REPORTS IN INFORMATICS

ISSN 0333-3590

Monomial and Quadratic Bent Functions over the Finite Fields of Odd Characteristic

Tor Helleseth and Alexander Kholosha

REPORT NO 310 **September 2005**

Department of Informatics

UNIVERSITY OF BERGEN

Bergen, Norway

This report has URL http://www.ii.uib.no/publikasjoner/texrap/ps/2005-310.ps

Reports in Informatics from Department of Informatics, University of Bergen, Norway, is available at http://www.ii.uib.no/publikasjoner/texrap/.

Requests for paper copies of this report can be sent to:

Department of Informatics, University of Bergen, Høyteknologisenteret,
P.O. Box 7800, N-5020 Bergen, Norway

Monomial and Quadratic Bent Functions over the Finite Fields of Odd Characteristic[†]

Tor Helleseth and Alexander Kholosha[*]

Department of Informatics
University of Bergen
N-5020 Bergen
Norway

September 21, 2005

Abstract

We consider p-ary bent functions of the form $f(x) = \mathrm{Tr}_n\left(\sum_{i=0}^{s} a_i x^{d_i}\right)$. A new class of ternary monomial regular bent function with the Dillon exponent is discovered. The existence of Dillon bent functions in the general case is an open problem of deciding whether a certain Kloosterman sum can take on the value -1. Also described is the general Gold-like form of a bent function that covers all the previously known monomial quadratic cases. We also discuss the (weak) regularity of our new as well as of known monomial bent functions and give the first example of a not weakly regular bent function. Finally we prove some criteria for an arbitrary quadratic functions to be bent.

1 Introduction

Boolean bent functions were first introduced by Rothaus in 1976 as an interesting combinatorial object with the important property of having the maximum Hamming distance to the set of all affine functions. Later the research in this area was stimulated by the significant relation to the following topics in computer science: coding theory, sequences and cryptography (design of stream ciphers and S-boxes for block ciphers). Kumar, Scholtz and Welch in [1] generalized the notion of Boolean bent functions to the case of functions over an arbitrary finite field. Complete classification of bent functions looks hopeless even in the binary case. In the case of generalized bent functions things are naturally much more complicated. However, many explicit methods are proved for constructing bent functions either from scratch or based on other, more simple bent functions.

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

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

[†]This work was supported by the Norwegian Research Council. The material in this paper was presented in part at the IEEE ITSOC Information Theory Workshop on Coding and Complexity, Rotorua, New Zealand, August/September 2005.

[*]Email: {torh,Alexander.Kholosha}@ii.uib.no, WWW: http://www.ii.uib.no/~torh/

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. In the sequel $S_a(b)$ is also used to denote the Walsh transform coefficient of a function that depends on parameter a when it is clear from the context which function we mean. Let $N_b(j)$ denote the number of solutions of the equation $f(x) - \mathrm{Tr}_n(bx) = j$ for $j \in \mathrm{GF}(p)$ and $b \in \mathrm{GF}(p^n)$. Then

$$S_f(b) = N_b(0) + N_b(1)\omega + \cdots + N_b(p-1)\omega^{p-1} \ . \tag{1}$$

According to [1], $f(x)$ is called a *p-ary bent function* (or *generalized bent function*) if all its Walsh coefficients satisfy $|S_f(b)|^2 = p^n$. A bent function $f(x)$ is called *regular* (see [1, Definition 3] and [2, p. 576]) if for every $b \in \mathrm{GF}(p^n)$ the normalized Walsh coefficient $p^{-n/2}S_f(b)$ is equal to a complex p^{th} root of unity, i.e., $p^{-n/2}S_f(b) = \omega^{f^*(b)}$ 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 $up^{-n/2}S_f(b) = \omega^{f^*(b)}$ for all $b \in \mathrm{GF}(p^n)$. We call $u^{-1}p^{n/2}$ the *magnitude* of $S_f(b)$. Throughout this paper $p^{n/2}$ with odd n stands for the *positive* square root of p^n. A function $F(x)$ mapping $\mathrm{GF}(p^n)$ to itself will also be called generalized bent if $\mathrm{Tr}_n(F(x))$ is bent according to the above definition. In the present paper we take an odd prime p and examine prospective p-ary bent functions having the form $f(x) = \mathrm{Tr}_n\left(\sum_{i=0}^{s} a_i x^{d_i}\right)$ with $a_i, x \in \mathrm{GF}(p^n)$ and arbitrary integer exponents d_i. Functions of this type with only one coefficient a_i being nonzero are called *monomial* and are called *multinomial* otherwise.

Weakly regular bent functions always appear in pairs. Indeed, if $f(x)$ is a (weakly) regular bent function and $S_f(b) = u^{-1}p^{n/2}\omega^{f^*(b)}$ for $b \in \mathrm{GF}(p^n)$ then the function $f^*(b)$ is called the *dual* of f. The inverse Walsh transform of such $f(x)$ gives

$$up^{n/2}\omega^{f(x)} = \sum_{b \in \mathrm{GF}(p^n)} \omega^{f^*(b)+\mathrm{Tr}_n(bx)} = S_{f^*}(-x) \ .$$

Thus, the dual of a (weakly) regular bent function is again a (weakly) regular bent function and $f^{**}(x) = f(-x)$, $f^{***}(x) = f^*(-x)$, $f^{****}(x) = f(x)$.

Considering [1, Property 8] it can be readily seen that the Walsh transform coefficients of a p-ary bent function f with odd p satisfy the following

$$p^{-n/2}S_f(b) = \begin{cases} \pm\,\omega^{f^*(b)}, & \text{if } n \text{ is even or } n \text{ is odd and } p \equiv 1 \pmod 4 \ , \\ \pm\,i\,\omega^{f^*(b)}, & \text{if } n \text{ is odd and } p \equiv 3 \pmod 4 \ , \end{cases} \tag{2}$$

where i is a complex primitive 4^{th} root of unity. Thus, regular bent functions can only be found for even n and for odd n with $p \equiv 1 \pmod 4$. Here we note a minor inaccuracy found in [3, Theorem 9] that contains a statement equivalent to (2). In the correct version e there should be replaced with n and $\pm\,\omega^k$ should also stand for the case of even n.

Take a generalized bent function $f(x)$. Consider first the case when n is even. From (1) and (2) we get that for any $b \in \mathrm{GF}(p^n)$

$$\sum_{j=0}^{p-1} N_b(j)\omega^j \mp p^{n/2}\omega^{f^*(b)} = 0 \ ,$$

where all the coefficients are integer numbers. It is well known that the polynomial $p(x) = x^{p-1} + \cdots + x^2 + x + 1$ is irreducible over the rational number field, $p(\omega) = 0$ and, thus, $p(x)$ is the minimal polynomial of ω over the rational numbers. Therefore,

for a bent function of an even number of variables and a fixed b, the values of $N_b(j)$ are all equal except for $N_b(f^*(b))$ that differs from the rest by $\pm p^{n/2}$. Thus, $N_b(j)$ takes on two different values.

Now consider the case of odd $n = 2k + 1$. First recall the well known formula (see, for instance, [4, Theorem 5.15]) that

$$S = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \omega^j = \begin{cases} p^{1/2}, & \text{if } p \equiv 1 \pmod 4 , \\ ip^{1/2}, & \text{if } p \equiv 3 \pmod 4 , \end{cases} \tag{3}$$

where $\left(\frac{j}{p}\right)$ denotes the Legendre symbol that is equal to 0 if p divides j (in particular, $\left(\frac{0}{p}\right) = 0$), equal to 1 if j is a square modulo p and to -1 otherwise. Combining (1), (2) and (3) we get that for any $b \in \mathrm{GF}(p^n)$

$$\sum_{j=0}^{p-1} \left(N_b(j) \mp \left(\frac{j - f^*(b)}{p}\right) p^k \right) \omega^j = 0 \ .$$

Therefore, for a bent function of an odd number of variables and a fixed b, the difference between $N_b(j)$ and $N_b(f^*(b))$ is equal to p^k for a half of those $j \neq f^*(b)$ and is equal to $-p^k$ for the rest. In particular, $N_b(f^*(b)) \geq p^k$. Thus, $N_b(j)$ takes on three different values.

Following the definition of a bent function, the standard method for proving that a function is bent would be to evaluate the absolute square of its Walsh coefficients. However, this technique does not help in telling if the function is (weakly) regular. Citing the recent work [2] by Hou, "it appears that all known p-ary bent functions are weakly regular". In the current paper we not only describe new classes of bent functions but also prove a stronger property that they are (weakly) regular. We also give the first proof of (weak) regularity for some known quadratic monomial cases. An interesting open problem remains to prove that Coulter-Matthews monomial bent functions are (weakly) regular since this claim is currently supported only by the direct computations. Moreover, we have also found an example of a ternary bent function that is not weakly regular, which is the first example of this kind (see Fact 1).

There are only a few proven cases of monomial bent functions. These are Sidelnikov, Kumar-Moreno [3], Kasami [5], Kim et alia [6] and Coulter-Matthews [7] bent functions. Note that all these functions, except Coulter-Matthews case, are quadratic. In Section 2 we describe a new class of ternary (i.e., $p = 3$) monomial regular non-quadratic bent functions that can be seen as a p-ary version of Boolean bent functions first described by Dillon in [8]. Whether such functions exist in the general non-ternary case poses an interesting open problem of deciding whether a certain Kloosterman sum can take on the value -1. The existence of another new class of ternary non-quadratic bent functions is conjectured in Section 3 where some strong arguments in favor of this conjecture are also given. Note that Coulter-Matthews functions exist only if $p = 3$ as well. In Section 4 we prove the general Gold-like form of a monomial quadratic bent function that covers Sidelnikov, Kumar-Moreno, Kasami, and Kim et alia cases. We also evaluate the exact value of the Walsh transform coefficients for Sidelnikov and Kasami bent functions. Our computations (see Section 6) point to the fact that there are no other examples of monomial bent functions that, up to cyclotomic equivalence, are not covered by the previously known classes plus the new families described in this paper and listed in Table 1. In Section 5 we prove some criteria for quadratic functions to be bent and show that all quadratic bent function are (weakly) regular. Particular class of

quadratic bent functions was earlier described in [6] with the proof that contained some inaccuracies and relied on a formidable theoretical background. The results we present here include this known class as a special case while the given proof is self-contained. In Section 6 we provide computational results, describe some tricks helping to improve the efficiency of the computer search for generalized bent functions and give an example of a not weakly regular ternary bent function.

2 Non-binary Dillon Bent Functions

We start by proving the result that is not immediately related to the subject of this paper. It will be used further to describe a new class of bent functions. Moreover, this result is of theoretical interest in itself since it gives an important characterization of the weight distribution of irreducible cyclic codes of a special type.

According to [4, Definition 5.42], for any nontrivial additive character χ of $\mathrm{GF}(p^k)$ and any $a, b \in \mathrm{GF}(p^k)$ the sum

$$K(\chi; a, b) = \sum_{c \in \mathrm{GF}(p^k)^*} \chi\left(ac + bc^{-1}\right)$$

is called a *Kloosterman sum*. Let $\mathrm{Tr}_k^n()$ also denote the trace function from $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p^k)$ for $n = 2k$. Finally, the *Gaussian sum* [4, p. 192] is defined by

$$G(\psi, \chi) = \sum_{c \in \mathrm{GF}(p^n)^*} \psi(c)\chi(c) \ ,$$

where χ is an additive and ψ a multiplicative character of $\mathrm{GF}(p^n)$.

Theorem 1 *Let $n = 2k$, $a \in \mathrm{GF}(p^n)$ is nonzero and prime p is odd. Then for any nontrivial additive character χ of $\mathrm{GF}(p^k)$*

$$\sum_{j=0}^{p^k} \chi\left(\mathrm{Tr}_k^n\left(a\xi^{j(p^k-1)}\right)\right) = -K\left(\chi; 1, a^{p^k+1}\right) \ ,$$

where ξ is a primitive element of $\mathrm{GF}(p^n)$.

Proof: Let χ be a *nontrivial* additive and ψ a multiplicative character of $\mathrm{GF}(p^k)$ and define the following additive and multiplicative characters of $\mathrm{GF}(p^n)$ respectively as $\chi'(a) = \chi(a + a^{p^k})$ and $\psi'(a) = \psi(a^{p^k+1})$, where $a \in \mathrm{GF}(p^n)$. Then by the Davenport-Hasse theorem [4, Theorem 5.14]

$$G(\psi', \chi') = -G(\psi, \chi)^2 \ , \tag{4}$$

where $G(\psi, \chi)$ denotes the Gaussian sum. Select and fix a primitive element ξ of $\mathrm{GF}(p^n)$. Then ξ^{p^k+1} belongs to $\mathrm{GF}(p^k)$ and is a primitive element of this field. The square on the right hand side of (4) can be extended as follows

$$\begin{aligned}
G(\psi, \chi)^2 &= \left(\sum_{b \in \mathrm{GF}(p^k)^*} \psi(b)\chi(b)\right)^2 = \sum_{b,d \in \mathrm{GF}(p^k)^*} \psi(bd)\chi(b+d) \\
&= \sum_{b,c \in \mathrm{GF}(p^k)^*} \psi(c)\chi\left(b + \frac{c}{b}\right) = \sum_{c \in \mathrm{GF}(p^k)^*} \psi(c)K(\chi; 1, c) \\
&= \sum_{i=0}^{p^k-2} \psi\left(\xi^{i(p^k+1)}\right)K\left(\chi; 1, \xi^{i(p^k+1)}\right) = \sum_{i=0}^{p^k-2} \gamma^i K\left(\chi; 1, \xi^{i(p^k+1)}\right) \ ,
\end{aligned}$$

where the substitution $c = bd$ is made, $K(\chi; 1, c)$ denotes the Kloosterman sum and γ is some complex, $(p^k - 1)$ root of unity that is defined by the concrete selection of the multiplicative character ψ.

Any nonzero $a \in \mathrm{GF}(p^n)$ can be represented uniquely as $\xi^i = \xi^{j_1(p^k-1)+j_2}$ for some $i \in \{0, \ldots, p^n - 2\}$ or equivalently for some $j_1 \in \{0, \ldots, p^k\}$ and $j_2 \in \{0, \ldots, p^k - 2\}$. Therefore, the Gaussian sum on the left hand side of (4) can be extended as follows

$$\begin{aligned} G(\psi', \chi') &= \sum_{a \in \mathrm{GF}(p^n)^*} \psi'(a)\chi'(a) = \sum_{i=0}^{p^n-2} \psi'(\xi^i)\chi'(\xi^i) \\ &= \sum_{i=0}^{p^n-2} \psi\big(\xi^{i(p^k+1)}\big)\chi\big(\xi^i + \xi^{ip^k}\big) = \sum_{i=0}^{p^n-2} \gamma^i \chi\big(\mathrm{Tr}_k^n(\xi^i)\big) \\ &= \sum_{j_2=0}^{p^k-2} \gamma^{j_2} \sum_{j_1=0}^{p^k} \chi\left(\mathrm{Tr}_k^n\big(\xi^{j_1(p^k-1)+j_2}\big)\right) \ . \end{aligned}$$

Since χ is a nontrivial additive character, (4) holds for any multiplicative character ψ of $\mathrm{GF}(p^k)$ and we conclude that for any γ being a complex $(p^k - 1)$ root of unity

$$\sum_{i=0}^{p^k-2} \gamma^i \left(\sum_{j=0}^{p^k} \chi\left(\mathrm{Tr}_k^n\big(\xi^{j(p^k-1)+i}\big)\right) + K\big(\chi; 1, \xi^{i(p^k+1)}\big)\right) = 0 \ .$$

The matrix of this system of linear equations (obtained by taking all $p^k - 1$ roots of unity γ) is the Vandermonde matrix $V(1, \Gamma, \Gamma^2, \ldots, \Gamma^{p^k-2})$ with $\Gamma = e^{\frac{2\pi i}{p^k-1}}$, which is nonsingular (see [9, p. 35]). Thus, the system has only the zero solution and for any $i \in \{0, \ldots, p^k - 2\}$

$$\sum_{j=0}^{p^k} \chi\left(\mathrm{Tr}_k^n\big(\xi^{j(p^k-1)+i}\big)\right) = -K\big(\chi; 1, \xi^{i(p^k+1)}\big) \ . \tag{5}$$

Finally note that for any nonzero $a \in \mathrm{GF}(p^n)$ if $a = \xi^l$ where $l \in \{0, \ldots, p^n - 2\}$ and $l \pmod{(p^k - 1)} = i$ (assume that $l = i + d(p^k - 1)$ for some nonnegative integer d) then

$$\sum_{j=0}^{p^k} \chi\left(\mathrm{Tr}_k^n\big(a\xi^{j(p^k-1)}\big)\right) = \sum_{j=0}^{p^k} \chi\left(\mathrm{Tr}_k^n\big(\xi^{(j+d)(p^k-1)+i}\big)\right) = \sum_{j=0}^{p^k} \chi\left(\mathrm{Tr}_k^n\big(\xi^{j(p^k-1)+i}\big)\right)$$

and

$$K\big(\chi; 1, a^{p^k+1}\big) = K\big(\chi; 1, \xi^{i(p^k+1)}\big) \ ,$$

since $a^{p^k+1} = \big(\xi^{i+d(p^k-1)}\big)^{p^k+1} = \xi^{i(p^k+1)}$. The last identities together with (5) lead to the claimed result. □

Now, using the result of Theorem 1, we can prove the criterion for a new family of p-ary bent functions in terms of the Kloosterman sums. This family can be considered as a p-ary version of the known class of Boolean bent functions that was first described by Dillon in [8]. The *canonical additive character* of $\mathrm{GF}(p^k)$ [4, p. 190] is defined by $\chi_1(a) = e^{2\pi i \mathrm{Tr}_k(a)/p}$ for $a \in \mathrm{GF}(p^k)$.

