AIMS Mathematics, 7(2): 1971–1981.
DOI: 10.3934/math.2022113
Received: 21 June 2021
Accepted: 27 August 2021
Published: 05 November 2021

http://www.aimspress.com/journal/Math

Research article

On a class of bent, near-bent, and 2-plateaued functions over finite fields of odd characteristic

Samed Bajrić*

Laboratory for Open Systems and Networks, Jozef Stefan Institute, 1000 Ljubljana, Slovenia

* **Correspondence:** Email: samed@e5.ijs.si; Tel: +38614773758.

Abstract: The main purpose of this paper is to study a class of the p-ary functions $f_{\lambda,u,v}(x) = Tr_1^k(\lambda x^{p^k+1}) + Tr_1^n(ux)Tr_1^n(vx)$ for any odd prime p and $n = 2k, \lambda \in GF(p^k)^*, u, v \in GF(p^n)^*$. With the help of Fourier transforms, we are able to subdivide the class of all $f_{\lambda,u,v}$ into sublcasses of bent, near-bent and 2-plateaued functions. It is shown that the choice of λ, u and v, ensuring that f is bent, 2-plateaued or near-bent, is directly related to finding the subset $A \subset GF(p)^3$. The efficient method for defining the set $A \subset GF(p)^3$ is described in detail.

Keywords: Fourier transform; p-ary functions; nonbinary finite field; s-plateaued; near-bent functions
Mathematics Subject Classification: 06E30, 94A60, 11T06

1. Introduction

Bent functions are extreme combinatorial objects with several areas of application, such as coding theory, maximum length sequences, cryptography, and the theory of difference sets to name a few. Boolean bent functions were introduced by Rothaus [6], who also considered two classes of bent functions. Among other equivalent characterizations of bent functions, the one that is most often used is a characterization of bent functions as a class of Boolean functions having so-called flat Walsh spectrum. It means that for any bent function over $GF(2)^n$, its Hamming distance to any affine function in n variables is constant, including the distance to the all-zero function (or all-one function). The bent property of f is commonly specified in terms of its flat Walsh spectrum, that is requiring that $W_f(\lambda) = \pm 2^{n/2}$ for any $\lambda \in GF(2^n)$, where,

$$W_f(\lambda) = \sum_{x \in GF(2^n)} (-1)^{f(x)+Tr_1^n(\lambda x)}. \tag{1.1}$$

Here, $Tr_1^n : GF(2^n) \to GF(2)$ denotes the absolute trace function defined by $Tr_1^n(x) = x + x^2 + \ldots + x^{2^{n-1}}$.

On the other hand, a generalization to finite fields of odd characteristic was first suggested in [3] and a function $f : GF(p^n) \to GF(p)$ is bent if and only if its Fourier transform defined by

$$\widehat{f}(a) = \sum_{x \in GF(p^n)} \omega^{f(x) - Tr_1^n(ax)}, \tag{1.2}$$

is flat, that is, $|\widehat{f}(a)| = p^{n/2}$ for any $a \in GF(p^n)$. Here, $\omega = e^{\frac{2\pi\iota}{p}}$ denotes the primitive root of unity where $\iota = \sqrt{-1}$. Some surveys of known results on p-ary bent functions can be found in [1, 3, 5] and the references therein.

The classes of plateaued functions introduced by Zheng and Zhang [10] are good candidates for designing cryptographic functions since they possess various desirable cryptographic characteristics. They can be balanced for both odd and even number of variables, and they do not possess nonzero linear structures. In particular, the functions whose Fourier spectrum belong to $\{0, \pm p^{\frac{n+1}{2}}\}$ are known as near-bent functions and, they play a significant role in certain cryptographic primitives.

In 2016 and 2017, *G. Xu et. al.* [8, 9] characterised the Fourier transform of the p-ary functions of the form

$$Tr_1^k(\lambda x^{p^k+1}) + Tr_1^n(ux)Tr_1^n(vx), \tag{1.3}$$

for the special case $p = 3$ and $n = 2k, \lambda \in GF(p^k)^*, u, v \in GF(p^n)^*$. The authors proved that some of these p-ary functions are also bent under certain conditions. Furthermore, a construction of quadratic ternary bent, near-bent and 2-plateaued functions from some known ternary bent functions are presented.

In this work we generalise the method for computing Fourier transform originally given in [8] for multinomial trace functions $f = f_{\lambda,u,v} : GF(p^n) \to GF(p)$ of the form $Tr_1^k(\lambda x^{p^k+1}) + Tr_1^n(ux)Tr_1^n(vx)$ for any odd prime p, where $n = 2k, \lambda \in GF(p^k)^*, u, v \in GF(p^n)^*$. It is shown that the choice of λ, u and v, ensuring that f is bent, 2-plateaued or near-bent is directly related to finding the subset $A \subset GF(p)^3$ (cf. Section 4). Moreover, we give an efficient method for defining the set A that corresponds for any odd prime p. This is not the case in the previous works, where the set A is only explicitly defined just for the case $p = 3$.

