A Note on Character Sums with Polynomial Arguments

S. Gangopadhyay
Mathematics Group, Birla Institute of Technology and Science
Pilani (Rajasthan) 333031 INDIA

Abstract

An improvement of Weil bound for a class of polynomials over $GF(2^n)$ is obtained.

Keywords : Character sum, Weil bound, interleaved sequence.

1 Introduction

Let $GF(p)$ be a prime field of characteristic p and $GF(p^n)$ be an extension of degree $n \geq 1$. For any element $x \in GF(p^n)$ the trace of x over $GF(p^m)$ where $m|n$ is defined by

$$Tr_m^n(x) = x + x^{p^m} + x^{p^{2m}} + \ldots + x^{p^{(\frac{n}{m}-1)m}}.$$

The homomorphism from the additive group of $GF(p^n)$ to $\mathbf{C}^*$, $\chi_1(x) = e^{\frac{2\pi i Tr_1^n(x)}{p}}$ is called the canonical additive character of $GF(p^n)$. The set of all functions $\chi_\alpha(x) = \chi_1(\alpha x)$ where $\alpha \in GF(p^n)$ form the set of all additive characters of $GF(p^n)$. The function χ_0 is called the trivial character.

Let χ be a *nontrivial* additive character of the field $GF(p^n)$ and $g(x) \in GF(p^n)[x]$ of degree $deg(g(x))$. The following result is well known, see Weil [8] and also Stepanov [6]

$$\left|\sum_{x\in GF(p^n)} \chi(g(x))\right| \leq (deg(g(x)) - 1)p^{\frac{n}{2}} \tag{1}$$

where $gcd(deg(g(x)), p) = 1$. We shall refer to the sum $\sum_{x\in GF(p^n)} \chi(g(x))$ as the *Weil sum* for $g(x)$ and the above upper bound as the *Weil bound.* Stepanov [7] has stated the following problem for additive characters

Problem 1 *Determine the class of polynomials $g \in GF(p^n)[x]$ of degree m, $1 \leq m \leq p^n - 1$, for which the upper bound (1) can be sharpened and absolute value of the Weil sum can be estimated nontrivially for $m \geq p^{\frac{n}{2}} + 1$.*

Mullen and Shparlinski [3] have mentioned the problem of evaluating the upper bounds of the absolute value of the Weil sum for special fields and polynomials. Several such bounds are described in [4]. Recently Shparlinski [5] has proved a sharper bound for $\left|\sum_{x\in GF(p^n)} \chi(\alpha x^m)\right|$ than that in (1), where p is any prime.

In this note we prove that when $p = 2$ it is possible to obtain an improvement over the Weil bound for a class of polynomials in $GF(p^n)[x]$ of the form $g(x) = x^c + \sum_{i=1}^{N} \beta_i x^{a_i(2^t-1)}$ where $\beta_i \in GF(p^n)$, a_i is a positive integer for all $i = 1, \ldots, N$, for some positive integer N, $t|n$ and $gcd(c, p^n - 1) = 1$. Our technique involves use of interleaved sequence as introduced by Youssef and Gong [2, 9, 10].

Remark 1 *In the following sections whenever we refer to $g(x) = x^c + \sum_{i=1}^{N} \beta_i x^{a_i(2^t-1)}$ it is to be assumed that $p = 2$, c is coprime to $2^n - 1$, $t|n$, N is a positive integer and $\beta_i \in GF(p^n)$ and a_i is a positive integer for all $i = 1, \ldots, N$, if not stated otherwise.*

2 Interleaved sequence

A binary sequence of length m is denoted by $\mathbf{a} = \{a_0, a_1, a_2, \ldots, a_{m-1}\}$ where $a_i \in \{0, 1\}$ for all $i = 0, 1, 2, \ldots, (m-1)$. In case $m = 2^n - 1$ for some positive integer n we can choose a primitive element $\zeta \in GF(2^n)$ and construct a function such that $f(0) = 0$ and $f(\zeta^i) = a_i$ where $i = 0, 1, 2, \ldots, 2^n - 2$. This function f is called the function corresponding to the sequence $\mathbf{a}$ with respect to the primitive element ζ. If we change the primitive element then we obtain a different function. Again if f is a function from $GF(2^n)$ to $GF(2)$ with $f(0) = 0$ and $\zeta \in GF(2^n)$ is a primitive element then the sequence $\{f(1), f(\zeta), f(\zeta^2), \ldots, f(\zeta^{2^n-2})\}$ is referred to as the sequence associated to f with respect to ζ. When there is no chance of confusion the primitive element ζ is not mentioned.

