

On Generalized Bent Functions

Tor Helleseeth and Alexander Kholosha

The Selmer Center

Department of Informatics, University of Bergen, P.O. Box 7800

N-5020 Bergen, Norway

Email: {Tor.Helleseeth, Alexander.Kholosha}@ii.uib.no

Abstract—Bent functions were first introduced by Rothaus in 1976 as an interesting combinatorial object with the important property of having the maximum distance to all affine functions. Bent functions have many applications to coding theory, cryptography and sequence designs. For many years the focus was on the construction of binary bent functions. There are several known examples of binary monomial and binomial bent functions. In 1985, Kumar, Scholtz and Welch generalized bent functions to the case of an arbitrary finite field. In the recent years, new results on nonbinary bent functions have appeared. This paper gives an updated overview of some of the recent results and open problems on generalized bent functions. This includes some recent constructions of weakly regular monomial and binomial bent functions and examples of non-weakly regular bent functions.

I. INTRODUCTION

Bent functions were introduced by Rothaus [1] as Boolean functions $f(x_0, x_1, \dots, x_{n-1})$ that map binary n -tuples to $\text{GF}(2) = \{0, 1\}$ and whose Walsh transform has constant magnitude. Bent functions are named this way since they have maximum distance from all affine functions. This property is extremely useful and important in cryptographic applications where one frequently needs functions which can not be easily approximated by linear functions. The construction of Bent functions is also quite heavily related to the covering radius of the first order Reed-Muller code.

In the next two sections, we give some background information and a brief introduction to binary bent functions. In Section IV. we give an overview of recent results on generalized bent functions.

II. BINARY BENT FUNCTIONS

Let $f(x) : \text{GF}(2)^n \mapsto \text{GF}(2)$ be a Boolean function. Define the Walsh transform coefficients $S_f(b)$ for any $b \in \text{GF}(2)^n$ by

$$S_f(b) = \sum_{x \in \text{GF}(2)^n} (-1)^{f(x)+x \cdot b} ,$$

where $x \cdot b = \sum_{i=1}^n x_i b_i$ denotes the inner product between the two binary vectors $b = (b_1, b_2, \dots, b_n)$ and $x = (x_1, x_2, \dots, x_n)$ in $\text{GF}(2)^n$.

From the definition of the Walsh transform it follows that the function $(-1)^{f(x)}$ can easily be reconstructed from the

This work was supported by the Norwegian Research Council and partially by the grant NIL-I-004 from Iceland, Liechtenstein and Norway through the EEA and Norwegian Financial Mechanisms.

Walsh transform coefficients via the relation

$$(-1)^{f(x)} = \frac{1}{2^n} \sum_{b \in \text{GF}(2)^n} S_f(b) (-1)^{x \cdot b} .$$

Some useful properties involving the Walsh transform coefficients are

$$\begin{aligned} \sum_{b \in \text{GF}(2)^n} (S_f(b))^2 &= \sum_b \sum_x \sum_y (-1)^{f(x)+f(y)+b \cdot (x+y)} \\ &= \sum_x \sum_y (-1)^{f(x)+f(y)} \sum_b (-1)^{b \cdot (x+y)} \\ &= 2^n \sum_x (-1)^0 \\ &= 2^{2n} , \end{aligned}$$

where the summations b, x, y run through $\text{GF}(2)^n$. This implies that the average value of the square of the Walsh transform coefficients is 2^n . The Boolean functions obtained when all these squared coefficients are the same are called *bent functions*.

Definition 1: The Boolean function $f(x)$ is a *bent function* if $S_f(b) = \pm 2^{n/2}$ for all $b \in \text{GF}(2)^n$.

Thus, if all magnitudes of $|S_f(b)| = \sqrt{2^n}$ are the same, the function f is called a bent function. It follows as a consequence that binary bent functions exist for *even* n only.

There are many constructions of bent functions. The best known such constructions are the Maiorana-McFarland constructions. Frequently, several apparently different constructions of bent functions turn out to be special cases of the Maiorana-McFarland constructions.