The rest of this article is organized as follows. In Section 2 some basic definitions and notions are given. The analysis of the Fourier transform of the function f is presented in Section 3. Some sufficient conditions for a given function to be bent, 2-plateaued and near-bent are derived in Section 4. Some concluding remarks are found in Section 5.

2. Preliminaries

In the sequel, let $\mathbf{F}_{p^n}$ denote the finite Galois field $GF(p^n)$ consisting of p^n elements. The group of units of $\mathbf{F}_{p^n}$, denoted by $\mathbf{F}_{p^n}^*$, is a cyclic group consisting of $p^n - 1$ elements. An element $\alpha \in \mathbf{F}_{p^n}$ is said to be a primitive element if it is a generator of the multiplicative group $\mathbf{F}_{p^n}^*$. $\mathbf{F}_{p^n}$ is an n-dimensional vector space over $\mathbf{F}_p$. After fixing an $\mathbf{F}_p$-basis $(\gamma_0, \ldots, \gamma_{n-1})$ of $\mathbf{F}_{p^n}$, the mapping

$$\mathbf{F}_p^n \ni (\alpha_0, \ldots, \alpha_{n-1}) \mapsto \alpha_0\gamma_0 + \ldots + \alpha_{n-1}\gamma_{n-1} \in \mathbf{F}_{p^n}$$

defines an isomorphism of vector spaces over $\mathbf{F}_p$.

A bent function $f(x)$ is called regular if for every $a \in \mathbf{F}_{p^n}$ the normalized Fourier coefficient $p^{-\frac{n}{2}}\widehat{f}(a)$ equals to complex p-th root of unity, that is, $p^{-\frac{n}{2}}\widehat{f}(a) = \omega^{f^*(a)}$ where the function $f^*(a)$ is called the dual of $f(x)$. A binary bent function is always regular. For odd p, a p-ary bent function $f(x)$ may not be regular, but its Fourier transform coefficients [3] satisfy

$$\widehat{f}(a) = \begin{cases} \pm p^{\frac{n}{2}}\omega^{f^*(a)}, & \text{if } p \equiv 1 \pmod 4 \\ \pm \imath p^{\frac{n}{2}}\omega^{f^*(a)}, & \text{if } p \equiv 3 \pmod 4 \text{ and } n \text{ is odd} \end{cases}. \tag{2.1}$$

Such a function is called weakly regular, if for all $a \in \mathbf{F}_{p^n}$, $\imath$ is fixed.
If for all $a \in \mathbf{F}(p^n)$, $\widehat{f}(a) \in \{0, \pm p^{\frac{n+s}{2}}\}$, where $0 \leq s \leq n$, then a p-ary function $f(x)$ is called s-plateaued. In the case of $s = 1$, f is called near-bent.

The trace function $Tr_k^n : \mathbf{F}_{p^n} \to \mathbf{F}_{p^k}$, a mapping to the subfield $\mathbf{F}_{p^k}$, where $k \mid n$, is defined as

$$Tr_k^n(x) = x + x^{p^k} + x^{p^{2k}} + \ldots + x^{p^{(n/k-1)k}}, \text{ for all } x \in \mathbf{F}_{p^n}. \tag{2.2}$$

3. The Fourier coefficients of $f_{\lambda,u,v}$

Let $f_{\lambda,u,v}(x) = Tr_1^k(\lambda x^{p^k+1}) + Tr_1^n(ux)Tr_1^n(vx)$, where $n = 2k, \lambda \in \mathbf{F}_{p^k}^*, u, v \in \mathbf{F}_{p^n}^*$. In this section we compute the Fourier transform of the function $f(x)$ for any odd prime p. This result will help us to divide the class of functions $f_{\lambda,u,v}$ into subclasses of bent, near-bent and 2-plateaued functions.

Before we prove the main theorem we need the following preparatory result.

Lemma 1. *[2, 4] Let $n = 2k$ and $\lambda \in \mathbf{F}_{p^k}^*$. For any odd prime p, the p-ary monomial $g(x) = Tr_1^k(\lambda x^{p^k+1})$ is a weakly regular bent function. Moreover, for $a \in \mathbf{F}_{p^n}$ the corresponding Fourier transform coefficient of $g(x)$ is equal to*

$$\widehat{g}(a) = -p^k\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})}. \tag{3.1}$$

The authors in [8] computed the Fourier transform of the function $f_{\lambda,u,v}$ for $p = 3$. In what follows, we continue the work of [8, 9] and present the general form of the Fourier transform of $f_{\lambda,u,v}$ for any odd prime p.

