A NOTE ON PARTIAL SPREAD GENERALIZED BENT FUNCTION

XIAO ZHANG

ABSTRACT. In this paper, we give a necessary and sufficient condition for a function with the form $\mathrm{tr}(\sum_{i=1}^{q} a_i x^{i(q-1)})$ being generalized bent function. We indicate that these generalized bent functions are just those which could be constructed from partial spreads. We also introduce a method to calculate these generalized bent functions by means of interpolation.

1. INTRODUCTION

Boolean bent functions were first introduced by Rothaus [5] in 1976. In [3], the authors generalized the notion of boolean bent functions to the case of functions over an arbitrary finite field. Let F_q be a finite field with q elements. Let f be a function mapping F_{p^n} to F_p, where p is a prime number. The *Walsh coefficient* of f at $b \in F_{p^n}$ is defined by

$$W_f(b) := \sum_{x \in F_{p^n}} \xi_p^{f(x)+\mathrm{tr}(bx)},$$

where ξ_p is a complex primitive p-th root of unity and $\mathrm{tr}(x)$ is the absolute trace function, i.e. $\mathrm{tr}(x) = \sum_{i=0}^{n-1} x^{p^i}$. The function f is said to be a *generalized bent function* if all its Walsh coefficients satisfy $|W_f(b)|^2 = p^n$.

In this paper we concentrate on generalized bent functions defined on the finite fields $F_{p^{2n}}$, having the form

$$f(x) = \mathrm{tr}(\sum_{i=1}^{p^n} a_i x^{i(p^n-1)}),$$

with $a_i \in F_{p^{2n}}$. Bent functions having the form $\mathrm{tr}(ax^{2^n-1})$, with $a \in F_{2^{2n}}$, defined on the finite field $F_{2^{2n}}$, are called Dillon bent functions[4]. In the second section of [1], the authors studied the generalized Dillon bent functions, which are of the form $\mathrm{tr}(ax^{t(p^n-1)})$ with $a \in F_{p^{2n}}$ and t an integer, defined on the finite field $F_{p^{2n}}$ for an odd prime p. Our main interest is the following question.

2010 Mathematics Subject Classification. 05E99, 06E30, 94A60.

This work was supported by National Natural Science Foundation of China(10331030).

Let $q = p^n$. For a function $f : F_{q^2} \to F_p$ with the form $f(x) = \mathrm{tr}(\sum_{i=1}^{q} a_i x^{i(q-1)})$, what conditions make it a bent function.

In section 2, we give a necessary condition for functions of this kind being generalized bent functions. In section 3, we point out the sufficiency of this necessary condition. In fact, we find these generalized bent functions are just those which can be constructed from partial spreads [2]. In section 4, we introduce a method to calculate the representation of such a generalized bent function as the form $\sum_{i=1}^{q} c_i x^{i(q-1)}$, when we know its values.

2. A Necessary Condition

Suppose that $f(x) = \mathrm{tr}(\sum_{i=1}^{q} a_i x^{i(q-1)})$ is a generalized bent function defined on F_{q^2} with $q > 3$. According to the equation (2) of [1], $W_f(0) = q\xi_p^{i_0}$ or $-q\xi_p^{i_0}$, with i_0 being some integer.

We claim that $W_f(0) = q$.

Proof of the claim.

Firstly, we have $f(x) = f(ax)$, for all nonzero $a \in F_q$, because $a^{q-1} = 1$. As a F_q-linear space of dimension 2 over F_q, F_{q^2} has $q+1$ non-trivial subspaces, the intersection of any two of which is $\{0\}$. So we can find $q+1$ elements α_1, α_2,...,α_{q+1} in F_{q^2} as the bases of the corresponding F_q-subspaces. Now we compute

$$\begin{aligned} W_f(0) &= \sum_{x \in F_{q^2}} \xi_p^{f(x)} = 1 + \sum_{x \neq 0} \xi_p^{f(x)} = 1 + \sum_{j=1}^{q+1} \sum_{x \in F_q^* \alpha_j} \xi_p^{f(x)} \\ &= 1 + \sum_{j=1}^{q+1} \sum_{x \in F_q^* \alpha_j} \xi_p^{f(\alpha_j)} = 1 + (q-1) \sum_{j=1}^{q+1} \xi_p^{f(\alpha_j)}. \end{aligned}$$

