On cryptographic properties of the Welch permutation and a related conjecture

Yibo Wang[†]
Wrya Kadir[‡] Chunlei Li[‡] Yongbo Xia[†*]

[†] Dept. of Mathematics and Statistics, South-Central University for Nationalities, China

‡ Department of Informatics, University of Bergen, Norway

Abstract

In this paper, we determine the differential spectrum and the Walsh transform of the Welch permutation $g(x) = x^{2^{m+1}+1} + x^3 + x$ of $\mathbb{F}_{2^{2m+1}}$, which was derived from the Welch APN power function x^{2^m+3}. As an application, the properties of $g(x)$ are used to partly resolve a conjecture by Ding [9] on a class of binary linear codes constructed from the Welch APN power functions.

Keywords: Permutation, Power mapping, Differential spectrum, Walsh spectrum, Linear codes

1 Introduction

Let $\mathbb{F}_{2^n}$ denote the finite field of 2^n elements and $\mathbb{F}_{2^n}^*$ be its multiplicative group. For a vectorial Boolean function $F(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, denote

$$N_F(a,b) = |\{x \in \mathbb{F}_{2^n} \mid F(x+a) + F(x) = b\}|. \tag{1}$$

The differential uniformity of $F(x)$ is defined by

$$\Delta_F = \max\{N_F(a,b) \mid a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\}.$$

Nyberg defined a mapping $F(x)$ to be differentially δ-uniform if $\Delta_F = \delta$ [14]. Differential uniformity is one of the most important notions in symmetric cryptography. It quantifies the security of S-boxes used in block ciphers with respect to the differential attack. For practical applications, cryptographic functions are desirable to have low differential uniformity. It is clear that the equation $F(x+a) + F(x) = b$ have solutions in pairs. Thus, $\Delta_F = 2$ is the smallest possible value for the differential uniformity of $F(x)$. A function $F(x)$ is said to be almost perfect nonlinear (APN) if its differential uniformity is 2. Equivalently, a function $F(x)$ is APN if its derivative function $D_aF(x) := F(x+a) + F(x)$,

*Corresponding author: xia@mail.scuec.edu.cn

for any $a \in \mathbb{F}_{2^n}^*$, is a two-to-one function over $\mathbb{F}_{2^n}$. APN functions are of great interest due to their importance in the design of S-boxes in block ciphers and their close connection to optimal objects in coding theory and combinatorial theory. Constructing APN functions has been intensively studied in the last three decades, and by far the known families of APN functions over $\mathbb{F}_{2^n}$ can be found in the recent paper [6]. Besides the differential uniformity, the differential spectrum of $F(x)$, namely the value distribution of $N_F(a,b)$ for $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, is also an important notion for estimating its resistance against variants of differential cryptanalysis [1, 2, 5, 8]. In addition to differential properties, nonlinearity and Walsh transform are important measurements to assess the properties of a vectorial Boolean function against linear cryptanalysis.

Nonlinear functions also have a number of applications in constructing error-correcting codes with good properties [7, 9]. An $[n,k,d]$ binary linear code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_2^n$ with minimum (Hamming) distance d. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by $1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$. The sequence $(1, A_1, A_2, \ldots, A_n)$ is called the weight distribution of $\mathcal{C}$. Clearly, the weight distribution gives the minimum distance of the code, and thus the error correcting capability. In addition, the weight distribution of a code allows the computation of the error probability of error detection and correction with respect to some error detection and error correction algorithms. A binary code $\mathcal{C}$ is said to be a t-weight code if the number of nonzero A_i in the sequence $(A_1, A_2, \ldots, A_n)$ is equal to t. Binary linear codes with few weights have many applications [7, 9], including secret sharing schemes, authentication codes, association schemes and strongly regular graphs.

Ding et. al in [10, 9] introduced a generic construction of binary linear codes from a subset $D = \{d_1, d_2, \ldots, d_\ell\}$ of $\mathbb{F}_{2^n}$ and the absolute trace function $\mathrm{Tr}_1^n(\cdot)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ as

$$\mathcal{C}_D = \{\mathbf{c}_a = (\mathrm{Tr}_1^n(ad_1), \mathrm{Tr}_1^n(ad_2), \ldots, \mathrm{Tr}_1^n(ad_\ell)) : a \in \mathbb{F}_{2^n}\}. \tag{2}$$

This construction is generic in the sense that many classes of known codes could be produced by selecting proper defining sets D. When the defining set D is properly chosen, the code $\mathcal{C}_D$ can have a few nonzero weights. In [9] Ding investigated the properties of binary linear codes from the images of certain functions on $\mathbb{F}_{2^n}$ and proposed several conjectures on properties of the constructed codes, including the following one from the Welch APN power functions.