Theorem 1. *Let $n = 2k$ be a positive integer and $u, v \in \mathbf{F}_{p^n}^*$. Define the function $f(x)$ by*

$$f(x) = g(x) + Tr_1^n(ux)Tr_1^n(vx), \tag{3.2}$$

where $g(x) = Tr_1^k(\lambda x^{p^k+1})$ is a p-ary function defined on $\mathbf{F}_{p^n}$. Then for any $a \in \mathbf{F}_{p^n}$, the corresponding Fourier transform coefficient of $f = f_{\lambda,u,v}$ is equal to

$$\widehat{f}(a) = \frac{1}{p}\sum_{0\leq i,j<p}\omega^{ij}\widehat{g}(a - jv + iu). \tag{3.3}$$

Proof. For $i, j = 0, \ldots, p-1$ and $u, v \in \mathbf{F}_{p^n}^*$ define the sets $T_i = \{x \in \mathbf{F}_{p^n} \mid Tr_1^n(ux) = i\}$ and denote

$$S_i(a) = \sum_{x\in T_i}\omega^{g(x)-Tr_1^n(ax)}, \quad R_i(a - jv) = \sum_{x\in T_i}\omega^{g(x)-Tr_1^n((a-jv)x)}.$$

The Fourier transform coefficient of $f(x)$ at a is equal to

$$\begin{aligned}\widehat{f}(a) &= \sum_{x\in\mathbf{F}_{p^n}} \omega^{f(x)-Tr_1^n(ax)} = \sum_{x\in\mathbf{F}_{p^n}} \omega^{g(x)+Tr_1^n(ux)Tr_1^n(vx)-Tr_1^n(ax)} \\ &= \sum_{x\in T_0} \omega^{g(x)-Tr_1^n(ax)} + \sum_{x\in T_1} \omega^{g(x)-Tr_1^n((a-v)x)} + \sum_{x\in T_2} \omega^{g(x)-Tr_1^n((a-2v)x)} + \ldots + \sum_{x\in T_{p-1}} \omega^{g(x)-Tr_1^n((a-(p-1)v)x)} \\ &= S_0(a) + R_1(a-v) + R_2(a-2v) + \ldots + R_{p-1}(a-(p-1)v) \\ &= S_0(a) + \sum_{j=1}^{p-1} R_j(a-jv)\end{aligned}$$

Let us first compute $S_0(a)$. By definition of T_i we have

$$\sum_{x\in T_i} \omega^{g(x)-Tr_1^n((a+u)x)} = \sum_{x\in T_i} \omega^{g(x)-Tr_1^n(ax)-i} = \omega^{-i} S_i(a).$$

Therefore, for any $b \in \mathbf{F}_p$ the Fourier transform of the function g at the point $a + bu$ can be computed as

$$\widehat{g}(a+bu) = \sum_{i=0}^{p-1} \omega^{-bi} S_i(a). \tag{3.4}$$

Since $\omega \in \mathbb{C}$ is a primitive p-root of unity, $1 + \omega + \omega^2 + \ldots + \omega^{p-1} = 0$. Hence, adding p equations of (3.4) gives

$$S_0(a) = \frac{1}{p} \sum_{i=0}^{p-1} \widehat{g}(a+iu). \tag{3.5}$$

Next we calculate $R_j(a - jv)$. Similar to the above, using the definition of T_i, we have

$$\widehat{g}(a-jv+bu) = \sum_{i=0}^{p-1} \omega^{-bi} R_i(a-jv)$$

The last expression can be written in the matrix form as

$$\begin{bmatrix} \widehat{g}(a-jv) \\ \widehat{g}(a-jv+u) \\ \widehat{g}(a-jv+2u) \\ \vdots \\ \widehat{g}(a-jv+(p-1)u) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 1 & \omega^{p-1} & \omega^{p-2} & \ldots & \omega^2 & \omega \\ 1 & \omega^{p-2} & \omega^{2\cdot(p-2)} & \ldots & \omega^{(p-2)\cdot(p-2)} & \omega^{(p-1)\cdot(p-2)} \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 1 & \omega & \omega^2 & \ldots & \omega^{p-2} & \omega^{p-1} \end{bmatrix} \cdot \begin{bmatrix} R_0(a-jv) \\ R_1(a-jv) \\ R_2(a-jv) \\ \vdots \\ R_{p-1}(a-jv) \end{bmatrix}.$$

where the coefficient matrix represents Discrete Fourier Transform (DFT) matrix. It is well-known that the inverse DFT matrix is

$$\frac{1}{p} \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 1 & \omega & \omega^2 & \ldots & \omega^{p-2} & \omega^{p-1} \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 1 & \omega^{p-2} & \omega^{2\cdot(p-2)} & \ldots & \omega^{(p-2)\cdot(p-2)} & \omega^{(p-1)\cdot(p-2)} \\ 1 & \omega^{p-1} & \omega^{p-2} & \ldots & \omega^2 & \omega \end{bmatrix}.$$

Therefore, we have

$$R_j(a - jv) = \frac{1}{p}\sum_{i=0}^{p-1} \omega^{i\cdot j}\widehat{g}(a - jv + iu). \tag{3.6}$$

Then the desired conclusion follows from (3.5) and (3.6). □

In what follows, we give explicit formulas for computing $S_0(a)$ and $R_j(a - jv)$ given by (3.5) and (3.6), respectively.

