Cryptogr. Commun. (2011) 3:281–291
DOI 10.1007/s12095-011-0048-0

Crosscorrelation of *m*-sequences, exponential sums, bent functions and Jacobsthal sums

Tor Helleseth · Alexander Kholosha

Received: 19 January 2011 / Accepted: 2 June 2011 / Published online: 30 June 2011

Abstract The crosscorrelation of maximal length linear shift register sequences is a well-studied problem that has many applications in sequence designs. This problem is known to have many important connections to exponential sums. In recent years, the study of *p*-ary bent functions has received a lot of attention and several new functions have been found that are related to the crosscorrelation function and that lead to new connections and problems on Jacobsthal sums. This paper gives a survey of some of these connections.

Keywords Crosscorrelation · *m*-Sequence · *p*-Ary bent function · Jacobsthal sum · Polynomial over finite field

Mathematics Subject Classifications (2010) 11T23 · 94A55

1 Introduction

The crosscorrelation of maximal length linear shift register sequences (or *m*-sequences) has been a research topic for more than 40 years. Traditionally, the crosscorrelation properties of binary *m*-sequences were mainly studied due to their applications in sequence designs. The crosscorrelation between *m*-sequences leads to several challenging and difficult problems and is closely related to exponential sums over finite fields. For example, the crosscorrelation between an *m*-sequence and its reverse sequence is equivalent to the classical mathematical notion of Kloosterman

This work was supported by the Norwegian Research Council.

T. Helleseth (✉) · A. Kholosha
The Selmer Center, Department of Informatics, University of Bergen,
PB 7800, 5020 Bergen, Norway
e-mail: Tor.Helleseth@ii.uib.no

A. Kholosha
e-mail: Alexander.Kholosha@ii.uib.no

sums. Many important results have been obtained using a variety of methods on exponential sums but several open problems remain.

In the recent years, the study of binary bent functions, motivated by cryptography, has been an important research topic. Several classes of bent functions have been constructed using m-sequences and their correlation properties.

In 1985, binary bent functions were generalized to p-ary bent functions by Kumar et al. [23]. Generalized bent functions have received a lot of attention and several new p-ary bent functions are also closely related to the crosscorrelation of m-sequences. Study of p-ary bent functions also leads to connections and problems on Jacobsthal sums. This paper is based on an invited talk for the 70th birthday of Jacques Wolfmann and gives a rather short survey of some of these recent connections. We also include some of the contributions by Jacques Wolfmann on Kloosterman sums that have applications to the crosscorrelation of m-sequences and to the construction of bent functions.

2 Preliminaries

Let GF(p) be the finite field with p elements. The initial state $(s_0, s_1, \ldots, s_{n-1})$ and the linear recursion of degree n over GF(p) defined by

$$\sum_{i=0}^{n} c_i s_{t+i} = 0, \quad \text{where } c_0, c_n \neq 0,$$

generates a periodic sequence $\{s_t\}$. The characteristic polynomial of the linear recursion is

$$f(x) = \sum_{i=0}^{n} c_i x^i.$$

Since n consecutive elements of the sequence determine the sequence completely, the maximal period for a recursion of degree n is $p^n - 1$. In the case when $f(x) \in \mathrm{GF}(p)[x]$ is a primitive polynomial, the recursion is known to generate a maximal linear sequence (or an m-sequence) of period $p^n - 1$.

Some important and well-known properties of m-sequences are:

- The m-sequence has period $p^n - 1$, each nonzero element occurs p^{n-1} times and the zero element occurs $p^{n-1} - 1$ times.
- For any m-sequence $\{s_t\}$ and $\tau \neq 0 \pmod{p^n - 1}$ it holds that $\{s_{t+\tau} - s_t\}$ is also an m-sequence.

Let $\{u_t\}$ and $\{v_t\}$ be two p-ary sequences of period ε. The crosscorrelation between the two sequences at shift τ, $0 \leq \tau < \varepsilon$, is

$$C_{u,v} = \sum_{t=0}^{\varepsilon-1} \omega^{u_{t+\tau} - v_t}$$

where ω is a complex primitive p-th root of unity. If the two sequences are the same we use the term autocorrelation instead of crosscorrelation. A useful property for m-sequences is their optimal two-level autocorrelation, which is important for synchronization purposes in many communication systems.