Conjecture 1. [9, Conjecture 33] Let $n = 2m+1$, $F(x) = x^{2^m+3}$, $f(x) = F(x) + F(x+1) + 1$ and $D(f) = \{d_1, d_2, \ldots, d_\ell\} = \{f(x) \,|\, x \in \mathbb{F}_{2^n}\}$. Define the binary code $\mathcal{C}_{D(f)}$ as

$$\mathcal{C}_{D(f)} = \{\mathbf{c}_a = (\mathrm{Tr}_1^n(ad_1), \mathrm{Tr}_1^n(ad_2), \ldots, \mathrm{Tr}_1^n(ad_\ell)) : a \in \mathbb{F}_{2^n}\}.$$

If $n \in \{5, 7\}$, then $\mathcal{C}_{D(f)}$ is a three-weight code with length 2^{n-1} and dimension n. If $n \geq 9$, then $\mathcal{C}_{D(f)}$ is a five-weight code with length 2^{n-1} and dimension n.

In this paper, we investigate certain cryptographic properties, namely, the differential spectrum and the Walsh spectrum, of the permutation polynomial $g(x) = x^{2^{m+1}+1} + x^3 + x$ over $\mathbb{F}_{2^{2m+1}}$ for a positive integer $m \geq 2$. Here we call $g(x)$ the Welch permutation

polynomial since via it Dobbertion proved that the Welch power function $F(x) = x^{2^m+3}$ is APN [11]. Furthermore, based on an observation, the weight of a codeword in $\mathcal{C}_{D(f)}$ defined in Conjecture 1 can be expressed in terms of the Walsh transform of $g(x)$ at certain points. This enables us to show that the binary linear code $\mathcal{C}_{D(f)}$ has dimension n and at most five nonzero weights as described in Conjecture 1.

The remainder of this paper is organized as follows. Section 2 introduces basic notation and definitions. Section 3 studies the differential spectrum and Walsh transform of $g(x)$. Section 4 provides a positive answer to Conjecture 1.

2 Preliminaries

2.1 Cryptographic properties of vectorial Boolean functions

Definition 1. Let $F(x)$ be a function from $\mathbb{F}_{2^n}$ to itself, and $N_F(a,b)$ be defined as in (1). Denote

$$\omega_i = |\{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} \mid N_F(a,b) = i\}|.$$

The differential spectrum of $F(x)$ is defined as the multi-set

$$\Omega_F = \{\omega_0, \omega_1, \ldots, \omega_\delta\}, \tag{3}$$

where δ is the differential uniformity of $F(x)$.

It is easily seen that $\omega_i = 0$ in the differential spectrum if i is odd. Moreover, we have the following identities

$$\sum_{i=0}^{\delta} \omega_i = 2^n(2^n-1) \text{ and } \sum_{i=0}^{\delta} (i \times \omega_i) = 2^n(2^n-1). \tag{4}$$

For any APN function over $\mathbb{F}_{2^n}$, there are only two possible values 0 and 2 in its differential spectrum. Thus, from the equalities in (4), the differential spectrum of an APN function over $\mathbb{F}_{2^n}$ can be uniquely determined.

Another important criterion of a vectorial Boolean function $F(x)$ is its nonlinearity, which can be given in terms of the Walsh transforms of $F(x)$.

Definition 2. Let $F(x)$ be a function from $\mathbb{F}_{2^n}$ to itself. The Walsh transform of $F(x)$ at (a,b) is defined by

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(aF(x)+bx)} \tag{5}$$

for each $a, b \in \mathbb{F}_{2^n}$. The Walsh spectrum of $F(x)$ is the multi-set

$$\Lambda_F = \{W_F(a,b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}. \tag{6}$$

The nonlinearity of $F(x)$ is given by

$$NL(F) = 2^{n-1} - \frac{1}{2}\max\{|\, W_F(a,b) \,| : a, b \in \mathbb{F}_{2^n}, a \neq 0\}.$$

Given a quadratic Boolean function $Q(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, the function $Q(x+z)+Q(x)+Q(z)$ is a bilinear function in x and z. Define

$$V_Q = \{x \in \mathbb{F}_{2^n} \mid Q(x+z)+Q(x)+Q(z) = 0, \forall\ z \in \mathbb{F}_{2^n}\}. \tag{7}$$

The rank of $Q(x)$ is defined by $\mathrm{Rank}(Q) = n - \dim_{\mathbb{F}_2}(V_Q)$. Note that

$$\left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{Q(x)}\right)^2 = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Q(x)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{Q(x+z)+Q(x)+Q(z)} = 2^n \sum_{x\in V_Q} (-1)^{Q(x)}, \tag{8}$$

where V_Q is the $\mathbb{F}_2$-linear space defined as in (7). It is readily seen that $Q(x)$ is linear over V_Q. Hence one has

$$\sum_{x\in\mathbb{F}_{2^n}} (-1)^{Q(x)} = \begin{cases} \pm 2^{n-\mathrm{Rank}(Q)/2}, & \text{if } Q(x)=0 \text{ for any } x \in V_Q, \\ 0, & \text{otherwise.} \end{cases}$$

This implies that the $\mathrm{Rank}(Q)$ is always an even number $2h$ with $2 \le 2h \le n$ [13].