Theorem 2 *Let $n = 2k$ and t be an arbitrary positive integer with $\gcd(t, p^k+1) = 1$ and $p^k > 3$ for an odd prime p. Then for any nonzero $a \in \mathrm{GF}(p^n)$ the p-ary function $f(x)$ mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$ and given by*

$$f(x) = \mathrm{Tr}_n\big(ax^{t(p^k-1)}\big) \tag{6}$$

is bent if and only if the following Kloosterman sum over $\mathrm{GF}(p^k)$ satisfies

$$K\big(\chi_1; 1, a^{p^k+1}\big) = -1 \ , \tag{7}$$

where χ_1 is the canonical additive character of $\mathrm{GF}(p^k)$. Moreover, if (7) holds then $f(x)$ is a regular bent function and for $b \in \mathrm{GF}(p^n)^*$ the corresponding Walsh transform coefficient of $f(x)$ is equal to

$$S_a(b) = p^k \omega^{-\mathrm{Tr}_n\left(ab^{-t(p^k-1)}\right)}$$

and $S_a(0) = p^k$.

Proof: Select and fix a primitive element ξ of $\mathrm{GF}(p^n)$. Any nonzero element $x \in \mathrm{GF}(p^n)$ can be represented uniquely as $\xi^i = \xi^{(p^k+1)j_1+j_2}$ for some $i \in \{0, \ldots, p^n-2\}$ or equivalently for some $j_1 \in \{0, \ldots, p^k-2\}$ and $j_2 \in \{0, \ldots, p^k\}$. Then for any nonzero $x \in \mathrm{GF}(p^n)$

$$\mathrm{Tr}_n\big(ax^{t(p^k-1)} + x\big) = \mathrm{Tr}_n\big(a\xi^{t(p^k-1)j_2} + \xi^{(p^k+1)j_1+j_2}\big) = \mathrm{Tr}_n\left(a\beta^{j_2} + \gamma^{j_1}\xi^{j_2}\right)$$

and $\mathrm{Tr}_n\big(ax^{t(p^k-1)}\big) = \mathrm{Tr}_n\left(a\beta^{j_2}\right)$, where $\beta = \xi^{t(p^k-1)}$ and $\gamma = \xi^{p^k+1} \in \mathrm{GF}(p^k)$.

The Walsh transform coefficient of the function $f(x)$ evaluated at -1 is equal to

$$S_a(-1) = \sum_{x \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^{t(p^k-1)}+x\right)} = 1 + \sum_{j_2=0}^{p^k} \omega^{\mathrm{Tr}_n\left(a\beta^{j_2}\right)} \sum_{j_1=0}^{p^k-2} \omega^{\mathrm{Tr}_n\left(\gamma^{j_1}\xi^{j_2}\right)} \ .$$

Consider the latter sum

$$\sum_{j_1=0}^{p^k-2} \omega^{\mathrm{Tr}_n\left(\gamma^{j_1}\xi^{j_2}\right)} = \sum_{j_1=0}^{p^k-2} \omega^{\mathrm{Tr}_k\left(\gamma^{j_1}\left(\xi^{j_2}+\xi^{p^k j_2}\right)\right)} = \begin{cases} p^k-1, & \text{if} \quad \xi^{j_2}+\xi^{p^k j_2} = 0\,, \\ -1, & \text{otherwise}\,, \end{cases}$$

since the multiplicative order of γ is equal to p^k-1 and thus γ is a primitive element of $\mathrm{GF}(p^k)$ and γ^{j_1} runs through all nonzero elements of $\mathrm{GF}(p^k)$. Further, $\xi^{j_2} + \xi^{p^k j_2} = 0$ if and only if $\xi^{j_2(p^k-1)} = -1 = \xi^{\frac{p^n-1}{2}}$ which means that $j_2 = \frac{p^k+1}{2}$.

Therefore, $S_a(-1)$ is equal to

$$1 - \sum_{j_2=0}^{p^k} \omega^{\mathrm{Tr}_n\left(a\beta^{j_2}\right)} + p^k \omega^{\mathrm{Tr}_n\left(a\beta^{\frac{p^k+1}{2}}\right)} = 1 - \sum_{j_2=0}^{p^k} \omega^{\mathrm{Tr}_n\left(a\beta^{j_2}\right)} + p^k \omega^{-\mathrm{Tr}_n(a)} \ , \tag{8}$$

since $\beta^{\frac{p^k+1}{2}} = \xi^{\frac{t(p^n-1)}{2}} = -1$ as t is odd. Now if $\sum_{j=0}^{p^k} \omega^{\mathrm{Tr}_n\left(a\beta^j\right)} = 1$ then $S_a(-1) = p^k\omega^{-\mathrm{Tr}_n(a)}$ and $S_a(-1)$ meets the requirements on Walsh coefficients of a bent function. Note that the sets $\{\beta^j \mid j = 0, \ldots, p^k\}$ and $\{\xi^{j(p^k-1)} \mid j = 0, \ldots, p^k\}$ are equal because t and p^k+1 are coprime. Having this in mind, the above condition on a can be written as

$$\sum_{j=0}^{p^k} \chi_1\left(\mathrm{Tr}_k^n\big(a\xi^{j(p^k-1)}\big)\right) = \sum_{j=0}^{p^k} \omega^{\mathrm{Tr}_n\left(a\xi^{j(p^k-1)}\right)} = 1 \ .$$

By Theorem 1, this is equivalent to condition (7).

For any $b \in \mathrm{GF}(p^n)^*$ we have $S_a(-b) = S_{ab^{-t(p^k-1)}}(-1)$ and $\left(ab^{-t(p^k-1)}\right)^{p^k+1} = a^{p^k+1}$. Thus, if (7) holds for a and $S_a(-1) = p^k\omega^{-\mathrm{Tr}_n(a)}$ then (7) also holds for $ab^{-t(p^k-1)}$ and $S_a(-b) = p^k\omega^{-\mathrm{Tr}_n\left(ab^{-t(p^k-1)}\right)} = S_a(b)$. Finally, if (7) holds then the Walsh transform coefficient of the function $f(x)$ evaluated at 0 is equal to

$$S_a(0) = \sum_{x\in\mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^{t(p^k-1)}\right)} = 1 + \sum_{j_1=0}^{p^k-2}\sum_{j_2=0}^{p^k} \omega^{\mathrm{Tr}_n\left(a\beta^{j_2}\right)} = p^k \ .$$

Therefore, $f(x)$ is a regular bent function.

Now prove that condition (7) is necessary for function f to be bent. Take a bent function $f(x)$. Then by (2), $S_a(-1) = \pm\, p^k\omega^{f^*(-1)}$ and by (8),

$$1 - \sum_{j=0}^{p^k} \omega^{\mathrm{Tr}_n\left(a\beta^j\right)} + p^k\omega^{-\mathrm{Tr}_n(a)} \mp\, p^k\omega^{f^*(-1)} = \sum_{j=0}^{p-1} d_j\omega^j = 0 \ ,$$

where d_j $(j = 0, \ldots, p-1)$ are integer coefficients at the corresponding powers of ω. It is well known that $x^{p-1} + \cdots + x^2 + x + 1$ is the minimal polynomial of ω over the rational numbers and thus, all coefficients d_j should be equal. Obviously, $\sum_{j=0}^{p^k} \omega^{\mathrm{Tr}_n\left(a\beta^j\right)} = \sum_{j=0}^{p-1} c_j\omega^j$ for some integer $0 \le c_j \le p^k+1$ with $c_0+\cdots+c_{p-1} = p^k+1$. Denote $p - \mathrm{Tr}_n(a) = s_1$ and $f^*(-1) = s_2$. Suppose first that $s_1 \ne s_2$. If $S_a(-1) = p^k\omega^{f^*(-1)}$ then $d_{s_1} \ge p^k - c_{s_1} > -p^k - c_{s_2} + 1 \ge d_{s_2}$ that contradicts with $d_{s_1} = d_{s_2}$. If $S_a(-1) = -p^k\omega^{f^*(-1)}$ then for any $j \notin \{s_1, s_2\}$ we have $p^k - c_{s_i} \le d_{s_i} = d_j \le -c_j+1$, where $i = (1, 2)$. Thus, $c_{s_1}+c_{s_2} \ge 2p^k+2c_j-2 > p^k+1$ if $p^k > 3$ and we get the contradiction with $c_0 + \cdots + c_{p-1} = p^k + 1$. Therefore, we conclude that $s_1 = s_2 = s$. If in this case $S_a(-1) = -p^k\omega^{f^*(-1)}$ then for any $j \ne s$ we have $2p^k - c_s \le d_s = d_j \le -c_j + 1$ that gives $c_s - c_j \ge 2p^k - 1$ which is a contradiction. We are left with the only possibility when $s_1 = s_2$ and $S_a(-1) = p^k\omega^{f^*(-1)}$ that leads to $\sum_{j=0}^{p^k} \omega^{\mathrm{Tr}_n\left(a\beta^j\right)} = 1$ which was earlier proved to be equivalent to (7). □

Note that the extreme case when $p = 3$ and $k = 1$, i.e., $p^k = 3$ gives two cyclotomic equivalent Dillon exponents $d = 2$ and $d = 6$ that correspond to the quadratic bent function of the Sidelnikov type (see Corollary 3).

Let A_i denote the number of coordinates equal to $i \in \mathrm{GF}(p)$ in the codeword $c(a) = \left(\mathrm{Tr}_n\left(a\xi^{j(p^k-1)}\right) \mid j = 0, \ldots, p^k\right)$. Then $A_i = A_{-i}$ since $\xi^{\frac{p^{2k}-1}{2}} = -1$ and for $j = 0, \ldots, \frac{p^k-1}{2}$

$$\mathrm{Tr}_n\left(a\xi^{j(p^k-1)}\right) = -\mathrm{Tr}_n\left(a\xi^{\left(j+\frac{p^k+1}{2}\right)(p^k-1)}\right) \ .$$

Corollary 1 *In the ternary case (i.e., when $p = 3$) and given the conditions of Theorem 2, there exists at least one $a \in \mathrm{GF}(p^n)$ such that function (6) is bent. Moreover, (6) is bent if and only if the Hamming weight of the codeword $c(a) = \left(\mathrm{Tr}_n\left(a\xi^{j(3^k-1)}\right) \mid j = 0, \ldots, 3^k\right)$ is equal to $2 \cdot 3^{k-1}$, where ξ is a primitive element of $\mathrm{GF}(3^n)$. In this case (6) is a regular bent function.*

Proof: Note that the set of codewords $c(a)$ for all $a \in \mathrm{GF}(3^n)$ makes up a $(3^k+1, n)$ irreducible cyclic code over GF(3) (see [4, p. 484]). According to the result

of Katz [10, Theorem 2.1] (unfortunately, the proof is not published till now and the result was confirmed through personal communication), the set of Kloosterman sums $K\big(\chi_1; 1, c\big)$ for all nonzero $c \in \mathrm{GF}(3^k)$ is equal to the set of *all* integers in the range $(-2\sqrt{3^k}, 2\sqrt{3^k})$ and equal to -1 modulo 3. In particular, there exists at least one $a \in \mathrm{GF}(3^n)$ such that $K\big(\chi_1; 1, a^{3^k+1}\big) = -1$ (since the norm function maps $\mathrm{GF}(3^n)$ *onto* $\mathrm{GF}(3^k)$).

In the ternary case condition (7) takes on the form $A_0 - A_1 = 1$, taking into account Theorem 1, since $\omega + \omega^2 = -1$ and $A_1 = A_2$ as was noted above. We also have the second equation $A_0 + A_1 + A_2 = A_0 + 2A_1 = 3^k + 1$. The only solution satisfying these two equations is $A_0 = 3^{k-1} + 1$ and $A_1 + A_2 = 2 \cdot 3^{k-1}$. □

We were not able to find any examples when condition (7) holds in a non-binary and non-ternary case. Here we want to mention the known conjecture of Helleseth [11, Conjecture 5.1] that if $d \equiv 1 \pmod{p-1}$ then the periodic correlation of an m-sequence and its d-decimation contains the value -1. Note that the set of Kloosterman sums is equal to the periodic correlation of an m-sequence and its reverse (so $d = -1$). Only in the binary and ternary cases $d = -1 \equiv 1 \pmod{p-1}$ and it is known that the Kloosterman sum always takes on the value -1 for these values of p (see [12, Theorem 3.4] and [10, Theorem 2.1]). However, the conjecture in the opposite direction is not true (concrete examples can be found, e.g., $p = 5$, $d = 3$, $n = 3$). But if it was true for $d = -1$ then the Kloosterman sum would never be equal to -1 in a non-binary and non-ternary case, which means that there would be no bent functions having the form (6) for $p > 3$.

3 New Class of Ternary Monomial Bent Functions

In this section we define a new class of ternary monomial functions and conjecture that these functions are bent. We start with proving few lemmas, that hold under more general conditions on p compared to the restriction of $p = 3$. These lemmas are interesting as independent statements as well. Basing on these results we give an outline for proving the conjecture. We are planning to have a full proof in the final version of the paper.

Further assume p be an odd prime, $n = 2k$ and let C_i $(i = 0, 1, 2, 3)$ denote the *cyclotomic classes* of order four in the multiplicative group of $\mathrm{GF}(p^n)$, i.e., $C_i = \{\xi^{4t+i} \mid t = 0, \ldots, f-1\}$, where ξ is a primitive element of $\mathrm{GF}(p^n)$ and $f = \frac{p^n-1}{4}$. Throughout this section all expressions in the indices numbering the cyclotomic classes are calculated modulo 4.

Lemma 1 *Let p be an odd prime with $p \equiv 3 \pmod 4$ and let $n = 2k$ with k odd. Raising elements of C_i to the power of $p^k + 1$ results in a $\frac{p^k+1}{2}$ -to-1 mapping onto the cyclotomic classes of order two in the multiplicative group of $\mathrm{GF}(p^k)$. Moreover, C_0 and C_2 map onto the squares and C_1 and C_3 onto the non-squares in $\mathrm{GF}(p^k)^*$.*

Proof: Take the following polynomial over $\mathrm{GF}(p)$ that factors in $\mathrm{GF}(p^k)$ as

$$p(z) = z^{\frac{p^n-1}{4}} - 1 = (z^t)^{p^k-1} - 1 = \prod_{\alpha \in \mathrm{GF}(p^k)^*} (z^t - \alpha) \ ,$$

where $t = \frac{p^k+1}{4}$. The roots of $p(z)$ are exactly all the elements from C_0. Therefore, it can be concluded that raising elements of C_0 to the power of t results in a t-to-1

mapping onto the multiplicative group of $\mathrm{GF}(p^k)$. In general, raising elements of $C_i = \xi^i C_0$ to the power of t results in a t-to-1 mapping onto the coset $\xi^{it}\mathrm{GF}(p^k)^*$.