Lemma 1 *The autocorrelation function $C_{s,s}(\tau)$ of the m-sequence $\{s_t\}$ has the property,*

$$C_{s,s}(\tau) = \begin{cases} p^n - 1 & \text{if } \tau = 0 \pmod{p^n - 1} \\ -1 & \text{if } \tau \neq 0 \pmod{p^n - 1}. \end{cases}$$

This result is an easy consequence of the balanced distribution of the elements in an m-sequence and that $\{s_{t+\tau} - s_t\}$ is an m-sequence for $\tau \neq 0 \pmod{p^n - 1}$.

Let Tr_n be the trace function from $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$ defined by

$$\mathrm{Tr}_n(x) = \sum_{i=0}^{n-1} x^{p^i}.$$

The m-sequence $\{s_t\}$ can (after a suitable cyclic shift) be described simply by

$$s_t = \mathrm{Tr}_n\left(\xi^t\right),$$

where ξ is a zero of the characteristic polynomial $f(x)$. The different shifts of the m-sequence are obtained by

$$s_{t+\tau} = \mathrm{Tr}_n\left(c\xi^t\right),$$

where $c = \xi^\tau \in \mathrm{GF}(p^n)^* = \mathrm{GF}(p^n) \setminus \{0\}$. Two m-sequences $\{u_t\}$ and $\{v_t\}$ of the same period $p^n - 1$ are related by a decimation d such that $u_t = v_{dt+\tau}$ and $\gcd(d, p^n - 1) = 1$.

The crosscorrelation between any two m-sequences of the same period $\varepsilon = p^n - 1$ that differ by a decimation d can be described by the following exponential sum by using the trace function representation

$$\begin{aligned} C_d(\tau) &= \sum_{t=0}^{\varepsilon-1} \omega^{s_{t+\tau} - s_{dt}} \\ &= \sum_{t=0}^{\varepsilon-1} \omega^{\mathrm{Tr}_n(\xi^{t+\tau} - \xi^{dt})} \\ &= \sum_{x \in \mathrm{GF}(p^n)^*} \omega^{\mathrm{Tr}_n(cx - x^d)} \end{aligned}$$

where $c = \xi^\tau$. Determining the values and the number of occurrences of each value in the crosscorrelation function $C_d(\tau)$ when τ runs through $\{0, 1, \cdots, p^n - 2\}$ is equivalent to finding the distribution of this exponential sum for any $c \neq 0$.

The following result was stated for $p = 2$ by Golomb [8] without proof and first proved and generalized to any odd p by Helleseth [10].

Theorem 1 *If $d \notin \{1, p, \cdots, p^{n-1}\}$, (i.e., when the two m-sequences are cyclically distinct), then $C_d(\tau)$ is at least three-valued when $\tau = 0, 1, \cdots, p^n - 2$.*

Therefore, the crosscorrelation between m-sequences takes on at least three values. For binary sequences of length $2^n - 1$, the following is a complete list of all decimations known to give three-valued crosscorrelation. It is a challenging and open problem to decide whether this list is complete.

Theorem 2 *The crosscorrelation $C_d(\tau)$ is three-valued and the complete correlation distribution is known for the following values of d:*

(i) $d = 2^k + 1$, $\frac{n}{\gcd(k,n)}$ *odd* [7].
(ii) $d = 2^{2k} - 2^k + 1$, $\frac{n}{\gcd(k,n)}$ *odd* [19].
(iii) $d = 2^{\frac{n}{2}} + 2^{\frac{n+2}{4}} + 1$, $n \equiv 2 \pmod 4$ [3].
(iv) $d = 2^{\frac{n+2}{2}} + 3$, $n \equiv 2 \pmod 4$ [3].
(v) $d = 2^{\frac{n-1}{2}} + 3$, n *odd* [1].
(vi) [5, 18]

$$d = \begin{cases} 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} - 1, & n \equiv 1 \pmod 4 \\ 2^{\frac{n-1}{2}} + 2^{\frac{3n-1}{4}} - 1, & n \equiv 3 \pmod 4. \end{cases}$$