For a quadratic Boolean function $Q(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, the definition of its Walsh transform is modified slightly as

$$\widehat{Q}(\lambda) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Q(x)+\mathrm{Tr}_1^n(\lambda x)}.$$

Moreover, when λ runs through $\mathbb{F}_{2^n}$, the distribution of $\widehat{Q}(\lambda)$ can be characterized below.

Lemma 1. *[13, Theorem 6.2] Let $Q(x)$ be a quadratic form on $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ with rank $2h$. Then its Walsh transform $\widehat{Q}(\lambda)$ has the following distribution*

$$\widehat{Q}(\lambda) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Q(x)+\mathrm{Tr}_1^n(\lambda x)} = \begin{cases} \pm 2^{n-h}, & 2^{2h-1} \pm 2^{h-1} \text{ times}, \\ 0, & 2^n - 2^{2h} \text{ times}. \end{cases}$$

For cryptographic applications, a vectorial Boolean function is desired to have low differential uniformity and high nonlinearity [6].

2.2 The binary code from the Welch power function

Let $n = 2m+1$ for a positive integer m and $F(x) = x^{2^m+3}$. In Conjecture 1, the image of $f(x) = F(x+1)+F(x)+1 = D_1F(x)+1$ on $\mathbb{F}_{2^n}$, denoted by $D(f)$, is chosen as the defining set. Note that $f(x)$ is a two-to-one function on $\mathbb{F}_{2^n}$. Thus, the set $D(f)$ has size 2^{n-1}. Using the generic construction method in (2), the linear code $\mathcal{C}_{D(f)}$ in Conjecture 1 is obtained.

Let $\mathbf{c}_a$ be a codeword in $\mathcal{C}_{D(f)}$. Then, its weight is given by

$$\begin{aligned}\mathrm{wt}(\mathbf{c}_a) &= \left|\{1 \le i \le 2^{n-1} : \mathrm{Tr}_1^n(ad_i) = 1\}\right| \\ &= \frac{1}{2}\left(2^{n-1} - \sum_{d\in D(f)} (-1)^{\mathrm{Tr}_1^n(ad)}\right) \\ &= \frac{1}{2}\left(2^{n-1} - \frac{1}{2}\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(af(x))}\right) \\ &= 2^{n-2} - \frac{1}{4}\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(af(x))}.\end{aligned} \tag{9}$$

The above formula shows that for studying the Hamming weight properties of the code $\mathcal{C}_{D(f)}$, it is critical to investigate the Walsh transform of $f(x)$ at $(a, 0)$, i.e., $W_f(a, 0)$.

3 The differential spectrum and the Walsh spectrum of the Welch permutation

For the permutation $g(x) = x^{2^{m+1}+1} + x^3 + x$ over $\mathbb{F}_{2^n}$ with $n = 2m + 1$, this section will determine the differential spectrum Ω_g defined as in (3) and the Walsh spectrum Λ_g defined as in (6).

Theorem 2. *Let $n = 2m + 1$ and $g(x) = x^{2^{m+1}+1} + x^3 + x$. Then $g(x)$ is differentially 4-uniform. Furthermore, its differential spectrum is given by*

$$\{\omega_0 = 2^{2n-1} + 2^{2n-3} - 3 \cdot 2^{n-2}, \omega_2 = 2^{2n-2}, \omega_4 = 2^{2n-3} - 2^{n-2}\}.$$

Proof. Let $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, and $N(a, b)$ be the number of solutions of $g(x+a)+g(x) = b$ in $\mathbb{F}_{2^n}$. Note that

$$\begin{aligned} & g(x + a) + g(x) + b \\ = \; & x^{2^{m+1}}a + xa^{2^{m+1}} + a^{2^{m+1}+1} + x^2a + xa^2 + a^3 + a + b \\ = \; & ax^{2^{m+1}} + ax^2 + (a^{2^{m+1}} + a^2)x + g(a) + b.\end{aligned}$$

Since $a \neq 0$, $g(x + a) + g(x) + b = 0$ is equivalent to that

$$x^{2^{m+1}} + x^2 + cx + d = 0, \tag{10}$$

where

$$c = a^{2^{m+1}-1} + a \text{ and } d = \frac{g(a) + b}{a}. \tag{11}$$

Note that $c = 0$ if and only if $a = 1$. Next we consider the following linearized polynomial

$$x^{2^{m+1}} + x^2 + cx = 0. \tag{12}$$

If $c = 0$ (i.e., $a = 1$), then (12) have two solutions in $\mathbb{F}_{2^n}$, which are 0 and 1. If $c \neq 0$ (i.e., $a \notin \mathbb{F}_2$), then by raising (12) to the power 2^m, we get