Denote $f(\alpha_j)$ by f_j. If $W_f(0) = q\xi_p^{i_0}$, we get

$$1 + \sum_{j=1}^{q+1} (q-1)\xi_p^{f_j} = q\xi_p^{i_0} = (q-1)\xi_p^{i_0} + \xi_p^{i_0}.$$

Hence, $\xi_p^{i_0} - 1 = (q-1)(\sum_{j=1}^{q+1} \xi_p^{f_j} - \xi_p^{i_0})$, which is impossible unless $i_0 = 0$, because otherwise the principal ideal $(\xi_p^{i_0} - 1)$ is the prime ideal over (p) in the algebraic integers ring $Z[\xi_p]$, and coprime to $(q-1)$. For the basic facts on cyclotomic fields, please refer to the second chapter of [6].

If $W_f(0) = -q\xi_p^{i_0}$, we get

$$1 + \sum_{j=1}^{q+1} (q-1)\xi_p^{f_j} = -q\xi_p^{i_0} = (1-q)\xi_p^{i_0} - \xi_p^{i_0}.$$

Hence $\xi_p^{i_0} + 1 = (1-q)(\sum_{j=1}^{q+1} \xi_p^{f_j} + \xi_p^{i_0})$, which is contradictory to the fact that $1 + \xi_p^{i_0}$ is a unit in the algebraic integers ring $Z[\xi_p]$ in case of $i_0 \neq 0$.

If $i_0 = 0$, we get $2 = (1-q)(\sum_{j=1}^{q+1} \xi_p^{f_j} + 1)$ which is contradictory to the condition $q > 3$. Thus we prove the claim. □

Using the notations in the proof, we have $1 + \sum_{j=1}^{q+1}(q-1)\xi_p^{f_j} = q$. Consequently, $\sum_{j=1}^{q+1} \xi_p^{f_j} = 1$, which implies that for any nonzero $a \in F_p$, there are $\frac{q}{p}$ j's satisfying $f_j = a$ and there are $1 + \frac{q}{p}$ j's satisfying $f_j = 0$.

Taking f as a function mapping F_{q^2} to F_q, we can write f as a polynomial with coefficients in F_{q^2}, $f(x) = \sum_{i=1}^{q} c_i x^{i(q-1)}$. Associate with f another polynomial function $g(x) = \sum_{i=1}^{q} c_i x^i$. Obviously, $g(x^{q-1}) = f(x)$. We know all α^{q-1}, for nonzero $\alpha \in F_{q^2}$, constitute the subgroup of order $q+1$ in the multiplicative group $F_{q^2}^*$. Thus we get a necessary condition for f being a bent function.

Theorem 1 If $f(x) = \mathrm{tr}(\sum_{i=1}^{q} a_i x^{i(q-1)})$ is a bent function defined on F_{q^2}, then as x runs over all the elements of the subgroup of order $q+1$ in the multiplicative group $F_{q^2}^*$, the function $g(x) = \sum_{i=1}^{q} c_i x^i$ takes every nonzero element in F_p exactly $\frac{q}{p}$ times and takes 0 $1 + \frac{q}{p}$ times.

3. Sufficiency

Now we indicate that the above necessary condition is also sufficient.

Suppose that $f(x) = \mathrm{tr}(\sum_{i=1}^{q} a_i x^{i(q-1)})$ is associated with $g(x) = \sum_{i=1}^{q} c_i x^i$. We know that f takes the same value on the nonzero elements of a F_q-subspace in F_{q^2}. All the F_q-subspaces of dimension one make a spread for F_{q^2}. As $g(x^{q-1}) = f(x)$ and by condition, as x runs over all the elements of the subgroup of order $q+1$ in $F_{q^2}^*$, g takes every nonzero element in F_p exactly $\frac{q}{p}$ times and takes 0 $1 + \frac{q}{p}$ times, f satisfies the condition (4) in [2]. So f must be a generalized bent function.