Lemma 1: Take a permutation $\pi : \text{GF}(2)^{n/2} \mapsto \text{GF}(2)^{n/2}$ and any mapping $g : \text{GF}(2)^{n/2} \mapsto \text{GF}(2)$. Then

$$f_{g,\pi}(x, y) = x \cdot \pi(y) + g(y)$$

is a bent function.

There is a close connection between bent functions and the covering radius of the first order Reed-Muller code. Let $x = (x_1, x_2, \dots, x_n)$ and let v_f be a vector of length 2^n obtained by evaluating $f(x)$ for all $x \in \text{GF}(2)^n$, such that

$$v_f = (f(x))_{x \in \text{GF}(2)^n} .$$

The *first order Reed-Muller code* of length 2^n , is obtained using all binary affine polynomials $f(x) = \sum_{i=1}^n b_i x_i + b_0$, i.e.,

$$RM(1, n) = \{v_f \mid \deg(f) \leq 1\} .$$

The parameters of the $RM(1, n)$ are $[2^n, n + 1, d = 2^{n-1}]$.

For example, for $n = 3$ the following matrix is a generator matrix of $RM(1, 3)$,

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

In the special case when $f(x) = x_1 + x_3 + 1$ we obtain the codeword $v_f = (10100101)$.

Definition 2: The *covering radius* of a code is the smallest integer ρ such that the spheres of radius ρ around the codewords cover the complete space.

The distance from an arbitrary vector $v_f = (f(x))_{x \in \text{GF}(2)^n}$ to a codeword $c = b \cdot x + a \in RM(1, n)$ can be found via the Walsh transform by

$$\begin{aligned} (-1)^a S_f(b) &= \sum_{x \in \text{GF}(2)^n} (-1)^{f(x) + b \cdot x + a} \\ &= (2^n - d(v_f, c)) - d(v_f, c) \\ &= 2^n - 2d(v_f, c), \end{aligned}$$

where $d(v_f, c)$ denotes the Hamming distance between the binary vectors v_f and c .

Since the average value of $|S_f(b)|$ is $2^{n/2}$, it holds for the covering radius of $RM(1, n)$ that

$$\rho_n \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Thus, bent functions lead to vectors with maximum distance from $RM(1, n)$.

Bent functions exist for an even number of variables. For example, the Boolean function

$$f(x_1, x_2, \dots, x_{2n}) = x_1 x_2 + x_3 x_4 + \dots + x_{2n-1} x_{2n}$$

is a bent function in $2n$ variables. Therefore, the covering radius of the first order Reed-Muller code equals

$$\rho_n = 2^{n-1} - 2^{\frac{n}{2}-1} \text{ for even } n.$$

For odd values of n it appears to be a very difficult and challenging problem to compute the covering radius of the first order Reed-Muller code of period 2^n . One can use the covering radius of $RM(1, n-1)$ and the inductive structure of the Reed-Muller code to show a simple bound for the covering radius (see [2])

$$2^{n-1} - 2^{\frac{n-1}{2}} \leq \rho_n \leq 2^{n-1} - 2^{\frac{n}{2}-1} \text{ for odd } n.$$

For the first few values of the covering radius of $RM(1, n)$ the following is known:

n	3	4	5	6	7	8	9	10	
ρ_n	2	6	12	28	56	120	242 - 244	496	.

Let v be a vector of distance ρ_n to the $RM(1, n)$ (without loss of generality, since the code is linear, we can assume the distance to the all-zero codeword is ρ_n). Consider the code

C obtained by restricting the codewords in $RM(1, n)$ to the positions where v has a 1.

$$\begin{array}{cccc} v & 111 \dots 111 & 111 \dots 111 & 000 \dots 000 & 000 \dots 000 \\ c & \underbrace{111 \dots 111}_w & \underbrace{000 \dots 000}_{\rho_n - w} & \underbrace{111 \dots 111}_{2^{n-1} - w} & 000 \dots 000 \end{array}.$$

Since $d(v, c) = \rho_n - w + 2^{n-1} - w \geq \rho_n$ we have $w \leq 2^{n-2}$, and since the all-one vector belongs to C its parameters are

$$[\rho_n, n + 1, \rho_n - 2^{n-2}]$$

and with dual minimum distance $d^\perp \geq 4$.