Let $g(x) = Tr_1^k(\lambda x^{p^k+1})$. According to (3.1) and using the fact $Tr_1^n(x) = Tr_1^k(Tr_k^n(x))$, we have

$$\widehat{g}(a + iu) = -p^k\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})-iTr_1^n(\lambda^{-1}a^{p^k}u)-i^{p^k+1}Tr_1^k(\lambda^{-1}u^{p^k+1})}, \quad i = 0, \ldots, p-1.$$

Denote $c_1 = Tr_1^n(\lambda^{-1}a^{p^k}u)$ and $t_1 = Tr_1^k(\lambda^{-1}u^{p^k+1})$. By (3.5) it follows

$$S_0(a) = -\frac{1}{p}p^k\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})}[1 + \omega^{-c_1-t_1} + \omega^{-2c_1-2^{p^k+1}t_1} + \ldots + \omega^{-(p-1)c_1-(p-1)^{p^k+1}t_1}].$$

Since ω is a primitive p-th root of unity it holds $\omega^{p^k} = 1$, i.e., $\omega^{p^k+1} = \omega$. Therefore

$$S_0(a) = -\frac{1}{p}p^k\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})}[1 + \omega^{-c_1-t_1} + \omega^{-2c_1-2\cdot 2t_1} + \ldots + \omega^{2c_1-2\cdot 2t_1} + \omega^{c_1-t_1}]. \tag{3.7}$$

On the other side,

$$\widehat{g}(a - jv + iu) = -p^k\omega^{-Tr_1^k(\lambda^{-1}(a-v)^{p^k+1})-ijTr_1^n(\lambda^{-1}a^{p^k}u)+ijTr_1^n(\lambda^{-1}v^{p^k}u)-(ij)^{p^k+1}Tr_1^k(\lambda^{-1}u^{p^k+1})}.$$

Denote $c_2 = Tr_1^n(\lambda^{-1}a^{p^k}v)$, $t_2 = Tr_1^k(\lambda^{-1}v^{p^k+1})$ and $t_0 = Tr_1^n(\lambda^{-1}v^{p^k}u)$. By (3.6) it follows

$$\begin{aligned} R_j(a - jv) = &-\frac{1}{p}p^k\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})}[\omega^{jc_2-j\cdot jt_2} + \omega^{j+jc_2-j\cdot jt_2-c_1+jt_0-t_1} + \omega^{2j+jc_2-j\cdot jt_2-2c_1+2jt_0-2\cdot 2t_1}\ldots + \\ &\omega^{(p-1)j+jc_2-j\cdot jt_2-(p-1)c_1+j(p-1)\cdot t_0-(p-1)(p-1)\cdot t_1}]. \end{aligned} \tag{3.8}$$

In the next section we apply the above computation to construct some (near)-bent and 2-plateaued functions in the form of (3.2).

4. Quadratic p-ary bent, near-bent and 2-plateaued functions

To make it easier construction of bent, near-bent and 2-plateaued functions, we are going to construct a subset A of $\mathbf{F}_p^3$, $p > 3$, which will help us to separate bent from non-bent functions. Its construction is described in the following way:

$$
\begin{aligned}
A \quad = \{ \quad & \boxed{(0, 1, \tfrac{1}{4} \mod p)}, (0, 2, a_{02}), \ldots, (0, p-1, a_{0(p-1)}), \\
& \boxed{(1, 1, 1)}, (1, 2, a_{12}), (1, 3, a_{13}), \ldots, (1, p-1, a_{1(p-1)}), \\
& (2, 1, a_{21}), (2, 2, a_{22}), (2, 3, a_{23}), \ldots, (2, p-1, a_{2(p-1)}), \\
& \boxed{(3, 1, 4)}, (3, 2, a_{32}), (3, 3, a_{33}), \ldots, (3, p-1, a_{3(p-1)}), \\
& \vdots \\
& (\frac{p-3}{2}, 1, a_{(\frac{p-3}{2})1}), (\frac{p-3}{2}, 2, a_{(\frac{p-3}{2})2}), \ldots, (\frac{p-3}{2}, p-1, a_{(\frac{p-3}{2})(p-1)}), \\
& (\frac{p-1}{2}, 1, a_{(\frac{p-3}{2})1}), (\frac{p-1}{2}, 2, a_{(\frac{p-3}{2})2}), \ldots, (\frac{p-1}{2}, p-1, a_{(\frac{p-3}{2})(p-1)}), \qquad (4.1) \\
& \vdots \\
& (p-3, 1, 1), (p-3, 2, a_{12}), (p-3, 3, a_{13}), \ldots, (p-3, p-1, p-1), \\
& (p-2, 1, \frac{1}{4} \mod p), (p-2, 2, a_{02}), (p-2, 3, a_{13}), \ldots, (p-2, p-1, a_{0(p-1)}), \\
& \boxed{(p-1, 0, 0)}, \ldots, (p-1, 0, p-1), (p-1, 1, 0), \ldots, (p-1, p-1, 0) \ \}
\end{aligned}
$$

where $a_{ij} \in \{0, 1, \ldots, p-1\}$ and the boxed triples are fixed for any prime number p. The remaining coefficients a_{ij} must satisfy the following conditions:

1. In each row, the product of the second and third numbers of a triple satisfies

$$1 \cdot a_{i1} \equiv 2 \cdot a_{i2} \equiv 3 \cdot a_{i3} \equiv \ldots \equiv (p-1) \cdot a_{i(p-1)} \mod p$$

2. The first $\frac{p-1}{2}$ rows are symmetric to the next $\frac{p-1}{2}$ rows in such a way that first and $(p-2)$ row, second and $(p-3)$, third and $(p-4)$, and so on, have the same second and third number of each triple.
3. In each column, the sum of the third numbers of a triple satisfies

$$a_{0j} + a_{1j} + a_{2j} + \ldots + a_{(\frac{p-3}{2})j} \equiv 0 \mod p$$

Remark 1. *Note that we have $p-1$ rows with $p-1$ triples, and the last row has $2p-1$ triples, which means that the cardinality of the subset A is*

$$\#A = (p-1) \cdot (p-1) + (2p-1) = p^2.$$

Remark 2. *The equation in third condition has more than one solution for any odd prime $p > 7$. In total, there is $(\frac{p-7}{2})! \cdot (\frac{p-7}{2})!$ possible solutions taking into account the first two conditions.*

Example 1. *Let us compute the set A for $p = 11$. At the beginning we have*

$$
\begin{aligned}
A \quad = \{ \quad & \boxed{(0, 1, \tfrac{1}{4} \mod 11)}, (0, 2, a_{02}), \ldots, (0, 9, a_{09}), (0, 10, a_{010}), \\
& \boxed{(1, 1, 1)}, (1, 2, a_{12}), \ldots, (1, 9, a_{19}), (1, 10, a_{110}), \\
& (2, 1, a_{21}), (2, 2, a_{22}), \ldots, (2, 9, a_{29}), (2, 10, a_{210}),
\end{aligned}
$$

$$\boxed{(3,1,4)}, (3,2,a_{32}), \ldots, (3,9,a_{39}), (3,10,a_{310}),$$
$$(4,1,a_{41}), (4,2,a_{42}), \ldots, (4,9,a_{49}), (4,10,a_{410}),$$
$$(5,1,a_{41}), (5,2,a_{42}), \ldots, (5,9,a_{49}), (5,10,a_{410}),$$
$$\boxed{(6,1,4)}, (6,2,a_{32}), \ldots, (6,9,a_{39}), (6,10,a_{310}),$$
$$(7,1,a_{21}), (7,2,a_{22}), \ldots, (7,9,a_{29}), (7,10,a_{210}),$$
$$\boxed{(8,1,1)}, (8,2,a_{12}), \ldots, (8,9,a_{19}), (8,10,a_{110}),$$
$$\boxed{(9,1,\tfrac{1}{4} \mod p)}, (9,2,a_{02}), \ldots, (9,9,a_{09}), (9,10,a_{010}),$$
$$\boxed{(10,0,0)}, (10,0,1), \ldots, (10,9,0), (10,10,0) \}$$

With the help of boxed triples and given conditions the remaining coefficients in the rows can be computed. For instance, in the first row, since $\frac{1}{4} \equiv 3 \mod 11$*, we are solving the following equations*

$$1 \cdot 3 \equiv 2 \cdot a_{02} \equiv \ldots \equiv 9 \cdot a_{09} \equiv 10 \cdot a_{010} \equiv 3 \mod 11$$

It is easy to see that $a_{02} = 7, a_{03} = 1, a_{04} = 9, a_{05} = 5, a_{06} = 6, a_{07} = 2, a_{08} = 10, a_{09} = 4, a_{010} = 8$*. After other computations we get*