Let $\eta = \xi^{p^k+1}$ be a a primitive element of $\mathrm{GF}(p^k)$. When k is odd, the cyclic subgroups generated by η^2 and by η^4 are equal since they have the same multiplicative order equal to

$$\mathrm{ord}\,\eta^4 = \frac{p^k-1}{\gcd(p^k-1,4)} = \frac{p^k-1}{2} = \mathrm{ord}\,\eta^2 \ .$$

Thus, raising elements of $\mathrm{GF}(p^k)^*$ to the 4^{th} power is a mapping onto the subgroup generated by η^2 and since both α and $-\alpha$ produce the same image for any $\alpha \in \mathrm{GF}(p^k)^*$, this is a 2-to-1 mapping.

Also note that $\xi^{4it} = \xi^{i(p^k+1)} = \eta^i$. Therefore, combination of these two mappings that is equivalent to raising elements of C_i to the power of $4t = p^k + 1$, results in a $\frac{p^k+1}{2}$ -to-1 mapping onto the cyclotomic classes of order two in $\mathrm{GF}(p^k)^*$. Moreover, C_0 and C_2 map onto the squares and C_1 and C_3 onto the non-squares in $\mathrm{GF}(p^k)^*$. □

Lemma 2 *Let p be an odd prime with $p \equiv 3 \pmod 8$ and let $n = 2k$ with k odd. Then for any $c \in \mathrm{GF}(p^k)$ and $z \in \mathrm{GF}(p^n)$, both being nonzero, and any cyclotomic class C_j $(j = 0, 1, 2, 3)$*

$$\sum_{y \in C_j} \omega^{\mathrm{Tr}_n\left(cz^{p^k}y\right)} = \begin{cases} \frac{3p^k-1}{4}, & \text{if} \quad z \in C_{j+2}\,, \\ -\frac{p^k+1}{4}, & \text{otherwise}\,. \end{cases}$$

Proof: To prove this identity first note that for even n raising elements of $y \in \mathrm{GF}(p^n)^*$ to the 4^{th} power results in a 4-to-1 mapping onto C_0. Also note that in our case $(p+1)/4$ is odd. Thus, for any $q \in \mathrm{GF}(p^n)$

$$4\sum_{y \in C_0} \omega^{\mathrm{Tr}_n(qy)} = \sum_{y \in \mathrm{GF}(p^n)^*} \omega^{\mathrm{Tr}_n\left(qy^4\right)} \overset{(*)}{=} \begin{cases} p^n - 1, & \text{if} \quad q = 0\,, \\ 3p^k - 1, & \text{if} \quad q \in C_2\,, \\ -p^k - 1, & \text{otherwise}\,, \end{cases}$$

where (*) follows from [11, Lemma 3.5, Item (i)] (see also [13] for the proof). Moreover, for any nonzero $q \in \mathrm{GF}(p^n)$ and $j \in \{0, 1, 2, 3\}$

$$\sum_{y \in C_j} \omega^{\mathrm{Tr}_n(qy)} = \sum_{y \in C_0} \omega^{\mathrm{Tr}_n\left(q\xi^j y\right)} = \begin{cases} \frac{3p^k-1}{4}, & \text{if} \quad q\xi^j \in C_2\,, \\ -\frac{p^k+1}{4}, & \text{otherwise}\,. \end{cases}$$

Note that $q\xi^j \in C_2$ is equivalent to $q \in C_{2-j}$. In our particular sum $q = cz^{p^k} \neq 0$ with $c \in \mathrm{GF}(p^k)$. Since $\mathrm{GF}(p^k)^* \subset C_0$ (because $p^k + 1 \equiv 0 \pmod 4$ for odd k and ξ^{p^k+1} that generates $\mathrm{GF}(p^k)^*$ belongs to C_0) then $c \in C_0$. Thus, we are interested if $z^{p^k} \in C_{2-j}$. Note that $p^k \equiv 3 (\mathrm{mod}\ 4)$ for odd k and thus $z \in C_{j+2}$ is equivalent to $z^{p^k} \in C_{3(j+2)} = C_{2-j}$. □

Lemma 3 *Let p be an odd prime with $p \equiv 3 \pmod 8$ and let $n = 2k$ with k odd. For any $c \in \mathrm{GF}(p^k)$ and $j = 0, 1, 2, 3$ denote*

$$T_j = \sum_{x \in C_i} \omega^{\mathrm{Tr}_k\left(c(x+1)^{p^k+1}-c\right)} \ .$$

Then for any j

$$-\overline{T_j} = \omega^{\mathrm{Tr}_k(c)} T_{j+2} + \frac{p^k+1}{4}\left(\omega^{\mathrm{Tr}_k(c)}+1\right) \ ,$$

where the line over a complex value denotes the complex conjugate and the index is calculated modulo 4.

Proof: First, it is easy to see that for any nonzero $c \in \mathrm{GF}(p^k)$

$$\begin{aligned} 1+T_0+T_1+T_2+T_3 &= \sum_{x\in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_k\left(c(x+1)^{p^k+1}-c\right)} \\ &= \omega^{-\mathrm{Tr}_k(c)} \sum_{y\in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_k\left(cy^{p^k+1}\right)} \overset{(*)}{=} \omega^{-\mathrm{Tr}_k(c)} \left((p^k+1) \sum_{z\in \mathrm{GF}(p^k)^*} \omega^{\mathrm{Tr}_k(cz)} + 1 \right) \\ &= -p^k \omega^{-\mathrm{Tr}_k(c)} \ , \end{aligned} \tag{9}$$

where (*) holds since raising elements of $\mathrm{GF}(p^n)^*$ to the power of p^k+1 is a (p^k+1)-to-1 mapping onto $\mathrm{GF}(p^k)^*$ as proved in [14, Lemma 1].

Let $C_i \cdot C_j$ denote the *strong union* of C_i and C_j, i.e., the set of elements of $\mathrm{GF}(p^n)$ that can be represented as a sum of two addends from C_i and C_j respectively and counting the multiplicity of such a representation. Thus, $C_i \cdot C_j$ consists of the elements $\xi^{4t+i}+\xi^{4d+j} = \xi^{4d+j}(1+\xi^{4(t-d)+i-j})$ for all $t,d = 0,\ldots,f-1$. Therefore,

$$\begin{aligned} C_i \cdot C_j &= C_j(1+C_{i-j}) \\ &= (i-j,0)C_j \cup (i-j,1)C_{j+1} \cup (i-j,2)C_{j+2} \cup (i-j,3)C_{j+3} \\ &= (i-j,-j)C_0 \cup (i-j,1-j)C_1 \cup (i-j,2-j)C_2 \cup (i-j,3-j)C_3 \end{aligned} \tag{10}$$

if $i \neq j$ and otherwise, since $-1 \in C_0$,

$$C_i \cdot C_i = (0,-i)C_0 \cup (0,1-i)C_1 \cup (0,2-i)C_2 \cup (0,3-i)C_3 \cup f\{0\} \ , \tag{11}$$

where (i,j) denotes the *cyclotomic number* that is equal to the number of elements $x \in C_i$ such that $x+1 \in C_j$ and $f\{0\}$ denotes the zero-element of $\mathrm{GF}(p^n)$ taken with the multiplicity f. The components i, j in cyclotomic numbers are taken modulo 4.

Also denote $C_i^j = \{x \in C_i \mid 1+x \in C_j\}$ (obviously, $|C_i^j| = (i,j)$). In our case $-1 \in C_0$ and we can prove that $(i,j) = (j,i)$. Indeed, the elements of C_i^j correspond to the pairs (t,d) with $t,d \in \{0,\ldots,f-1\}$ that satisfy the equation $\xi^{4t+i}+1 = \xi^{4d+j}$. Multiplying both sides of the equation by $-1 = \xi^{4l}$ we get the equivalent equation $\xi^{4(d+l)+j}+1 = \xi^{4(t+l)+i}$ whose solutions give the elements of C_j^i. Therefore, for any $i \in \{0,1,2,3\}$ we have

$$\sum_{j=0}^{3}(j,i) = \sum_{j=0}^{3}(i,j) = |C_i^0 \cup C_i^1 \cup C_i^2 \cup C_i^3| = \begin{cases} |C_i| = f, & \text{if} \quad i \neq 0 \, , \\ |C_0 \backslash \{-1\}| = f-1, & \text{otherwise} \ , \end{cases}$$

since $-1+1=0$ that does not belong to any C_i. A good introduction into this subject can be found in [15].

Now for $i,j \in \{0,1,2,3\}$ and $i \neq j$ we evaluate the product

$$\begin{aligned}
T_i\overline{T_j} &= \sum_{x\in C_i,\, y\in C_j} \omega^{\mathrm{Tr}_k\left(c(x+1)^{p^k+1}-c-c(y+1)^{p^k+1}+c\right)} \\
&= \sum_{x\in C_i,\, y\in C_j} \omega^{\mathrm{Tr}_k\left(c\left(x^{p^k+1}-y^{p^k+1}+(x-y)^{p^k}+(x-y)\right)\right)} \\
&\overset{\{C_j=-C_j\}}{=} \sum_{x\in C_i,\, y\in C_j} \omega^{\mathrm{Tr}_k\left(c\left(x^{p^k+1}-y^{p^k+1}+(x+y)^{p^k}+(x+y)\right)\right)} \\
&= \sum_{z\in C_i\cdot C_j} \omega^{\mathrm{Tr}_k\left(c\left((z-y)^{p^k+1}-y^{p^k+1}+z^{p^k}+z\right)\right)} \\
&= \sum_{z\in C_i\cdot C_j} \omega^{\mathrm{Tr}_k\left(c(z+1)^{p^k+1}-c\right)}\omega^{-\mathrm{Tr}_k\left(c\left(zy^{p^k}+z^{p^k}y\right)\right)} \\
&= \sum_{z\in C_i\cdot C_j} \omega^{\mathrm{Tr}_k\left(c(z+1)^{p^k+1}-c\right)}\omega^{-\mathrm{Tr}_n\left(cz^{p^k}y\right)} \\
&= \sum_{t=0}^{3}\sum_{z\in C_t} \omega^{\mathrm{Tr}_k\left(c(z+1)^{p^k+1}-c\right)} \sum_{q\in C_{i-j}^{t-j}} \omega^{-\mathrm{Tr}_n\left(cz^{p^k}\frac{z}{1+q}\right)}\ , \qquad (12)
\end{aligned}$$

where $z = x+y \in C_i\cdot C_j$ and the value of y is uniquely defined by z. Therefore, if $z = x+y \in C_t$ with $x\in C_i$ and $y\in C_j$ then $z = y(1+xy^{-1})$ with $xy^{-1}\in C_{i-j}^{t-j}$. By (10), the multiplicity of $z\in C_t$ in $C_i\cdot C_j$ is equal to $(i-j,t-j) = \left|C_{i-j}^{t-j}\right|$. Thus, for a fixed $z\in C_t$ the set $\left\{\frac{z}{1+q} \mid q\in C_{i-j}^{t-j}\right\}$ contains all $(i-j,t-j)$ values for $y\in C_j$ that correspond to this z taken with the appropriate multiplicity $(i-j,t-j)$ as a member of $C_i\cdot C_j$. For $i=j$ we just have additionally to consider the zero-element of $\mathrm{GF}(p^n)$ that is found in $C_i\cdot C_i$ with the multiplicity f (see (11)). Then

$$T_i\overline{T_i} = \sum_{t=0}^{3}\sum_{z\in C_t} \omega^{\mathrm{Tr}_k\left(c(z+1)^{p^k+1}-c\right)} \sum_{q\in C_0^{t-i}} \omega^{-\mathrm{Tr}_n\left(cz^{p^k}\frac{z}{1+q}\right)} + f\ . \qquad (13)$$

Let $t,j\in\{0,1,2,3\}$ and $z\in C_t$ be fixed. Then for any $i\in\{0,1,2,3\}$ and $q\in C_{i-j}^{t-j}$ we have $\frac{z}{1+q}\in C_j$. Further, $\sum_{i=0}^{3}\left|C_{i-j}^{t-j}\right| = \sum_{i=0}^{3}(i,t-j)$ is equal to $|C_{t-j}| = f$ if $t\neq j$ and is equal to $|C_0|-1 = f-1$ otherwise. Since the cardinality of C_j is f, we have proven that

$$\left\{\frac{z}{1+q} \mid q\in C_{i-j}^{t-j},\ i=0,1,2,3\right\} = \begin{cases} C_j, & \text{if} \quad t\neq j\,, \\ C_j\backslash\{z\}, & \text{otherwise}\,, \end{cases}$$

since $q\neq 0$. Therefore, for any $t,j\in\{0,1,2,3\}$ and $z\in C_t$

$$\sum_{i=0}^{3}\sum_{q\in C_{i-j}^{t-j}} \omega^{-\mathrm{Tr}_n\left(cz^{p^k}\frac{z}{1+q}\right)} = \begin{cases} \sum_{y\in C_j}\omega^{-\mathrm{Tr}_n\left(cz^{p^k}y\right)}, & \text{if} \quad t\neq j\,, \\ \sum_{y\in C_j\backslash\{z\}}\omega^{-\mathrm{Tr}_n\left(cz^{p^k}y\right)}, & \text{otherwise}\,. \end{cases} \qquad (14)$$

Note that since $n=2k$ and $p\equiv 3 \pmod 8$ then $(p^n-1)/2 \equiv 0 \pmod 4$ and $-1 = \xi^{\frac{p^n-1}{2}} \in C_0$. Therefore, $-C_j = C_j$ and

$$\overline{T_j} = \sum_{z\in C_j}\omega^{\mathrm{Tr}_k\left(c(-z^{p^k+1}-z^{p^k}-z)\right)} = \sum_{z\in C_j}\omega^{\mathrm{Tr}_k\left(c(-z^{p^k+1}+z^{p^k}+z)\right)}\ . \qquad (15)$$

Making use of Lemma 2 we get that

$$
\begin{aligned}
&(T_0+T_1+T_2+T_3)\overline{T_j}\\
&\stackrel{(12,13)}{=} \sum_{t=0}^{3}\sum_{z\in C_t}\omega^{\mathrm{Tr}_k\left(c(z+1)^{p^k+1}-c\right)}\sum_{i=0}^{3}\sum_{q\in C_{i-j}^{t-j}}\omega^{-\mathrm{Tr}_n\left(cz^{p^k}\frac{z}{1+q}\right)}+f\\
&\stackrel{(14)}{=} \sum_{t=0}^{3}\sum_{z\in C_t}\omega^{\mathrm{Tr}_k\left(c(z+1)^{p^k+1}-c\right)}\sum_{y\in C_j}\omega^{-\mathrm{Tr}_n\left(cz^{p^k}y\right)}\\
&-\sum_{z\in C_j}\omega^{\mathrm{Tr}_k\left(c(z+1)^{p^k+1}-c\right)}\omega^{-\mathrm{Tr}_n\left(cz^{p^k+1}\right)}+f\\
&=-\frac{p^k+1}{4}\sum_{t\neq j+2}T_t+\frac{3p^k-1}{4}T_{j+2}-\sum_{z\in C_j}\omega^{\mathrm{Tr}_k\left(c(-z^{p^k+1}+z^{p^k}+z)\right)}+f\\
&\stackrel{(15)}{=} -\frac{p^k+1}{4}(T_0+T_1+T_2+T_3)+p^kT_{j+2}-\overline{T_j}+f\ .
\end{aligned}
$$

Now, using (9), we get

$$
\begin{aligned}
-p^k\omega^{-\mathrm{Tr}_k(c)}\overline{T_j} &= (p^k\omega^{-\mathrm{Tr}_k(c)}+1)\frac{p^k+1}{4}+p^kT_{j+2}+\frac{p^n-1}{4} \quad \text{and}\\
-\overline{T_j} &= \omega^{\mathrm{Tr}_k(c)}T_{j+2}+\frac{p^k+1}{4}(\omega^{\mathrm{Tr}_k(c)}+1)
\end{aligned}
$$

that was claimed. □

Conjecture 1 *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 $b\in\mathrm{GF}(3^n)$ the corresponding Walsh transform coefficient of $f(x)$ is equal to*

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

where I is a primitive 4^{th} root of unity over $\mathrm{GF}(3^n)$.