The PhD thesis of 1972 by Niho [25] provided new ideas that lead to new decimations with four-valued crosscorrelation for the case $n = 2k$. The decimations considered were of the form

$$d = s\left(2^k - 1\right) + 1.$$

For such values of d Niho showed that the crosscorrelation is given by

$$C_d(\tau) = -1 + (N_a - 1)2^k$$

where N_a is the number of common solutions of the two equations

$$x^{2s-1} + ax^s + a^{2^k} x^{s-1} + 1 = 0 \quad \text{and} \quad x^{2^k+1} = 1.$$

For $p = 2$, several known classes of binary four-valued decimations of this form are given in the theorem below. The first two are due to Niho [25]. One should observe the second decimation that turns out to give interesting p-ary bent functions if $p = 2$ is replaced by a general p.

Theorem 3 *Let $e_2(i)$ be the highest power of 2 dividing the integer i and assume $n = 2k$. The crosscorrelation $C_d(\tau)$ is four-valued and the complete correlation distribution is known for the following values of d:*

(i) $d = 2^{k+1} - 1$ *with* $n \equiv 0 \pmod 4$ [25].
(ii) $d = (2^k + 1)(2^{k/2} - 1) + 2$ *with* $n \equiv 0 \pmod 4$ [25].
(iii) $d = \frac{2^{(k+1)r} - 1}{2^r - 1}$ *for* $(0 < r < k, \gcd(r, n) = 1)$ *with* $n \equiv 0 \pmod 4$ [4].
(iv) $d = \frac{2^n + 2^{r+1} - 2^{k+1} - 1}{2^r - 1}$ *with* $2r$ *dividing* k *and* $n \equiv 0 \pmod 4$ [16].
(v) $d = (2^k - 1)s + 1$, $s \equiv 2^r(2^r \pm 1)^{-1} \pmod{2^k + 1}$, $e_2(r) < e_2(k)$ [6].

There are also some sporadic cases known with more than four-valued crosscorrelation for which the distribution is known. One important case is when $d = -1$. In this case, the crosscorrelation function $C_{-1}(\tau) + 1$ is the famous Kloosterman sum over $\mathrm{GF}(p^n)$

$$K(a) = \sum_{x \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n(x + ax^{-1})}.$$

An astonishing results by Lachaud and Wolfmann [24] is that for $p = 2$, the Kloosterman sum (or equivalently $C_{-1}(\tau) + 1$) takes on *all* the integer values satisfying $|K(a)| \leq 2\sqrt{2^n}$ with $K(a) = 0 \pmod 4$.

Two long standing conjectures from Helleseth [10] on the crosscorrelation are to show that (a) if $n = 2^i$ then the crosscorrelation is at least four-valued (recently proven in the binary case [20]) and (b) the crosscorrelation function always takes on -1 as one of the values when $p = 1 \pmod{d-1}$.

3 Bent functions

Let $f(x) : \mathrm{GF}(p^n) \mapsto \mathrm{GF}(p)$ be a p-ary function. The Walsh transform coefficients of $f(x)$ are defined for any $y \in \mathrm{GF}(p^n)$ to be

$$S_f(y) = \sum_{x \in \mathrm{GF}(p^n)} \omega^{f(x) - \mathrm{Tr}_n(yx)}.$$

Then $\omega^{f(x)}$ can be recovered from

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

The function $f(x)$ is called a *bent function* if it holds for any $y \in \mathrm{GF}(p^n)$ that

$$|S_f(y)|^2 = p^n.$$

In the binary case, bent functions are functions that have maximal distance to all affine functions. Nonbinary bent functions were introduced in 1985 by Kumar et al. [23] and are sometimes referred to as generalized bent functions. A bent function $f(x)$ is called *regular* if

$$p^{-\frac{n}{2}} S_f(y) = \omega^{f^*(y)}$$

for some $f^*(y) : \mathrm{GF}(p^n) \mapsto \mathrm{GF}(p)$. A bent function $f(x)$ is said to be *weakly regular* if there exists a complex number u having unit magnitude such that

$$up^{-\frac{n}{2}} S_f(y) = \omega^{f^*(y)}$$

for all $y \in \mathrm{GF}(p^n)$. The function f^* is also a (weakly) regular bent function and is called the *dual* of f. 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 [2, 26, 27]). This justifies why the classes of (weakly) regular bent functions are of independent interest.

