

On the Fourier spectra of new APN functions

Tan, Yin; Qu, Longjiang; Ling, San; Tan, Chik How

2013

Tan, Y., Qu, L., Ling, S., & Tan, C. H. (2013). On the Fourier spectra of new APN functions. *SIAM journal on discrete mathematics*, 27(2), 791-801.

<https://hdl.handle.net/10356/101532>

<https://doi.org/10.1137/120865756>

© 2013 Society for Industrial and Applied Mathematics (SIAM). This paper was published in SIAM Journal on Discrete Mathematics and is made available as an electronic reprint (preprint) with permission of SIAM. The paper can be found at the following official DOI: [<http://dx.doi.org/10.1137/120865756>]. One print or electronic copy may be made for personal use only. Systematic or multiple reproduction, distribution to multiple locations via electronic or other means, duplication of any material in this paper for a fee or for commercial purposes, or modification of the content of the paper is prohibited and is subject to penalties under law.

Downloaded on 09 Apr 2024 21:54:23 SGT

ON THE FOURIER SPECTRA OF NEW APN FUNCTIONS*

YIN TAN[†], LONGJIANG QU[‡], SAN LING[§], AND CHIK HOW TAN[†]

Abstract. Almost perfect nonlinear (APN) functions on \mathbb{F}_{2^n} are functions achieving the lowest possible differential uniformity. All APN functions discovered until now are either power or quadratic ones, except for one sporadic multinomial nonquadratic example on \mathbb{F}_{2^6} due to Edel and Pott. It is well known that certain binary codes with good properties can be obtained from APN functions, and determining their (Hamming) weight distribution is equivalent to determining the Fourier spectra of the corresponding functions. The Fourier spectra of all known infinite families of quadratic APN functions discovered through 2010 have been determined, and it was found that they are the same as the ones of the Gold APN functions, i.e., a 5-valued set when n is even and a 3-valued set when n is odd, while a sporadic example on \mathbb{F}_{2^6} found by Dillon has a 7-valued Fourier spectrum. In 2011, two new generic constructions of APN functions were presented in [Y. Zhou and A. Pott, *Adv. Math.*, 234 (2013), pp. 43–60] and [C. Carlet, *Des. Codes Cryptogr.*, 59 (2011), pp. 89–109]. In this paper, we determine the Fourier spectra of the APN functions obtained from them and show that their Fourier spectra are again the same as those of the Gold APN functions. Moreover, since the APN functions in [C. Bracken, C. H. Tan, and Y. Tan, *On a Class of Quadratic Polynomials with No Zeros and Its Applications to APN Functions*, preprint, arXiv:1110.3177v1, 2011], which are demonstrated to exist when $n \equiv 0 \pmod{4}$ and $3 \nmid n$, are covered by the construction in [C. Carlet, *Des. Codes Cryptogr.*, 59 (2011), pp. 89–109], a positive answer to the conjecture proposed in the former paper on determining their Fourier spectrum is given in this paper.

Key words. APN function, quadratic functions, Fourier spectrum, nonlinearity, bent function, weight distribution

AMS subject classifications. 11T23, 11T71, 94B05

DOI. 10.1137/120865756

1. Introduction. Let \mathbb{F}_{2^n} be a finite field with 2^n elements and let F be a function on \mathbb{F}_{2^n} . We call F an *almost perfect nonlinear* (APN) function if the equation $F(x+a) + F(x) = b$ has at most two solutions for all $a, b \in \mathbb{F}_{2^n}$ and $a \neq 0$. APN functions were first defined by Nyberg in [19] as they are optimally resistant to the differential attack proposed in [1]. Moreover, in addition to the applications of APN functions in cryptography, they have been found to be related to many topics in, for example, finite geometry and coding theory, garnering much research interest (see [11, 17] and the references therein). Since Nyberg's characterization, many CCZ-inequivalent (defined in section 2.1) APN functions have been discovered. Before 2006, all known APN functions were power mappings, except for a binomial sporadic example on \mathbb{F}_{2^6} , which is CCZ inequivalent to all known ones, found in [16]. Subsequently, many new APN polynomials were found. First, the aforementioned

*Received by the editors February 13, 2012; accepted for publication (in revised form) December 19, 2012; published electronically April 18, 2013. The work of the second and third authors was supported by the Singapore National Research Foundation Competitive Research Program under grant NRF-CRP2-2007-03.

[†]<http://www.siam.org/journals/sidma/27-2/86575.html>

[‡]Temasek Laboratories, National University of Singapore, Singapore 117411 (itanyinmath@gmail.com, tsltch@nus.edu.sg).

[§]Department of Mathematics and System Science, Science College, National University of Defense Technology, ChangSha, 410073, China, and Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371 (ljqu_happy@hotmail.com). This author's work was supported by the NSFC of China under grant 61272484.

[§]Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371 (lingsan@ntu.edu.sg).

sporadic example was generalized into an infinite family in [10]. Many other infinite families were then obtained in [3, 5, 6, 8, 9, 10]. We should mention that all the new infinite families of APN functions found since 2005 are quadratic ones, while in 2008 a multinomial nonquadratic sporadic example was found in [17]. One may refer to [5] for a complete list of all APN functions discovered through 2010. Recently, two new constructions of quadratic APN functions were presented in [12, 20]. We list these constructions below for the convenience of the reader.

It is well known that the finite field \mathbb{F}_{2^m} may be identified with an m -dimensional vector space $(\mathbb{F}_2^m, +)$ over \mathbb{F}_2 (see [18, Chapter 1]). We will switch between these two points of view in the rest of the paper without explanation if the context is clear. As a result, by the fact that $\mathbb{F}_2^{2m} = \mathbb{F}_2^m \times \mathbb{F}_2^m$ as \mathbb{F}_2 -vector spaces, we may regard the finite field $\mathbb{F}_{2^{2m}}$ as $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, where “ \times ” is the Cartesian product.