Actually, from the proof of the claim of section 2, we know that the generalized bent functions of the form $\mathrm{tr}(\sum_{i=1}^{p^n} a_i x^{i(p^n-1)})$ are just the partial spreads generalized bent functions constructed in [2].

4. A method to calculate partial spreads generalized bent functions

Suppose that $f(x) = \mathrm{tr}(\sum_{i=1}^{q} a_i x^{i(q-1)})$ associating with $g(x) = \sum_{i=1}^{q} c_i x^i$ is a bent function defined on F_{q^2}, and suppose we know its values. We want to calculate all the c_i's.

Take an element of order $q+1$ in $F_{q^2}^*$, say ω_0. Then ω_0, ω_0^2, ..., ω_0^q, and $\omega_0^{q+1} = 1$ constitute the subgroup of order $q+1$ in $F_{q^2}^*$. By the necessary condition, for any nonzero $a \in F_p$ there are $\frac{q}{p}$ j's satisfying $g(\omega_0^j) = a$ and there are $1 + \frac{q}{p}$ j's satisfying $g(\omega_0^j) = 0$. Denote $g(\omega_0^j) = r_j$, $j \in \{1, 2, ..., q+1\}$. Define b as

$$\begin{pmatrix} 0 & 0 & 1 & 2 & \dots & p-1 & 0 & 1 & \dots & p-1 & \dots & 0 & 1 & 2 & \dots & p-1 \end{pmatrix},$$

containing $\frac{q}{p}$ copies of F_p and one more 0. Define r as

$$\begin{pmatrix} r_1 & r_2 & \dots & r_{q+1} \end{pmatrix}.$$

Then f is a generalized bent function if and only if r can become b after some permutation.

We know g is a polynomial of degree $\leq q$. So, as we have already known the values of g on $q+1$ different points, $\omega_0, \omega_0^2, \dots, \omega_0^{q+1}$, we can recover the coefficients c_i's by interpolation as follows.

Write $g(x) = \sum_{i=1}^{q} c_i x^i$ as $g(x) = \sum_{i=0}^{q} c_i x^i$, with c_0 being 0. For

$$g(\omega_0^j) = \sum_{i=0}^{q} c_i (\omega_0^j)^i = r_j, j \in \{1, 2, \dots, q+1\},$$

we obtain a system of linear equations defined on F_{q^2} in variates $c_0, c_1, c_2, \dots, c_q$. After some permutation among these equations, we get a system of linear equations with the following coefficients matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \omega_0 & \omega_0^2 & \omega_0^3 & \dots & \omega_0^{q-1} & \omega_0^q \\ 1 & \omega_0^2 & \omega_0^4 & \omega_0^6 & \dots & \omega_0^{2(q-1)} & \omega_0^{2q} \\ \dots & \dots & & & & \dots & \\ 1 & \omega_0^q & \omega_0^{2q} & \omega_0^{3q} & \dots & \omega_0^{q(q-1)} & \omega_0^{q^2} \end{pmatrix},$$

denoted by A. Define C as

$$\begin{pmatrix} c_0 & c_1 & c_2 & \dots & c_q \end{pmatrix}.$$

Then these equations can be written by matrix equation $AC' = R'$, where C' and R' are the transposed vectors of C and R respectively, and R is a permutation of r. A is a Vandermond matrix and its inverse A^{-1} is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \omega_0^q & \omega_0^{2q} & \omega_0^{3q} & \dots & \omega_0^{(q-1)q} & \omega_0^{q^2} \\ 1 & \omega_0^{q-1} & \omega_0^{2(q-1)} & \omega_0^{3(q-1)} & \dots & \omega_0^{(q-1)^2} & \omega_0^{q(q-1)} \\ \dots & \dots & & & & \dots & \\ 1 & \omega_0 & \omega_0^2 & \omega_0^3 & \dots & \omega_0^{q-1} & \omega_0^q \end{pmatrix}.$$

So, as we know the values of f, it is easy to calculate these c_i's. And then, it is easy to represent f as the form $\mathrm{tr}(\sum_{i=1}^{q} a_i x^{i(q-1)})$.