The largest odd value of n with known ρ_n is $n = 7$ where $\rho_7 = 56$. This was proved by Mykkeltveit [3] by showing that a [57, 8, 25] self-complementary code with $d^\perp \geq 4$ does not exist. The next odd case of $n = 9$ has been open for more than 30 years. To settle this case one has to decide whether a self-complementary code with one of the parameters [243, 10, 115] or [244, 10, 116] and $d^\perp \geq 4$ does exist. For odd values of $n \geq 15$, ρ_n was already shown in [4] to be strictly greater than the lower bound.

Definition 3: A code C (possibly) nonlinear has strength $s(C) = 2$ if all pairs occur equally often in each pair of coordinates. (For a linear code $d^\perp = s(C) + 1$.)

Theorem 1 ([2]): Let C be a code of length n and strength $s(C) = 2$. Then the covering radius obeys

$$\rho \leq \frac{n - \sqrt{n}}{2}.$$

Sketch of proof: The result follows by considering the coset $v + C$ where $d(v, C) = \rho$ and using well known expressions for the sum of the squares of the weights of all binary vectors in the coset.

The bound above, which is called the Nourse bound, can be improved for codes of strength $s > 2$.

III. BENT FUNCTIONS VIA TRACE FUNCTIONS

One way to define new bent functions is to use a one-to-one mapping between $\text{GF}(2^n)$ and $\text{GF}(2)^n$ obtained by considering $\text{GF}(2^n)$ as an n -dimensional vector space over $\text{GF}(2)$. Then all binary functions can be considered to be of the form $\text{Tr}_n(f(x))$ where $f(x)$ is a univariate polynomial over $\text{GF}(2^n)$.

Furthermore, all linear functions can be written as $\text{Tr}_n(bx)$ where $\text{Tr}_n(x)$ is the Froebenius trace mapping. Hence, when considering the Walsh transform we can instead study the equivalent Walsh transform coefficients given by

$$S_f(b) = \sum_{x \in \text{GF}(2^n)} (-1)^{\text{Tr}_n(f(x)) + \text{Tr}_n(bx)}.$$

Therefore, it is interesting to study the trace function from a finite field $\text{GF}(p^n)$ to a subfield $\text{GF}(p^k)$ given by $\text{Tr}_k^n : \text{GF}(p^n) \mapsto \text{GF}(p^k)$, and defined by

$$\text{Tr}_k^n(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{p^{ki}}.$$

For $k = 1$ we use the notation $\text{Tr}_n(x) = \sum_{i=0}^{n-1} x^{p^i}$.

Some important and useful properties of the trace mapping are provided in the next lemma.

- Lemma 2:*
- (i) $\text{Tr}_n(ax + by) = a\text{Tr}_n(x) + b\text{Tr}_n(y)$ for any $x, y \in \text{GF}(p^n)$ and $a, b \in \text{GF}(p)$.
 - (ii) $\text{Tr}_n(x^p) = \text{Tr}_n(x)$.
 - (iii) $\text{Tr}_k(\text{Tr}_n^n(x)) = \text{Tr}_n(x)$ for any $x \in \text{GF}(p^n)$.
 - (iv) $\text{Tr}_n(ax)$ takes on all elements on $\text{GF}(p)$ equally often when $a \neq 0$.

A well-known bent function which is quite simply constructed via the trace map is the following (this is a consequence of a result by Kasami).

Theorem 2 (Kasami): Let $n = 2k$ and $a \in \text{GF}(2^n)$. Then the function

$$f(x) = \text{Tr}_n(ax^{2^k+1})$$

is bent if $a + a^{2^k} \neq 0$.