RESULT 1 (see [20]). *Let $n = 2m$, where $m \geq 2$ is an even integer, and let k be an integer such that $\gcd(k, m) = 1$. Define a function F on $\mathbb{F}_{2^{2m}} = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ as follows:*

$$(1) \quad F(x, y) = (x^{2^k+1} + \alpha y^{(2^k+1)2^i}, xy), \quad x, y \in \mathbb{F}_{2^m},$$

where the nonzero $\alpha \in \mathbb{F}_{2^m}$ is a noncube and i is even. Then F is an APN function.

RESULT 2 (see [12]). *Let $n = 2m$ be any even integer, let i, j be integers such that $\gcd(m, i - j) = 1$, and let $g_1 \neq 0, g_4 \neq 0, g_2, g_3$ be elements of \mathbb{F}_{2^m} . Set $G(x, y) = g_1 x^{2^i+2^j} + g_2 x^{2^i} y^{2^j} + g_3 x^{2^j} y^{2^i} + g_4 y^{2^i+2^j}$. Define a function F on $\mathbb{F}_{2^{2m}} = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by*

$$(2) \quad F(x, y) = (G(x, y), xy), \quad x, y \in \mathbb{F}_{2^m}.$$

Then F is an APN function if and only if the polynomial $G(x, 1) = g_1 x^{2^i+2^j} + g_2 x^{2^i} + g_3 x^{2^j} + g_4$ has no root in \mathbb{F}_{2^m} .

It has been shown through computer verification that Result 1 may produce new APN functions. Furthermore, Result 2 is shown to cover several known infinite APN families by choosing appropriate i, j, g_k there; see [12, pp. 103–105].

Clearly, APN functions achieve the lowest possible differential uniformity for functions over \mathbb{F}_{2^n} . Moreover, for cryptographic purposes, the functions are also required to have high nonlinearity (defined in section 2.1). Highly nonlinear functions are also interesting from the point of view of coding theory. To each such function, one may associate a linear error-correcting code (see section 2.2), whose (Hamming) weight distribution may be obtained directly from the Fourier spectrum (including multiplicity) of the function. Moreover, by the MacWilliams identities, if the Fourier spectrum has at most five values, we may then determine the multiplicity of each value. This will be explained in more detail in section 2.2. The Fourier spectra of all infinite families of APN functions listed in [5] have been determined (see [4, 7] and the references therein).

In particular, for quadratic APN functions on \mathbb{F}_{2^n} , it is known that as long as n is odd, their Fourier spectrum is $\{0, \pm 2^{(n+1)/2}\}$, and such functions are also called *almost bent* (AB) functions (see [17]). However, when n is even, quadratic APN functions may have different Fourier spectra. Precisely, it was found that all known infinite quadratic families have a 5-valued Fourier spectrum $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$ when n is even, except for one sporadic example:

$$x^3 + \beta^{11} x^5 + \beta^{13} x^9 + x^{17} + \beta^{11} x^{33} + x^{48}$$

over \mathbb{F}_{2^6} with a 7-valued Fourier spectrum found by Dillon [14], where β is a primitive element. It would be interesting to generalize this sporadic example into an infinite family.

In this paper, we show that the Fourier spectra of the APN functions obtained in Results 1 and 2 are also the 5-valued set mentioned above (Theorem 2), and hence we may determine the weight distribution of the codes associated with these APN functions. Moreover, since Result 2 covers several known APN families, some remarks on Theorem 2 are given as follows. The multinomial APN function in [3, Theorem 1] is a special case of Result 2, and its Fourier spectrum was also determined in [2]; the hexanomial APN function in [8] is another special case of Result 2, and the existence of such APN functions relies on a quadratic polynomial with no zeros in $\mathbb{F}_{2^{2m}}$. It is shown in [6] that when m is odd, this hexanomial function is CCZ-equivalent to the multinomial one in [3]; and when m is even and $3 \nmid m$, the required quadratic polynomials were constructed and hence the existence of the hexanomial APN function was guaranteed. It is conjectured that the Fourier spectra of these hexanomial APN functions are also the 5-valued set in [6, Conjecture 2]. We give a positive answer to this conjecture in Theorem 2.

It is shown in [11] that the Boolean function $\text{Tr}(vF(x))$ is bent (defined in section 2.1) for at least $\frac{2}{3}(2^{2m} - 1)$ values of v for any quadratic APN function F on $\mathbb{F}_{2^{2m}}$. We show that in Theorem 3, for the APN functions F in Results 1 and 2, the function $\text{Tr}(vF(x))$ is bent for all $v \in \mathbb{F}_{2^m}$, $v \neq 0$.

The rest of the paper is organized as follows. In section 2, we give the necessary definitions and results. In section 3, we determine the Fourier spectra of the APN functions obtained in Results 1 and 2. Some concluding remarks are given in section 4.

2. Preliminaries.

2.1. Differential and Fourier spectra. For a function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ and any $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, define

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

The multiset $\{\delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}$ is called the *differential spectrum* of F . The value

$$\Delta_F := \max_{a, b \in \mathbb{F}_{2^n}, a \neq 0} \delta_F(a, b)$$

is called the *differential uniformity* of F . We also call F a *differentially Δ_F -uniform* function. In particular, we call those functions with $\Delta_F = 2$ *almost perfect nonlinear* (APN) functions.