Further, given any permutation of b, it is easy to calculate a bent function with the form $f(x) = \sum_{i=1}^{q} c_i x^{i(q-1)}$.

Example Let $q = p = 5$, and w is a primitive element in the multiplicative group F_{25}^*. Denote $g = \sum_{i=0}^{5} c_i x^i$. Suppose that R is

$$\begin{pmatrix} 0 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Then we have $g(1) = 0$, $g(w^4) = 0$, $g(w^8) = 1$, $g(w^{12}) = 2$, $g(w^{16}) = 3$, $g(w^{20}) = 4$. We know that $F_p w^{4j}$, $j = 1, 2, \dots, 6$, are all the one-dimensional subspaces of F_{p^2}, and then constitute a spread. $f(x) = g(x^{p-1})$ takes the same value at the nonzero elements of a subspace. So f satisfies our necessary and sufficient condition and is a bent function.

Now, A is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w^4 & w^8 & w^{12} & w^{16} & w^{20} \\ 1 & w^8 & w^{16} & w^{24} & w^{32} & w^{40} \\ 1 & w^{12} & w^{24} & w^{36} & w^{48} & w^{60} \\ 1 & w^{16} & w^{32} & w^{48} & w^{64} & w^{80} \\ 1 & w^{20} & w^{40} & w^{60} & w^{80} & w^{100} \end{pmatrix},$$

and A^{-1} is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w^{20} & w^{40} & w^{60} & w^{80} & w^{100} \\ 1 & w^{16} & w^{32} & w^{48} & w^{64} & w^{80} \\ 1 & w^{12} & w^{24} & w^{36} & w^{48} & w^{60} \\ 1 & w^8 & w^{16} & w^{24} & w^{32} & w^{40} \\ 1 & w^4 & w^8 & w^{12} & w^{16} & w^{20} \end{pmatrix}.$$

Then

$$C' = A^{-1}R' = \begin{pmatrix} 0 & 0 & w^{17} & 1 & w^{13} & 0 \end{pmatrix}$$

determining a bent function on F_{25}, $f(x) = w^{17}x^8 + x^{12} + w^{13}x^{16} = \mathrm{tr}(w^{17}x^8 + 3x^{12})$. □

The above method is also valid for boolean bent functions, as the construction from spreads is valid for fields of characteristic two [2].

We note that in [2], the authors have given the functions constructed from spreads in another form, but they didn't try to calculate the c_i's.

ACKNOWLEDGEMENT

The author wishes to thank Professor Weisheng Qiu and Dr. Yin Tan for their helpful discussions.

REFERENCES

[1] Tor Helleseth, Alexander Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, *IEEE Transcations on information theory*, vol.52(5)(2006):2018–2032.

[2] Sunghwan Kim, Gang-Mi Gil, Kyung-Hee Kim, Jong-Seon No, Generalized Bent Funcitons Constructed From Partial Spreads, ISIT 2002, Lausanne, Switerland, June 30- July 5, 2002.

[3] P. V. Kumar, R. A. Scholtz, and L. R. Welch, Generalized bent functions and their properties, *J. Combin. Theory Ser. A*, vol.40(1): 90–107, (1985).

[4] P. Langevin, G. Leander, Monomial bent functions and Stickelberger's theorem, *Finite Fields and Their Applications*, vol.14:727–742, (2008).

[5] O. S. Rothaus, On bent functions, *J. Combin. Theory Ser. A*, vol.20(3)(1976):300–305.

[6] L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, (1997), second edtion.

LMAM and School of Mathematical Sciences, Peking University, Beijing, 100871, PRC

E-mail address: zhangxiao@math.pku.edu.cn