Definition 1 *Suppose m is a composite number such that $m = d.k$ where d and k are both positive integers greater than 1, $\mathbf{a}$ is a binary sequence $\{a_0, a_1, a_2, \ldots, a_{m-1}\}$ where $a_i \in \{0, 1\}$ for all i, then the (d, k)-interleaved sequence $\mathbf{a}_{d,k}$ corresponding to the binary sequence $\mathbf{a}$ is defined as*

$$\mathbf{a}_{d,k} = \begin{bmatrix} a_0 & a_1 & a_2 & \ldots & a_{(d-1)} \\ a_d & a_{1+d} & a_{2+d} & \ldots & a_{(d-1)+d} \\ a_{2d} & a_{1+2d} & a_{2+2d} & \ldots & a_{(d-1)+2d} \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{(k-1)d} & a_{1+(k-1)d} & a_{2+(k-1)d} & \ldots & a_{(d-1)+(k-1)d} \end{bmatrix}$$

Let $2^n - 1 = d.k$, $\mathbf{a}_{d,k}$ be an interleaved sequence and $\zeta \in GF(2^n)$ be a primitive element. Then a function $f : GF(2^n) \to GF(2)$ with $f(0) = 0$ and $f(\zeta^{i+\lambda d}) = a_{i+\lambda d}$ where $i = 0, 1, 2, \ldots, (d-1)$ and $\lambda = 0, 1, 2, \ldots, (k-1)$ is defined as the function corresponding to the interleaved sequence $\mathbf{a}_{d,k}$ with respect to the primitive element ζ. Conversely, for any function $f : GF(2^n) \to GF(2)$ and a primitive element $\zeta \in GF(2^n)$ an interleaved sequence $\mathbf{a}_{d,k}$ can be constructed such that $a_{i+\lambda d} = f(\zeta^{i+\lambda d})$ for all $i = 0, 1, 2, \ldots, (d-1)$ and $\lambda = 0, 1, 2, \ldots, (k-1)$. This interleaved sequence is called the interleaved sequence corresponding to f with respect to ζ. Again as in the case of binary sequences we drop the reference to ζ when there is no chance of confusion. The rows and columns of $\mathbf{a}_{d,k}$ are numbered from 0 to $(k-1)$ and 0 to $(d-1)$ respectively. For detailed discussion on interleaved sequence see Gong [2].

Definition 2 *Weight of a (d, k)-interleaved sequence $a_{d,k}$ denoted by $wt(a_{d,k})$ is equal to the number of non-zero entries in $a_{d,k}$.*

The following lemmas can be easily derived from the definition of trace.

Lemma 1 *Let $f(x) = Tr_1^n(x^c)$, where $gcd(c, 2^n - 1) = 1$. Then the $(d, 2^t - 1)$-interleaved sequence of f with respect to a primitive element $\zeta \in GF(2^n)$ for all $t|n$ is such that*

1. *the columns are either zero columns or cyclic shifts of the binary sequence corresponding to $Tr_1^t(x)$ when evaluated at $1, \zeta^{cd}, \zeta^{c2d}, \ldots, \zeta^{c(2^n-2)d}$ which contains 2^{t-1} ones,*

2. *the number of zero columns is $d - 2^{n-t}$.*

Lemma 2 *The $(d, 2^t - 1)$- interleaved sequence corresponding to*

$$f(x) = \sum_{i=1}^{N} Tr_1^n(\beta_i x^{a_i(2^t-1)})$$

is such that each row is a fixed binary sequence **b** *of length d.*

Proof : Let $v_{i,\lambda}$ be the entry in the i- th column and λ- th row of the interleaved sequence corresponding to the function $f(x)$.

$$\begin{aligned} v_{i,\lambda} &= \sum_{i=1}^{N} Tr_1^n(\beta_i \zeta^{(i+\lambda d)a_i(2^t-1)}) \\ &= \sum_{i=1}^{N} Tr_1^n(\beta_i \zeta^{ia_i(2^t-1)+\lambda a_i(2^n-1)}) \\ &= \sum_{i=1}^{N} Tr_1^n(\beta_i \zeta^{ia_i(2^t-1)}). \end{aligned}$$

Thus $v_{i,\lambda}$ is independent of λ. Hence the interleaved sequence corresponding to $f(x)$ has a fixed binary sequence **b** as rows. ∎