Proof: If C_i is the cyclotomic class of order four then any $x\in C_i$ satisfies $x^{\frac{3^n-1}{4}}=\xi^{\frac{i(3^n-1)}{4}}=I^i$, where I is a primitive 4^{th} root of unity over $\mathrm{GF}(3^n)$ (obviously $I^2=-1$). Then $a^{3^k}=aI$ and $\mathrm{Tr}_k^n(a)=a+a^{3^k}=a(I+1)$. On the other hand, $\mathrm{Tr}_k^n(aI)=aI-a^{3^k}I=aI+a=a(I+1)=\mathrm{Tr}_k^n(a)$ since $3^k\equiv 3 \pmod 4$ for odd k. Therefore, the Walsh transform coefficient of the function $f(x)$ evaluated at b is

equal to

$$S_a(b)-1=\sum_{x\in \mathrm{GF}(3^n)}\omega^{\mathrm{Tr}_n\left(ax^{\frac{3^n-1}{4}+3^k+1}-bx\right)}-1=\sum_{i=0}^{3}\sum_{x\in C_i}\omega^{\mathrm{Tr}_n\left(aI^ix^{3^k+1}-bx\right)}$$
$$=\sum_{x\in C_0\cup C_1}\omega^{\mathrm{Tr}_k\left(a_1x^{3^k+1}-bx-b^{3^k}x^{3^k}\right)}+\sum_{x\in C_2\cup C_3}\omega^{\mathrm{Tr}_k\left(-a_1x^{3^k+1}-bx-b^{3^k}x^{3^k}\right)}$$
$$=\sum_{x\in C_0\cup C_1}\omega^{\mathrm{Tr}_k\left(a_1(x-\beta)^{3^k+1}-a_1\beta^{3^k+1}\right)}+\sum_{x\in C_2\cup C_3}\omega^{-\mathrm{Tr}_k\left(a_1(x+\beta)^{3^k+1}-a_1\beta^{3^k+1}\right)}$$
$$=\sum_{y\in C_j\cup C_{j+1}}\omega^{\mathrm{Tr}_k\left(c(y-1)^{3^k+1}-c\right)}+\sum_{y\in C_{j+2}\cup C_{j+3}}\omega^{-\mathrm{Tr}_k\left(c(y+1)^{3^k+1}-c\right)}\ ,$$

where $a_1=a(I+1)\neq 0$ belongs to $\mathrm{GF}(3^k)$, $b=a_1\beta^{3^k}$ and $c=a_1\beta^{3^k+1}=\frac{b^{3^k+1}}{a_1}\in\mathrm{GF}(3^k)$. In the latest identity we assumed $b\neq 0$ and made the substitution $y=\beta^{-1}x$ assuming $\beta^{-1}\in C_j$ (i.e., $\mathrm{ind}(\beta^{-1})\equiv j(\bmod\ 4)$). Thus, $\beta^{-1}C_i=C_{i+j}$ for any $i\in\{0,1,2,3\}$. Since $n=2k$ then $(3^n-1)/2\equiv 0(\bmod\ 4)$ and $-1=\xi^{\frac{3^n-1}{2}}\in C_0$. Therefore, $-C_i=C_i$ and

$$\sum_{y\in C_i}\omega^{\mathrm{Tr}_k\left(c(y-1)^{3^k+1}\right)}=\sum_{y\in C_i}\omega^{\mathrm{Tr}_k\left(c(y+1)^{3^k+1}\right)}\ .$$

Assume first $\beta=0$ that corresponds to $b=0$. Then, by Lemma 1,

$$\begin{aligned}S_a(0)&=1+\sum_{x\in C_0\cup C_1}\omega^{\mathrm{Tr}_k\left(a_1x^{3^k+1}\right)}+\sum_{x\in C_2\cup C_3}\omega^{-\mathrm{Tr}_k\left(a_1x^{3^k+1}\right)}\\&=1+\frac{3^k+1}{2}\sum_{y\in\mathrm{GF}(3^k)^*}\left(\omega^{\mathrm{Tr}_k(a_1y)}+\omega^{-\mathrm{Tr}_k(a_1y)}\right)=-3^k\ .\end{aligned}$$

Further assume $\beta\neq 0$ (thus, $c\neq 0$). Take T_i $(i=0,1,2,3)$ as defined in Lemma 3. Then if $\beta^{-1}\in C_j$ and $b=a_1\beta^{3^k}$ then $S_a(b)=1+T_j+T_{j+1}+\overline{T_{j+2}}+\overline{T_{j+3}}$, where the line over a complex value denotes the complex conjugate. If $T_{j+2}+T_{j+3}$ is a real number then by (9)

$$S_a(b)=-3^k\omega^{-\mathrm{Tr}_k(c)}=-3^k\omega^{-\mathrm{Tr}_k\left(\frac{b^{3^k+1}}{a(I+1)}\right)}\ .$$

Using Lemma 3 we can get that

$$S_a(b)=1+T_j+T_{j+1}+\overline{T_{j+2}}+\overline{T_{j+3}}=(1-\omega^{\mathrm{Tr}_k(c)})\left(T_j+T_{j+1}+\frac{3^k+1}{2}\right)-3^k\ .$$

In particular, if $\mathrm{Tr}_k(c)=0$ then $S_a(b)=-3^k$.

Using the similar technique as before when evaluating the product $T_i\overline{T_j}$, we can

write for any $i,j \in \{0,1,2,3\}$ and $i \neq j$

$$\begin{aligned}
T_iT_j &= \sum_{x\in C_i,\, y\in C_j} \omega^{\mathrm{Tr}_k\left(c(x+1)^{3^k+1}-c+c(y+1)^{3^k+1}-c\right)} \\
&= \sum_{x\in C_i,\, y\in C_j} \omega^{\mathrm{Tr}_k\left(c\left(x^{3^k+1}+y^{3^k+1}+(x+y)^{3^k}+(x+y)\right)\right)} \\
&= \sum_{z\in C_i\cdot C_j} \omega^{\mathrm{Tr}_k\left(c\left((z-y)^{3^k+1}+y^{3^k+1}+z^{3^k}+z\right)\right)} \\
&= \sum_{z\in C_i\cdot C_j} \omega^{\mathrm{Tr}_k\left(c(z+1)^{3^k+1}-c\right)}\omega^{\mathrm{Tr}_k\left(c\left(2y^{3^k+1}-y^{3^k}z-yz^{3^k}\right)\right)} \\
&= \sum_{z\in C_i\cdot C_j} \omega^{\mathrm{Tr}_k\left(c(z+1)^{3^k+1}-c\right)}\omega^{\mathrm{Tr}_n\left(cy(y-z)^{3^k}\right)} \\
&= \sum_{t=0}^{3}\sum_{z\in C_t} \omega^{\mathrm{Tr}_k\left(c(z+1)^{3^k+1}-c\right)} \sum_{q\in C_{i-j}^{t-j}} \omega^{-\mathrm{Tr}_n\left(cz^{3^k+1}\frac{q}{(1+q)^{3^k+1}}\right)} \ ,
\end{aligned}$$

where $z = x + y \in C_i \cdot C_j$ and the value of y is uniquely defined by z.

Numerics shows that for any $c \in \mathrm{GF}(3^k)$ there exists some $i \in \{0,1,2,3\}$ such that $T_i = T_{i+2}$ and if $\mathrm{Tr}_k(c) = 0$ then also $T_{i+1} = T_{i+3}$ (thus, by (9), $T_0 + T_1 = -\frac{3^k+1}{2}$ and $\overline{T_0} = T_1$).

4 Quadratic Monomial Bent Functions

In this section we consider quadratic monomial functions with the exponent of the Gold type. These functions can also be analyzed using a more general result provided by Proposition 2. However, our particular approach to the quadratic monomial bent functions allows to derive more explicit requirements on the value of the coefficient a. Moreover, this result provides the generalization for the known monomial cases of p-ary bent functions due to Sidelnikov, Kumar-Moreno, Kasami, and Kim et alia. We also study closely the property of bent functions to be (weakly) regular. To that end we prove that some of the known constructions of quadratic bent functions lead to (weakly) regular functions and give the exact value of the Walsh transform coefficients for Sidelnikov and Kasami cases. We start with the following lemma. Let $v(b)$ denote the (additive) 2-adic valuation of integer b (i.e., the maximal power of 2 dividing b). Let ξ be a primitive element of $\mathrm{GF}(p^n)$ and for $a \in \mathrm{GF}(p^n)^*$ define $\mathrm{ind}(a)$ as the unique integer t with $a = \xi^t$ and $0 \le t < p^n - 1$.

Lemma 4 *For an odd prime p*

$$\gcd(p^j+1, p^n-1) = \begin{cases} p^{\,\gcd(j,n)}+1, & \text{if} \quad v(j) < v(n)\ , \\ 2, & \text{otherwise}\ . \end{cases}$$

Proof: Denote $d = \gcd(p^j+1, p^n-1)$. It is easy to see that if $v(p^{2j}-1) \le v(p^n-1)$ then

$$p^{\,\gcd(2j,n)} - 1 = \gcd(p^{2j}-1, p^n-1) = d\gcd(p^j-1, p^n-1) = d(p^{\,\gcd(j,n)}-1)\ ,$$

since $\gcd(p^j-1, p^j+1) = 2$. Alternatively, if $v(p^n-1) < v(p^{2j}-1)$ then

$$2(p^{\,\gcd(2j,n)}-1) = d(p^{\,\gcd(j,n)}-1)\ .$$

Note that if n is odd then $d = 2$. Further consider only even n.

It is well known that $v(p^b - 1) = v(p + 1) + v(b)$ if $p \equiv 3 \pmod 4$ and b is even; in the remaining cases $v(p^b - 1) = v(p - 1) + v(b)$. Thus, for even n the condition $v(p^n - 1) < v(p^{2j} - 1)$ is equivalent to $v(n) \le v(j)$. In this case $d = 2$ as well. Otherwise we have

$$d = \frac{p^{\gcd(2j,n)} - 1}{p^{\gcd(j,n)} - 1} = \frac{p^{2\gcd(j,n)} - 1}{p^{\gcd(j,n)} - 1} = p^{\gcd(j,n)} + 1$$

when $v(j) < v(n)$. □

Lemma 5 *Let p be an odd prime, $j \in \{1, \ldots, n\}$ and $a \in \mathrm{GF}(p^n)$ is nonzero.*

(i) If $v(n) \le v(j)$ then

$$\sum_{x \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^{p^j+1}\right)} = \begin{cases} \eta(a)(-1)^{n-1}p^{n/2}, & \text{if } \ p \equiv 1 \pmod 4\,, \\ \eta(a)(-1)^{n-1}i^n p^{n/2}, & \text{if } \ p \equiv 3 \pmod 4\,. \end{cases}$$

(ii) If $v(n) > v(j) + 1$ then

$$\sum_{x \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^{p^j+1}\right)} = \begin{cases} -p^{n/2+\gcd(j,n)}, & \text{if } \ a \in C_0\,, \\ p^{n/2}, & \text{otherwise}\,. \end{cases}$$

(iii) If $v(n) = v(j) + 1$ then

$$\sum_{x \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^{p^j+1}\right)} = \begin{cases} p^{n/2+\gcd(j,n)}, & \text{if } \ a \in C_{d/2}\,, \\ -p^{n/2}, & \text{otherwise}\,, \end{cases}$$

where $d = p^{\gcd(j,n)} + 1$ and $C_t = \{a \in \mathrm{GF}(p^n)^* \mid \mathrm{ind}(a) \equiv t \pmod d\}$.

Proof: Obviously, the exponent $p^j + 1$ can be replaced with $d = \gcd(p^j + 1, p^n - 1)$ without affecting the value of the questioned sum. The value of d is given by Lemma 4. For those values of j giving $d = 2$ we use [4, Theorems 5.15, 5.33] and the remaining cases when $v(j) < v(n)$ are settled by [11, Lemma 3.5] (see also [13] for the proofs). □

Theorem 3 *Let $a \in \mathrm{GF}(p^n)$ be nonzero and a prime p be odd. Then for any $j \in \{1, \ldots, n\}$ the quadratic p-ary function $f(x)$ mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$ and given by*

$$f(x) = \mathrm{Tr}_n\left(ax^{p^j+1}\right) \tag{16}$$

is bent if and only if

$$p^{\gcd(2j,n)} - 1 \not\Big| \frac{p^n - 1}{2} - i_0(p^j - 1) \quad , \tag{17}$$

where $a = \xi^{i_0}$ and ξ is a primitive element of $\mathrm{GF}(p^n)$. Moreover, if (17) holds then $f(x)$ is a (weakly) regular bent function. The magnitude of $S_a(b)$ can be determined using Lemma 5 given the concrete values of j and n.

Proof: Here we apply the classical squaring method for proving that the function is bent. For instance, the Kumar-Moreno case (see [16, Theorem 7.6]) is proved similarly.

The Walsh transform coefficient of the function $f(x)$ evaluated at $-b$ is equal to

$$S_a(-b) = \sum_{x \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^{p^j+1}+bx\right)} \ .$$

The absolute square of a complex number is equal to the product of this number and its complex conjugate. Thus,

$$\begin{aligned} |S_a(-b)|^2 &= \sum_{x,y \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(a\left(x^{p^j+1}-y^{p^j+1}\right)+b(x-y)\right)} \\ &= \sum_{y,z \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(a\left((y+z)^{p^j+1}-y^{p^j+1}\right)+bz\right)} \\ &= \sum_{y,z \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(a\left(yz^{p^j}+zy^{p^j}+z^{p^j+1}\right)+bz\right)} \\ &= \sum_{z \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(az^{p^j+1}+bz\right)} \sum_{y \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(y^{p^j}\left(az+a^{p^j}z^{p^{2j}}\right)\right)} \ , \end{aligned}$$

where $z = x - y$. The inner sum is equal to zero unless $-az = a^{p^j} z^{p^{2j}}$. If z is not zero then equivalently $z^{p^{2j}-1} = -a^{1-p^j}$. Let ξ is a primitive element of $\mathrm{GF}(p^n)$ and $a = \xi^{i_0}$ for some $i_0 \in \{0, \ldots, p^n - 2\}$. Then $-a^{1-p^j} = \xi^{\frac{p^n-1}{2} - i_0(p^j-1)}$. Consider the following equation of the unknown $t \in \{0, \ldots, p^n - 2\}$

$$\xi^{\frac{p^n-1}{2} - i_0(p^j-1)} = \xi^{(p^{2j}-1)t} \ ,$$

which holds if and only if $\frac{p^n-1}{2} - i_0(p^j - 1) \equiv (p^{2j} - 1)t \pmod{(p^n - 1)}$. The latter congruence has a solution in t if and only if

$$\gcd\left(p^{2j} - 1, p^n - 1\right) = p^{\gcd(2j,n)} - 1 \ \Big| \ \frac{p^n - 1}{2} - i_0(p^j - 1) \ .$$

Thus, if condition (17) holds then $-az \neq a^{p^j} z^{p^{2j}}$ for any nonzero $z \in \mathrm{GF}(p^n)$ which means that $|S_a(-b)|^2 = p^n$ for any $b \in \mathrm{GF}(p^n)$ and, therefore, $f(x)$ is bent. Moreover, by Proposition 1, f is a (weakly) regular bent function.

The value of the Walsh transform of $f(x)$ in point zero is equal to $S_a(0) = \sum_{x \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^{p^j+1}\right)}$ and can be found using Lemma 5. Since f is a (weakly) regular bent function, the magnitude of $S_a(b)$ does not depend on b and is equal to the magnitude of $S_a(0)$.

Now prove that condition (17) is necessary for function f to be bent. Take a bent function f and consider separately three cases as in Lemma 5. Assume first that $v(n) \leq v(j)$ which is equivalent to $\gcd(2j, n) = \gcd(j, n)$ and to $\frac{n}{\gcd(j,n)}$ is odd. Thus, $p^{\gcd(2j,n)} - 1$ divides $p^j - 1$. On the other hand,

$$\frac{p^n - 1}{p^{\gcd(j,n)} - 1} = p^{\gcd(j,n)(e-1)} + p^{\gcd(j,n)(e-2)} + \cdots + 1 \equiv e \pmod 2 \ , \qquad (18)$$

where $e = \frac{n}{\gcd(j,n)}$ is odd. Thus, $p^{\gcd(2j,n)} - 1$ does not divide $(p^n - 1)/2$ and (17) holds for any i_0. This case corresponds to the Kumar-Moreno class of bent functions (see Corollary 6).