The following discussion will consider polynomial functions

$$f(x) = \mathrm{Tr}_n\left(\sum_{i=0}^{s} a_i x^{d_i}\right)$$

with $a_i, x \in \mathrm{GF}(p^n)$. An interesting problem is to find simple polynomials that give bent functions.

3.1 Ternary monomial bent functions

A well-known construction by Dillon is known to give a binary bent function over $\mathrm{GF}(2^{2k})$ in the cases when the Kloosterman sum $K(a)$ over $\mathrm{GF}(2^k)$ takes on the value 0 for some $a \in \mathrm{GF}(2^k)$. This was proved affirmatively by Lachaud and Wolfmann [24] as a consequence of the fact that the binary Kloosterman sum over $\mathrm{GF}(2^k)$ takes on all values being equal zero modulo 4 in the range $|K(a)| \leq 2 \cdot \sqrt{2^k}$ and, therefore, zero is one of the values that always occurs in the Kloosterman sum. This construction was generalized by Helleseth and Kholosha [12] to p-ary bent functions in the following result.

Theorem 4 *Let $n = 2k$ and t be an arbitrary positive integer with $\gcd(t, p^k + 1) = 1$ for an odd prime p. For any nonzero $a \in \mathrm{GF}(p^n)$, define the following p-ary function mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$*

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

Then for any $b \in \mathrm{GF}(p^n)^*$, the corresponding Walsh transform coefficient of $f(x)$ is equal to

$$S_a(b) = K\left(a^{p^k+1}\right) + p^k \omega^{-\mathrm{Tr}_n(a^{p^k} b^{t(p^k-1)})} \quad \text{and}$$

$$S_a(0) = p^k - \left(p^k - 1\right) K\left(a^{p^k+1}\right).$$

Assuming $p^k > 3$, then $f(x)$ is bent if and only if the following Kloosterman sum over $\mathrm{GF}(p^k)$ satisfies $K(a^{p^k+1}) = 0$. Moreover, if $K(a^{p^k+1}) = 0$ then $f(x)$ is a regular bent function.

Take $p = 2$, without loss of generality assume $a \in \mathrm{GF}(2^k)$ and drop the requirement for $2^k > 3$. Then exactly the same result as in Theorem 4 holds in the binary case giving the above mentioned Dillon class of Boolean bent functions. The proof of the nonbinary version is more complicated than in the binary case even though the final results are quite similar.

For $p = 3$, we learned from Wolfmann [28] (private communication) that Katz has shown that 0 always occurs as a value in the ternary Kloosterman sum and thus the construction above leads to bent functions. For more details on the ternary Klosterman sum see Katz and Livné [21]. Recently, it was shown by Kononen et al. [22] that for any $p > 3$ the Kloosterman sum does not take on the value 0. Thus, the only cases where this construction leads to bent functions are the binary and ternary cases.

The following ternary bent function was first conjectured and proved in part by Helleseth and Kholosha [12]. The complete proof that this is a weakly regular bent functions with a particular form of the Walsh transform was given in [9, 17].

Theorem 5 *Let $n = 2k$ with k odd. Then the ternary function $f(x)$ mapping $\mathrm{GF}(3^n)$ to $\mathrm{GF}(3)$ and given by*

$$f(x) = \mathrm{Tr}_n\left(ax^{\frac{3^n-1}{4}+3^k+1}\right)$$

is a weakly regular bent function if $a = \xi^{\frac{3^k+1}{4}}$ *and* ξ *is a primitive element of* $\mathrm{GF}(3^n)$. *Moreover, for any* $b \in \mathrm{GF}(3^n)$ *the corresponding Walsh transform coefficient of* $f(x)$ *is equal to*

$$S_f(b) = -3^k \omega_3^{\pm \mathrm{Tr}_k\left(\frac{b^{3^k+1}}{a(\delta+1)}\right)},$$

where $\delta = \xi^{\frac{3^n-1}{4}}$.

An interesting not weakly regular bent function is the following function, for which we do not know whether it belongs to an infinite family. It would be important to construct infinite families of not weakly regular bent functions from monomials or other simple polynomials.