Proof: Any $x \in \text{GF}(2^n)^*$ can be written uniquely as $x = \alpha\beta$ where $\alpha \in \text{GF}(2^k)^*$ has order $2^k - 1$ and β has order $2^k + 1$. Then the Walsh transform gives

$$\begin{aligned} S_f(b) - 1 &= \sum_{x \neq 0} (-1)^{\text{Tr}_k((a+a^{2^k})x^{2^k+1} + bx + b^{2^k}x^{2^k})} \\ &= \sum_{\beta} \sum_{\alpha} (-1)^{\text{Tr}_k(\alpha^2(a+a^{2^k})\beta^{2^k+1} + b\beta^2 + b^{2^k}\beta^{-2})} \\ &= (2^k - 1)N(a, b) - (2^k + 1 - N(a, b)) \\ &= (N(a, b) - 1)2^k - 1, \end{aligned}$$

where $N(a, b)$ is the number of solutions β of

$$a + a^{2^k} + b^2\beta^2 + b^{2^k+1}\beta^{-2} = 0.$$

Since $N(a, b)$ is 0 or 2 if $a + a^{2^k} \neq 0$, then $S_f(b) = \pm 2^k$ and thus $f(x) = \text{Tr}_n(ax^{2^k+1})$ is a bent function. \square

This is an example of what we call a monomial bent function. Another class of monomial bent functions found by Canteaut, Charpin and Kyureghyan in [5] is the following.

Theorem 3: Let $n = 6r$ and $d = 2^{2r} + 2^r + 1$. Then the function $f(x) = \text{Tr}_n(\lambda x^d)$ is bent for some λ (characterized in [5]). Moreover, if $f(x)$ is bent then it is of the Maiorana-McFarland type.

Other monomial bent functions of the form $\text{Tr}_n(\lambda x^d)$ of the Maiorana-McFarland type are:

- $d = t(2^k - 1)$ with $n = 2k$ and $\gcd(t, 2^k + 1) = 1$ (Dillon exponent, see [6], [7]).
- $d = (2^r + 1)^2$ with $n = 4r$ (see [8], [9]).

The following monomial bent functions were constructed by Dillon and Dobbertin [10].

Theorem 4: Let $d = 2^{2i} - 2^i + 1$, where $\gcd(i, n) = 1$. Then the function $f(x) = \text{Tr}_n(\lambda x^d)$ is bent for some λ .

New bent functions can be constructed in the binomial form $f(x) = \text{Tr}_n(x^{d_1} + x^{d_2})$, where $d_i = 2^t \pmod{2^k - 1}$ for some t . The following bent functions are due to Dobbertin et.al. [11].

Theorem 5 ([11]): Let $n = 2k$ and $\alpha_1 + \alpha_1^{2^k} = 1$, then the following functions are bent

$$\begin{aligned} &\text{Tr}_n(\alpha_1 x^{2^k+1} + x^{3 \cdot 2^{k-1} - 1}), \\ &\text{Tr}_n(\alpha_1 x^{2^k+1} + x^{2^k+3}), \\ &\text{Tr}_n(\alpha_1 x^{2^k+1} + x^{(2^k+5)/3}). \end{aligned}$$

Sketch of proof. In principle, based on the same method as in Theorem 2 but much more tricky and complicated. Uses ideas from properties of Dickson polynomials as well as many other inventive tricks. In this case, $d_1 = x^{2^k+1}$ and $d_2 = 2^t \pmod{2^k - 1}$ and one reduces the problem to an equation that, as in the Kasami case, can be shown to have either 0 or 2 roots.

IV. GENERALIZED BENT FUNCTIONS

In this section, we discuss nonbinary (or generalized) bent functions. These were introduced in 1985 by Kumar, Scholtz and Welch [12].