Further assume that $v(n) > v(j) + 1$. In this case $\gcd(2j, n) = 2\gcd(j, n)$. By Lemma 5, if f is a bent function then $a \notin C_0$ meaning that i_0 is not a multiple of $p^{\gcd(j,n)} + 1$ (otherwise, $|S_a(0)| = p^{n/2+\gcd(j,n)}$). By (18), $\frac{p^n-1}{p^{\gcd(2j,n)}-1} \equiv \frac{n}{\gcd(2j,n)} \equiv 0 \pmod 2$ and thus, $p^{\gcd(2j,n)} - 1$ divides $(p^n - 1)/2$. Therefore, (17) holds if and only if $p^{\gcd(2j,n)} - 1$ does not divide $i_0(p^j - 1)$ or equivalently $p^{\gcd(j,n)} + 1$ does not divide $i_0(p^j - 1)/(p^{\gcd(j,n)} - 1)$. Note that $v(j) = v(\gcd(j, n))$ and by Lemma 4, $\gcd(p^{\gcd(j,n)} + 1, p^j - 1) = 2$. Again by (18), $\frac{p^j-1}{p^{\gcd(j,n)}-1} \equiv \frac{j}{\gcd(j,n)} \equiv 1 \pmod 2$ and thus, $p^{\gcd(j,n)} + 1$ is coprime to $(p^j - 1)/(p^{\gcd(j,n)} - 1)$ and (17) holds if and only if $p^{\gcd(j,n)} + 1$ does not divide i_0 that is equivalent to $a \notin C_0$.

Finally, assume that $v(n) = v(j) + 1$. In this case $\gcd(2j, n) = 2\gcd(j, n)$. By Lemma 5, if f is a bent function then $a \notin C_{d/2}$ with $d = p^{\gcd(j,n)} + 1$ (otherwise, $|S_a(0)| = p^{n/2+\gcd(j,n)}$). Note that $a \in C_{d/2}$ if and only if $d/2$ divides i_0 and $2i_0/d$ is odd. By (18), both $(p^n - 1)/(p^{\gcd(2j,n)} - 1)$ and $(p^j - 1)/(p^{\gcd(j,n)} - 1)$ are odd. Similarly to the previous case it can be proved that the condition

$$\frac{p^{\gcd(2j,n)} - 1}{2} \;\Big|\; \frac{p^n - 1}{2} - i_0(p^j - 1)$$

holds if and only if $d/2$ divides i_0. Therefore, (17) does not hold if and only if $d/2$ divides i_0 and

$$\frac{p^n - 1}{p^{\gcd(2j,n)} - 1} - \frac{2i_0}{p^{\gcd(j,n)} + 1}\frac{p^j - 1}{p^{\gcd(j,n)} - 1}$$

is even or equivalently $2i_0/(p^{\gcd(j,n)} + 1) = 2i_0/d$ is odd. □

Corollary 2 *Given the conditions of Theorem 3, if* $\frac{n}{\gcd(2j,n)}$ *is odd then* $f(x) = \mathrm{Tr}_n\left(x^{p^j+1}\right)$ *is a (weakly) regular bent function.*

Proof: Consider function (16) with $a = 1$. This is a (weakly) regular bent function if condition (17) holds for $i_0 = 0$, i.e., when $p^{\gcd(2j,n)} - 1 \nmid \frac{p^n-1}{2}$. The latter holds if and only if $\frac{p^n-1}{p^{\gcd(2j,n)}-1}$ is odd. But by (18), $\frac{p^n-1}{p^{\gcd(2j,n)}-1} \equiv \frac{n}{\gcd(2j,n)} \pmod 2$ since p is odd. □

Assuming $j = n$ for arbitrary n and $j = k$ for even $n = 2k$ in Theorem 3 leads directly to the Sidelnikov and Kasami p-ary bent functions. In the following two corollaries we find the actual value of the Walsh transform coefficients for these two classes of functions. According to [4, Example 5.10], the real-valued function η on $\mathrm{GF}(p^n)^*$ with $\eta(c) = 1$ if c is the square of an element of $\mathrm{GF}(p^n)^*$ and $\eta(c) = -1$ otherwise, is called the *quadratic character* of $\mathrm{GF}(p^n)$.

Corollary 3 (Sidelnikov) *For any nonzero* $a \in \mathrm{GF}(p^n)$ *and odd prime* p *the function* $f(x) = \mathrm{Tr}_n\left(ax^2\right)$ *is a (weakly) regular bent function. Moreover, for* $b \in \mathrm{GF}(p^n)$ *the corresponding Walsh transform coefficient of* $f(x)$ *is equal to*

$$S_a(b) = \eta(a)(-1)^{n-1}p^{n/2}\omega^{-\mathrm{Tr}_n\left(\frac{b^2}{4a}\right)} \quad \textit{if} \quad p \equiv 1 \pmod 4$$

and

$$S_a(b) = \eta(a)(-1)^{n-1}i^n p^{n/2}\omega^{-\mathrm{Tr}_n\left(\frac{b^2}{4a}\right)} \quad \textit{if} \quad p \equiv 3 \pmod 4 \ ,$$

where i *is the complex primitive* 4^{th} *root of unity and* η *is the quadratic character of* $\mathrm{GF}(p^n)$.

Proof: From Theorem 3 it readily follows that Sidelnikov functions are (weakly) regular bent function for any nonzero $a \in \mathrm{GF}(p^n)$ (assume $j = n$). The exact values of the Walsh transform coefficients can be obtained using [4, Theorem 5.33] as following

$$S_a(b) = \sum_{x \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^2 - bx\right)} = \omega^{-\mathrm{Tr}_n\left(\frac{b^2}{4a}\right)} \eta(a) G(\eta, \chi_1) \ ,$$

where χ_1 is the canonical additive character of $\mathrm{GF}(p^n)$ and $G(\eta, \chi_1)$ is the Gaussian sum. By [4, Theorem 5.15],

$$G(\eta, \chi_1) = \begin{cases} (-1)^{n-1} p^{n/2}, & \text{if} \quad p \equiv 1 \pmod 4 \ , \\ (-1)^{n-1} i^n p^{n/2}, & \text{if} \quad p \equiv 3 \pmod 4 \ . \end{cases}$$

In particular, when n is even

$$S_a(b) = -\eta(a)(-1)^{\frac{(p-1)n}{4}} p^{n/2} \omega^{-\mathrm{Tr}_n\left(\frac{b^2}{4a}\right)} = \pm p^{n/2} \omega^{-\mathrm{Tr}_n\left(\frac{b^2}{4a}\right)}$$

and, depending on a, p and n, $f(x)$ can be regular or weakly regular. Alternatively, when n is odd

$$p^{-n/2} \omega^{\mathrm{Tr}_n\left(\frac{b^2}{4a}\right)} S_a(b) = \begin{cases} \eta(a), & \text{if} \quad p \equiv 1 \pmod 4 \ , \\ \eta(a)(-1)^{(n-1)/2} i, & \text{if} \quad p \equiv 3 \pmod 4 \end{cases}$$

and $f(x)$ can be regular or weakly regular in the first case and only weakly regular in the second. These identities completely agree with (2). □

Corollary 4 (p-ary Kasami [5]) *Let $n = 2k$ and $a \in \mathrm{GF}(p^n)$ for an odd prime p. Then the function $f(x) = \mathrm{Tr}_n\left(ax^{p^k+1}\right)$ is a weakly regular bent function if $a + a^{p^k} \neq 0$. Moreover, for $b \in \mathrm{GF}(p^n)$ the corresponding Walsh transform coefficient of $f(x)$ is equal to*

$$S_a(b) = -p^k \omega^{-\mathrm{Tr}_k\left(\frac{b^{p^k+1}}{a + a^{p^k}}\right)} \ .$$

Proof: It follows easily from Theorem 3 that our function is bent. Indeed, for $n = 2k$ and $j = k$ the condition opposite to (17) is $p^n - 1 \ \Big| \ \frac{p^n-1}{2} - i_0(p^k - 1)$. On the other hand, any nonzero $a = \xi^{i_0} \in \mathrm{GF}(p^n)$ satisfies $a + a^{p^k} = 0$ (which is equivalent to $a^{p^k-1} = -1$) if and only if $i_0(p^k - 1) \equiv \frac{p^n-1}{2} \pmod{(p^n - 1)}$.

For any nonzero $\alpha \in \mathrm{GF}(p^k)$ consider a square matrix H_α of size p^n whose rows and columns are indexed with the elements of $\mathrm{GF}(p^n)$ and the entry in row y and column x is defined as

$$H_\alpha(y, x) = \omega^{\mathrm{Tr}_k\left(\alpha(x-y)^{p^k+1}\right)}$$

with $x, y \in \mathrm{GF}(p^n)$. It was proved in [14, Theorem 4] (see also [11, Lemma 3.6]) that matrices H_α are Hadamard matrices having a constant row sum equal $-p^k$.

Therefore, the Walsh transform coefficient for the p-ary Kasami bent function evaluated at b is equal to

$$\begin{aligned} S_a(b) &= \sum_{x\in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^{p^k+1}-bx\right)} = \sum_{x\in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_k\left(\left(a+a^{p^k}\right)x^{p^k+1}-bx-b^{p^k}x^{p^k}\right)} \\ &= \sum_{x\in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_k\left(a_1(x-\beta)^{p^k+1}-a_1\beta^{p^k+1}\right)} \\ &= \omega^{-\mathrm{Tr}_k\left(a_1\beta^{p^k+1}\right)} \sum_{x\in \mathrm{GF}(p^n)} H_{a_1}(\beta,x) = -p^k\omega^{-\mathrm{Tr}_k\left(\frac{b^{p^k+1}}{a+a^{p^k}}\right)} \ , \end{aligned}$$

where $a_1 = a + a^{p^k} \neq 0$ and $b = a_1\beta^{p^k}$ and thus $\beta^{p^k+1} = \frac{b^{p^k+1}}{a_1^2}$. Thus, the p-ary Kasami function is a weakly regular bent function. □

The class of bent functions due to Kumar and Moreno is an immediate consequence of Theorem 3 as well.

Corollary 5 (Kumar, Moreno [3]) *Let $n = ek$ for an odd integer k and integer r in the range $1 \le r \le k$ with $\gcd(r,k) = 1$. Then the function $f(x) = \mathrm{Tr}_n\left(ax^{p^{er}+1}\right)$ is a (weakly) regular bent function for any nonzero $a \in \mathrm{GF}(p^n)$ and odd prime p.*

Proof: If $n = ek$ and $j = er$ then $\gcd(2j,n) = \gcd(2er,ek) = e\gcd(2r,k) = e$. The condition opposite to (17) looks like $p^e - 1 \ \Big|\ \frac{p^{ek}-1}{2} - i_0(p^{er}-1)$ that is equivalent to $p^e - 1 \ \Big|\ \frac{p^{ek}-1}{2}$ and holds if and only if $\frac{p^{ek}-1}{p^e-1}$ is even. However, $\frac{p^{ek}-1}{p^e-1} = p^{(k-1)e} + p^{(k-2)e} + \cdots + 1 \equiv k \pmod 2$ since p is odd and k is odd. □

The following corollary contains an equivalent definition of the Kumar-Moreno class of p-ary bent functions that appeared in [16, Definition 7.5]. Note that if $\frac{n}{\gcd(j,n)}$ is odd (as required in Corollary 6) then $\frac{n}{\gcd(2j,n)}$ is odd as well and this is a condition of Corollary 2. Moreover, if one of the following equivalent conditions is fulfilled - either $\gcd(2j,n)$ divides j or $\frac{n}{\gcd(j,n)}$ is odd or $\gcd(2j,n) = \gcd(j,n)$ (in particular, this is true for an odd n) then (17) is equivalent to $p^{\gcd(j,n)} - 1 \not\Big|\ \frac{p^n-1}{2}$ which holds if and only if $\frac{p^n-1}{p^{\gcd(j,n)}-1}$ is odd. By (18), $\frac{p^n-1}{p^{\gcd(j,n)}-1} \equiv \frac{n}{\gcd(j,n)} \equiv 1 \pmod 2$. Thus, (17) holds for any nonzero $a \in \mathrm{GF}(p^n)$ and $j \in \{1,\ldots,n\}$ meaning that all monomial quadratic bent functions in this case are of the Kumar-Moreno type.

Corollary 6 ([16]) *Let j be an integer with $1 \le j \le n$ such that $\frac{n}{\gcd(j,n)}$ is odd. Then the function $f(x) = \mathrm{Tr}_n\left(ax^{p^j+1}\right)$ is a (weakly) regular bent function for any nonzero $a \in \mathrm{GF}(p^n)$ and odd prime p. Moreover, for $b \in \mathrm{GF}(p^n)$ the magnitude of $S_a(b)$ is equal to*

$$\omega^{-f^*(b)}S_a(b) = \begin{cases} \eta(a)(-1)^{n-1}p^{n/2}, & \text{if} \quad p \equiv 1 \pmod 4 \ , \\ \eta(a)(-1)^{n-1}i^n p^{n/2}, & \text{if} \quad p \equiv 3 \pmod 4 \ , \end{cases}$$

where i is the complex primitive 4^{th} root of unity and η is the quadratic character of $\mathrm{GF}(p^n)$.

Proof: We will prove that the conditions of Corollaries 5 and 6 are equivalent. Denote $e = \gcd(j, n)$ and $k = n/e$ that is odd under the hypothesis. Since e divides j, let $j = er$ with $\gcd(r, k) = 1$. Finally, the requirement $1 \le j \le n$ guarantees that $1 \le r \le k$.

Since $\frac{n}{\gcd(j,n)}$ is odd it can be concluded that $v(n) \le v(j)$. Thus, we get in the conditions of Lemma 5 Item (i) that gives us the magnitude of $S_a(b)$. □

Note 1 *Recall that conditions of Theorem 3 allow the values of j in the range $\{1, \ldots, n\}$. On the other hand, if $n = 2k + 1$ or $n = 2k$ then for any $j > k$ we can write $(p^j + 1)p^{n-j} = p^n + p^{n-j} \equiv p^{n-j} + 1 \pmod{p^n - 1}$. Thus, exponents $p^j + 1$ and $p^{n-j} + 1$ are cyclotomic equivalent and we can assume j be in the range $\{0, \ldots, k\}$.*

Note 2 *The only known to us example of a monomial p-ary bent function that is not covered in Theorem 2, Conjecture 1, Theorem 3 and Fact 1 is the ternary case proved by Coulter-Matthews in [7, Theorem 4.1]. Namely, they showed that polynomial $F(x) = x^{\frac{3^k+1}{2}}$ is planar over $\mathrm{GF}(3^n)$ if and only if $\gcd(k, n) = 1$ and k is odd. By the definition, $F(x)$ is* planar *if for any nonzero $c \in \mathrm{GF}(3^n)$ the function $F(x+c) - F(x)$ is a bijection over $\mathrm{GF}(3^n)$. Therefore, for any nonzero $a \in \mathrm{GF}(3^n)$ the absolute square of the Walsh transform coefficient of $\mathrm{Tr}_n(aF(x))$ evaluated at b is equal to*

$$\begin{aligned} |S_a(b)|^2 &= \sum_{x,y \in \mathrm{GF}(3^n)} \omega^{\mathrm{Tr}_n(a(F(x)-F(y))+b(y-x))} \\ &= \sum_{z \in \mathrm{GF}(3^n)} \omega^{\mathrm{Tr}_n(bz)} \sum_{y \in \mathrm{GF}(3^n)} \omega^{\mathrm{Tr}_n(a(F(y-z)-F(y)))} = 3^n \ , \end{aligned}$$

where $z = y - x$ and since $\sum_{y \in \mathrm{GF}(3^n)} \omega^{\mathrm{Tr}_n(a(F(y-z)-F(y)))} = 0$ for any nonzero z and a with planar $F(x)$. Consequently, for any nonzero $a \in \mathrm{GF}(3^n)$ the function $\mathrm{Tr}_n\left(ax^{\frac{3^k+1}{2}}\right)$ over $\mathrm{GF}(3^n)$ is bent if $\gcd(k, n) = 1$ and k is odd.