3 A Bound on Character Sums

Let A, B be $(d, 2^t - 1)$- interleaved sequences corresponding to the functions $Tr_1^n(x^c)$ and $Tr_1^n(\sum_{i=1}^{N} \beta_i x^{a_i(2^t-1)})$. We construct the sum $A + B$ by element wise adding modulo 2 the interleaved sequences A and B. Clearly $A + B$ is the interleaved sequence corresponding to the function

$$Tr_1^n(x^c + \sum_{i=1}^{N} \beta_i x^{a_i(2^t-1)}).$$

Theorem 1 *For any non-trivial additive character χ of $GF(2^n)$*

$$\left| \sum_{x \in GF(2^n)} \chi(g(x)) \right| \leq 2^{n-t+1}$$

where

$$g(x) = x^c + \sum_{i=1}^{N} \beta_i x^{a_i(2^t-1)}$$

Proof : Canonical additive character χ_1 of $GF(2^n)$ is

$$\chi_1(x) = (-1)^{Tr_1^n(x)}.$$

For any non-trivial additive character χ of $GF(2^n)$ there exists a $b \in GF(2^n)^*$ such that

$$\chi(x) = \chi_1(bx).$$

Therefore

$$\begin{aligned}
\sum_{x \in GF(2^n)} \chi(g(x)) &= \sum_{x \in GF(2^n)} \chi_1(bg(x)) \\
&= \sum_{x \in GF(2^n)} (-1)^{Tr_1^n(bx^c + \sum_{i=1}^{N} b\beta_i x^{a_i(2^t-1)})}.
\end{aligned}$$

Since c is coprime to $2^n - 1$ therefore inverse of c, denoted by c^{-1} exists modulo $2^n - 1$. Putting $x = b^{-c^{-1}} y$ in $bg(x)$

$$\begin{aligned}
bx^c + \sum_{i=1}^{N} b\beta_i x^{a_i(2^t-1)} &= b(b^{-c^{-1}} y)^c + \sum_{i=1}^{N} b\beta_i (b^{-c^{-1}} y)^{a_i(2^t-1)} \\
&= y^c + \sum_{i=1}^{N} b^{1-c^{-1}a_i(2^t-1)} \beta_i y^{a_i(2^t-1)} \\
&= h(y)
\end{aligned}$$

$h(y)$ is also a polynomial of the type under consideration. Thus

$$\sum_{x \in GF(2^n)} \chi(g(x)) = \sum_{x \in GF(2^n)} \chi_1(h(x)).$$

The character sum

$$\sum_{x \in GF(2^n)} \chi_1(g(x)) = 2^n - 2wt(A + B).$$

There are 2^{n-t} non-zero columns of A and r non-zero columns of B. Let s zero columns of A are added to non-zero columns of B. The remaining $r - s$ non-zero columns of B are added to non-zero columns of A and $2^{n-t} - (r - s)$ non-zero columns of A are added to zero columns of B. Finally $(d - 2^{n-t}) - s$ number of zero columns of A are added to zero columns of B. Thus we must have $r \leq d$, $s \leq d - 2^{n-t}$, $r - s \leq 2^{n-t}$ and $s \leq r$ along with $r, s \geq 0$. The weight of $A + B$

$$\begin{aligned}
wt(A + B) &= (2^t - 1)s + (2^{t-1} - 1)(r - s) + 2^{t-1}(2^{n-t} - (r - s)) \\
&= 2^t s - r + 2^{n-1}.
\end{aligned}$$

The character sum

$$\begin{aligned}
\sum_{x \in GF(2^n)} \chi_1(g(x)) &= 2^n - 2(2^t s - r + 2^{n-1}) \\
&= 2r - 2^{t+1} s.
\end{aligned}$$

Finding the upper bound of the absolute value of the above character sum is equivalent to the following problem:

$$\text{Maximize } \Gamma \;=\; \left|\sum_{x\in GF(2^n)} \chi_1(g(x))\right| \;=\; \left|2r - 2^{t+1}s\right|$$

Subject to the constraints:

$$\begin{aligned} r &\leq d \\ s &\leq d - 2^{n-t} \\ r - s &\leq 2^{n-t} \\ s &\leq r \\ r, s &\geq 0. \end{aligned}$$