$$x + x^{2^{m+1}} + c^{2^m} x^{2^m} = 0. \tag{13}$$

Adding up (12) and (13), we get

$$c^{2^m} x^{2^m} + x^2 + (c+1)x = 0,$$

which implies

$$x^{2^m} = \frac{x^2}{c^{2^m}} + \frac{c+1}{c^{2^m}} x. \tag{14}$$

Substituting (14) into (13), we get

$$x^4 + (c^{2^{m+1}} + c^2 + 1)x^2 + c^{2^{m+1}+1} x = 0. \tag{15}$$

The above argument shows that if x is a solution of (12), it must be a solution of (15). Note that (15) is a linearized polynomial over $\mathbb{F}_{2^n}$ and the number of its solutions in $\mathbb{F}_{2^n}$ is 1, 2 or 4. Thus, we can conclude that the number of solutions of (12) in $\mathbb{F}_{2^n}$ is also 1, 2 or 4. Moreover, note that

$$c = a^{2^{m+1}-1} + a = \frac{a^{2^{m+1}} + a^2}{a}.$$

Thus, for any given $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, $x = a$ must be a solution of (12). Thus, when $c \neq 0$, i.e., $a \notin \mathbb{F}_2$, the number of solutions of (12) in $\mathbb{F}_{2^n}$ is 2 or 4.

Denote by M_1 (resp. M_2) the number of $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that (12) has two (resp. four) solutions in $\mathbb{F}_{2^n}$. In what follows, we need to determine M_1 and M_2. We further investigate the linearized polynomial (15). Since $x = 0$ and $x = a$ are its solutions, the polynomial on the left hand side of (15) has a factorization over $\mathbb{F}_{2^n}$ as follows

$$x^4 + (c^{2^{m+1}} + c^2 + 1)x^2 + c^{2^{m+1}+1} x = x(x+a)(x^2 + ax + \frac{c^{2^{m+1}+1}}{a}),$$

where $c = \frac{a^{2^{m+1}}+a^2}{a}$. (One can verify that $a^2 + \frac{c^{2^{m+1}+1}}{a} = c^{2^{m+1}} + c^2 + 1$.) To check the exact number of solutions of (12), we should investigate the solutions of the following quadratic equation

$$x^2 + ax + \frac{c^{2^{m+1}+1}}{a} = 0. \tag{16}$$

Note that

$$\begin{aligned}
& \mathrm{Tr}_1^n\left(\tfrac{c^{2^{m+1}+1}}{a^3}\right) \\
= \ & \mathrm{Tr}_1^n\left(\tfrac{a^2+a^{2^{m+2}}}{a^{2^{m+1}}} \cdot \tfrac{a^{2^{m+1}}+a^2}{a^4}\right) \\
= \ & \mathrm{Tr}_1^n\left(\tfrac{a^4+a^2\cdot a^{2^{m+1}}+a^{2^{m+2}}\cdot a^{2^{m+1}}+a^2\cdot a^{2^{m+2}}}{a^{2^{m+1}}\cdot a^4}\right) \\
= \ & \mathrm{Tr}_1^n\left(\tfrac{1}{a^{2^{m+1}}} + \tfrac{1}{a^2} + \tfrac{a^{2^{m+2}}}{a^4} + \tfrac{a^{2^{m+1}}}{a^2}\right) \\
= \ & \mathrm{Tr}_1^n\left(\tfrac{1}{a}\right) + \mathrm{Tr}_1^n\left(\tfrac{1}{a}\right) + \mathrm{Tr}_1^n\left(\tfrac{a^{2^{m+1}}}{a^2}\right) + \mathrm{Tr}_1^n\left(\tfrac{a^{2^{m+1}}}{a^2}\right) \\
= \ & 0.
\end{aligned}$$

Thus, (16) has two solutions in $\mathbb{F}_{2^n}$. This also shows that for any $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, (15) always has four solutions in $\mathbb{F}_{2^n}$. By Theorem 1 in [12], one can get the solutions of (16), which are

$$x_1 = a \sum_{i=1}^{m} \left(\frac{c^{2^{m+1}+1}}{a^3} \right)^{2^{2i-1}}, \text{ and } x_2 = x_1 + a.$$

Next the main task is to verify that whether x_1 is a solution of (12) or not.