Another important method for characterizing the nonlinearity of F is as follows. For the above function F , the *Fourier (Walsh) transform* $F^{\mathcal{W}} : \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} \rightarrow \mathbb{C}$ of F is defined as

$$F^{\mathcal{W}}(a, b) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(aF(x) + bx)}, \quad a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n},$$

where $\text{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$ denotes the absolute trace function and $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$. The set $\mathcal{W}(F) := \{F^{\mathcal{W}}(a, b) \mid a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\}$ is called the *Fourier (Walsh) spectrum* of F . The *nonlinearity* of F is defined as

$$\text{NL}(F) := 2^{n-1} - \frac{1}{2} \max_{x \in \mathcal{W}(F)} |x|.$$

It is known that if n is odd, the nonlinearity $\text{NL}(F)$ is upper-bounded by $2^{n-1} - 2^{\frac{n-1}{2}}$; and when n is even, it is conjectured that $\text{NL}(F)$ is upper-bounded by $2^{n-1} - 2^{\frac{n}{2}}$. For a Boolean function $f = \text{Tr}(F(x)) : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$, its Fourier spectrum is defined to be $\mathcal{W}(f) = \{f^{\mathcal{W}}(b) := F^{\mathcal{W}}(1, b) \mid b \in \mathbb{F}_{2^n}\}$, and f is said to be a *bent* function if $f^{\mathcal{W}}(b) \in \{\pm 2^{n/2}\}$ for all $b \in \mathbb{F}_{2^n}$. Clearly, bent functions exist only when n is even.

For a function $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$, $a_i \in \mathbb{F}_{2^n}$, its *algebraic degree*, denoted by $\deg F$, is defined to be the maximal 2-weight of the exponent i such that $a_i \neq 0$, where the 2-weight of an integer i is the number of ones in the binary representation of i . We call F a *quadratic* function if $\deg F = 2$ and an *affine* function if $\deg F \leq 1$.

Two functions F and G on \mathbb{F}_{2^n} are called *extended affine* (EA) equivalent if there exist affine permutations $L, L' : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ and an affine function A such that $G = L' \circ F \circ L + A$. They are called *Carlet–Charpin–Zinoviev* (CCZ) equivalent if their graphs $\{(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mid y = F(x)\}$ and $\{(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mid y = G(x)\}$ are affine equivalent, that is, if there exists an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $L_2(x, y) = G(L_1(x, y))$, where $y = F(x)$. It is well known that EA equivalence implies CCZ equivalence, but not vice versa. Moreover, both EA and CCZ equivalence preserve the differential and Fourier spectra, and EA equivalence preserves the algebraic degree.

2.2. Linear codes associated with APN functions. A relationship between APN functions and coding theory has been given in several papers; see, for instance, [4, 17]. We briefly recall it here to make the exposition self-contained.

Regarding the finite field \mathbb{F}_{2^n} as a vector space of dimension n over \mathbb{F}_2 , and then fixing a basis of \mathbb{F}_{2^n} , we may express each element $x \in \mathbb{F}_{2^n}$ as a vector of length n . Let F be a function on \mathbb{F}_{2^n} , and define a matrix $C_F \in \mathbb{F}_2^{2^n \times 2^n}$ as follows:

$$C_F = \begin{bmatrix} \cdots & x & \cdots \\ \cdots & F(x) & \cdots \end{bmatrix},$$

where the columns of C_F are ordered with respect to some ordering of the elements of \mathbb{F}_{2^n} . Then the rows of C_F generate a binary linear code \mathcal{C}_F . Clearly, all codewords of \mathcal{C}_F are of the form

$$v(f_a, f_b) := (f_a(x) + (f_b \circ F)(x))_{x \in \mathbb{F}_{2^n}}, \quad a, b \in \mathbb{F}_{2^n},$$

where $f_a, f_b : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ are linear functions defined by $f_a(x) = \text{Tr}(ax)$ and $f_b(x) = \text{Tr}(bx)$. It is not difficult to show that

$$F^{\mathcal{W}}(b, a) = 2^n - 2w_H(v(f_a, f_b)),$$

where $w_H(v(f_a, f_b))$ is the Hamming weight of the vector $v(f_a, f_b)$. Therefore, to determine the Fourier spectrum (including multiplicity) of the function F is equivalent to determining the weight distribution of the codewords in \mathcal{C}_F .

Now suppose F is an APN function; then the dual code \mathcal{C}_F^\perp has minimum distance 5. Let a_w denote the number of times the weight w occurs in \mathcal{C}_F , and let b_j denote the number of codewords of weight j in \mathcal{C}_F^\perp . If there are at most five nonzero Hamming weights in \mathcal{C}_F , then the MacWilliams (or Pless) identities yield five independent equations, $b_0 = 1$, $b_1 = \dots = b_4 = 0$, for the unknowns a_w , which can be solved uniquely. Thus the weight distribution of \mathcal{C}_F is determined once the Fourier spectrum of F has at most five values. Moreover, the weight w in \mathcal{C}_F corresponds to the value $2^n - 2w$ in the Fourier spectrum of F .

More results about the codes and APN functions, including the characterization of the CCZ equivalence between two APN functions, may be found in [4, 17].

2.3. An important lemma. We conclude this section with an important lemma which will be used in the next section to determine the nonlinearity of the quadratic APN functions. We should mention that this lemma is applicable not only to the APN functions in Results 1 and 2, but also to other previously known infinite families.

Let $L(x)$ be a linearized polynomial over \mathbb{F}_{2^n} ; let K be the kernel of L , the linear map given by $L(x)$; and let s be an integer with $\gcd(s, n) = 1$. A polynomial $C(x) = \sum_{0 \leq i < j \leq n-1} c_{ij}x^{2^i+2^j} \in \mathbb{F}_{2^n}[x]$ is called a *crucial s-polynomial* of $L(x)$ if it satisfies the following two properties:

1. $C(x) + C(x)^{2^s} \equiv xL(x) + (xL(x))^{2^t} \pmod{x^{2^n} - x}$, where s and t are some positive integers such that $\gcd(s, n) = 1$;
2. for $u \in K$, $C(u) = 0$ if and only if $u = 0$.