Let $f(x) : \text{GF}(p^n) \mapsto \text{GF}(p)$ be a p -ary function. Then the Walsh transform $S_f(b)$ of f is defined by

$$S_f(b) = \sum_{x \in \text{GF}(p^n)} \omega^{f(x) - \text{Tr}_n(bx)}$$

and

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

where $\text{Tr}_n : \text{GF}(p^n) \mapsto \text{GF}(p)$ is the absolute trace function, $\omega = e^{\frac{2\pi i}{p}}$ is the complex primitive p^{th} root of unity and elements of $\text{GF}(p)$ are considered as integers modulo p . The p -ary bent functions are defined as a natural generalization of the binary case.

Definition 4: Let $f(x) = \text{Tr}_n(\sum_{i=0}^s a_i x^{d_i})$ be a mapping from $\text{GF}(p^n)$ to $\text{GF}(p)$. Then $f(x)$ is a p -ary bent function if

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

The bent function is said to be a *regular bent function* if

$$p^{-n/2} S_f(b) = \omega^{f^*(b)},$$

where $f^* : \text{GF}(p^n) \mapsto \text{GF}(p)$.

The bent function is said to be a *weakly regular bent function* if

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

for some complex number u with $|u| = 1$.

Walsh transform coefficients of a p -ary bent function f with odd p satisfy

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

where i is a complex primitive 4th root of unity.

Let

$$S_f(b) = N_b(0) + N_b(1)\omega + \dots + N_b(p-1)\omega^{p-1},$$

where

$$N_b(j) := \#\{x \in \text{GF}(p^n) \mid f(x) - \text{Tr}_n(bx) = j\} .$$

For a bent function $f(x)$ with even n (b fixed) holds

$$N_b(j) \equiv \text{const}$$

for $j \neq f^*(b)$ and $N_b(f^*(b))$ differs from the rest by $\pm p^{n/2}$. If $n = 2k + 1$ is odd (b fixed) then

$$N_b(j) - N_b(f^*(b)) = p^k$$

for half of $j \neq f^*(b)$ and is equal to $-p^k$ for the rest.

Let χ be a nontrivial additive character of $\text{GF}(p^k)$ and take $a, b \in \text{GF}(p^k)$. The Kloosterman sum is defined by

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

The Gaussian sum is defined by

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

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

Theorem 6 ([13]): Let $n = 2k$ and $a \in \text{GF}(p^n)$ is nonzero. Then for any nontrivial additive character χ of $\text{GF}(p^k)$

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

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

Using this result, Helleseth and Kholosha in [13] proved the following criterion for a new family of ternary bent functions. This family can be seen as an extension of the Dillon class of binary bent functions to the ternary case.

Theorem 7: 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 . For any nonzero $a \in \text{GF}(p^n)$, define the following p -ary function mapping $\text{GF}(p^n)$ to $\text{GF}(p)$

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

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

$$S_a(b) = 1 + K(\chi_1; 1, a^{p^k+1}) + p^k \omega^{-\text{Tr}_n(a^{p^k} b^{t(p^k-1)})}$$

and

$$S_a(0) = 1 - (p^k - 1)K(\chi_1; 1, a^{p^k+1}) ,$$

where χ_1 is the canonical additive character of $\text{GF}(p^k)$. Consequently, $f(x)$ is bent if and only if the following Kloosterman sum over $\text{GF}(p^k)$ satisfies

$$K(\chi_1; 1, a^{p^k+1}) = -1 . \quad (1)$$

Moreover, if (1) holds then $f(x)$ is a regular bent function.

Corollary 1: In the ternary case (i.e., when $p = 3$), there exists at least one $a \in \text{GF}(p^n)$ such that function $f(x)$ is bent. Moreover, $f(x)$ is bent if and only if the Hamming weight

of the codeword $c(a) = (\text{Tr}_n(a\xi^{j(3^k-1)}) \mid j = 0, \dots, 3^k)$ is equal to $2 \cdot 3^{k-1}$, where ξ is a primitive element of $\text{GF}(3^n)$.

Although not proven, it is unlikely that condition (1) can hold in a nonbinary and nonternary case. Here we want to mention the following conjecture of Helleseth.