$$\begin{aligned} A = \{&(0,1,3), (0,2,7), (0,3,1), (0,4,9), (0,5,5), (0,6,6), (0,7,2), (0,8,10), (0,9,4), (0,10,8)\\ &(1,1,1), (1,2,6), (1,3,4), (1,4,3), (1,5,9), (1,6,2), (1,7,8), (1,8,7), (1,9,5), (1,10,10)\\ &(2,1,a_{21}), (2,2,a_{22}), (2,3,a_{23}), (2,4,a_{24}), (2,5,a_{25}), (2,6,a_{26}), (2,7,a_{27}), (2,8,a_{28}),\\ &(2,9,a_{29}), (2,10,a_{210}), (3,1,4), (3,2,2), (3,3,5), (3,4,1), (3,5,3), (3,6,8), (3,7,10),\\ &(3,8,6), (3,9,9), (3,10,7), (4,1,a_{41}), (4,2,a_{42}), (4,3,a_{43}), (4,4,a_{44}), (4,5,a_{45}), (4,6,a_{46}),\\ &(4,7,a_{47}), (4,8,a_{48}), (4,9,a_{49}), (4,10,a_{410}), (5,1,a_{41}), (5,2,a_{42}), (5,3,a_{43}), (5,4,a_{44}), (5,5,a_{45}),\\ &(5,6,a_{46}), (5,7,a_{47}), (5,8,a_{48}), (5,9,a_{49}), (5,10,a_{410}), (6,1,4), (6,2,2), (6,3,5), (6,4,1),\\ &(6,5,3), (6,6,8), (6,7,10), (6,8,6), (6,9,9), (6,10,7), (7,1,a_{21}), (7,2,a_{22}), (7,3,a_{23}), (7,4,a_{24}),\\ &(7,5,a_{25}), (7,6,a_{26}), (7,7,a_{27}), (7,8,a_{28}), (7,9,a_{29}), (7,10,a_{210}), (8,1,1), (8,2,6), (8,3,4),\\ &(8,4,3), (8,5,9), (8,6,2), (8,7,8), (8,8,7), (8,9,5), (8,10,10), (9,1,3), (9,2,7), (9,3,1),\\ &(9,4,9), (9,5,5), (9,6,6), (9,7,2), (9,8,10), (9,9,4), (9,10,8), (10,0,0), (10,0,1), (10,0,2),\\ &(10,0,3), (10,0,4), (10,0,5), (10,0,6), (10,0,7), (10,0,8), (10,0,9), (10,0,10), (10,1,0),\\ &(10,2,0), (10,3,0), (10,4,0), (10,5,0), (10,6,0), (10,7,0), (10,8,0), (10,9,0), (10,10,0) \} \end{aligned}$$

With the help of third condition we can calculate the rest of the coefficients. In fact, we only need to solve the following equation

$$\begin{aligned} 3 + 1 + a_{21} + 4 + a_{41} &\equiv 0 \mod 11\\ a_{21} + a_{41} &\equiv 3 \mod 11 \end{aligned}$$

The possible solutions are $a_{21} = 5, a_{41} = 9$*, or* $a_{21} = 9, a_{41} = 5$*, or* $a_{21} = 8, a_{41} = 6$ *or* $a_{21} = 6, a_{41} = 8$*. We can choose whatever solution we want. Therefore, for* $a_{21} = 9$ *and* $a_{41} = 5$ *we have*

$$\begin{aligned} A = \{&(0,1,3), (0,2,7), (0,3,1), (0,4,9), (0,5,5), (0,6,6), (0,7,2), (0,8,10), (0,9,4), (0,10,8) \end{aligned}$$

$(1,1,1),(1,2,6),(1,3,4),(1,4,3),(1,5,9),(1,6,2),(1,7,8),(1,8,7),(1,9,5),(1,10,10)$
$(2,1,9),(2,2,10),(2,3,3),(2,4,5),(2,5,4),(2,6,7),(2,7,6),(2,8,8),(2,9,1),(2,10,2)$
$(3,1,4),(3,2,2),(3,3,5),(3,4,1),(3,5,3),(3,6,8),(3,7,10),(3,8,6),(3,9,9),(3,10,7)$
$(4,1,5),(4,2,8),(4,3,9),(4,4,4),(4,5,1),(4,6,10),(4,7,7),(4,8,2),(4,9,3),(4,10,6)$
$(5,1,5),(5,2,8),(5,3,9),(5,4,4),(5,5,1),(5,6,10),(5,7,7),(5,8,2),(5,9,3),(5,10,6)$
$(6,1,4),(6,2,2),(6,3,5),(6,4,1),(6,5,3),(6,6,8),(6,7,10),(6,8,6),(6,9,9),(6,10,7)$
$(7,1,9),(7,2,10),(7,3,3),(7,4,5),(7,5,4),(7,6,7),(7,7,6),(7,8,8),(7,9,1),(7,10,2)$
$(8,1,1),(8,2,6),(8,3,4),(8,4,3),(8,5,9),(8,6,2),(8,7,8),(8,8,7),(8,9,5),(8,10,10)$
$(9,1,3),(9,2,7),(9,3,1),(9,4,9),(9,5,5),(9,6,6),(9,7,2),(9,8,10),(9,9,4),(9,10,8)$
$(10,0,0),(10,0,1),(10,0,2),(10,0,3),(10,0,4),(10,0,5),(10,0,6),(10,0,7),(10,0,8),$
$(10,0,9),(10,0,10),(10,1,0),(10,2,0),(10,3,0),(10,4,0),(10,5,0),(10,6,0),$
$(10,7,0),(10,8,0),(10,9,0),(10,10,0)\ \}$

The following conjecture is the main result of this section and shows how the set A defined above can be used in the construction of quadratic bent, near-bent and 2-plateaued functions. Unfortunately, we are unable to give a complete proof, for the following reasons: first, not all triples of the set A are described in a general way, so we are not able to verify all triples, and second, the triples of $\mathbf{F}_p^3$ cannot be described in a way that is suitable for our proof technique. Therefore, we give a partial proof, and complete proof remains as an interesting problem for all mathematics enthusiasts.