The following result gives an upper bound for the dimension of the kernel K of the linear map given by a linearized polynomial under the existence of a crucial s -polynomial $C(x)$.

LEMMA 1. *Let $L(x)$ be a linearized polynomial over \mathbb{F}_{2^n} . If there exists a crucial s -polynomial $C(x)$ of $L(x)$, then the dimension of the kernel of L is at most 2.*

Proof. Denote by K the kernel of L . Take an arbitrary element $u \in K \setminus \{0\}$. By property 1 above, $C(u) = C(u)^{2^s}$, and therefore $C(u)$ lies in the prime subfield \mathbb{F}_2 since $\gcd(s, n) = 1$. Then, by property 2 of $C(x)$, we have $C(u) = 1$.

Assume, to the contrary, that $\dim(K) \geq 3$. Fix an element $v \in K$, $v \neq 0$. As $C(u) = 1$ holds for any nonzero element u in K , we have $C(u) = C(v) = C(u+v) = 1$ for every $u \in K \setminus \{0, v\}$. Therefore

$$1 = C(u) + C(v) + C(u+v) = \sum_{i < j} c_{ij}(v^{2^i}u^{2^j} + u^{2^i}v^{2^j}) = \sum_{i=0}^{n-1} F_i u^{2^i},$$

where $F_i = \sum_{j=0, j \neq i}^{n-1} c_{ij}v^{2^j} \in \mathbb{F}_{2^n}$ (note that F_i depends on v but not on $u \in K \setminus \{0, v\}$). Thus any element $u \in K \setminus \{0, v\}$ is a root of the polynomial $a(x) := l(x) + 1$, where we set $l(x) := \sum_{i=0}^{n-1} F_i x^{2^i}$. Note that $l(x)$ is a linearized polynomial.

Since the dimension of K is at least 3, there exist distinct elements $v, u, w \in K$ such that $u, w, u+w \in K \setminus \{0, v\}$. As discussed above, $u, w, u+w$ are all roots of the polynomial $a(x)$ defined above, so we have $1 = l(u)$, $1 = l(w)$, and $1 = l(u+w)$. However, as $l(X)$ is a linearized polynomial, these equations imply that

$$1 = l(u+w) = l(u) + l(w) = 1 + 1 = 0,$$

which is obviously a contradiction. \square

3. The Fourier spectra of the Zhou–Pott and the Carlet APN functions.

In this section, we determine the Fourier spectra of the APN functions F defined in Results 1 and 2.

We first sketch the idea of the proof as follows. Assume that $F(x)$ is an arbitrary quadratic function over \mathbb{F}_{2^n} , where n is even. Then for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} F^{\mathcal{W}}(a, b)^2 &= \sum_{x, y} (-1)^{\text{Tr}(aF(x)+aF(y)+bx+by)} \\ &= \sum_u (-1)^{\text{Tr}(aF(u)+bu)} \sum_x (-1)^{\text{Tr}(a(F(x+u)+F(x)+F(u)))}. \end{aligned}$$

Since $F(x)$ is a quadratic function, there exists a unique linearized polynomial $L_a(x)$ over \mathbb{F}_{2^n} such that $\text{Tr}(a(F(x+u)+F(x)+F(u))) = \text{Tr}(L_a(u)x)$ holds for any

$u, x \in \mathbb{F}_{2^n}$, so

$$\begin{aligned} F^W(a, b)^2 &= \sum_u (-1)^{\text{Tr}(bu+aF(u))} \sum_x (-1)^{\text{Tr}(L_a(u)x)} \\ &= 2^n \sum_{u \in K} (-1)^{\text{Tr}(bu+aF(u))}, \end{aligned}$$

where K is the kernel of the linear map L_a given by $L_a(x)$. If the kernel size is at most 2^3 , then clearly

$$0 \leq \sum_{u \in K} (-1)^{\text{Tr}(bu+aF(u))} \leq 2^3.$$

Since $F^W(a, b)$ is an integer and n is even, this sum can be only 0, 1, 4, and therefore the Fourier spectrum of F is $\{0, \pm 2^{n/2}, \pm 2^{n/2+1}\}$. Thus it suffices to demonstrate that $|K| \leq 8$. In light of Lemma 1, if, for each linearized polynomial $L_a(x)$, we can find a crucial s -polynomial $C_a(x)$, then we can demonstrate that the kernel K of L_a has dimension at most 2, which then guarantees that $|K| \leq 8$. Lemma 1, together with the aforementioned discussion, leads to the following theorem.

THEOREM 1. *Let $n = 2m$ be two positive integers and let F be a quadratic function over \mathbb{F}_{2^n} . For any $a \in \mathbb{F}_{2^n}^*$, let $L_a(x)$ be the linearized polynomial over \mathbb{F}_{2^n} such that $\text{Tr}(a(F(x+u) + F(x) + F(u))) = \text{Tr}(L_a(u)x)$ holds for any $u, x \in \mathbb{F}_{2^n}$. If, for any $a \in \mathbb{F}_{2^n}^*$, there exists a crucial s -polynomial $C_a(x)$ of $L_a(x)$, then the Fourier spectrum of F is $\{0, \pm 2^m, \pm 2^{m+1}\}$.*

In the following, we apply Theorem 1 to determine the Fourier spectrum of the quadratic APN functions in Results 1 and 2.

THEOREM 2. *The Fourier spectrum of the APN functions defined in Results 1 and 2 is $\{0, \pm 2^m, \pm 2^{m+1}\}$.*

Proof. We divide the proof into two parts according to which class the function F is in.