Conjecture 1 ([14]): If $d \equiv 1 \pmod{p-1}$ then the periodic correlation of an m -sequence and its d -decimation contains the value -1 (not true in the opposite direction in general).

Note that Kloosterman sum values make up 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 [7, Theorem 3.4] and [15]). If the above conjecture was true in the opposite direction 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 Dillon bent functions for $p > 3$.

Theorem 8 ([16]): Let $n = 2k$ with k odd. Then the ternary function $f(x)$ mapping $\text{GF}(3^n)$ to $\text{GF}(3)$ and given by

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

is a weakly regular bent function if $a = \xi^{\frac{3^k+1}{4}}$ and ξ is a primitive element of $\text{GF}(3^n)$.

The values of the Walsh coefficients have been conjectured as follows.

Conjecture 2 ([13]): For $b \in \text{GF}(3^n)$ the corresponding Walsh coefficient of $f(x)$ is equal to

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

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

Some results towards the proof of this conjecture are known. Let p be an odd prime and ξ a primitive element of $\text{GF}(p^n)$. Furthermore, let $n = 2k$ and define for $i = 0, 1, 2, 3$

$$C_i := \left\{ \xi^{4t+i} \mid t = 0, \dots, \frac{p^n-1}{4} - 1 \right\}$$

the cyclotomic class of order 4 in $\text{GF}(p^n)^*$.

Let

$$T_j := \sum_{x \in C_j} \omega^{\text{Tr}_k(c(x+1)^{p^k+1}-c)}$$

for $c \in \text{GF}(p^k)$ and $j = 0, 1, 2, 3$.

Lemma 3 ([17]): Let p be an odd prime with $p \equiv 3 \pmod{8}$ and let $n = 2k$ with k odd. Then for any j

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

Let $c = \frac{b^{3^k+1}}{a^{I+1}} \in \text{GF}(3^k)$, $b = a(I+1)\beta^{3^k} \neq 0$ and $\beta^{-1} \in C_j$ then

$$\begin{aligned} S_f(b) &= 1 + T_j + T_{j+1} + \overline{T_{j+2}} + \overline{T_{j+3}} \\ &= (1 - \omega^{\text{Tr}_k(c)}) \left(T_j + T_{j+1} + \frac{3^k+1}{2} \right) - 3^k . \end{aligned}$$

TABLE I
KNOWN CLASSES OF NONQUADRATIC p -ARY MONOMIAL BENT FUNCTIONS

Bent Functions	n	d	a	References
Coulter-Matthews (r, wr)		$\frac{3^k+1}{2}, \gcd(k, n) = 1, k\text{-odd}$	$a \neq 0$	[18], [16]
Dillon (r)	$2k$	$t(3^k - 1), \gcd(t, 3^k + 1) = 1$	(1)	Th. 7, Cor. 1 [13]
HK (wr)	$2k$	$\frac{3^n-1}{4} + 3^k + 1$	$\xi^{\frac{3^k+1}{4}}$	Th. 8 [17], [16]
Fact (not wr)	6	98	ξ^7	

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

Further, we consider monomial quadratic bent functions. Let ξ be a primitive element of $\text{GF}(p^n)$ and for $a \in \text{GF}(p^n)^*$ define $\text{ind}(a)$ as the unique integer t with $a = \xi^t$ and $0 \leq t < p^n - 1$.

Theorem 9 ([13], [19]): Let $a \in \text{GF}(p^n)$ be nonzero and a prime p be odd. Then for any $j \in \{1, \dots, n\}$, the quadratic p -ary function $f(x)$ mapping $\text{GF}(p^n)$ to $\text{GF}(p)$ and given by

$$f(x) = \text{Tr}_n(ax^{p^j+1})$$

is bent if and only if

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

where $i_0 = \text{ind}(a)$. Moreover, if (2) holds then $f(x)$ is a (weakly) regular bent function and for $b \in \text{GF}(p^n)$ the corresponding Walsh transform coefficient of $f(x)$ is equal to