The set of feasible solutions of the above problem is a convex region in the (r, s) plane. The vertices of this convex region are $(0, 0)$, $(2^{n-t}, 0)$, $(d, d - 2^{n-t})$, $(d - 2^{n-t}, d - 2^{n-t})$. It is known that the optimum is obtained at the vertices. The values of Γ at the above vertices are 0, 2^{n-t+1}, 2, 0 and $|2^{n-t+1} - 2|$ respectively. Since $n \geq t$, $2^{n-t+1} \geq |2^{n-t+1} - 2|$ and the value of Γ is maximum at $(2^{n-t}, 0)$. Therefore

$$\Gamma \;\leq\; 2^{n-t+1} \tag{2}$$

Since we have already proved that the character sum of any non-trivial additive character with argument $g(x)$ is equal to that of the canonical additive character with a polynomial of the same form as argument the theorem is proved. ∎

Remark 2 *The Weil bound is improved if the degree of $g(x)$, $deg(g(x)) > 2^{\frac{n}{2}-t+1} + 1$. Particularly when n is even and $t = \frac{n}{2}$ the bound obtained is $2^{\frac{n}{2}+1}$ which is an improvement over the Weil bound for any $g(x)$ of the above form.*

In the following theorem we prove the existence of a polynomial for which the bound (2) is attained for odd n.

Theorem 2 *Let $n > 1$ be an odd number. There exists a polynomial $g \in GF(2^n)[x]$ of the form*

$$g(x) = x^c + \sum_{i=1}^{N} \beta_i x^{a_i(2^t-1)}$$

such that

$$\left|\sum_{x\in GF(2^n)} \chi_1(g(x))\right| \;=\; 2^{n-t+1}.$$

Proof : Suppose A is a $(d, 2^t - 1)$-interleaved sequence corresponding to $Tr_1^n(x^c)$ for some c coprime to $2^n - 1$ and B is a $(d, 2^t - 1)$-interleaved sequence corresponding to a function of the form $Tr_1^n(\sum_{i=1}^{N} \beta_i x^{a_i(2^t-1)})$. From theorem 1 we note that the bound is attained when $r = 2^{n-t}$ and $s = 0$, where r is the number of 'all one' columns in B and s is the number of zero columns of A that are added to 'all one' columns of B. It is possible to construct a

$(d, 2^t-1)$-interleaved sequence such that each column is either an 'all one' column or a zero column and altogether there are 2^{n-t} 'all one' columns. Further it is possible to choose the 'all one' columns in such a way that none of them has the same column number as any of the zero columns of A. It is to be noted that since A has $d - 2^{n-t}$ zero columns there is exactly one way such a choice can be made. In ([1], Theorem 2) it is proved that corresponding to such an interleaved sequence there exists a function of the form

$$f(x) = \sum_{a(2^t-1)\in T} Tr_1^{s_{a(2^t-1)}}(\beta_a x^{a(2^t-1)})$$

where $\beta_a \in GF(2^{s_{a(2^t-1)}})$, $a(2^t-1) \in T$, the set of coset leaders modulo 2^n-1 and $s_{a(2^t-1)}$ is the size of the cyclotomic coset modulo 2^n-1 containing $a(2^t-1)$. Since n is odd, each $s_{a(2^t-1)}$ is also odd and we obtain

$$\begin{aligned} f(x) &= \sum_{a(2^t-1)\in T} Tr_1^{s_{a(2^t-1)}}(\beta_a x^{a(2^t-1)}) \\ &= \sum_{a(2^t-1)\in T} \frac{n}{s_{a(2^t-1)}} Tr_1^{s_{a(2^t-1)}}(\beta_a x^{a(2^t-1)}) \\ &= Tr_1^n(\sum_{a(2^t-1)\in T} \beta_a x^{a(2^t-1)}) \end{aligned}$$

We take $g(x) = x^c + \sum_{a(2^t-1)\in T} \beta_a x^{a(2^t-1)}$. Then by the above discussion and theorem 1

$$\left| \sum_{x\in GF(2^n)} \chi_1(g(x)) \right| = 2^{n-t+1}.$$

■

For even n we are able to prove the following,

Theorem 3 *Let $n > 1$ be an even number. There exists a polynomial $g \in GF(2^n)[x]$ of the form*

$$g(x) = x^c + \sum_{i=1}^{N} \beta_i x^{a_i(2^{n/2}-1)}$$

such that $\left|\sum_{x\in GF(2^n)} \chi_1(g(x))\right| \neq 0$.