Conjecture 1. *Let $n = 2k$ with $k > 1$ and $\lambda \in \mathbf{F}_{p^k}^*$, $u, v \in \mathbf{F}_{p^n}^*$. Let the subset $A \subset \mathbf{F}_p^3$ be defined as in (4.1) and $f_{\lambda,u,v}(x)$ be a p-ary function defined as $f = f_{\lambda,u,v}(x) = Tr_1^k(\lambda x^{p^k+1}) + Tr_1^n(ux)Tr_1^n(vx)$. Denote a triple $T = (Tr_1^n(\lambda^{-1}v^{p^k}u), Tr_1^k(\lambda^{-1}u^{p^k+1}), Tr_1^k(\lambda^{-1}v^{p^k+1}))$. Then*

1. *If $T \in \mathbf{F}_p^3 \setminus A$, then f is bent.*
2. *If $T \in A \setminus \{(p-1,0,0)\}$, then f is near-bent.*
3. *If $T = (p-1,0,0)$, then f is a 2-plateaued function.*

Idea of Proof. Let us show the proof technique for the third statement. According to (3.7) and (3.8) we have

$$\begin{aligned} S_0(a) &= -\frac{1}{p}p^k\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})}[1+\omega^{-c_1}+\omega^{-2c_1}+\ldots+\omega^{2c_1}+\omega^{c_1}] \\ R_j(a-jv) &= -\frac{1}{p}p^k\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})}[\omega^{jc_2}+\omega^{j+jc_2-c_1}+\ldots+\omega^{j(p-1)+jc_2-(p-1)c_1}]. \end{aligned}$$

Then, using equation (3.3) we get

$$\widehat{f}(a) = -\frac{1}{p}p^k\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})}[\sum_{i=0}^{p-1}(\omega^{ic_2}+\omega^{i(c_2+p)-c_1}+\ldots+\omega^{i(c_2+(p-1)p)-(p-1)c_1})]$$

If $c_2 = 0$, then

$$\widehat{f}(a) = -\frac{1}{p}p^k\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})}[p+\omega^{-c_1}p+\omega^{-2c_1}p+\ldots+\omega^{-(p-1)c_1}p]$$

$$= \quad -p^k\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})}[1+\omega^{-c_1}+\omega^{-2c_1}+\ldots+\omega^{-(p-1)c_1}].$$

If $c_1 = 0$, then $\widehat{f}(a) = -p^{k+1}\omega^{-Tr_1^k(\lambda^{-1}a^{p^k+1})}$, otherwise is 0.

If $c_2 \neq 0$, then $\widehat{f}(a) = 0$.

Therefore, $|\widehat{f}(a)| \in \{0, p^{k+1}\}$ for all $a \in \mathbf{F}_{p^n}$. Then f is 2-plateaued.

This technique can also be used to prove either of the first two statements, but we are unable to check all possible triples.

Example 2. *Let $p = 7$ and define the function $f(x) = Tr_1^k(\lambda x^{7^k+1}) + Tr_1^n(ux)Tr_1^n(vx)$. By (4.1) we can define the set A as*

$$\begin{aligned} A \quad = \{ \quad & (0,1,2),(0,2,1),(0,3,3),(0,4,4),(0,5,6),(0,6,5),\\ & (1,1,1),(1,2,4,(1,3,5),(1,4,2),(1,5,3),(1,6,6),\\ & (2,1,4),(2,2,2),(2,3,6),(2,4,1),(2,5,5),(2,6,3),\\ & (3,1,4),(3,2,2),(3,3,6),(3,4,1),(3,5,5),(3,6,3),\\ & (4,1,1),(4,2,4),(4,3,5),(4,4,2),(4,5,3),(4,6,6),\\ & (5,1,2),(5,2,1),(5,3,3),(5,4,4),(5,5,6),(5,6,5),\\ & (6,0,0),(6,0,1),(6,0,2),(6,0,3),(6,0,4),(6,0,5),(6,0,6),\\ & (6,1,0),(6,2,0),(6,3,0),(6,4,0),(6,5,0),(6,6,0) \ \} \end{aligned}$$