1. *Zhou–Pott APN functions:* First, we compute the explicit forms of $F(x)$ and $L_a(x)$. Let β be a primitive element of $\mathbb{F}_{2^{2m}}$, and then clearly each element z in $\mathbb{F}_{2^{2m}}$ can be uniquely written as $z = x+y\beta$ for some $x, y \in \mathbb{F}_{2^m}$. Now, from $z^{2^m} = x+y\beta^{2^m}$, we obtain

$$x = \frac{\beta^{2^m} z + \beta z^{2^m}}{\beta + \beta^{2^m}}, \quad y = \frac{z + z^{2^m}}{\beta + \beta^{2^m}}.$$

Let $z' = z/(\beta + \beta^{2^m})$. We may rewrite x, y as

$$(3) \quad x = \beta^{2^m} z' + \beta z'^{2^m}, \quad y = z' + z'^{2^m}.$$

Substituting x, y above into the function F defined in (1) and abusing notation, we may rewrite F as a function $F : \mathbb{F}_{2^{2m}} \rightarrow \mathbb{F}_{2^{2m}}$ given by

$$(4) \quad F(x) = (\beta^{2^m} x + \beta x^{2^m})^{2^k+1} + \alpha(x^{2^m} + x)^{(2^k+1)2^i} + (x^{2^m} + x)(\beta^{2^m} x + \beta x^{2^m})\beta.$$

Now, for any $a \in \mathbb{F}_{2^n}^*$ and any $u \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} & \text{Tr}(a(F(x+u) + F(x) + F(u))) \\ &= \text{Tr}\left(a\left[\beta^{2^{m+k}+2^m}(ux^{2^k} + u^{2^k}x) + \beta^{2^{m+k}+1}(u^{2^m}x^{2^k} + u^{2^k}x^{2^m})\right.\right. \\ &\quad + \beta^{2^k+2^m}(ux^{2^{m+k}} + u^{2^{m+k}}x) + \beta^{2^k+1}(u^{2^m}x^{2^{m+k}} + u^{2^{m+k}}x^{2^m}) \\ &\quad + \alpha(u^{2^{m+i}}x^{2^{m+k+i}} + u^{2^{m+k+i}}x^{2^{m+i}}) + \alpha(u^{2^i}x^{2^{m+k+i}} + u^{2^{m+k+i}}x^{2^i}) \\ &\quad + \alpha(u^{2^{m+i}}x^{2^{k+i}} + u^{2^{k+i}}x^{2^{m+i}}) + \alpha(u^{2^i}x^{2^{k+i}} + u^{2^{k+i}}x^{2^i}) \\ &\quad \left.\left. + \beta(\beta^{2^m} + \beta)(ux^{2^m} + u^{2^m}x)\right]\right) \\ &= \text{Tr}(L_a(u)x), \end{aligned}$$

where

$$\begin{aligned} L_a(u) &= (au\beta^{2^{m+k}+2^m})^{2^{-k}} + au^{2^k}\beta^{2^{m+k}+2^m} \\ &\quad + (au^{2^m}\beta^{2^{m+k}+1})^{2^{-k}} + (au^{2^k}\beta^{2^{m+k}+1})^{2^m} + (au\beta^{2^k+2^m})^{2^{m-k}} \\ &\quad + au^{2^{m+k}}\beta^{2^k+2^m} + (au^{2^m}\beta^{2^k+1})^{2^{m-k}} + (au^{2^{m+k}}\beta^{2^k+1})^{2^m} + (au^{2^{m+i}}\alpha)^{2^{m-k-i}} \\ &\quad + (au^{2^{m+k+i}}\alpha)^{2^{m-i}} + (au^{2^i}\alpha)^{2^{m-k-i}} + (au^{2^{m+k+i}}\alpha)^{2^{-i}} + (au^{2^{m+i}}\alpha)^{2^{-k-i}} \\ &\quad + (au^{2^{k+i}}\alpha)^{2^{m-i}} + (au^{2^i}\alpha)^{2^{-k-i}} + (au^{2^{k+i}}\alpha)^{2^{-i}} + (au\beta(\beta^{2^m} + \beta))^{2^m} \\ &\quad + au^{2^m}\beta(\beta^{2^m} + \beta). \end{aligned}$$

Let $B = a + a^{2^m}$. Then $B \in \mathbb{F}_{2^m}$. After simplifying $L_a(u)$ we may rewrite it in the form

$$(5) \quad L_a(u) = A_1u^{2^{m+k}} + A_2u^{2^k} + A_3u^{2^{m-k}} + A_4u^{2^{-k}} + A_5u^{2^m},$$

where

$$\begin{aligned} A_1 &= \beta^{2^{m+2^k}}B + \alpha^{2^{-i}}B^{2^{-i}}, & A_2 &= \beta^{2^{m+k}+2^m}B + \alpha^{2^{-i}}B^{2^{-i}}, \\ A_3 &= \beta^{2^{m+2^{-k}}}B^{2^{-k}} + \alpha^{2^{-k-i}}B^{2^{-k-i}}, & A_4 &= \beta^{2^{m+2^{m-k}}}B^{2^{-k}} + \alpha^{2^{-k-i}}B^{2^{-k-i}}, \\ A_5 &= (a\beta + a^{2^m}\beta^{2^m})(\beta^{2^m} + \beta). \end{aligned}$$

Note that we have used the fact $\alpha = \alpha^{2^m}$ here as $\alpha \in \mathbb{F}_{2^m}$. It should be remarked that $A_3 = A_1^{2^{m-k}}$, $A_4 = A_2^{2^{-k}}$, $A_5 = A_5$.

In the following, we demonstrate that $|K| \leq 8$, where K is the kernel of L_a .

First, if $B = 0$, then $a \in \mathbb{F}_{2^m}^*$, and $A_5 = a(\beta^{2^m} + \beta)^2 \neq 0$ since $\beta \notin \mathbb{F}_{2^m}$. Thus $L_a(u) = A_5u^{2^m} = 0$ if and only if $u = 0$.