Proof : Suppose A is a $(2^{n/2}+1, 2^{n/2}-1)$-interleaved sequence corresponding to $Tr_1^n(x^c)$ for some c coprime to 2^n-1 and B is a $(2^{n/2}+1, 2^{n/2}-1)$-interleaved sequence corresponding to a function of the form $Tr_1^n(\sum_{i=1}^N \beta_i x^{a_i(2^{n/2}-1)})$. B consists of only zero columns and 'all one' columns. Suppose the number of 'all one' column of B is denoted by r. From theorem 1

$$\Gamma = \left| \sum_{x\in GF(2^n)} \chi_1(g(x)) \right| = \left|2r - 2^{t+1}s\right|.$$

Since the interleaved sequence A has only one zero column, s, being the number of zero columns of A that get added to 'all one' columns of B, can take the value 0 or 1. In case

$s = 0$ the sum $\Gamma = 2r \neq 0$ whenever $r \neq 0$. In case $s = 1$ it is possible to choose an element $\gamma \in GF(2^n)$ in such a way that the zero column of the $(2^{n/2}+1, 2^{n/2}-1)$-interleaved sequence corresponding to $Tr_1^n((\gamma x)^c)$ is not added to a 'all one' column of B provided $r < d = 2^{\frac{n}{2}} + 1$. Thus we obtain a polynomial of the form $h(x) = (\gamma x)^c + \sum_{i=1}^{N} \beta_i x^{a_i(2^{n/2}-1)}$ such that $\left|\sum_{x \in GF(2^n)} \chi_1(h(x))\right| \neq 0$. Replacing γx by x in $h(x)$ we get a polynomial $g(x)$ of the required form such that $\left|\sum_{x \in GF(2^n)} \chi_1(g(x))\right| \neq 0$. In case $r = 2^{\frac{n}{2}} + 1$ then $s = 1$ and corresponding sum $\Gamma = 2$.

Finally we construct a function of the form $Tr_1^n(\sum_{i=1}^{N} \beta_i x^{a_i(2^{n/2}-1)})$ such that the $(d, 2^{\frac{n}{2}} - 1)$-interleaved sequence B corresponding to it contains atleast a nonzero column. There exists $\beta \in GF(2^n)$ such that $Tr_1^n(\beta) \neq 0$. Construct $Tr_1^n(\beta x^{\frac{n}{2}-1})$. Clearly the first column of the $(d, 2^{\frac{n}{2}} - 1)$-interleaved sequence corresponding to this function is nonzero. This proves the theorem. ■

Acknowledgement: The author likes to acknowledge Dr. P. H. Keskar of Mathematics Group BITS Pilani, India, Dr. S. Maitra of Applied Statistics Unit, ISI Kolkata, India and anonymous reviewers for their valuable comments which improved both the technical quality and presentation of this paper.

References

[1] S. Gangopadhyay and S. Maitra. *Further Results related to Generalized Nonlinearity.* Proceedings of INDOCRYPT 2002, volume 2551 in Lecture Notes in Computer Science, Pages 260-274, Springer-Verlag, 2002.

[2] G. Gong. *Theory and applications of q-ary interleaved sequences.* IEEE Trans. on Inform. Theory, vol. 41, No. 2, 1995, pp. 400 - 411.

[3] G. L. Mullen, I. E. Shparlinski. *Open Problems and Conjectures in finite fields.* LMS Lect. Notes Series, vol. 233, pp. , 1996.

[4] I. E. Shparlinski. *Computational and algorithmic problems in finite fields.* Kluwer Acad. Publ., Dordrecht, The Netherlands, 1992.

[5] I. E. Shparlinski. *Bounds of Gauss Sums in Finite Fields.* Proceedings of the AMS (to appear).

[6] S. A. Stepanov. *Arithmetic of Algebraic Curves.* Plenum, New York 1994.

[7] S. A. Stepanov. *Character sums and coding theory.* LMS Lect. Notes Series 233 pp. 355 - 378, 1996.

[8] A. Weil. *On some exponential sums.* Proc. Nat. Acad. Sci. U.S.A. 1948, **34** pp. 204 - 207.

[9] A. Youssef and G. Gong. *Hyper-bent Functions.* Advances in Cryptology, Proc. of Eurocrypt'2001, LNCS 2045, pp. 406-419, Springer-Verlag, 2001.

[10] A. Youssef and G. Gong. *Boolean Functions with Large Distance to all Bijective Monomials: N odd case.* LNCS, 2259, p. 49 ff, Springer-Verlag, 2001.