Fact 6 *The ternary function* $f(x)$ *mapping* $\mathrm{GF}(3^6)$ *to* $\mathrm{GF}(3)$ *and given by*

$$f(x) = \mathrm{Tr}_6\left(\xi^7 x^{98}\right) \ ,$$

where ξ *is a primitive element of* $\mathrm{GF}(3^6)$, *is bent and not weakly regular bent.*

3.2 Binomial bent functions

For $p = 2$, the Niho decimation $d = 2^{3k} - 2^{2k} + 2^k + 1$ leads to 4-valued cross-correlation function between two binary m-sequences of period $p^{4k} - 1$ [11, 25]. This is equivalent to case (ii) in Theorem 3. For $p > 2$ the decimation $d = p^{3k} - p^{2k} + p^k + 1$ is interesting for another reason since it leads to an infinite family of bent functions [14].

Theorem 7 *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 solution in* $\mathrm{GF}(p^k)$ *of the equation*

$$y^{p^{2k}+1} + \left(y^2 + X\right)^{(p^{2k}+1)/2} + y^{p^k(p^{2k}+1)} + \left(y^2 + X\right)^{p^k(p^{2k}+1)/2} = 0.$$

In particular, if $y^2 \in \mathrm{GF}(p^{2k})$ *then* $x_0 = -\mathrm{Tr}_k^{2k}\left(y^2\right)$. *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 dual bent function is defined in the lemma and shows that even if a bent function has an easy description, in this case a simple binomial polynomial, the dual function, that involves defining x_0 from y, can be quite complicated.

Similarly to Fact 6, there is a special binomial polynomial that also leads to a not weakly regular bent function and where the same question remains open, namely to find an infinite family of such bent functions.

Fact 8 *The ternary function* $f(x)$ *mapping* $\mathrm{GF}(3^4)$ *to* $\mathrm{GF}(3)$ *and given by*

$$f(x) = \mathrm{Tr}_4\left(ax^{22} + x^4\right) \quad \textit{with} \quad a \in \left\{\pm\xi^{10}, \xi^{30}\right\},$$

where ξ *is a primitive element of* $\mathrm{GF}(3^4)$*, is bent and not weakly regular bent.*

All known univariate polynomials representing a p-ary bent function are listed in the tables below. For further details on quadratic bent functions the reader is referred to [12, 13]. Here ξ denotes a primitive element of $\mathrm{GF}(3^n)$, r and wr refer to regular and weakly regular bent functions respectively. The first eight families in the table are monomials of the form $\mathrm{Tr}_n(ax^d)$ while the last two are binomial bent functions in the form $\mathrm{Tr}_n(F(x))$.

n	d or $F(x)$	a	deg	Remarks
	2	$a \neq 0$	2	r, wr
$2k$	$p^k + 1$	$a + a^{p^k} \neq 0$	2	wr
	$p^j + 1$, $\frac{n}{\gcd(n,j)}$-odd	$a \neq 0$	2	r, wr
	$p^j + 1$	Some condition on a	2	r, wr
	$\frac{3^k+1}{2}$, $\gcd(k, n) = 1$, k-odd	$a \neq 0$	$k + 1$	r, wr
$2k$	$t(3^k - 1)$, $\gcd(t, 3^k + 1) = 1$	$K(a^{p^k+1}) = 0$		ternary r
$2k$	$\frac{3^n-1}{4} + 3^k + 1$	$\xi^{\frac{3^k+1}{4}}$	n	ternary wr
6	98	ξ^7	6	ternary not wr
4	$ax^{22} + x^4$	$\pm\xi^{10}, \pm\xi^{30}$	4	ternary not wr
$4k$	$x^{p^{3k}+p^{2k}-p^k+1} + x^2$		$(p-1)k + 2$	wr

The following table gives further examples of ternary binomial bent functions of the form $\mathrm{Tr}_n(a_1x^{d_1} + a_2x^{d_2})$ obtained from a computer search. Cases excluded are quadratic binomial bent functions where exponents are of the form $p^i + p^j$ and bent functions of Dillon type where the two exponents are of the form $t(p^{n/2} - 1)$.