Let $y = \frac{x_1}{a}$, then by (16) we have

$$y^2 + y + \frac{c^{2^{m+1}+1}}{a^3} = 0. \tag{17}$$

If x_1 is a solution of (12), we also have

$$y^{2^{m+1}} + \frac{a^2}{a^{2^{m+1}}} y^2 + \frac{ca}{a^{2^{m+1}}} y = 0. \tag{18}$$

Combining (17) and (18), we have

$$y^{2^{m+1}} + y + \left(\frac{c}{a} \right)^{2^{m+1}+1} = 0. \tag{19}$$

On the other hand, by (17) we have

$$\begin{aligned}
& y^{2^{m+1}} + y \\
= & \sum_{i=0}^{m} \left(y^2 + y\right)^{2^i} \\
= & \sum_{i=0}^{m} \left(\tfrac{c^{2^{m+1}+1}}{a^3} \right)^{2^i} \\
= & \sum_{i=0}^{m} \left(\tfrac{1}{a^{2^{m+1}}} + \tfrac{1}{a^2} + \tfrac{a^{2^{m+2}}}{a^4} + \tfrac{a^{2^{m+1}}}{a^2} \right)^{2^i} \\
= & \sum_{i=0}^{m} \left(\left(\tfrac{1}{a^2}\right)^{2^m} + \tfrac{1}{a^2} + \left(\tfrac{a^{2^{m+1}}}{a^2} \right)^2 + \tfrac{a^{2^{m+1}}}{a^2} \right)^{2^i} \\
= & \mathrm{Tr}_1^n \left(\tfrac{1}{a^2} \right) + \tfrac{1}{a^{2^{m+1}}} + \tfrac{a^{2^{m+1}}}{a^2} + \left(\tfrac{a^{2^{m+1}}}{a^2} \right)^{2^{m+1}} \\
= & \mathrm{Tr}_1^n \left(\tfrac{1}{a^2} \right) + \tfrac{1}{a^{2^{m+1}}} + \tfrac{a^{2^{m+1}}}{a^2} + \tfrac{a^2}{a^{2^{m+2}}} \\
= & \mathrm{Tr}_1^n \left(\tfrac{1}{a^2} \right) + 1 + \left(\tfrac{a^{2^{m+1}}+a^2}{a^2} \right)^{2^{m+1}} \cdot \tfrac{a^{2^{m+1}}+a^2}{a^2} \\
= & \mathrm{Tr}_1^n \left(\tfrac{1}{a^2} \right) + 1 + \left(\tfrac{c}{a} \right)^{2^{m+1}+1}.
\end{aligned} \tag{20}$$

By (20) and (19), we can conclude that for each $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, the solution x_1 of (16) is also a solution of (12) if and only if $\mathrm{Tr}_1^n \left(\frac{1}{a} \right) = 1$. This means that for each $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, (12) has two (resp. four) solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n \left(\frac{1}{a} \right) = 0$ (resp. $\mathrm{Tr}_1^n \left(\frac{1}{a} \right) = 1$). It is obvious that the number of $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $\mathrm{Tr}_1^n \left(\frac{1}{a} \right) = 0$ (resp. $\mathrm{Tr}_1^n \left(\frac{1}{a} \right) = 1$) is equal to $2^{n-1} - 1$. Thus, we obtain that $M_1 = M_2 = 2^{n-1} - 1$.

For each given $a \in \mathbb{F}_{2^n}^*$, let $L_a(x) = x^{2^{m+1}} + x^2 + cx$, and recall that $c = \frac{a^{2^{m+1}}+a^2}{a}$. Then, $L_a(x)$ is a linear transformation from $\mathbb{F}_{2^n}$ into itself. Let $A_i = \{a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \mid \mathrm{Tr}_1^n(\frac{1}{a}) = i\}$,

where $i = 0, 1$. Note that $\mathbb{F}_{2^n}^* = \{1\} \cup A_0 \cup A_1$. The above arguments have shown that $L_a(x) = 0$ has two solutions in $\mathbb{F}_{2^n}$ if $a \in \{1\} \cup A_0$ and has four solutions in $\mathbb{F}_{2^n}$ if $a \in A_1$. Moreover, when (12) has two (resp. four) solutions in $\mathbb{F}_{2^n}$, i.e., the kernel of $L_a(x)$ has cardinality two (resp. four), then by the homomorphism theorem the image of $L_a(x)$ has cardinality 2^{n-1} (resp. 2^{n-2}), and for each element d in the image, there exist exactly two (resp. four) elements x's in $\mathbb{F}_{2^n}$ such that $L_a(x) = d$.

For each $a \in \mathbb{F}_{2^n}^*$, let B_a denote the image of the linear transformation $L_a(x) = x^{2^{m+1}} + x^2 + cx$. We have obtained that $|B_a| = 2^{n-1}$ if $a \in \{1\} \cup A_0$ and $|B_a| = 2^{n-2}$ if $a \in A_1$. By (11), for a given element $a \in \mathbb{F}_{2^n}^*$, the correspondence between d and b is one-to-one. Thus, we can conclude that for each $a \in \{1\} \cup A_0$ (resp. $a \in A_1$), $N(a, b) = 2$ (resp. 4) if and only if $b \in aB_a + g(a) = \{ad + g(a) \mid d \in B_a\}$, where $N(a, b)$ denotes the number of solutions of (10) in $\mathbb{F}_{2^n}$. In other cases, we all have $N(a, b) = 0$. Thus, the number of pairs $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ such that $N(a, b) = 2$ (resp. 4) is equal to $2^{n-1} \cdot 2^{n-1}$ (resp. $(2^{n-1} - 1) \cdot 2^{n-2}$). This together with (4) gives the differential spectrum. □

Note that $\mathrm{Tr}_1^n(ag(x)) = \mathrm{Tr}_1^n(a(x^{2^{m+1}+1} + x^3 + x))$ is a quadratic Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. According to Lemma 1, the Walsh transform of $\mathrm{Tr}_1^n(ag(x))$ heavily depends on its rank. Below is an auxiliary result for the rank of $\mathrm{Tr}_1^n(ag(x))$.