$$S_a(b) = S_a(0)\omega^{-\text{Tr}_n(ax_0^{p^j+1})},$$

where x_0 is a unique solution of the equation $a^{p^j}x^{p^{2j}} + ax = -b^{p^j}$. Further, if $e = n/\gcd(j, n)$ is odd then (2) is satisfied by any nonzero a and

$$2x_0 = -a^{-1}b^{p^j} - \sum_{t=1}^{(e-1)/2} (-1)^t \left((-1)^{\frac{e-1}{2}} a^{-\frac{p^{2jt}+p^je}{p^j+1}} b^{p^{2jt}} + a^{-\frac{p^j(2t+1)+1}{p^j+1}} b^{p^j(2t+1)} \right)$$

(for $e = 1$, the sum over the empty set is equal to zero). If e is even and (2) holds then $D(a)$ defined by

$$D(a) = (-1)^{\frac{e}{2}} \left(a^{\frac{p^je-1}{p^j+1}} + a^{-\frac{p^je-1}{p^j+1}} \right) - 2.$$

is nonzero and

$$D(a)x_0 = \sum_{t=0}^{e/2-1} (-1)^t \left((-1)^{\frac{e}{2}+1} a^{-\frac{p^j(2t+1)+p^je}{p^j+1}} + a^{-\frac{p^j(2t+1)+1}{p^j+1}} \right) b^{p^j(2t+1)}.$$

Finally, the magnitude of $S_a(b)$ that is equal to $S_a(0)$ can be determined using [19, Lemma 2] given the concrete values of j and n .

The following corollary provides the generalization of Theorem 2 to the p -ary case.

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

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

Corollary 3 ([20]): Let $n = ek$ for an odd integer e and take integer r in the range $1 \leq r \leq e$ with $\gcd(r, e) = 1$. Then the function $f(x) = \text{Tr}_n(ax^{p^{rk}+1})$ is a (weakly) regular bent function for any nonzero $a \in \text{GF}(p^n)$ and odd prime p .

All currently known nonquadratic generalized monomial bent functions are summarized in Table I. Note that all functions are ternary. 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.

In the following theorem, we describe the class of bent functions consisting of two terms (so called binomial functions). This is the only proven infinite class of nonquadratic generalized bent functions over the fields of an arbitrary odd characteristic.

Theorem 10: Let $n = 4k$. Then p -ary function $f(x)$ mapping $\text{GF}(p^n)$ to $\text{GF}(p)$ and given by

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

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

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

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

$$b^{p^{2k}+1} + (b^2 + x)(p^{2k}+1)/2 + b^{p^k}(p^{2k}+1) + (b^2 + x)^{p^k}(p^{2k}+1)/2.$$

If $b^2 \in \text{GF}(p^{2k})$ then x_0 can be found explicitly as $x_0 = -\text{Tr}_k^{2k}(b^2)$. It is interesting that in the binary case when $p = 2$, the decimation $2^{3k} - 2^{2k} + 2^k + 1$ which is cyclotomic equivalent to the exponent in the first term of the above bent function, was studied by Niho in [21, Theorem 3-7] and Hellesteth in [22]. They proved that the cross-correlation function between two binary m -sequences that differ by this decimation is four-valued and found the distribution.

To conclude, in Table II we present results of the computer search for binomial *ternary* bent functions having the form

TABLE II
BINOMIAL NONQUADRATIC TERNARY BENT FUNCTIONS

n	d_1	d_2	Remarks
3	8	14	not wr
4	4	22	not wr
6	14	70	not wr
6	14	98	wr
6	20	92	not wr
6	28	140	wr
8	20	100	wr
8	40	280	wr
8	88	136	wr

$f(x) = \text{Tr}_n(a_1x^{d_1} + a_2x^{d_2})$ (exponents are taken up to cyclotomic equivalence). The values of coefficients $a_1, a_2 \in \text{GF}(3^n)^*$ are not given since in some cases, many possibilities are allowed. Also skipped are numerous examples of quadratic and binomial ternary bent functions consisting of two Dillon type exponents (see Theorem 7).