In what follows, we give some triples (t_0, t_1, t_2) such that the function f is bent, near-bent and 2-plateaued, respectively. It can be easily verified that for any $T \in \mathbf{F}_7^3 \setminus A$ the function f is bent. For instance, if $T = (2,3,4)$, then

$$\widehat{f}(a) = \begin{cases} 7^k\omega^{-Tr_1^k(\lambda^{-1}a^{7^k+1})}, & if\,(c_1,c_2) = \{(0,0)\} \\ 7^k\omega^{-Tr_1^k(\lambda^{-1}a^{7^k+1})+1}, & if\,(c_1,c_2) = \{(1,0),(1,1),(2,3),(2,6),\\ & \qquad (5,1),(5,4),(6,0),(6,6)\} \\ 7^k\omega^{-Tr_1^k(\lambda^{-1}a^{7^k+1})+2}, & if\,(c_1,c_2) = \{(1,3),(1,5),(3,0),(3,3),\\ & \qquad (4,0),(4,4),(6,2),(6,4)\} \\ 7^k\omega^{-Tr_1^k(\lambda^{-1}a^{7^k+1})+3}, & if\,(c_1,c_2) = \{(0,2),(0,5),(1,4),(2,4),\\ & \qquad (2,5),(5,2),(5,3),(6,3)\} \\ 7^k\omega^{-Tr_1^k(\lambda^{-1}a^{7^k+1})+4}, & if\,(c_1,c_2) = \{(2,0),(2,2),(3,1),(3,2),\\ & \qquad (4,5),(4,6),(5,0),(5,5)\} \\ 7^k\omega^{-Tr_1^k(\lambda^{-1}a^{7^k+1})+5}, & if\,(c_1,c_2) = \{(0,3),(0,4),(2,1),(3,4),\\ & \qquad (3,6),(4,1),(4,3),(5,6)\} \\ 7^k\omega^{-Tr_1^k(\lambda^{-1}a^{7^k+1})+6}, & if\,(c_1,c_2) = \{(0,1),(0,6),(1,2),(1,6),\\ & \qquad (3,5),(4,2),(6,1),(6,5)\} \end{cases}.$$

Similarly, for any $T \in A \setminus (6,0,0)$ the function f is near-bent. For instance, if $T = (1,1,1)$, then

$$\widehat{f}(a) = \begin{cases} \pm 7^{k+\frac{1}{2}}\omega^{-Tr_1^k(\lambda^{-1}a^{7^k+1})}, & if\,(c_1,c_2) = \{(0,0),(1,1),(2,2),(3,3),\\ & \qquad (4,4),(5,5),(6,6)\} \\ 0, & otherwise \end{cases}.$$

At the end, if $T = (6, 0, 0)$ *then* f *is 2-plateaued, i.e.,*

$$\widehat{f}(a) = \begin{cases} -7^{k+1}\omega^{-Tr_1^k(\lambda^{-1}a^{7^k+1})}, & \text{if } (c_1, c_2) = \{(0,0)\} \\ 0, & \text{otherwise} \end{cases}.$$

5. Conclusions

The exact computation of the Fourier transform for a given p-ary function of the form $f_{\lambda,u,v}$ has been established. Also, certain conditions such that a given p-ary function is bent, near-bent or 2-plateaued has been presented. It will be interesting to completely determine the distribution of the Fourier spectrum of these functions and try to determine the Fourier transform of the other p-ary functions using the presented method.

Acknowledgments

The research presented in this paper was financially supported by the Slovenian Research Agency under research program No. P2-0037 – Future Internet technologies: Concepts, architectures, services and socio-economic issues.

Conflict of interest

The author declares that he has no conflict of interest.

References

1. C. Carlet, S. Mesnager, Four decades of research on bent functions, *Design, Codes Cryptogr.*, **78** (2016), 5–50. doi: 10.1007/s10623-015-0145-8.
2. T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, *IEEE T. Inform. Theory*, **52** (2006), 2018–2032. doi: 10.1109/TIT.2006.872854.
3. P. V. Kumar, R. A. Scholtz, L. R. Welch, Generalized bent functions and their properties, *J. Comb. Theory, Series A*, **40** (1985), 90–107. doi: 10.1016/0097-3165(85)90049-4.
4. S. C. Liu, J. J. Komo, Nonbinary Kasami sequences over $GF(p)$, *IEEE T. Inform. Theory*, **38** (1992), 1409–1412. doi: 10.1109/18.144728.
5. S. Mesnager, *Bent functions: Fundamentals and results*, Springer, Berlin, 2016. doi: 10.1007/978-3-319-32595-8.
6. O. S. Rothaus, On bent functions, *J. Comb. Theory, Series A*, **20** (1976), 300–305. doi: 10.1016/0097-3165(76)90024-8.
7. Y. Qi, C. Tang, Z. Zhou, C. Fan, New infinite families of p-ary weakly regular bent functions, *arXiv: 1508.05672*, 2015. doi: 10.3934/amc.2018019.
8. G. Xu, X. Cao, S. Xu, Constructing new APN functions and bent functions over finite fields of odd characteristic via the switching method, *Cryptogr. Commun.* **8** (2016), 155–171. doi: 10.1007/s12095-015-0145-6.

9. G. Xu, X. Cao, S. Xu, Several classes of quadratic ternary bent, near-bent and 2-plateaued functions, *Int. J. Found. Comput. S.*, **28** (2017), 1–18. doi: 10.1142/S0129054117500010.

10. Y. Zheng, X. M. Zhang, On plateaued functions, *IEEE T. Inform. Theory*, **47** (2001), 1215–1223. doi: 10.1109/18.915690.

AIMS Press