Lemma 3. *Let s, n, k be positive integers satisfying $\gcd(s, n) = 1$, and without loss of generality we also assume that $k \le n/2$. Let*

$$Q(x) = \sum_{i=1}^{k} \mathrm{Tr}_1^n(c_i x^{2^{si}+1}),$$

where $c_i \in \mathbb{F}_{2^n}$ and at least one c_i is nonzero for $1 \le i \le k$. Then, the rank $2h$ of $Q(x)$ is in the range $n - 2k \le 2h \le n$.

Proof. We consider the following equation

$$\begin{aligned} & Q(x) + Q(z) + Q(x+z) \\ = \; & \mathrm{Tr}_1^n\left(\sum_{i=1}^{k}\left(c_i x^{2^{si}} z + c_i x z^{2^{si}}\right)\right) \\ = \; & \mathrm{Tr}_1^n\left(\sum_{i=1}^{k}\left(c_i x^{2^{si}} z + c_i^{2^{-is}} x^{2^{-is}} z\right)\right) \\ = \; & \mathrm{Tr}_1^n\left(z \sum_{i=1}^{k}\left(c_i x^{2^{si}} + c_i^{2^{-is}} x^{2^{-is}}\right)\right) \\ = \; & 0 \end{aligned}$$

for all $z \in \mathbb{F}_{2^n}$. The above equation holds if and only if

$$\sum_{i=1}^{k}\left(c_i x^{2^{si}} + c_i^{2^{-is}} x^{2^{-is}}\right) = 0,$$

which is equivalent to

$$\sum_{i=1}^{k}\left(c_i x^{2^{si}} + c_i^{2^{-is}} x^{2^{-is}}\right)^{2^{ks}} = \sum_{i=1}^{k}\left(c_i^{2^{ks}} x^{2^{s(k+i)}} + c_i^{2^{s(k-i)}} x^{2^{s(k-i)}}\right) = 0. \tag{21}$$

Table 1: The Walsh spectrum of $x^{2^{m+1}+1}+x^3+x$

Value	Frequency
0	$9\cdot 2^{2n-4}+3\cdot 2^{n-3}-1$
$\pm 2^{m+1}$	$\frac{(5\cdot 2^{n-1}-2)}{3}\left(2^{n-2}\pm 2^{\frac{n-3}{2}}\right)$
$\pm 2^{m+2}$	$\frac{(2^{n-1}-1)}{3}\left(2^{n-4}\pm 2^{\frac{n-5}{2}}\right)$

We can rewrite (21) in the following form

$$\sum_{i=0}^{2k} a_i x^{2^{si}} = 0, \tag{22}$$

where $a_i = c_{k-i}^{2^{si}}$ for $i = 0, 1, \ldots, k-1$, $a_k = 0$ and $a_i = c_{i-k}^{2^{ks}}$ for $i = k+1, k+2, \ldots, 2k$. Since $\gcd(s, n) = 1$, according to [4, Corollary 1], the equation (22) has at most 2^{2k} solutions in $\mathbb{F}_{2^n}$. The desired result then follows. □

With Theorem 3 and Lemma 3, we are ready to prove the following theorem.

Theorem 4. *Let $n = 2m+1$ and $g(x) = x^{2^{m+1}+1}+x^3+x$. Then the Walsh spectrum of $g(x)$ is given in Table 1.*

Proof. It is easily seen that

$$W_g(0,b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bx)} = \begin{cases} 2^n, \text{ if } b = 0, \\ 0, \text{ if } b \neq 0. \end{cases}$$

When $a \neq 0$, $W_g(a,b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(ax^{2^{m+1}+1}+ax^3+(a+b)x\right)}$, and $\mathrm{Tr}_1^n(ax^{2^{m+1}+1}+ax^3)$, denoted by $Q_a(x)$, is a quadratic form on $\mathbb{F}_{2^n}$. Note that

$$Q_a(x) = \mathrm{Tr}_1^n(ax^{2^{m+1}+1}+ax^3) = \mathrm{Tr}_1^n(a^{2^m}x^{2^m+1}+a^{2^{2m}}x^{2^{2m}+1}).$$