From now on, we assume that $B \neq 0$. Let

$$C(u) = A_1u^{2^{m+k}+1} + A_1^{2^m}u^{2^{m+2^k}} + A_2u^{2^k+1} + A_2^{2^m}u^{2^{m+k}+2^m}.$$

Now we claim that $C(x)$ is a crucial s -polynomial of $L_a(x)$, where $s = n - k$ satisfies $\gcd(n, s) = 1$ since $n = 2m$, $\gcd(k, m) = 1$, and m is even. First, for any $u \in K$, it is easy to verify that

$$0 = uL_a(u) + u^{2^m}L_a(u)^{2^m} = C(u) + C(u)^{2^{-k}}.$$

Next, we need to prove that $C(u) = 0$ if and only if $u = 0$.

Let $C(u) = 0$. Then we have

$$\begin{aligned} 0 = C(u) &= B(\beta^{2^m+2^k} u^{2^{m+k}+1} + \beta^{2^{m+k}+1} u^{2^m+2^k}) + \alpha^{2^{-i}} B^{2^{-i}} (u^{2^{m+k}+1} + u^{2^m+2^k}) \\ &\quad + B(\beta^{2^{m+k}+2^m} u^{2^k+1} + \beta^{2^k+1} u^{2^{m+k}+2^m}) + \alpha^{2^{-i}} B^{2^{-i}} (u^{2^k+1} + u^{2^{m+k}+2^m}) \\ &= B(\beta u^{2^m} + \beta^{2^m} u)^{2^k+1} + \alpha^{2^{-i}} B^{2^{-i}} (u^{2^m} + u)^{2^k+1}. \end{aligned}$$

If $u^{2^m} + u \neq 0$, then

$$\alpha^{2^{-i}} = B^{1-2^{-i}} \left(\frac{\beta u^{2^m} + \beta^{2^m} u}{u^{2^m} + u} \right)^{2^k+1},$$

which contradicts the assumption that α is a noncube, i is even, and k is odd. Hence $u^{2^m} + u = 0$, and then we have $\beta u^{2^m} + \beta^{2^m} u = u(\beta + \beta^{2^m}) = 0$. From $\beta \notin \mathbb{F}_{2^m}$, we have $u = 0$. Therefore, $C(u) = 1$ holds for any $0 \neq u \in K$.

Thus $C(x)$ is a crucial $(n - k)$ -polynomial of $L_a(x)$. Then, by Lemma 1, we conclude that $\dim(K) \leq 2$. The proof for the first part is now complete.

2. Carlet APN function: Similar to the computations at the beginning of the first part, substituting x, y into (3) in the function F defined in (2) and abusing notation, we may rewrite F as a function $F : \mathbb{F}_{2^{2m}} \rightarrow \mathbb{F}_{2^{2m}}$ given by

$$\begin{aligned} F(x) &= g_1(\beta^{2^m} x + \beta x^{2^m})^{2^i+2^j} + g_2(\beta^{2^m} x + \beta x^{2^m})^{2^i} (x + x^{2^m})^{2^j} \\ (6) \quad &\quad + g_3(\beta^{2^m} x + \beta x^{2^m})^{2^j} (x + x^{2^m})^{2^i} + g_4(x + x^{2^m})^{2^i+2^j} \\ &\quad + \beta(x + x^{2^m})(\beta^{2^m} x + \beta x^{2^m}) + \beta^{2^m+1} x^2 + \beta^2 x^{2^{m+1}}. \end{aligned}$$

Expanding the function F , we may rewrite it in the form

$$F(x) = l_1 x^{2^i+2^j} + l_2 x^{2^i+2^{m+j}} + l_3 x^{2^j+2^{m+i}} + l_4 x^{2^{m+i}+2^{m+j}} + l_5 x^{2^m+1} + l_0(x),$$

where

$$\begin{aligned} l_1 &= g_1 \beta^{2^{m+i}+2^{m+j}} + g_2 \beta^{2^{m+i}} + g_3 \beta^{2^{m+j}} + g_4, \\ l_2 &= g_1 \beta^{2^{m+i}+2^j} + g_2 \beta^{2^{m+i}} + g_3 \beta^{2^j} + g_4, \\ l_3 &= l_2^{2^m}, \quad l_4 = l_1^{2^m}, \\ l_5 &= \beta(\beta + \beta^{2^m}), \quad l_0(x) = \beta^{2^m+1} x^2 + \beta^2 x^{2^{m+1}}. \end{aligned}$$

Now we compute $L_a(x)$. For any $a \in \mathbb{F}_{2^n}^*$ and any $u \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} &\text{Tr}(a(F(x+u) + F(x) + F(u))) \\ &= \text{Tr}\left(a(l_1(u^{2^j} x^{2^i} + u^{2^i} x^{2^j}) + l_2(u^{2^{m+j}} x^{2^i} + u^{2^i} x^{2^{m+j}}) + l_3(u^{2^{m+i}} x^{2^j} + u^{2^j} x^{2^{m+i}})\right. \\ &\quad \left.+ l_4(u^{2^{m+i}} x^{2^{m+j}} + u^{2^{m+j}} x^{2^{m+i}}) + l_5(ux^{2^m} + u^{2^m} x)\right) \\ &= \text{Tr}\left((A_1 u^{2^{i-j}} + A_2 u^{2^{m+i-j}} + A_3 u^{2^{j-i}} + A_4 u^{2^{m-i+j}} + A_5 u^{2^m})x\right), \end{aligned}$$

where

$$\begin{aligned} B &= a + a^{2^m}, \\ A_1 &= (Bl_1)^{2^{-j}}, \quad A_2 = (Bl_2^{2^m})^{2^{-j}}, \\ A_3 &= (Bl_1)^{2^{-i}}, \quad A_4 = (Bl_2)^{2^{-i}}, \\ A_5 &= (al_5)^{2^m} + al_5. \end{aligned}$$

Thus

$$(7) \quad L_a(u) = A_1 u^{2^{i-j}} + A_2 u^{2^{m+i-j}} + A_3 u^{2^{j-i}} + A_4 u^{2^{m-i+j}} + A_5 u^{2^m}.$$

Similar to the proof of the first part, it suffices to demonstrate $|K| \leq 8$, where K is the kernel of L_a .

