Cross Correlation of Sequences, Generalized Bent Functions, Jacobsthal Sums and Related Topics

Tor Helleseth and Alexander Kholosha

The Selmer Center
Department of Informatics, University of Bergen
P.O. Box 7800, N-5020 Bergen, Norway
{Tor.Helleseth,Alexander.Kholosha}@uib.no

1 Introduction

Niho in [1, Theorem 3-7] and Helleseth in [2] studied the cross correlation between two binary m-sequences that differ by the decimation $2^{3k} - 2^{2k} + 2^k + 1$. They proved that the cross-correlation function is four-valued and found the distribution. We take $n = 4k$, an odd prime p and examine p-ary functions having the form $f(x) = \mathrm{Tr}_n\left(ax^d + bx^2\right)$ with $a, b, x \in \mathrm{GF}(p^n)$ and $d = p^{3k} + p^{2k} - p^k + 1$. Note that d is cyclotomic equivalent to the Niho exponent (with 2 changed to p) and that $\gcd(d, p^n - 1) = 2$ since $d = (p^{2k} - 1)(p^k + 1) + 2$.

Given a function $f(x)$ mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$, the direct and inverse *Walsh transform* operations on f are defined at a point by the following respective identities:

$$S_f(y) = \sum_{x \in \mathrm{GF}(p^n)} \omega^{f(x) - \mathrm{Tr}_n(yx)} \quad \text{and} \quad \omega^{f(x)} = \frac{1}{p^n} \sum_{y \in \mathrm{GF}(p^n)} S_f(y) \omega^{\mathrm{Tr}_n(yx)}$$

where $\mathrm{Tr}_n() : \mathrm{GF}(p^n) \to \mathrm{GF}(p)$ denotes the absolute trace function, $\omega = e^{\frac{2\pi i}{p}}$ is the complex primitive p^{th} root of unity and elements of $\mathrm{GF}(p)$ are considered as integers modulo p.

According to [3], $f(x)$ is called a *p-ary bent function* (or *generalized bent function*) if all its Walsh coefficients satisfy $|S_f(y)|^2 = p^n$. A bent function $f(x)$ is called *regular* (see [3, Definition 3] and [4, p. 576]) if for every $y \in \mathrm{GF}(p^n)$ the normalized Walsh coefficient $p^{-n/2} S_f(y)$ is equal to a complex p^{th} root of unity, i.e., $p^{-n/2} S_f(y) = \omega^{f^*(y)}$ for some function f^* mapping $\mathrm{GF}(p^n)$ into $\mathrm{GF}(p)$. A bent function $f(x)$ is called *weakly regular* if there exists a complex u having unit magnitude such that $up^{-n/2} S_f(y) = \omega^{f^*(y)}$ for all $y \in \mathrm{GF}(p^n)$. Recently, weakly regular bent functions were shown to be useful for constructing certain combinatorial objects such as partial difference sets, strongly regular graphs and association schemes (see [5, 6]). This justifies why the classes of (weakly) regular bent functions are of independent interest. For a comprehensive reference on monomial and quadratic p-ary bent functions we refer reader to [7].

Taking $a = b = 1$, results in a weakly regular bent function and the exact value of its Walsh transform coefficients (and value distribution) can be found.

This gives the infinite class of nonquadratic generalized bent functions built over the fields of an arbitrary odd characteristic.

Theorem 1. *Let $n = 4k$. Then p-ary function $f(x)$ mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$ and given by*

$$f(x) = \mathrm{Tr}_n\left(x^{p^{3k}+p^{2k}-p^k+1} + x^2\right)$$

is a weakly regular bent function. Moreover, for $y \in \mathrm{GF}(p^n)$ the corresponding Walsh transform coefficient of $f(x)$ is equal to

$$S_f(y) = -p^{2k}\omega^{\mathrm{Tr}_k(x_0)/4} \ ,$$

where x_0 is a unique root in $\mathrm{GF}(p^k)$ of the polynomial

$$y^{p^{2k}+1} + (y^2+X)^{(p^{2k}+1)/2} + y^{p^k(p^{2k}+1)} + (y^2+X)^{p^k(p^{2k}+1)/2} \ .$$

In particular, if $y^2 \in \mathrm{GF}(p^{2k})$ then $x_0 = -\mathrm{Tr}_k^{2k}(y^2)$. Also, every value $-p^{2k}\omega^i$ with $i = \{1, \ldots, p-1\}$ occurs $p^{2k-1}(p^{2k}+1)$ times in the Walsh spectrum of $f(x)$ and $-p^{2k}$ occurs $(p^{2k-1}-1)(p^{2k}+1)+1$ times.