The term "planar functions" is typical for the area of finite geometries while such functions elsewhere are called perfect nonlinear. *It is known that function $F(x)$ mapping $\mathrm{GF}(p^n)$ to itself is perfect nonlinear if and only if for every nonzero $a \in \mathrm{GF}(p^n)$ the function $aF(x)$ is generalized bent (see [17, Remark 2.2]). Therefore, Sidelnikov, Kumar-Moreno and Coulter-Matthews functions appear to be perfect nonlinear. It is also known that $F(x) = x^{10} + x^6 - x^2$ is a perfect nonlinear function over $\mathrm{GF}(3^n)$ when n is odd or $n = 2$ (see [7, Theorem 3.4]). Moreover, up to equivalence, these are all currently known perfect nonlinear functions from $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p^n)$ for an odd prime p.*

5 Quadratic Bent Functions

First multinomial p-ary bent functions were constructed from the planar function found in [7, Theorem 3.4]. These bent functions are ternary and quadratic having the form $f(x) = \mathrm{Tr}_n\left(a(x^{10} + x^6 - x^2)\right)$ with arbitrary nonzero $a \in \mathrm{GF}(p^n)$ when n is odd or $n = 2$ (see Note 2). Recently, another class of quadratic functions was discovered and presented in [6] with the proof that was based on such a powerful tool as Deligne's theorem. These are the only known examples of multinomial bent

functions. In this section we prove two criteria for an arbitrary quadratic function over $\mathrm{GF}(p^n)$ to be bent and show that all quadratic bent function are (weakly) regular. Results from [6] are covered as a special case while the technique we use here is much easier. At the same time we point out and fix an inaccuracy found in the proof of Theorem 2 in [6]. An alternative approach using Deligne's theorem is presented in Appendix A.

Any function $F(x)$ mapping $\mathrm{GF}(p^n)$ to itself has a unique representation as a univariate polynomial over $\mathrm{GF}(p^n)$ of degree smaller than p^n, i.e., $F(x) = \sum_{i=0}^{p^n-1} a_i x^i$ with $a_i \in \mathrm{GF}(p^n)$. Besides, if $\mathrm{GF}(p^n)$ is identified with the n-dimensional vector space over $\mathrm{GF}(p)$ then $F(x)$ can also be uniquely represented as a polynomial of n p-ary variables and coefficients in $\mathrm{GF}(p^n)$ that is called the *Algebraic Normal Form* (ANF) of $F(x)$. The degree of such a multivariate polynomial is called the *algebraic degree* of $F(x)$.

Assume $f(x) = \mathrm{Tr}_n(F(x))$. Then the ANF of $f(x)$ (i.e., polynomial of n p-ary variables with coefficients in $\mathrm{GF}(p)$ representing $f(x)$) can be obtained from the ANF of $F(x)$ by substituting the coefficients in $\mathrm{GF}(p^n)$ with their traces in $\mathrm{GF}(p)$. Thus, if function $F(x)$ is quadratic then $f(x)$ is either quadratic or linear. On the other hand, function $f(x)$ can be quadratic even if $F(x)$ has the algebraic degree bigger than 2 (coefficients at the high-order terms may all have a zero trace). Using the theory of quadratic forms it is easy to prove that there exist at most $n+1$ quadratic bent functions mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$ that are not equivalent under the affine transformation of variables.

For any integer $d \in \{0, \ldots, p^n - 1\}$ let $\sum_{i=0}^{n-1} p^i d_i$ with $0 \le d_i \le p-1$ be its p-ary expansion, then the number $w_p(d) = d_0 + \cdots + d_{n-1}$ is called the *p-weight* of d. It is well known that the algebraic degree of $F(x)$ is equal to the maximal p-weight of the exponent i in the univariate polynomial of $F(x)$ with $a_i \neq 0$. In particular, if p is odd then quadratic functions (having no linear terms) are all expanded as

$$F(x) = \sum_{j=0}^{n-1} \sum_{i=j}^{n-1} a_{ij} x^{p^i + p^j} \quad \text{with} \quad a_{ij} \in \mathrm{GF}(p^n) \ .$$

Note that for $i \ge j$ exponents $p^i + p^j$ and $p^{i-j} + 1$ are cyclotomic equivalent and we can assume that $f(x) = \mathrm{Tr}_n\big(\sum_{i=0}^{n-1} a_i x^{p^i+1}\big)$. Moreover, recalling our Note 1 in Section 4, we can also assume i be in the range $\{0, \ldots, k\}$ if $n = 2k+1$ or $n = 2k$. Therefore, Proposition 2 covers all the quadratic cases having the form $f(x) = \mathrm{Tr}_n(F(x))$ with a quadratic function $F(x)$.

Proposition 1 *Any quadratic p-ary function $f(x)$ mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$ is bent if and only if the quadratic form associated with f is nondegenerate. Moreover all quadratic p-ary bent functions are (weakly) regular.*

Proof: Choose and fix a basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathrm{GF}(p^n)$ over $\mathrm{GF}(p)$ and let $x = \sum_{i=1}^{n} \alpha_i x_i$ be the expansion of x in this basis. The boldface $\vec{x} = (x_1, \ldots, x_n)^T \in \mathrm{GF}(p)^n$, where the superscript T denotes the transpose of a matrix, is used to denote the coefficients of this expansion. Take a quadratic p-ary function $f(x)$ represented by its ANF. Then f is equal to the sum of a quadratic form and an affine part. Let A be the coefficient matrix of the quadratic form associated with f. If p is odd then A can be made symmetric and we can write $f(\vec{x}) = \vec{x}^T A \vec{x} + \mathrm{Tr}_n(lx) + \epsilon$ for some $l \in \mathrm{GF}(p^n)$ and $\epsilon \in \mathrm{GF}(p)$. It is obvious that if we take $g(\vec{x}) = \vec{x}^T A \vec{x}$ then $S_f(b) = \omega^\epsilon S_g(b-l)$ and f is a (weakly regular) bent function if and only if such is function g. Therefore, it can be assumed that the affine part in f is zero. Consider

the set of equations $f(x) - \mathrm{Tr}_n(bx) = j$ for all $j \in \mathrm{GF}(p)$ and a fixed $b \in \mathrm{GF}(p^n)$. We can write these as follows

$$\vec{x}^T A\vec{x} - (\mathrm{Tr}_n(b\alpha_1), \ldots, \mathrm{Tr}_n(b\alpha_n))\vec{x} = \vec{x}^T A\vec{x} + c^T\vec{x} = j \ , \tag{19}$$

where $c \in \mathrm{GF}(p)^n$. Denote the number of solutions of (19) by $N_b(j)$.

According to [4, Theorem 6.21], any quadratic form over $\mathrm{GF}(p)$ with an odd p is equivalent to a diagonal quadratic form. This means that there exists a nonsingular matrix C over $\mathrm{GF}(p)$ such that $C^T AC = D = \mathrm{diag}\{d_1, \ldots, d_n\}$ is a diagonal matrix containing the elements $d_1, \ldots, d_n$ on the main diagonal. If the substitution $\vec{x} = C\vec{y}$ is made in (19) then we get $\vec{y}^T D\vec{y} + c^T C\vec{y} = \sum_{i=1}^n (d_i y_i^2 + c_i y_i) = j$, where $c^T C = (c_1, \ldots, c_n)^T \in \mathrm{GF}(p)^n$. Finally, making a substitution $y_i = z_i - \frac{c_i}{2d_i}$ we get $\sum_{i=1}^n d_i z_i^2 = j + \sum_{i=1}^n \frac{c_i^2}{4d_i}$. This equation has the same number of solutions as (19).

Define $f^*(b) = -\sum_{i=1}^n \frac{c_i^2}{4d_i}$. Assume that the quadratic form associated with f is nondegenerate, i.e., $\det(f) = \det(A) \neq 0$. Consider separately two cases. First let n be even. Then, by [4, Theorem 6.26], for a fixed b the values of $N_b(j)$ are all equal except for $N(f^*(b))$ that differs from the rest by $\left(\frac{(-1)^{n/2}\Delta}{p}\right)p^{n/2}$, where $\Delta = \det(D) = d_1 \cdot \cdots \cdot d_n$. Therefore, by (1),

$$S_f(b) = \left(\frac{(-1)^{n/2}\Delta}{p}\right)p^{n/2}\omega^{f^*(b)} = \left(\frac{\Delta}{p}\right)(-1)^{\frac{(p-1)n}{4}}p^{n/2}\omega^{f^*(b)} \ ,$$

since $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ (obviously, $-1 = q^{(p-1)/2}$ is a square modulo p if and only if $(p-1)/2$ is even, where q is a positive integer coprime to p). On the other hand, when n is odd then by (1) and [4, Theorem 6.27],

$$\begin{aligned} S_f(b) &= \sum_{j=0}^{p-1}\left(p^{n-1} + \left(\frac{(j - f^*(b))(-1)^{(n-1)/2}\Delta}{p}\right)p^{(n-1)/2}\right)\omega^j \\ &\overset{(3)}{=} i^{s(p)}\left(\frac{(-1)^{(n-1)/2}\Delta}{p}\right)p^{n/2}\omega^{f^*(b)} = i^{s(p)}\left(\frac{\Delta}{p}\right)(-1)^{\frac{(p-1)(n-1)}{4}}p^{n/2}\omega^{f^*(b)} \ , \end{aligned}$$

where $s(p) = 0$ if $p \equiv 1 \pmod 4$ and $s(p) = 1$ otherwise. These identities completely agree with (2) and prove that f is a bent function. The sign of $S_f(b)$ does not depend on b which means that f is a (weakly) regular bent function.

It remains to prove that a quadratic function f consisting of a degenerate quadratic form is not bent. Indeed, let $l < n$ be the rank of the quadratic form that is equal to the rank of A and D. Then the above equations for $S_f(b)$ also hold if we take l instead of n and multiply the right hand sides by p^{n-l}. This way we get $|S_f(b)| = p^{l/2}p^{n-l} = p^{(2n-l)/2}$ that is never equal $p^{n/2}$ unless $l = n$. □

For any quadratic p-ary bent function f let A be the coefficient matrix of the quadratic form associated with f. Define the determinant of f (denoted as $\det(f)$) being equal to the determinant of A. Defined in such a way, $\det(f)$ is nonzero and depends on the basis of $\mathrm{GF}(p^n)$ over $\mathrm{GF}(p)$ that we choose to represent f. Changing from one basis to another results in equivalent transformations of the quadratic form of f giving a new quadratic form with the coefficient matrix $C^T AC$ for some nonsingular matrix C. Therefore, the value of $\left(\frac{\det(f)}{p}\right)$ is independent of the basis since $\det(C^T AC) = \det(C)^2 \det(A)$. Thus, $\det(f)$ can be used instead of Δ in the formulas for $S_f(b)$ in Proposition 1. Comparing these identities with

Lemma 5 we get that for any quadratic bent function $f(x) = \mathrm{Tr}_n\big(ax^{p^j+1}\big)$ with $j \in \{1, \ldots, n\}$ and nonzero $a \in \mathrm{GF}(p^n)$ we have

$$\left(\frac{\det(f)}{p}\right) = \begin{cases} \eta(a)(-1)^{n-1}, & \text{if} \quad v(n) \le v(j)\ , \\ -(-1)^{(p-1)n/4}, & \text{if} \quad v(n) = v(j)+1\ , \\ (-1)^{(p-1)n/4}, & \text{if} \quad v(n) > v(j)+1\ , \end{cases}$$

where η is the quadratic character of $\mathrm{GF}(p^n)$ and $v(b)$ is the (additive) 2-adic valuation of integer b.

Proposition 2 *Let $n = 2k+1$ or $n = 2k$ and $a_i \in \mathrm{GF}(p^n)$ $(i = 0, \ldots, k)$ for an odd prime p. Then the quadratic p-ary function $f(x)$ mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$ and given by*

$$f(x) = \mathrm{Tr}_n\Big(\sum_{i=0}^{k} a_i x^{p^i+1}\Big) \tag{20}$$

is bent if and only if the following $n \times n$ matrix is nonsingular when $n = 2k+1$

$$\begin{pmatrix} 2a_0 & a_1 & \ldots & a_k & a_k^{p^{k+1}} & a_{k-1}^{p^{k+2}} & \ldots & a_2^{p^{2k-1}} & a_1^{p^{2k}} \\ a_1 & 2a_0^p & \ldots & a_{k-1}^p & a_k^p & a_k^{p^{k+2}} & \ldots & a_3^{p^{2k-1}} & a_2^{p^{2k}} \\ & & \ldots & & & & \ldots & & \\ a_2^{p^{2k-1}} & a_3^{p^{2k-1}} & \ldots & a_{k-1}^{p^k} & a_{k-2}^{p^{k+1}} & a_{k-3}^{p^{k+2}} & \ldots & 2a_0^{p^{2k-1}} & a_1^{p^{2k-1}} \\ a_1^{p^{2k}} & a_2^{p^{2k}} & \ldots & a_k^{p^k} & a_{k-1}^{p^{k+1}} & a_{k-2}^{p^{k+2}} & \ldots & a_1^{p^{2k-1}} & 2a_0^{p^{2k}} \end{pmatrix} \tag{21}$$

or the following $n \times n$ matrix is nonsingular when $n = 2k$

$$\begin{pmatrix} 2a_0 & a_1 & \ldots & a_{k-1} & a_k + a_k^{p^k} & a_{k-1}^{p^{k+1}} & \ldots & a_2^{p^{2k-2}} & a_1^{p^{2k-1}} \\ a_1 & 2a_0^p & \ldots & a_{k-2}^p & a_{k-1}^p & a_k^p + a_k^{p^{k+1}} & \ldots & a_3^{p^{2k-2}} & a_2^{p^{2k-1}} \\ & & \ldots & & & & \ldots & & \\ a_2^{p^{2k-2}} & a_3^{p^{2k-2}} & \ldots & a_{k-1}^{p^{k-1}} & a_{k-2}^{p^k} & a_{k-3}^{p^{k+1}} & \ldots & 2a_0^{p^{2k-2}} & a_1^{p^{2k-2}} \\ a_1^{p^{2k-1}} & a_2^{p^{2k-1}} & \ldots & a_k^{p^{2k-1}} + a_k^{p^{k-1}} & a_{k-1}^{p^k} & a_{k-2}^{p^{k+1}} & \ldots & a_1^{p^{2k-2}} & 2a_0^{p^{2k-1}} \end{pmatrix}.$$

Moreover, if this holds then $f(x)$ is a (weakly) regular bent function.

Proof: We prove this result using a similar, squaring technique as in the proof of Theorem 3. For any p-ary function $f(x)$ the absolute square of its Walsh transform coefficient evaluated at $-b$ is equal to

$$\begin{aligned} |S_f(-b)|^2 &= \sum_{x,y \in \mathrm{GF}(p^n)} \omega^{f(x)-f(y)+\mathrm{Tr}_n(b(x-y))} = \sum_{y,z \in \mathrm{GF}(p^n)} \omega^{f(y+z)-f(y)+\mathrm{Tr}_n(bz)} \\ &= \sum_{z \in \mathrm{GF}(p^n)} \omega^{f(z)+\mathrm{Tr}_n(bz)} \sum_{y \in \mathrm{GF}(p^n)} \omega^{f(y+z)-f(y)-f(z)}\ , \end{aligned}$$

where $z = x - y$. Now

$$\begin{aligned} f(y+z) - f(y) - f(z) &= \mathrm{Tr}_n\left(\sum_{i=0}^{k} a_i \left((y+z)^{p^i+1} - y^{p^i+1} - z^{p^i+1}\right)\right) \\ &= \mathrm{Tr}_n\left(\sum_{i=0}^{k} a_i \left(yz^{p^i} + y^{p^i} z\right)\right) = \mathrm{Tr}_n\left(y \sum_{i=0}^{k} \left(a_i z^{p^i} + a_i^{p^{n-i}} z^{p^{n-i}}\right)\right) \\ &= \mathrm{Tr}_n(yL(z))\ , \end{aligned}$$

denoting a linearized polynomial $L(z) = \sum_{i=0}^{k} \left(a_i z^{p^i} + a_i^{p^{n-i}} z^{p^{n-i}} \right)$. If $\mathrm{GF}(p^n)$ is viewed as an n-dimensional vector space over $\mathrm{GF}(p)$ then $L(z)$ defines a linear transformation of $\mathrm{GF}(p)^n$. Let the dimension of the kernel of L be l. Then,

$$|S_f(-b)|^2 = \sum_{z \in \mathrm{GF}(p^n)} \omega^{f(z)+\mathrm{Tr}_n(bz)} \sum_{y \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n(yL(z))}$$
$$= p^n \sum_{z\,:\,L(z)=0} \omega^{f(z)+\mathrm{Tr}_n(bz)} = \begin{cases} p^{n+l}, & \text{if } f(z)+\mathrm{Tr}_n(bz) \equiv 0 \text{ on} \ker L\ , \\ 0, & \text{otherwise}\ , \end{cases}$$

since $f(z) + \mathrm{Tr}_n(bz)$ is linear on the kernel of L. Therefore, $f(x)$ is bent if and only if $l = 0$. Moreover, by Proposition 1, it is a (weakly) regular bent function. Finally, by [18, Proposition 2.1], $n - l$ is equal to the rank of matrix (21). □

Particular cases of Proposition 2 provide necessary and sufficient conditions for a quadratic monomial function to be bent. In particular, assuming that $a_0 \neq 0$ in (20) and the rest of the coefficients are all zero leads to the Sidelnikov bent functions (see Corollary 3). In this case the corresponding matrix (21) has a diagonal form $\mathrm{diag}\big(2a_0, 2a_0^p, \ldots, 2a_0^{p^{n-1}}\big)$ and is obviously nonsingular. Assuming that $n = 2k$, $a_k \neq 0$ and the rest of the coefficients are all zero leads to the Kasami case (see Corollary 4). Then the corresponding matrix (21) is nonsingular if and only if $a_k + a_k^{p^k} \neq 0$. To handle the remaining monomial cases we need the following lemma.