If $B = 0$, then $A_1 = A_2 = A_3 = A_4 = 0$ and $A_5 = a(\beta + \beta^{2^m})^2 \neq 0$. It follows from (7) that $L_a(u) = 0$ if and only if $u = 0$, and we are done.

In the following, we assume $B \neq 0$ and split the proof into two cases according to whether $\gcd(n, i-j) = 1$ or $\gcd(n, i-j) = 2$. For each case, we construct a crucial polynomial of $L_a(x)$. Note that by simple calculations $l_1 + l_2 = (g_1\beta^{2^{m+i}} + g_3)(\beta + \beta^{2^m})^{2^j}$. This implies that l_1, l_2 cannot be zero at the same time as $g_1\beta^{2^{m+i}} + g_3 \neq 0$.

Case 1: $\gcd(m, i-j) = \gcd(2m, i-j) = 1$. Letting $s = i-j$, then $\gcd(n, s) = \gcd(n, n-s) = 1$, and we may rewrite (7) in the form

$$(8) \quad L_a(u) = A_1 u^{2^s} + A_2 u^{2^{m+s}} + A_3 u^{2^{-s}} + A_4 u^{2^{m-s}} + A_5 u^{2^m}.$$

Define

$$(9) \quad C(u) = A_2 u^{2^{m+i-j+1}} + A_2^{2^m} u^{2^m+2^{i-j}} + A_1 u^{2^{i-j+1}} + A_1^{2^m} u^{2^{m+i-j+2^m}}.$$

We claim that $C(x)$ is a crucial $(n-s)$ -polynomial of $L_a(x)$. First, it can be verified that

$$(10) \quad uL_a(u) + u^{2^m} L_a(u)^{2^m} = C(u) + C(u)^{2^{j-i}}.$$

The following arguments show that $C(u) = 0$ if and only if $u = 0$. Assuming that $C(u) = 0$ and substituting A_1, A_2 into (9), we have

$$B^{2^{-j}} \left(l_2^{2^{m-j}+1} u^{2^{m+i-j}} + l_2^{2^{-j}} u^{2^m+2^{i-j}} + l_1^{2^{-j}} u^{2^{i-j+1}} + l_1^{2^{m-j}} u^{2^{m+i-j+2^m}} \right) = 0.$$

Raising the above equation to the 2^j th power and substituting for l_1, l_2 , by using $B \neq 0$, we get

$$(11) \quad \begin{aligned} & g_1 (\beta^{2^m} u + \beta u^{2^m})^{2^i+2^j} + g_2 (u + u^{2^m})^{2^j} (\beta u^{2^m} + \beta^{2^m} u)^{2^i} \\ & + g_3 (u + u^{2^m})^{2^i} (\beta u^{2^m} + \beta^{2^m} u)^{2^j} \\ & + g_4 (u + u^{2^m})^{2^i+2^j} = G(\beta^{2^m} u + \beta u^{2^m}, u + u^{2^m}) = 0. \end{aligned}$$

If $u \notin \mathbb{F}_{2^m}$, then dividing both sides of (11) by $(u + u^{2^m})^{2^i+2^j}$ yields

$$G \left(\frac{\beta^{2^m} u + \beta u^{2^m}}{u + u^{2^m}}, 1 \right) = 0.$$

This contradicts the assumption that $G(x, 1)$ has no root in \mathbb{F}_{2^m} . Therefore, we have $u \in \mathbb{F}_{2^m}$, so $u + u^{2^m} = 0$. From (11), we see that

$$(12) \quad g_1 u^{2^i+2^j} (\beta + \beta^{2^m})^{2^i+2^j} = 0,$$

which is possible if and only if $u = 0$.

Thus $C(x)$ is a crucial $(n - s)$ -polynomial of $L_a(x)$. Hence, by Lemma 1, we have $\dim(K) \leq 2$.

Case 2: $\gcd(m, i - j) = 1$ and $\gcd(2m, i - j) = 2$. First, note that $\gcd(2m, m + i - j) = 1$ in this case. Letting $s' = m + i - j$, we may write $L_a(u)$ in the form

$$(13) \quad L_a(u) = A'_1 u^{2^{s'}} + A'_2 u^{2^{m+s'}} + A'_3 u^{2^{-s'}} + A'_4 u^{2^{m-s'}} + A'_5 u^{2^m},$$

where

$$A'_1 = A_2, \quad A'_2 = A_1, \quad A'_3 = A_4, \quad A'_4 = A_3, \quad A'_5 = A_5.$$

Let

$$(14) \quad C'(u) = A'_2 u^{2^{m+s'}+1} + A'_2 u^{2^m} u^{2^m+2^{s'}} + A'_1 u^{2^{s'}+1} + A'_1 u^{2^m} u^{2^{m+s'}+2^m}.$$

Similarly, one can prove that $C'(x)$ is a crucial $(n - s')$ -polynomial of $L_a(x)$. Then $\dim(K) \leq 2$ is also true in this case. We leave the details to the interested reader.

The proof is now complete. \square

We may obtain bent functions of the form $\text{Tr}(aF(x))$ from the proof of the above theorem, where $a \in \mathbb{F}_{2^{2m}}$ and F is the Zhou–Pott APN function or the Carlet APN function.