The general case when $a, b \in \mathrm{GF}(p^n)$ is much more complicated. It seems to be hard to find the Walsh transform coefficients of $f(x)$ at an arbitrary point, so we calculate the exponential sum of $f(x)$, i.e., $S_f(0)$. This is equal to the cross-correlation function between two sequences of length $(p^n-1)/2$ obtained by the decimation of an m-sequence by d and 2 or can be seen as a codeword weight in the corresponding p-ary linear code. We relate this value to the number of zeros, a particular polynomial has in a cyclic subgroup of order $p^{2k}+1$ of the multiplicative group of $\mathrm{GF}(p^n)$. Moreover, we show that if either $a^{p^k(p^k+1)} \neq b^{p^k+1}$ or $a^2 = b^d$ with $b \neq 0$ then the exponential sum of $f(x)$ is three-valued. Some steps towards finding the distribution of these values are made but the exact distribution remains an open problem. For the remaining options for choosing (a, b), we show that $S_f(0)$ can be expressed using the Jacobsthal sum of order p^k+1 which has the number of possible values growing with k.

2 Related Results

Let ν be a primitive element of $\mathrm{GF}(p^{2k})$ and let C_t $(t = 0, \ldots, p^k)$ denote the *cyclotomic classes* of order p^k+1 in $\mathrm{GF}(p^{2k})^*$, i.e., $C_t = \{\nu^{(p^k+1)i+t} \mid i = 0, \ldots, p^k-2\}$. The number of elements $x \in C_i$ such that $x+1 \in C_j$ is called the *cyclotomic number* and denoted (i, j). Since $-1 \in C_0$ in our case, we can also take $x-1$ in the definition of the cyclotomic numbers. Note that since the cyclotomic numbers of order p^k+1 are *uniform* (see [8]), their values can easily be determined.

Lemma 1. *For any $i, j = 0, \ldots, p^k$, the cyclotomic numbers of order p^k+1 in $\mathrm{GF}(p^{2k})$ are*

$$(i,j) = \begin{cases} 1, & \text{if} \quad i \neq j \text{ and } ij \neq 0 \\ p^k-2, & \text{if} \quad i = j = 0 \\ 0, & \text{otherwise} \ . \end{cases}$$

Following [9, Definition 5.49], for any $a \in \mathrm{GF}(q)^*$, define a *Jacobsthal sum* of order n as

$$H_n(a) = \sum_{x \in \mathrm{GF}(q)} \eta(x^{n+1} + ax) \ ,$$

where $\eta(\cdot)$ is the quadratic character of $\mathrm{GF}(q)$ extended by setting $\eta(0) = 0$. Define also a companion sum

$$I_n(a) = \sum_{x \in \mathrm{GF}(q)^*} \eta(x^n + a) \ .$$

It is well known (see, e.g., [9, Theorem 5.50]) that $I_{2n}(a) = I_n(a) + H_n(a)$.

In our case, $q = p^{2k}$ and we consider $n = p^k + 1$. If $a \in \mathrm{GF}(p^k)$ then, obviously, $I_{p^k+1}(a) = I_{2(p^k+1)}(a) = p^{2k} - 1$ and $H_{p^k+1}(a) = 0$. For any $a \in \mathrm{GF}(p^{2k}) \setminus \mathrm{GF}(p^k)$, we compute

$$I_{p^k+1}(a) = -(p^k + 1)(\eta(a) + 1) \ .$$

Calculating $H_{p^k+1}(a)$ (that is equivalent to calculating $I_{2(p^k+1)}(a)$) is not that easy.

Theorem 2. *For any $a \in \mathrm{GF}(p^{2k}) \setminus \mathrm{GF}(p^k)$, assume $a = a_0 + 2\mu^{1/2}a_1$ with $a_0, a_1 \in \mathrm{GF}(p^k)$ and μ being a primitive element of $\mathrm{GF}(p^k)$. Then*

$$H_{p^k+1}(a) = (N - p^k)(p^k + 1) \quad \textit{and} \quad |H_{p^k+1}(a)| \leq 2p^{k/2}(p^k + 1) \ ,$$

where N denotes the number of points on the elliptic curve $f^2 = z^3 - a_0 z^2 + \mu a_1^2 z$ over $\mathrm{GF}(p^k)$ excluding the point at infinity.

3 Calculating the Exponential Sum of $f(x)$

In this section, we consider the function $f(x)$ with arbitrary coefficients $a, b \in \mathrm{GF}(p^n)$. If n is even, let U denote a cyclic subgroup of order $p^{n/2} + 1$ of the multiplicative group of $\mathrm{GF}(p^n)$ (generated by $\xi^{p^{n/2}-1}$, where ξ is a primitive element of $\mathrm{GF}(p^n)$).

Theorem 3. *Let $n = 4k$. For any $a, b \in \mathrm{GF}(p^n)$, define the following p-ary function mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$*

$$f(x) = \mathrm{Tr}_n\left(ax^{p^{3k}+p^{2k}-p^k+1} + bx^2\right) \ .$$

Then the Walsh transform coefficient of $f(x)$ evaluated at point zero is equal to

$$S_f(0) = p^{2k}(2N(a, b) - 1) \ ,$$

where $2N(a, b)$ is the number of zeros in U of the polynomial

$$L(X) = b^{p^{2k}} X + aX^{p^k} + bX^{p^{2k}} + a^{p^{2k}} X^{p^{3k}} \ . \tag{1}$$

In what follows, we consider separately the cases when either $a^{p^k(p^k+1)} \neq b^{p^k+1}$ or $a^2 = b^d$ with $b \neq 0$; and when $a^{p^k(p^k+1)} = b^{p^k+1}$ with $a^2 \neq b^d$, where $d = p^{3k} + p^{2k} - p^k + 1$. This covers all the value space for the pairs $(a, b) \neq (0, 0)$.