REFERENCES

- [1] O. S. Rothaus, "On "bent" functions," *J. Combin. Theory Ser. A*, vol. 20, no. 3, pp. 300–305, May 1976.
- [2] T. Helleseeth, T. Kløve, and J. J. Mykkeltveit, "On the covering radius of binary codes," *IEEE Trans. Inf. Theory*, vol. 24, no. 5, pp. 627–628, Sep. 1978.
- [3] J. J. Mykkeltveit, "The covering radius of the (128, 8) Reed-Muller code is 56," *IEEE Trans. Inf. Theory*, vol. 26, no. 3, pp. 359–362, May 1980.
- [4] N. J. Patterson and D. H. Wiedemann, "The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 354–356, May 1983.
- [5] A. Canteaut, P. Charpin, and G. M. Kyureghyan, "A new class of monomial bent functions," *Finite Fields Appl.*, vol. 14, no. 1, pp. 221–241, Jan. 2008.
- [6] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, University of Maryland, 1974.
- [7] G. Lachaud and J. Wolfmann, "The weights of the orthogonals of the extended quadratic binary Goppa codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 3, pp. 686–692, May 1990.
- [8] P. Charpin and G.M. Kyureghyan, "On cubic bent functions in the class M," in: Proceedings of the Algebraic and Combinatorial Coding Theory, ACCT-10, Zvenigorod, Russia, September 2006.
- [9] N. G. Leander, "Monomial bent functions," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 738–743, Feb. 2006.
- [10] J. F. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters," *Finite Fields Appl.*, vol. 10, no. 3, pp. 342–389, Jul. 2004.
- [11] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, "Construction of bent functions via Niho power functions," *J. Combin. Theory Ser. A*, vol. 113, no. 5, pp. 779–798, Jul. 2006.
- [12] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *J. Combin. Theory Ser. A*, vol. 40, no. 1, pp. 90–107, Sep. 1985.
- [13] T. Helleseeth and A. Kholosha, "Monomial and quadratic bent functions over the finite fields of odd characteristic," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2018–2032, May 2006.
- [14] T. Helleseeth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, no. 3, pp. 209–232, Nov. 1976.
- [15] N. M. Katz and R. Livné, "Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3," *Comptes Rendus de l'Académie des Sciences Paris, Série I - Mathématique*, vol. 309, no. 11, pp. 723–726, 1989.
- [16] T. Helleseeth, H. D. L. Hollmann, A. Kholosha, Z. Wang, and Q. Xiang, "Proofs of two conjectures on ternary weakly regular bent functions," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 5272–5283, Nov. 2009.
- [17] T. Helleseeth and A. Kholosha, "Monomial and quadratic bent functions over the finite fields of odd characteristic," Reports in Informatics, Department of Informatics, University of Bergen, Bergen, Tech. Rep. 310, Sep. 2005, <http://www.ii.uib.no/publikasjoner/texrap/pdf/2005-310.pdf>.
- [18] R. S. Coulter and R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Des. Codes Cryptogr.*, vol. 10, no. 2, pp. 167–184, Feb. 1997.
- [19] T. Helleseeth and A. Kholosha, "On the dual of monomial quadratic p -ary bent functions," in *Sequences, Subsequences, and Consequences*, ser. Lecture Notes in Computer Science, S. Golomb, G. Gong, T. Helleseeth, and H.-Y. Song, Eds., vol. 4893. Berlin: Springer-Verlag, 2007, pp. 50–61.
- [20] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 603–616, May 1991.
- [21] Y. Niho, "Multi-valued cross-correlation functions between two maximal linear recursive sequences," Ph.D. dissertation, University of Southern California, Los Angeles, 1972.
- [22] T. Helleseeth, "A note on the cross-correlation function between two binary maximal length linear sequences," *Discrete Math.*, vol. 23, no. 3, pp. 301–307, 1978.