Then, by Lemma 3, the rank of $Q_a(x)$ is $n-3$ or $n-1$ since n is odd and $\gcd(m,n)=1$. When a runs through $\mathbb{F}_{2^n}^*$, assume that the number of $a \in \mathbb{F}_{2^n}^*$ such that $Q_a(x)$ has rank $n-(2i-1)$ is N_i, $i = 1, 2$. Then, by Lemma 1, when (a,b) runs through $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$, the Walsh transform $W_g(a,b)$ of $g(x)$ has the following distribution

$$W_g(a,b) = \begin{cases} 0, & (2^n-1)+N_1(2^n-2^{n-1})+N_2(2^n-2^{n-3}) \text{ times}, \\ \pm 2^{m+1}, & N_1(2^{n-2}\pm 2^{\frac{n-3}{2}}) \text{ times}, \\ \pm 2^{m+2}, & N_2(2^{n-4}\pm 2^{\frac{n-5}{2}}) \text{ times}. \end{cases}$$

Next we calculate the fourth power sum of $W_g(a,b)$. On one hand, we have

$$\sum_{a,b\in\mathbb{F}_{2^n}} (W_g(a,b))^4 = 2^{4n} + 2^{4m+4}\cdot 2^{n-1}\cdot N_1 + 2^{4m+8}\cdot 2^{n-3}\cdot N_2. \tag{23}$$

On the other hand, we have

$$\begin{aligned} & \sum_{a,b\in\mathbb{F}_{2^n}} (W_g(a,b))^4 \\ = & \sum_{x,y,u,v\in\mathbb{F}_{2^n}} \sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(x+y+u+v))} \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(g(x)+g(y)+g(u)+g(v)))} \\ = & 2^{2n}T, \end{aligned} \tag{24}$$

where T denotes the number of $(x,y,u,v)\in(\mathbb{F}_{2^n})^4$ satisfying

$$\begin{cases} x+y+u+v=0, \\ g(x)+g(y)+g(u)+g(v)=0. \end{cases}$$

Let $N(a,b)$ be the number of solutions of $g(x+a)+g(x)=b$ in $\mathbb{F}_{2^n}$. Then, we have $T=\sum_{a,b\in\mathbb{F}_{2^n}} N(a,b)^2$. Using the notation and results in Theorem 2 and its proof, we have

$$T=\sum_{a,b\in\mathbb{F}_{2^n}} N(a,b)^2 = 2^{2n}+4\omega_2+16\omega_4 = 4\cdot\left(2^{2n}-2^n\right). \tag{25}$$

Combining (23), (24), (25) and the fact that $N_1+N_2=2^n-1$, we obtain the distribution of the Walsh transform of $g(x)$ as in Table 1. □

4 Binary codes from the Welch APN power function

For the Welch APN power function $F(x)=x^{2^m+3}$ and $f(x)=F(x+1)+F(x)+1$, it is easy to verify that

$$f(x)=F(x+1)+F(x)+1=(x+x^{2^m})(x^2+x+1)=g(x+x^{2^m}),$$

where $g(x)$ is the Welch permutation discussed in Section 3. With the properties of $g(x)$ presented in Section 3, we obtain the following result on the code $\mathcal{C}_{D(f)}$ constructed in Conjecture 1.

Theorem 5. *Let $n=2m+1$ with a positive integer $m\geq 2$. The binary linear code $C_{D(f)}$ defined in Conjecture 1 has length 2^{n-1}, dimension n and its nonzero weights are contained in the following set:*

$$\left\{2^{n-2}, 2^{n-2}\pm 2^{\frac{n-3}{2}}, 2^{n-2}\pm 2^{\frac{n-1}{2}}\right\}.$$

Table 2: Some numerical results

Value of n	Weight enumerator of $\mathcal{C}_{D(f)}$
5	$1+6x^{10}+16x^{8}+10x^{6}$
7	$1+64x^{32}+36x^{28}+28x^{36}$
9	$1+x^{144}+108x^{120}+286x^{128}+108x^{136}+9x^{112}$
11	$1+440x^{496}+408x^{528}+22x^{480}+1156x^{512}+22x^{544}$

Proof. It is clear that the length of $\mathcal{C}_{D(f)}$ is 2^{n-1}. As for the dimension, since $\mathcal{C}_{D(f)}$ is linear, we need to consider the number of $a \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_1^n(af(x)) = 0$ for any $x \in \mathbb{F}_{2^n}$, equivalently, $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(af(x))} = 2^n$.

