_1, u_2, \dots, u_m of elements from \mathbb{F} be defined in accordance with the following recurrent relation:

$$u_{i+1} = u_i^2 + \frac{a^2}{u_i^2},$$

where $u_1 \in \mathbb{F}^*$ is any element of \mathbb{F}^* , such that

$$\text{Tr}(u_1) = 1 \quad \text{and} \quad \text{Tr}\left(u_1 + \frac{a}{u_1}\right) = 0.$$

Then $K(a) = 0$, if and only if $u_m = 0$, and the all $m - 1$ elements u_1, \dots, u_{m-1} are nonzero. Furthermore, if the first zero element in the sequence u_1, u_2, \dots, u_m appears on the k th place, where $k < m$, then k is the largest integer, such that 2^k divides $K(a)$.

References

1. BASSALYGO L.A., & ZINOVIEV V.A., *Polynomials of special form over finite fields with given values of exponential sum*, *Matematicheskie Zametki*, 2007, vol. 82, pp. 16 - 25.
2. L. CARLITZ, *Explicit evaluation of certain exponential sums*, *Math. Scand.*, 1979, vol. 44, pp. 5-16.
3. P. CHARPIN, T. HELLESETH & V.A. ZINOVIEV, *On cosets of weight 4 of binary primitive BCH codes of length 2^m (m even) with minimum distance 8 and exponential sums*, *SIAM J. of Discrete Math.*, 2008, vol. 23, No. 1, p. 59 - 78.
4. P. CHARPIN, T. HELLESETH & V.A. ZINOVIEV, *On divisibility properties of classical binary Kloosterman sums*, *Discrete Mathematics*, 2009, vol. 309, no. 12, pp. 3975-3984.
5. P. CHARPIN & G. GONG, *Hyperbent functions, Kloosterman sums, and Dickson polynomials*, *IEEE Transactions on Information Theory*, 2008, vol. 54, no. 9, pp. 4230-4238.
6. J.F. DILLON, *Elementary Hadamard difference sets*. In *Proc. Sixth Southeastern Conference on Combinatorics, Graph theory, and Computing*. *Congressus Numerantium*, No. XIV, Utilitas Math., Winnipeg, Man., 1975, pp. 237-249.
7. T. HELLESETH & V.A. ZINOVIEV, *On Z_4 -Linear Goethals Codes and Kloosterman Sums*, *Designs, Codes and Cryptography*, 1999 vol. 17, No. 1-3, pp. 246-262.
8. R. LIDL & H. NIEDERREITER, *"Finite Fields"*, *Encyclopedia of Mathematics and Its Applications*, Reading, MA: Addison Wesley, 1983, vol. 20.
9. P. LISONEK, M. MOISIO, *On zeros of Kloosterman sums*, *Designs, Codes and Cryptography*, 2011, to appear.
10. A. MENEZES, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, Boston-Dordrecht-London, 1993.