THEOREM 3. *Let the APN function F in Result 1 (resp., Result 2) be represented by (4) (resp., (6)). Then, for any $a \in \mathbb{F}_{2^m}^*$, the Boolean function $f_a(x) = \text{Tr}(aF(x))$ is bent.*

Proof. We prove only the first case and leave the second one to the interested reader. Let F be the APN function defined in Result 1. Given a nonzero element $a \in \mathbb{F}_{2^m}^*$, to prove that f_a is a bent function, we need to show that, for each $b \in \mathbb{F}_{2^{2m}}$, $f_a^W(b) := F^W(a, b) \in \{\pm 2^m\}$. From the proof of Theorem 2, we have

$$(15) \quad f_a^W(b)^2 = F^W(a, b)^2 = 2^n \sum_{u \in K} (-1)^{\text{Tr}(bu) + f_a(u)},$$

where K is the kernel of L_a in (5). Since $a \in \mathbb{F}_{2^m}$, we have $B = a + a^{2^m} = 0$. It then follows from the expression of $L_a(u)$ that $L_a(u) = A_5 u^{2^m} = 0$ if and only if $u = 0$, which implies $K = \{0\}$. Therefore, by (15), we have $f_a^W(b)^2 = 2^n = 2^{2m}$. The proof is now complete. \square

4. Conclusions. We have determined the Fourier spectra of the APN functions obtained in [20, 12] and shown that they are the same as those of the Gold APN functions. This shows that we cannot expect to find an APN function with a different Fourier spectrum from these two new constructions. Moreover, since the construction in [12] covers several known infinite APN families, the results in this paper give a unified treatment of determining their Fourier spectra, showing in particular that the Fourier spectra of these APN functions are the same as the ones of the Gold APN functions. This gives a positive answer to a conjecture in [6]. With the results in this paper, the Fourier spectra of all known infinite families of APN functions are now determined.

Acknowledgments. The authors would like to thank the anonymous reviewers, whose comments led to significant improvements in both the technical quality and the exposition of this paper. In particular, they are greatly indebted to one reviewer for suggesting Lemma 1, thereby resulting in a shorter proof of Theorem 2.

REFERENCES

- [1] E. BIHAM AND A. SHAMIR, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptology, 4 (1991), pp. 3–72.
- [2] C. BRACKEN, E. BYRNE, N. MARKIN, AND G. MCGUIRE, *Determining the nonlinearity of a new family of APN functions*, in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC 2007), Lecture Notes in Comput. Sci. 4851, Springer, Berlin, 2007, pp. 72–79.
- [3] C. BRACKEN, E. BYRNE, N. MARKIN, AND G. MCGUIRE, *New families of quadratic almost perfect nonlinear trinomials and multinomials*, Finite Fields Appl., 14 (2008), pp. 703–714.
- [4] C. BRACKEN, E. BYRNE, N. MARKIN, AND G. MCGUIRE, *Fourier spectra of binomial APN functions*, SIAM J. Discrete Math., 23 (2009), pp. 596–608.
- [5] C. BRACKEN, E. BYRNE, N. MARKIN, AND G. MCGUIRE, *A few more quadratic APN functions*, Cryptogr. Commun., 3 (2011), pp. 43–53.
- [6] C. BRACKEN, C. H. TAN, AND Y. TAN, *On a Class of Quadratic Polynomials with No Zeros and Its Applications to APN Functions*, preprint, arXiv:1110.3177v1, 2011.
- [7] C. BRACKEN AND Z. B. ZHA, *On the Fourier spectra of the infinite families of quadratic APN functions*, Adv. Math. Commun., 3 (2009), pp. 219–226.
- [8] L. BUDAGHYAN AND C. CARLET, *Classes of quadratic APN trinomials and hexanomials and related structures*, IEEE Trans. Inform. Theory, 54 (2008), pp. 2354–2357.
- [9] L. BUDAGHYAN AND C. CARLET, *Constructing new APN functions from known ones*, Finite Fields Appl., 15 (2009), pp. 150–159.
- [10] L. BUDAGHYAN, C. CARLET, AND G. LEANDER, *Two classes of quadratic APN binomials inequivalent to power functions*, IEEE Trans. Inform. Theory, 54 (2008), pp. 4128–4299.
- [11] C. CARLET, *Vectorial Boolean functions for cryptography*, in Boolean Methods and Models, Y. Crama and P. Hammer, eds., Cambridge University Press, Cambridge, UK, 2010, pp. 398–472.
- [12] C. CARLET, *Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions*, Des. Codes Cryptogr., 59 (2011), pp. 89–109.
- [13] C. CARLET, P. CHARPIN, AND V. ZINOVIEV, *Bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr., 15 (1998), pp. 125–156.
- [14] J. DILLON, *Slides from Talk Given at Polynomials over Finite Fields and Applications*, Banff International Research Station, Banff, AB, Canada, 2006; available online from <http://mathsci.ucd.ie/~gmg/Fq9Talks/Dillon.pdf>.
- [15] J. F. DILLON, *Almost perfect nonlinear polynomials: An update*, in Proceedings of the 9th International Conference on Finite Fields and Applications of Fq9, Dublin, Ireland, 2009.
- [16] Y. EDEL, G. KYUREGHYAN, AND A. POTT, *A new APN function which is not equivalent to a power mapping*, IEEE Trans. Inform. Theory, 52 (2006), pp. 744–747.
- [17] Y. EDEL AND A. POTT, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun., 3 (2009), pp. 59–81.
- [18] R. LIDL AND H. NIEDERREITER, *Finite Fields*, 2nd ed., Encyclopedia Math. Appl. 20, Cambridge University Press, Cambridge, UK, 1997.
- [19] K. NYBERG, *Differentially uniform mappings for cryptography*, in Advances in Cryptology—EUROCRYPT ’93 (Lofthus, 1993), Lecture Notes in Comput. Sci. 765, Springer, Berlin, 1994, pp. 55–64.
- [20] Y. ZHOU AND A. POTT, *A new family of semifields with 2 parameters*, Adv. Math., 234 (2013), pp. 43–60.