Lemma 6 *Take a square matrix M of size n which rows and columns are indexed by integers modulo n. Let M contain nonzero elements only on the main diagonal so that $M(i,i) = a_i$ and on the other diagonal so that $M(i, i+m \pmod n) = b_i$ $(i = 0, \ldots, n-1)$ for some positive $m < n$. Then the determinant of M is equal to*

$$\det M = \prod_{i=0}^{d-1} \left(\prod_{j=0}^{n/d-1} a_{i+jd} + (-1)^{\frac{m(n-m)}{d^2}} \prod_{j=0}^{n/d-1} b_{i+jd} \right)\ ,$$

where $d = \gcd(n, m)$ and all the indices are calculated modulo n.

Proof: To prove this fact we apply induction on d. For any $0 < t \leq n$ and two sets of indices $\{i_1, \ldots, i_t\}$ $\{j_1, \ldots, j_t\}$ lying in the range $\{0, \ldots, n-1\}$ let $M_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$ denote the submatrix of M that lies in the intersections of rows number $i_1, \ldots, i_t$ and columns number $j_1, \ldots, j_t$; let also $\overline{M}_{i_1,\ldots,i_t}^{j_1,\ldots,j_t}$ denote the submatrix of M obtained by deleting rows number $i_1, \ldots, i_t$ and columns number $j_1, \ldots, j_t$. First, let $d = \gcd(n, m) = 1$. Expanding the determinant of M by minors along the 0^{th} row we get

$$\begin{aligned} \det M &= a_0 \det \overline{M}_0^0 \pm b_0 \det \overline{M}_0^m = a_0 a_{-m} \det \overline{M}_{0,-m}^{0,-m} \pm b_0 b_m \det \overline{M}_{0,m}^{m,2m} = \ldots \\ &= \prod_{j=0}^{n-1} a_{-jm} \pm \prod_{j=0}^{n-1} b_{jm} = \prod_{j=0}^{n-1} a_j + (-1)^{m(n-m)} \prod_{j=0}^{n-1} b_j\ , \end{aligned}$$

where all the indices are calculated modulo n and since each of the considered submatrices contains a row consisting of just one nonzero element. The sign of the second term in the sum is equal to the parity of the permutation $(m, m+1, \ldots, n-1, 0, 1, \ldots, m-1)$.

Now, assuming that the formula is true for $d = l - 1$, we prove it for $d = l$. Expand the determinant of M by minors along n/d rows number $0, d, 2d, \ldots, n-d$. It is easy to see that the only nonsingular submatrix of M lying in these rows is $M^{0,d,\ldots,n-d}_{0,d,\ldots,n-d}$. It is also clear that this submatrix has a similar two-diagonal structure as M and the distance between the diagonals here is m/d which is coprime to the size n/d. Thus, using the basis of induction

$$\det M^{0,d,\ldots,n-d}_{0,d,\ldots,n-d} = \prod_{j=0}^{n/d-1} a_{jd} + (-1)^{\frac{m(n-m)}{d^2}} \prod_{j=0}^{n/d-1} b_{jd} \ .$$

On the other hand, $\overline{M}^{0,d,\ldots,n-d}_{0,d,\ldots,n-d}$ is also similar to M but has the size $n - n/d$ and the distance between the diagonals $m - m/d$ with $\gcd(n - n/d, m - m/d) = (d-1)\gcd(n/d, m/d) = d - 1$. Also note that each of the two nonzero diagonals in $\overline{M}^{0,d,\ldots,n-d}_{0,d,\ldots,n-d}$ is obtained from the corresponding diagonal in M just by deleting the elements a_i or b_i with $i \in \{0, d, 2d, \ldots, n-d\}$. Thus, decimating a nonzero diagonal in $\overline{M}^{0,d,\ldots,n-d}_{0,d,\ldots,n-d}$ with the step $d-1$ we get the same sequence of elements as decimating the corresponding diagonal in M with the step d starting from a_1 or b_1. By the induction hypothesis we conclude that

$$\det \overline{M}^{0,d,\ldots,n-d}_{0,d,\ldots,n-d} = \prod_{i=1}^{d-1} \left(\prod_{j=0}^{n/d-1} a_{i+jd} + (-1)^{\frac{m(n-m)}{d^2}} \prod_{j=0}^{n/d-1} b_{i+jd} \right) \ ,$$

Finally,

$$\det M = \det M^{0,d,\ldots,n-d}_{0,d,\ldots,n-d} \det \overline{M}^{0,d,\ldots,n-d}_{0,d,\ldots,n-d}$$

and this leads to the claimed formula. □

Now assume that $a_t \neq 0$ in (20) for some $0 < t \leq k$ with $t \neq k$ if $n = 2k$. Further we omit the index t and just write a instead of a_t. If M denotes the corresponding matrix (21) then $M(i, i+t) = a^{p^i}$ and $M(i, i-t) = a^{p^{i-t}}$ $(i = 0, \ldots, n-1)$ and the rest of the elements in M are all zero. With $t(n-1)$ column permutations M can be transformed into the kind of a matrix analyzed in Lemma 6 with $m = n - 2t$, $a_i = a^{p^i}$ and $b_i = a^{p^{i-t}}$. Then

$$\det M = (-1)^{t(n-1)} \prod_{i=0}^{d-1} \left(\prod_{j=0}^{n/d-1} a^{p^{i+jd}} + (-1)^{\frac{2t(n-2t)}{d^2}} \prod_{j=0}^{n/d-1} a^{p^{i+jd-t}} \right) \ ,$$

where $d = \gcd(n, n-2t) = \gcd(n, 2t)$ and all the powers of p are calculated modulo n.

Consider separately three cases as we did earlier in Theorem 3 when proving that condition (17) is necessary. Assume first that $v(n) \leq v(t)$ which is equivalent to $d \mid t$ and to $\frac{n}{\gcd(t,n)}$ is odd. Then

$$\det M = (-1)^{t(n-1)} \prod_{i=0}^{d-1} \left(2 \prod_{j=0}^{n/d-1} a^{p^{i+jd}} \right) = (-1)^{t(n-1)} 2^d a^{\frac{p^n-1}{p-1}} \neq 0 \ ,$$

that proves the existence of the Kumar-Moreno class of bent functions (see Corollary 6).

Otherwise, if $v(n) > v(t)$ or equivalently $d \nmid t$ then d is even and $d/2 = \gcd(n,t)$ divides t. This also means that n is even and $2t/d$ is odd. Then

$$\begin{aligned}
\det M &= (-1)^t \prod_{i=0}^{d-1} \left(\prod_{j=0}^{n/d-1} a^{p^{i+jd}} + (-1)^{n/d+1} \prod_{j=0}^{n/d-1} a^{p^{i+jd+d/2}} \right) \\
&= (-1)^{t+\frac{n+d}{2}} \prod_{i=0}^{d/2-1} \left(\prod_{j=0}^{n/d-1} a^{p^{i+jd}} + (-1)^{n/d+1} \prod_{j=0}^{n/d-1} a^{p^{i+jd+d/2}} \right)^2 \\
&= (-1)^{t+\frac{n+d}{2}} \prod_{i=0}^{d/2-1} \prod_{j=0}^{n/d-1} a^{2p^{i+jd}} \left(1 + (-1)^{n/d+1} \prod_{e=0}^{n/d-1} a^{p^{i+ed}(p^{d/2}-1)} \right)^2
\end{aligned}$$

and $\det M = 0$ if and only if $a^{p^i(p^{d/2}-1)\frac{p^n-1}{p^d-1}} = (-1)^{n/d}$. If ξ is a primitive element of $\mathrm{GF}(p^n)$ and $a = \xi^{i_0}$ then the latter identity is equivalent to

$$i_0 p^i \frac{p^n-1}{p^{d/2}+1} \equiv \frac{n(p^n-1)}{2d} \pmod{p^n-1} \ . \tag{22}$$

Now assume additionally that $v(n) > v(t)+1$ or equivalently n/d is even. Then (22) holds if and only if $p^n - 1$ divides $i_0 \frac{p^n-1}{p^{d/2}+1}$ that is equivalent to $(p^{d/2}+1) \mid i_0$. Finally, assume that $v(n) = v(t)+1$. Then n/d is odd and (22) holds if and only if $p^n - 1$ divides $i_0 p^i \frac{p^n-1}{p^{d/2}+1} - \frac{p^n-1}{2}$ that is equivalent to $(p^{d/2}+1)/2 \mid i_0$ together with $\frac{2i_0}{p^{d/2}+1}$ being odd. Note that in both of these cases the resulting conditions guaranteeing nonsingular M were earlier proved to be equivalent to (17) (see the last two paragraphs in the proof of Theorem 3). Therefore, criteria for quadratic monomial functions to be bent provided by Theorem 3 and Proposition 2 are equivalent.

We have to mention a minor mistake made in the final part of the proof of Theorem 2 in [6] that invalidated Corollary 1 in that paper as well. Instead of the complex primitive root of unity (as stated in [6, Theorem 2]) a primitive root of unity over $\mathrm{GF}(p)$ has to be used. Therefore, some additional conditions that guarantee the existence of such a root should be imposed (see the following Corollary 7). Our Corollary 8 gives a general, although more complicated, condition in terms of the algebraic number fields.

Corollary 7 ([6]) *Given the conditions of Proposition 2, assume that n is not divisible by p and $a_i \in \mathrm{GF}(p)$ $(i = 0, \ldots, k)$. Then (20) is a (weakly) regular bent function if and only if*

$$\sum_{i=0}^{k} a_i \left(\zeta^{il} + \zeta^{-il} \right) \neq 0 \quad \textit{for all} \quad l = 0, \ldots, n-1 \ , \tag{23}$$

where ζ is a primitive n^{th} root of unity over $\mathrm{GF}(p)$.

Proof: Note that matrix (21) is equal to $\sum_{i=0}^{k} a_i \left(A^i + A^{-i} \right)$, where A is a permutation matrix of the n-cycle. It is known [4, p. 64] that a primitive n^{th} root of unity ζ over $\mathrm{GF}(p)$ exists if n is not divisible by p. If this holds then exactly in the same way as if A was a matrix over complex numbers it can be proved that the eigenvalues of A are ζ^l $(l = 0, \ldots, n-1)$. Thus, the eigenvalues of (21) are $\sum_{i=0}^{k} a_i \left(\zeta^{il} + \zeta^{-il} \right)$ for $l = 0, \ldots, n-1$. □

The question about function (20) being bent can also be approached from the coding theory point of view if the conditions of Corollary 7 hold. Note that rows of matrix (21) span a cyclic (n, κ) code C having dimension κ equal to the rank of (21). The codewords in C can also be represented as polynomials over GF(p) of degree $< n$ modulo $x^n - 1$. The first row in (21) corresponds to the polynomial $c(x) = 2a_0 + \sum_{i=1}^{k} a_i \left(x^i + x^{n-i}\right)$. It is well known (see, for instance, [4]) that there exists a unique monic polynomial $g(x)$ (generator polynomial) such that $\kappa = n - \deg(g(x))$ and in our case $g(x) = \gcd(c(x), x^n - 1)$. Therefore, function (20) is bent if and only if matrix (21) has a full rank that is equivalent to

$$\gcd\left(2a_0 + \sum_{i=1}^{k} a_i \left(x^i + x^{n-i}\right), x^n - 1\right) = 1 \ .$$

It is obvious that the latter condition is equivalent to (23).

Note that $x^n - 1$ factors as $(x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$. Thus, the necessary condition for function (20) to be bent is $c(1) = 2\sum_{i=0}^{k} a_i \not\equiv 0 \pmod{p}$ or equivalently $\sum_{i=0}^{k} a_i \not\equiv 0 \pmod{p}$. Assume that n is prime and $p \neq n$. Then $Q_n(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$ is exactly the nth cyclotomic polynomial over GF(p). If the multiplicative order of p modulo n is $n-1$ then $Q_n(x)$ is irreducible. Therefore, if n is prime, $p \neq n$ and the multiplicative order of p modulo n is $n-1$ then function (20) is bent if and only if $\sum_{i=0}^{k} a_i \not\equiv 0 \pmod{p}$ and $c(x) \neq Q_n(x)$. Basic facts about the roots of unity and cyclotomic polynomials can be found in [4].

Corollary 8 *Given the conditions of Proposition 2, let $a_i \in$ GF(p) $(i = 0, \ldots, k)$. Then (20) is a (weakly) regular bent function if and only if*

$$\prod_{l=0}^{n-1} \sum_{i=0}^{k} a_i \left(\epsilon^{il} + \epsilon^{-il}\right) \not\equiv 0 \pmod{p\mathbf{Z}[\epsilon]} \ ,$$

where $\epsilon = e^{\frac{2\pi i}{n}}$ is the complex primitive n^{th} root of unity, a_i $(i = 0, \ldots, k)$ are considered as integers in the range $[0, \ldots, p-1]$ and the left hand side of the identity is treated as an element in $\mathbf{Z}[\epsilon]$.

Proof: Like in Corollary 7, matrix (21) under our conditions is circulant over GF(p). It is well known [9, p. 72] that the determinant of an $(n \times n)$ *complex-valued* circulant matrix that is defined by the set of elements $[c_1, \ldots, c_n]$ is equal to $\prod_{l=0}^{n-1} \left(c_1 + c_2\epsilon^l + c_3\epsilon^{2l} + \cdots + c_n\epsilon^{(n-1)l}\right)$. Now we can embed the elements of GF(p) into the complex numbers, evaluate the complex circulant determinant and finally reduce the integer result modulo p (i.e., modulo the principal ideal $p\mathbf{Z}[\epsilon]$) to get the correct determinant in GF(p). The rest follows immediately considering specific form of (21). □

6 Computational Details and Conclusion

By choosing and fixing a basis of GF(p^n) over GF(p) we can identify GF(p^n) with the n-dimensional vector space over GF(p). It is well known that any function $f(x)$ mapping GF$(p)^n$ to GF(p) has a unique representation as a polynomial of n

p-ary variables with coefficients in $\mathrm{GF}(p)$ known as the ANF of $f(x)$. The degree of the ANF is equal to the algebraic degree of $f(x)$. The maximal algebraic degree of a p-ary bent function is not known. The upper estimate proved recently in [2, Proposition 4.4] is currently the best. Namely, if f is a p-ary bent function then

$$\deg f \le \frac{(p-1)n}{2} + 1 \ .$$

Moreover, if f is a weakly regular bent function then, by [2, Proposition 4.5],

$$\deg f \le \frac{(p-1)n}{2} \ .$$

This estimate appears to be very helpful when screening the exponents of prospective bent functions. Doing this we use the following proposition that adapts the well known estimate [16, p. 1799] for the algebraic degree of Boolean power functions to the case of odd characteristic.

Proposition 3 *The p-ary function mapping $\mathrm{GF}(p)^n$ to $\mathrm{GF}(p)$ and defined by $f(x) = \mathrm{Tr}_n\big(ax^d\big)$ with $d \in \{0, \dots, p^n - 1\}$ and $a \in \mathrm{GF}(p^n)$ is either identically zero or has the algebraic degree equal to $w_p(d)$, the p-weight of d.*

The following proposition imposes another requirement on the exponent of a monomial bent function. In particular, we prove that the exponent of a p-ary bent function over $\mathrm{GF}(p^n)$ with odd p and even $n = 2k$ can not be of the Niho type (i.e., be equal to $s(p^k - 1) + 1$ for some integer s).