n	d_1	d_2	Remarks
3	8	14	not wr
6	14	70	not wr
6	14	98	wr
6	20	92	not wr
6	28	140	wr
8	20	100	wr
8	40	280	wr
8	88	136	wr

4 An exponential sum related to Jacobsthal sums

Since $f(x) = x^d + x^2$ is a bent function for $d = p^{3k} + p^{2k} - p^k + 1$, a natural question is to consider the distribution of the more general exponential sum $f(x) = \mathrm{Tr}_n(ax^d + bx^2)$ for any $a, b \in \mathrm{GF}(p^n)$. Thus, we consider

$$S_f(0) = \sum_{x \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n(ax^d + bx^2)}.$$

This is equivalent to finding the complete weight distribution of the cyclic code with zeros ξ^2 and ξ^d, where ξ is a primitive element of GF(p^n).

It turns out that this exponential sum leads to nice and surprising connections to Jacobsthal sums. Let $\eta(x)$ be the quadratic character of GF(q). The Jacobsthal sum $H_n(a)$ of order n is

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

The next result from [15] gives relations between the exponential sum and the number of solutions of a special equation. The proof of this theorem uses some ideas by Niho [25]. If n is even, let U denote a cyclic subgroup of order $p^{n/2}+1$ of the multiplicative group of GF(p^n) (generated by $\xi^{p^{n/2}-1}$, where ξ is a primitive element of GF(p^n)).

Theorem 9 *Let $n = 4k$. For any $a, b \in \mathrm{GF}(p^n)$, define the following p-ary function mapping* GF(p^n) *to* 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

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

Case 1 For most values of $a, b \in \mathrm{GF}(p^n)$ when either $a^{p^k(p^k+1)} \neq b^{p^k+1}$ or $a^2 = b^d$ with $b \neq 0$, the exponential sum takes on just three values $-p^{2k}$, p^{2k} or $3p^{2k}$. Equivalently, the polynomial $L(X)$ defined in (1) has none, two or four zeros in U, i.e., $N(a,b) \in \{0, 1, 2\}$.

Case 2 In the remaining cases, when $a^{p^k(p^k+1)} = b^{p^k+1}$ with $a^2 \neq b^d$ there are many more possible values for the exponential sum and $N(a,b)$. Then a detailed study in [15] shows that

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

where g is any element in GF(p^{2k})* with $g^{p^k-1} = -b^{p^{3k}}/a$, and that $2N(a,b)$ can be alternatively expressed as

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

and

$$S_f(0) = p^{2k}\left(p^k - \frac{H_{p^k+1}\left(-b^{p^k+1}/g^2\right)}{p^k+1}\right).$$

In [15, Theorem 2] a new nontrivial upper bound on the Jacobsthal sum of order $p^k + 1$ was proved and this gives the following estimate:

$$\left| N(a, b) - \frac{p^k + 1}{2} \right| \leq p^{k/2}.$$

5 Conclusions

This survey has given some connections between the crosscorrelation of m-sequences, exponential sums and a brief overview of decimations that provide three- and four- valued crosscorrelation for binary sequences. Furthermore, relations to p-ary bent functions and Jacobsthal sums have been discussed. In particular, it was shown that the decimation by Niho $d = 2^{3k} + 2^{2k} - 2^k + 1$ that led to four-valued crosscorrelation was closely related to an infinite family of p-ary bent functions defined by $\mathrm{Tr}_{4k}(x^2 + x^d)$ where $d = p^{3k} + p^{2k} - p^k + 1$ (i.e., d is obtained by replacing $p = 2$ by general p in the Niho decimation d). Finally, the values of the exponential sum $\mathrm{Tr}_{4k}(ax^2 + b\,x^d)$ were shown to be closely related to Jacobsthal sums of order $p^k + 1$.