Define $T_0 = \{x + x^{2^m} \,|\, x \in \mathbb{F}_{2^n}\}$ and $T_1 = \{x + 1 \,|\, x \in T_0\}$. Note that $x + x^{2^m}$ is a two-to-one function over $\mathbb{F}_{2^n}$. Thus $T_0 \cup T_1 = \mathbb{F}_{2^n}$. Since n is odd, we have $\mathrm{Tr}_1^n(1) = 1$ and $\mathrm{Tr}_1^n(x) = 1$ for any $x \in T_1$. Since $g(x)$ is a permutation of $\mathbb{F}_{2^n}$, one has

$$\sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n(bg(z))} + \sum_{z\in T_1}(-1)^{\mathrm{Tr}_1^n(bg(z))} = \sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(bg(z))} = 0.$$

Then for any $a \in \mathbb{F}_{2^n}^*$,

$$\begin{aligned}
\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(af(x))} &= 2\sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n(ag(z))} \\
&= \sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n(ag(z))} + \sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n(ag(z+1)+1)} \\
&= \sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n(ag(z)+z)} + \sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n(ag(z+1)+z+1)} \\
&= \sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n(ag(z)+z)} + \sum_{z\in T_1}(-1)^{\mathrm{Tr}_1^n(ag(z)+z)} \\
&= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(ag(x)+x)}.
\end{aligned} \tag{26}$$

By the Walsh spectrum of $g(x)$ in Theorem 4, it is clear that $W_f(a,0) = W_g(a,1) \neq 2^n$ for any nonzero $a \in \mathbb{F}_{2^n}$. This implies that $\mathcal{C}_{D(f)}$ has dimension n. Furthermore, it follows from (9) that

$$\mathrm{wt}(\mathbf{c}_a) = 2^{n-2} - \frac{1}{4}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(ag(x)+x)}. \tag{27}$$

From the Walsh spectrum of $g(x)$ in Table 1, the possible nonzero weights of the code $\mathcal{C}_{D(f)}$ can be directly determined. □

With the help of Magma, we obtain some numerical results list in Table 2 , which are in accordance with Theorem 5.

Acknowledgment

Y. Wang and Y. Xia were supported in part by National Natural Science Foundation of China under Grant 61771021, and in part by the Fundamental Research Funds for the Central Universities, South-Central University for Nationalities under Grant CZT20023. The work of C. Li and W. Kadir was supported by the Research Council of Norway under the grant 247742/O70.

References

[1] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of power functions," *Int. J. Information and Coding Theory*, 1(2): 149-170, 2010.

[2] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of $x \mapsto x^{2^t-1}$," *IEEE Trans. Inf. Theory*, 57(12): 27-8137, Dec. 2011.

[3] C. Blondeau and L. Perrin, "More differentially 6-uniform power functions", *Des. Codes Cryptogr.*, 73: 487-505, 2014.

[4] C. Bracken, E. Byrne, N. Markin, and G. MaGuire, "Determining the Nonlinearity of a New Family of APN Functions," in *Lecture Notes in Comput. Sci.*, 4851: 72-79, Springer-Verlag Berlin Heidelberg, 2007.

[5] C. Bracken and G. Leander, "A highly nonlinear differentially 4-uniform power mapping that permutes fields of even degree," *Finite Fields Appl.*, 16(4): 231-242, 2010.

[6] L. Budaghyan, M. Calderini, and I. Villa, "On equivalence between known families of quadratic APN functions," *Finite Fields Appl.*, 66: 101704, 2020.

[7] C. Carlet, C. Ding, and J. Yuan. "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Trans. Inf. Theory*, 51(6): 2089-2102, 2005.

[8] P. Charpin, G. Kyureghyan, and V. Sunder, "Sparse permutations with low differential uniformity," *Finite Fields Appl.*, 28: 214-243, 2014.

[9] C. Ding. "A construction of binary linear codes from Boolean functions," *Discrete Mathematics*, 339(9): 2288-2303, 2016.

[10] C. Ding and H. Niederreiter. "Cyclotomic linear codes of order 3," *IEEE Trans. Inf. Theory*, 53(6): 2274-2277, 2007.

[11] H. Dobbertin. "Almost perfect nonlinear power functions on GF(2^n): the Welch case," *IEEE Trans. Inf. Theory*, 45(4): 1271-1275, 1999.

[12] C. Chen, "Formulas for the solutions of quadratic equations over GF(2^m)," *IEEE Trans. Inf. Theory*, 28(5): 792-794, May, 1982.

[13] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998, vol. II, pp. 1765-1853.

[14] K. Nyberg, "Differentially uniform mappings for cryptography," in T. Helleseth (ed.) Advances in Cryptology - EUROCRYPT'93, Norway, 1993. *Lecture Notes in Comput. Sci.*, vol. 765, pp. 55-64. Springer, Berlin, 1994.

[15] M. Xiong and H. Yan, "A note on the differential specturm of a differentially 4-uniform power function," *Finite Fields Appl.*, 48: 117-125, 2017.

[16] M. Xiong, H. Yan, and P. Yuan,"On a conjecture of differenially 8-uniform power functions," *Des. Codes Cryptogr.*, 86: 1601-1621, 2018.

[17] Z. Zha, "Research on low differential uniformity functions," Ph.D. dissertation (Chinese), Hunan University, Changsha, China, 2008.