Proposition 1. *Let $n = 4k$ and take any $a, b \in \mathrm{GF}(p^n)$ such that either $a^2 = b^d$ with $b \neq 0$ or $a^{p^k(p^k+1)} \neq b^{p^k+1}$. Then polynomial $L(X)$ defined in (1) has none, two or four zeros in U, i.e., $N(a, b) \in \{0, 1, 2\}$.*

Proposition 2. *Let $n = 4k$ and take any $a, b \in \mathrm{GF}(p^n)$ such that $a^{p^k(p^k+1)} = b^{p^k+1}$ and $a^2 \neq b^d$. If $2N(a, b)$ is the number of zeros in U of the polynomial $L(x)$ defined in (1) then*

$$N(a,b) = \#\left\{c \in \mathrm{GF}(p^k) \mid (cg)^2 - b^{p^{2k}+1} \text{ is a nonsquare in } \mathrm{GF}(p^{2k})\right\} \ ,$$

where g is any element in $\mathrm{GF}(p^{2k})^*$ with $g^{p^k-1} = -b^{p^{3k}}/a$. Moreover,

$$2N(a,b) = p^k - \frac{H_{p^k+1}\big(-b^{p^{2k}+1}/g^2\big)}{p^k+1} + 1 \ .$$

Thus, the value distribution of $S_f(0)$ when $a^{p^k(p^k+1)} = b^{p^k+1}$ with $a^2 \neq b^d$, is defined by the value distribution of the Jacobsthal sums order $p^k + 1$ and is directly related to the number of elliptic curves with the prescribed number of points. This is the first direct connection between sequences and Jacobsthal sums we are aware of. We find it interesting and believe that this gives an important link between sequences/codes and classical character sums. In the following corollary, we list some basic properties of $N(a, b)$.

Corollary 1. *Under the conditions of Proposition 2,*

(i) $N(a,b) = \begin{cases} N(a^{-1}, b^{-1}), & \text{if } b^{(p^n-1)/2} = 1 \\ p^k + 1 - N(a^{-1}, b^{-1}), & \text{otherwise} \ ; \end{cases}$

(ii) $N(a,b) + N(-a,b) = N(a,b) + N(a,-b) = p^k + 1$;

(iii) $N(-a,b) = \begin{cases} p^k + 1 - N(a^{-1}, b^{-1}), & \text{if } b^{(p^n-1)/2} = 1 \\ N(a^{-1}, b^{-1}), & \text{otherwise} \ ; \end{cases}$

(iv) if $b^{(p^n-1)/2} = 1$ (resp. $b^{(p^n-1)/2} = -1$) then $N(a, b)$ is an even (resp. odd) number;

(v) $\left|N(a,b) - \frac{p^k+1}{2}\right| \leq p^{k/2}$, in particular, $N(a, b)$ is positive and, if $k > 2$ then $N(a, b) > 8$;

(vi) if $p \equiv -1 \pmod 4$, k is odd and $b^{(p^n-1)/2} = 1$ then $N(a,b) = N(-a,b) = (p^k+1)/2$ for $a = \nu^{(p^{2k}-1)/4} b^{d/2}$, where ν is a primitive element of $\mathrm{GF}(p^{2k})$;

(vii) for any $b \in \mathrm{GF}(p^n)^*$,

$$\sum_{a \in \mathrm{GF}(p^n):\ a^{p^k(p^k+1)} = b^{p^k+1},\ a^2 \neq b^d} N(a,b) = (p^k+1)\big(p^k - b^{(p^n-1)/2}\big)/2 \ . \quad (2)$$

References

1. Niho, Y.: Multi-Valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences. PhD thesis, University of Southern California, Los Angeles (1972)
2. Helleseth, T.: A note on the cross-correlation function between two binary maximal length linear sequences. Discrete Math. **23**(3) (1978) 301–307
3. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Combin. Theory Ser. A **40**(1) (September 1985) 90–107
4. Hou, X.D.: p-Ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields Appl. **10**(4) (October 2004) 566–582
5. Pott, A., Tan, Y., Feng, T., Ling, S.: Association schemes arising from bent functions. In Kholosha, A., Rosnes, E., Parker, M., eds.: WCC 09 Preproceedings - The International Workshop on Coding and Cryptography, Bergen (2009) 48–61
6. Tan, Y., Pott, A., Feng, T.: Strongly regular graphs associated with ternary bent functions. J. Combin. Theory Ser. A **117**(6) (August 2010) 668–682
7. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5) (May 2006) 2018–2032
8. Baumert, L., Mills, W., Ward, R.L.: Uniform cyclotomy. J. Number Theory **14**(1) (February 1982) 67–82
9. Lidl, R., Niederreiter, H.: Finite Fields. Volume 20 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge (1997)