References

1. Canteaut, A., Charpin, P., Dobbertin, H.: Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture. IEEE Trans. Inf. Theory **46**(1), 4–8 (2000)
2. Chee, Y.M., Tan, Y., Zhang, X.D.: Strongly regular graphs constructed from p-ary bent functions. J. Algebr. Comb. (2011, in press)
3. Cusick, T.W., Dobbertin, H.: Some new three-valued crosscorrelation functions for binary m-sequences. IEEE Trans. Inf. Theory **42**(4), 1238–1240 (1996)
4. Dobbertin, H.: One-to-one highly nonlinear power functions on GF(2^n). Appl. Algebra Eng. Commun. Comput. **9**(2), 139–152 (1998)
5. Dobbertin, H.: Almost perfect nonlinear power functions on GF(2^n): the Niho case. Inf. Comput. **151**(1–2), 57–72 (1999)
6. Dobbertin, H., Felke, P., Helleseth, T., Rosendahl, P.: Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums. IEEE Trans. Inf. Theory **52**(2), 613–627 (2006)
7. Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Trans. Inf. Theory **14**(1), 154–156 (1968)
8. Golomb, S.W.: Theory of transformation groups of polynomials over GF(2) with applications to linear shift register sequences. Inf. Sci. **1**(1), 87–109 (1968)
9. Gong, G., Helleseth, T., Hu, H., Kholosha, A.: On the dual of certain ternary weakly regular bent functions. IEEE Trans. Inf. Theory (2011, submitted)
10. Helleseth, T.: Some results about the cross-correlation function between two maximal linear sequences. Discrete Math. **16**(3), 209–232 (1976)
11. Helleseth, T.: A note on the cross-correlation function between two binary maximal length linear sequences. Discrete Math. **23**(3), 301–307 (1978)
12. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018–2032 (2006)
13. Helleseth, T., Kholosha, A.: On the dual of monomial quadratic p-ary bent functions. In: Golomb, S., Gong, G., Helleseth, T., Song, H.Y. (eds.) Sequences, Subsequences, and Consequences, Lecture Notes in Computer Science, vol. 4893, pp. 50–61. Springer, Berlin (2007)

14. Helleseth, T., Kholosha, A.: New binomial bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **56**(9), 4646–4652 (2010)
15. Helleseth, T., Kholosha, A.: Sequences, bent functions and Jacobsthal sums. In: Carlet, C., Pott, A. (eds.) Sequences and Their Applications—SETA 2010, Lecture Notes in Computer Science, vol. 6338, pp. 416–429. Springer, Berlin (2010)
16. Helleseth, T., Rosendahl, P.: New pairs of *m*-sequences with 4-level cross-correlation. Finite Fields Appl. **11**(4), 674–683 (2005)
17. Helleseth, T., Hollmann, H.D.L., Kholosha, A., Wang, Z., Xiang, Q.: Proofs of two conjectures on ternary weakly regular bent functions. IEEE Trans. Inf. Theory **55**(11), 5272–5283 (2009)
18. Hollmann, H.D.L., Xiang, Q.: A proof of the Welch and Niho conjectures on cross-correlations of binary *m*-sequences. Finite Fields Appl. **7**(2), 253–286 (2001)
19. Kasami, T.: The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. Inf. Control **18**(4), 369–394 (1971)
20. Katz, D.J.: Proof of a conjecture of Helleseth: maximal linear recursive sequences of period $2^{2^n} - 1$ never have three-valued cross-correlation. arXiv:1105.2291 (2011)
21. Katz, N.M., Livné, R.: Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. C. R. Acad. Sci. Paris, Sér. I Math. **309**(11), 723–726 (1989)
22. Kononen, K.P., Rinta-aho, M.J., Väänänen, K.O.: On integer values of Kloosterman sums. IEEE Trans. Inf. Theory **56**(8), 4011–4013 (2010)
23. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Comb. Theory, Ser. A **40**(1), 90–107 (1985)
24. Lachaud, G., Wolfmann, J.: The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Trans. Inf. Theory **36**(3), 686–692 (1990)
25. Niho, Y.: Multi-Valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences. Ph.D. thesis, University of Southern California, Los Angeles (1972)
26. Pott, A., Tan, Y., Feng, T., Ling, S.: Association schemes arising from bent functions. Des. Codes Cryptogr. **59**(1–3), 319–331 (2011)
27. Tan, Y., Pott, A., Feng, T.: Strongly regular graphs associated with ternary bent functions. J. Comb. Theory, Ser. A **117**(6), 668–682 (2010)
28. Wolfmann, J.: The weights of the dual code of the MELAS code over GF(3). Discrete Math. **74**(3), 327–329 (1989)