Proposition 4 *For an odd prime p take a monomial p-ary function $f(x) = \mathrm{Tr}_n\left(ax^d\right)$ with $a \in \mathrm{GF}(p^n)$ and integer exponent d. If $f(x)$ is bent then d is even and $f^*(0) = 0$.*

Proof: Suppose on the contrary that d is odd. Split the nonzero elements of $\mathrm{GF}(p^n)$ into two subsets C_+ and C_- in such a way that for every $x \in \mathrm{GF}(p^n)^*$ if $x \in C_+$ then $-x \in C_-$. Let

$$\sum_{x \in C_+} \omega^{\mathrm{Tr}_n\left(ax^d - bx\right)} = A_0 + A_1\omega + \cdots + A_{p-1}w^{p-1}$$

for some nonnegative integers A_i $(i = 0, \dots, p-1)$. Then for $b \in \mathrm{GF}(p^n)$ the corresponding Walsh transform coefficient of the bent function $f(x)$ is equal to

$$\begin{aligned} S_a(b) &= \sum_{x \in \mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^d - bx\right)} = 1 + \sum_{x \in C_+} \left(\omega^{\mathrm{Tr}_n\left(ax^d - bx\right)} + \omega^{-\mathrm{Tr}_n\left(ax^d - bx\right)}\right) \\ &= 1 + 2A_0 + (A_1 + A_{p-1})w + (A_2 + A_{p-2})w^2 + \cdots + (A_{p-1} + A_1)w^{p-1} \\ &\overset{(2)}{=} \begin{cases} \pm p^{n/2}\omega^{f^*(b)}, & \text{if } n \text{ is even or } n \text{ is odd and } p \equiv 1 \pmod 4 \ , \\ \pm p^{n/2} i\, \omega^{f^*(b)}, & \text{if } n \text{ is odd and } p \equiv 3 \pmod 4 \ . \end{cases} \end{aligned}$$

Suppose that $f^*(b) \neq 0$. If n is even then moving $\pm p^{n/2}\omega^{f^*(b)}$ to the left hand side of the last identity we get the polynomial of ω of degree $p-1$ with integer coefficients that is identically zero. Thus, all its coefficients are equal (since $x^{p-1} + \cdots + x^2 + x + 1$ is the minimal polynomial of ω over the rational numbers) and, in particular, equal are the coefficients at $\omega^{f^*(b)}$ and $\omega^{p - f^*(b)}$

$$A_{f^*(b)} + A_{p-f^*(b)} \mp p^{n/2} = A_{p-f^*(b)} + A_{f^*(b)}$$

that is impossible. If n is odd then making use of (3) similarly we get that

$$A_{f^*(b)} + A_{p-f^*(b)} = A_{p-f^*(b)} + A_{f^*(b)} \mp \left(\frac{p-2f^*(b)}{p}\right) p^{(n-1)/2}$$

that is also impossible since $p - 2f^*(b) \not\equiv 0 \pmod{p}$. Therefore, $f^*(b) \equiv 0$ for any $b \in \mathrm{GF}(p^n)$ and, depending on n and p, either $S_a(b) = \pm p^{n/2}$ or $S_a(b) = \pm i p^{n/2}$.

In particular, $\sum_{b\in\mathrm{GF}(p^n)} S_a(b)S_a(b+r) \neq 0$ for any $r \in \mathrm{GF}(p^n)$ since p^n is odd. On the other hand, for any nonzero $r \in \mathrm{GF}(p^n)$ we have that

$$\begin{aligned}
\sum_{b\in\mathrm{GF}(p^n)} S_a(b)S_a(b+r) &= \sum_{b\in\mathrm{GF}(p^n)} \sum_{x,y\in\mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^d - bx + ay^d - (b+r)y\right)} \\
&= \sum_{x,y\in\mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^d + ay^d - ry\right)} \sum_{b\in\mathrm{GF}(p^n)} \omega^{-\mathrm{Tr}_n(b(x+y))} \\
&\overset{y=-x}{=} p^n \sum_{x\in\mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^d + a(-x)^d + rx\right)} = 0
\end{aligned}$$

since the inner sum contributes only when $y = -x$ and d is odd. Thus, d has to be be even.

If d is even and $\sum_{x\in C_+} \omega^{\mathrm{Tr}_n\left(ax^d\right)} = A_0 + A_1\omega + \cdots + A_{p-1}w^{p-1}$ then

$$S_a(0) = 1 + 2A_0 + 2A_1 w + 2A_2 w^2 + \cdots + 2A_{p-1}w^{p-1} \ .$$

Suppose that $f^*(0) \neq 0$. Similarly as before one can see that if n is even then the coefficients at ω^0 and $\omega^{f^*(0)}$ are respectively equal to $1 + 2A_0$ and $2A_{f^*(0)} \mp p^{n/2}$ which are odd numbers while the rest of the coefficients are even. If n is odd then the coefficients at ω^0 and $\omega^{f^*(0)}$ are even and respectively equal to

$$1 + 2A_0 \mp \left(\frac{-f^*(0)}{p}\right) p^{(n-1)/2} \quad \text{and} \quad 2A_{f^*(0)} \ .$$

The remaining coefficients at ω^j for $j \notin \{0, f^*(0)\}$ are odd and equal to $2A_j \mp \left(\frac{j-f^*(0)}{p}\right) p^{(n-1)/2}$. Thus, $f^*(0) \neq 0$ is impossible both when n is odd or even. □

We have found the following ternary bent function that does not fall into any of the known classes. Moreover, this is the first example of a bent function that is not weakly regular. The fact was verified with computer, however, proving this result theoretically and probably finding the whole class of similar functions remains an open problem.

Fact 1 *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.

In Table 1 we summarize all the proven and conjectured classes of p-ary monomial bent functions having the form $f(x) = \mathrm{Tr}_n\left(ax^d\right)$ for an odd p. We have run an extensive computer search for ternary monomial bent functions of 13 variables at most (i.e., $n \leq 13$) and all the functions found appear to be cyclotomic equivalent to one of the listed cases. The search over the fields of larger characteristic $p >$

3 is much more computationally complicated and allows to cover the functions depending on less number of variables. This limited search did not provide any new exponents in addition to the known ones either. Shortcuts "r" and "wr" are used to denote regular and weakly regular bent functions respectively. When the value of n is not specified in the table it means that n is arbitrary. Naturally, all the exponents d and coefficients a can be replaced with their cyclotomic equivalents. Note that Gold class covers Sidelnikov, Kasami and Kumar-Moreno cases. Coulter-Matthews, Dillon and conjectured cases all hold only for $p = 3$. Also note that from Corollaries 3, 4 and Theorem 2 it follows that the dual of Sidelnikov, Kasami and Dillon functions belong to the same class of bent functions as the original ones. Here ξ denotes a primitive element of GF(p^n).

Acknowledgement. The authors would like to thank the anonymous reviewers for pointing out reference [18], suggesting a shorter proof of Corollary 7 and for thorough reviews containing constructive comments and valuable suggestions that helped to improve the manuscript significantly.

References

[1] Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. Journal of Combinatorial Theory, Series A **40** (1985) 90–107

[2] Hou, X.D.: p-Ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields and Their Applications **10** (2004) 566–582

[3] Kumar, P.V., Moreno, O.: Prime-phase sequences with periodic correlation properties better than binary sequences. IEEE Transactions on Information Theory **37** (1991) 603–616

[4] Lidl, R., Niederreiter, H.: Finite Fields. Volume 20 of Encyclopedia of Mathematics and its Applications. Addison-Wesley, Amsterdam (1983)

[5] Liu, S.C., Komo, J.J.: Nonbinary Kasami sequences over GF(p). IEEE Transactions on Information Theory **38** (1992) 1409–1412

[6] Kim, Y.S., Jang, J.W., No, J.S., Helleseth, T.: On p-ary bent functions defined on finite fields. In No, J.S., Song, H.Y., Helleseth, T., Kumar, P.V., eds.: Mathematical Properties of Sequences and other Combinatorial Structures. The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, Dordrecht (2003) 65–76

Table 1: Proven and conjectured classes of p-ary monomial bent functions

Bent Functions	n	d	a	Proven in
Sidelnikov (r, wr)		2	$a \neq 0$	Cor. 3
p-ary Kasami (wr)	$2k$	$p^k + 1$	$a + a^{p^k} \neq 0$	[5], Cor. 4
Kumar-Moreno (r, wr)		$p^j + 1$, $\frac{n}{\gcd(n,j)}$-odd	$a \neq 0$	[3], Cor. 5, 6
Coulter-Matthews		$\frac{3^k+1}{2}$, $\gcd(k, n) = 1$, k-odd	$a \neq 0$	[7], Note 2
p-ary Gold (r, wr)		$p^j + 1$	(17)	Th. 3, Pr. 1
p-ary Dillon (r)	$2k$	$t(3^k - 1)$, $\gcd(t, 3^k + 1) = 1$	(7)	Th. 2, Cor. 1
Conjectured (wr)	$2k$	$\frac{3^n-1}{4} + 3^k + 1$	$\xi^{\frac{3^k+1}{4}}$	Con. 1
Fact (not wr)	6	98	ξ^7	Fact 1

[7] Coulter, R.S., Matthews, R.W.: Planar functions and planes of Lenz-Barlotti class II. Designs, Codes and Cryptography **10** (1997) 167–184

[8] Dillon, J.F.: Elementary Hadamard Difference Sets. PhD thesis, University of Maryland (1974)

[9] Davis, P.J.: Circulant Matrices. John Wiley & Sons, New York (1979)

[10] Wolfmann, J.: The weights of the dual code of the MELAS code over GF(3). Discrete Mathematics **74** (1989) 327–329

[11] Helleseth, T.: Some results about the cross-correlation function between two maximal linear sequences. Discrete Mathematics **16** (1976) 209–232

[12] Lachaud, G., Wolfmann, J.: The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Transactions on Information Theory **36** (1990) 686–692

[13] Baumert, L., McEliece, R.: Weights of irreducible cyclic codes. Information and Control **20** (1972) 158–175

[14] Delsarte, P., Goethals, J.M.: Tri-weight codes and generalized Hadamard matrices. Information and Control **15** (1969) 196–206

[15] Storer, T.: Cyclotomy and Difference Sets. Lectures in Advanced Mathematics. Markham Publishing Company, Chicago (1967)

[16] Helleseth, T., Kumar, P.V.: Sequences with low correlation. In Pless, V., Huffman, W., eds.: Handbook of Coding Theory. Volume 2. Elsevier, Amsterdam (1998) 1765–1853

[17] Carlet, C., Dubuc, S.: On generalized bent and q-ary perfect nonlinear functions. In Jungnickel, D., Niederreiter, H., eds.: Finite Fields and Applications: Proceedings of the Fifth International Conference, Berlin, Springer-Verlag (2001) 81–94

[18] Hou, X.D.: Solution to a problem of S.Payne. Proceedings of the American Mathematical Society **132** (2004) 1–6

[19] MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. Volume 16 of North-Holland Mathematical Library. North-Holland, Amsterdam (1996) Ninth impression.

[20] Deligne, P.: La conjecture de Weil. I. Publications Mathématiques de l' Institute Hautes Études Sci. **43** (1974) 273–307

A Alternative Proof of Proposition 2

Proof: We start the proof similarly to [3, p. 609] and [6, Theorem 2]. By the definition of trace function, (20) is equal to

$$\begin{aligned} f(x) &= \sum_{i=0}^{k} \mathrm{Tr}_n\big(a_i x^{p^i+1}\big) = \sum_{i=0}^{k}\sum_{l=1}^{n} \big(a_i x^{p^i+1}\big)^{p^{l-1}} = \sum_{i=0}^{k}\sum_{l=1}^{n} a_i^{p^{l-1}} x^{p^{l-1}+p^{l+i-1}} \\ &= \sum_{i=0}^{k}\sum_{l=1}^{n} a_i^{p^{l-1}} y_l y_{l+i} = G(y_1,\ldots,y_n) \ , \end{aligned}$$

where $y_l = x^{p^{l-1}}$ for $l = 1, \ldots, n$ and $G(y_1, \ldots, y_n)$ is a quadratic function on $\mathrm{GF}(p^n)^n$.

Let $\vec{\mu} = \{\mu_1, \ldots, \mu_n\}$ and $\vec{\nu} = \{\nu_1, \ldots, \nu_n\}$ be a pair of complementary bases [19, p. 117] of $\mathrm{GF}(p^n)$ over $\mathrm{GF}(p)$ which means that

$$\mathrm{Tr}_n(\mu_i \nu_j) = \begin{cases} 1, & \text{if} \quad i = j, \\ 0, & \text{otherwise} \end{cases} \quad .$$

Let $\vec{x} = (x_1, \ldots, x_n)^T$ be the expansion of $x \in \mathrm{GF}(p^n)$ in basis $\vec{\mu}$ and let $\vec{y} = (y_1, \ldots, y_n)^T$, where $y_l = x^{p^{l-1}}$ for $l = 1, \ldots, n$ and the superscript T denotes transpose of a matrix. Then $x_i = \mathrm{Tr}_n(x\nu_i) = \sum_{l=1}^{n} y_l \nu_i^{p^{l-1}}$ for $i = 1, \ldots, n$. Thus, $\vec{x} = A\vec{y}$ with $n \times n$ matrix $A = [a_{il}]_{i,l=1,\ldots,n}$, where $a_{il} = \nu_i^{p^{l-1}}$. It is easy to see that matrix $B = [b_{lj}]_{l,j=1,\ldots,n}$ with $b_{lj} = \mu_j^{p^{l-1}}$ is the inverse of A and $\vec{y} = B\vec{x}$. Let $H(\vec{x})$ denote the function on $\mathrm{GF}(p)^n$ obtained by replacing variable x in (20) with $\sum_{i=1}^{n} x_i \mu_i$. Then $G(\vec{y}) = G(B\vec{x}) = H(\vec{x})$ is quadratic.

Assume that the system of linear equations $\left\{ \frac{\partial H(x_1, \ldots, x_n)}{\partial x_i} = 0, \quad i = 1, \ldots, n \right\}$ has the unique zero solution, i.e., $H(\vec{x})$ is nonsingular. Then by Deligne's theorem [20, 3], for any $\vec{b} = (b_1, \ldots, b_n)^T \in \mathrm{GF}(p)^n$

$$\left| \sum_{\vec{x} \in \mathrm{GF}(p)^n} \omega^{H(\vec{x}) - \langle \vec{b}, \vec{x} \rangle} \right| \leq p^{n/2} \quad , \tag{24}$$

where $\langle \vec{b}, \vec{x} \rangle = b_1 x_1 + \cdots + b_n x_n$ is the standard inner product over $\mathrm{GF}(p)$. The left hand side of (24) represents the Walsh transform coefficient of $f(x)$ evaluated at $b = \sum_{i=1}^{n} b_i \mu_i \in \mathrm{GF}(p^n)$ (since $\vec{\mu}$ can be chosen to be a trace-orthogonal basis [4, p. 75]). Moreover, if (24) holds then by the Parseval's equation

$$\left| \sum_{\vec{x} \in \mathrm{GF}(p)^n} \omega^{H(\vec{x}) - \langle \vec{b}, \vec{x} \rangle} \right| = p^{n/2}$$

and this means that function (20) is bent.

Due to the obvious identity $\left[\frac{\partial H(\vec{x})}{\partial x_1}, \ldots, \frac{\partial H(\vec{x})}{\partial x_n} \right] = \left[\frac{\partial G(\vec{y})}{\partial y_1}, \ldots, \frac{\partial G(\vec{y})}{\partial y_n} \right] B$, function $H(\vec{x})$ is nonsingular if and only if $G(\vec{y})$ is nonsingular. Differentiating $G(\vec{y})$ we obtain

$$\frac{\partial G(y_1, \ldots, y_n)}{\partial y_l} = \sum_{i=0}^{k} \left(a_i^{p^{l-1}} y_{l+i} + a_i^{p^{l-i-1}} y_{l-i} \right) \quad \text{for} \quad l = 1, \ldots, n \ ,$$

where index $l - i$ is calculated modulo n. Now it is easy to see that the matrix of the system of linear equations $\left\{ \frac{\partial G(y_1, \ldots, y_n)}{\partial y_l} = 0, \quad l = 1, \ldots, n \right\}$ is equal to one of the matrices (21) depending on whether n is odd or even. Thus, function $G(\vec{y})$ is nonsingular if and only if the corresponding matrix (21) is nonsingular. □