A note on the Walsh spectrum of Dobbertin APN functions

Lilya Budaghyan, Marco Calderini, Claude Carlet,
Diana Davidova and Nikolay Kaleyski

Department of Informatics
University of Bergen
Bergen, Norway

{lilya.budaghyan,marco.calderini,diana.davidova,nikolay.kaleyski}@uib.no,

claude.carlet@gmail.com

Abstract

Among the six known classes of APN power functions on $\mathbb{F}_{2^n}$, the Dobbertin function is the only one whose Walsh spectrum and, in particular, nonlinearity, are unknown. This problem has already been open for 20 years without any progress since the seminal work of Canteaut, Charpin and Dobbertin from 2000, in which they proved that all Walsh coefficients of the Dobbertin function over $\mathbb{F}_{2^{5m}}$ are divisible by 2^{2m}.

In this paper, we present a conjecture fully describing the Walsh spectrum of the Dobbertin function. We also show that the Dobbertin function can be represented as the composition of a cubic power function and the inverse of a quadratic power function; more precisely, the Dobbertin exponent over $\mathbb{F}_{2^{5m}}$ has the form $2^{2m+1}\frac{2^{2m}+2^m+1}{2^m+1}$. This representation is optimal in the sense that it is impossible to represent the Dobbertin function as the composition of a quadratic power map with the inverse of another quadratic power function.

1 Introduction

Differential cryptanalysis, introduced by Biham and Shamir [2], and linear cryptanalysis, introduced by Matsui [17], are two of the most powerful attacks against block ciphers known to date. The notions of almost perfect nonlinear (APN) and almost bent (AB) functions were introduced by Nyberg [18] and by Chabaud and Vaudenay [8], respectively, to designate the classes of functions providing optimal resistance to these attacks. Since then, much work has been done on these two topics.

Let n be a positive integer. An (n, n)-*function*, or *vectorial Boolean function*, is any mapping from the finite field $\mathbb{F}_{2^n}$ of 2^n elements to itself. For any positive integers n and δ, an (n, n)-function F is called *differentially δ-uniform* if, for every nonzero a and every b in $\mathbb{F}_{2^n}$, the equation $F(x) + F(x + a) = b$ admits at most δ solutions.

Given a positive integer i, its *2-weight* is the number of ones in its binary notation. More precisely, if $i = \sum_{j=0}^{K} c_j 2^j$ for some positive integer K and for $c_j \in \{0,1\}$ for $0 \leq j \leq K$, then the 2-weight is defined as $wt(i) = \sum_{j=0}^{K} c_j$. The largest 2-weight of any exponent i in the univariate representation of an (n,n)-function F with $a_i \neq 0$ is called the *algebraic degree* of F. A function of algebraic degree 1, resp, 2, resp. 3 is called *affine*, resp. *quadratic*, resp. *cubic*. An affine function F with $F(0) = 0$ is called *linear*.

Vectorial Boolean functions used as S-boxes in block ciphers must have low differential uniformity in order to provide high resistance to differential cryptanalysis. We note that over a finite field of even characteristic, the equation $F(x) + F(x+a) = b$ always has an even number of solutions for any $a, b \in \mathbb{F}_{2^n}$. In this sense, differentially 2-uniform functions, called *almost perfect nonlinear (APN) functions*, are optimal. The notion of an APN function is closely connected to that of an almost bent (AB) function, which can be described in terms of the so-called Walsh transform. Let $\mathrm{tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$ denote the absolute trace function from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_2$. The *Walsh transform* of an (n,n)-function F is the integer valued function $W_F : \mathbb{F}_{2^n}^2 \to \mathbb{Z}$ defined by

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(bF(x)+ax)}, \qquad a, b \in \mathbb{F}_{2^n}.$$

The set $W_F = \{W_F(a,b) : a, b \in \mathbb{F}_{2^n}, b \neq 0\}$ is called the *Walsh spectrum* of F and the set $\{|W_F(a,b)| : a, b \in \mathbb{F}_{2^n}, b \neq 0\}$ is called the *extended Walsh spectrum* of F. If the Walsh spectrum of F equals $\{0, \pm 2^{\frac{n+1}{2}}\}$, then F is called *almost bent (AB)*. AB functions exist only for odd n. Besides, every AB function is APN [8], and in the case of n odd, a quadratic (n,n)-function is APN if and only if it is AB [7].

The nonlinearity of a function measures its resistance to linear cryptanalysis, and can be expressed via the Walsh transform as $\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} |W_F(a,b)|$. AB functions have the highest possible nonlinearity, and thus provide optimum resistance to linear attacks [8]. Comprehensive surveys on APN and AB functions can be found in [3, 6].

Table 1 gives all known values of exponents d (up to multiplication by a power of 2 modulo $2^n - 1$, and up to taking the inverse when d is coprime with $2^n - 1$) such that the function x^d over $\mathbb{F}_{2^n}$ is APN. It is conjectured by Hans Dobbertin that there exists (up to equivalence) no other power APN function [12]. The conjecture has been verified computationally for $n \leq 24$ by Anne Canteaut as stated in [12], and later by Edel for $n \leq 34$ and $n = 36, 38, 40, 42$ (unpublished).

Table 1
Known APN power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions	Proven in
Gold	2^i+1	$\gcd(i,n)=1$	[13, 18]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	[15]
Welch	2^t+3	$n=2t+1$	[10]
Niho	$2^t+2^{\frac{t}{2}}-1$, t even $2^t+2^{\frac{3t+1}{2}}-1$, t odd	$n=2t+1$	[11]
Inverse	$2^{2t}-1$	$n=2t+1$	[1, 18]
Dobbertin	$2^{4m}+2^{3m}+2^{2m}+2^m-1$	$n=5m$	[12]

For n odd the Gold, Kasami, Welch and Niho APN functions from Table 1 are also AB (for the proofs of the AB property, see [4, 5, 13, 14, 15, 18]). In the case of n even, the Gold and the Kasami functions have the same Walsh spectrum: $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$. The Walsh transform of the inverse function takes any value divisible by 4 in the interval $[1-2^{\frac{n}{2}+1}, \ldots, 1+2^{\frac{n}{2}+1}]$ [16]. When n is even, the inverse function x^{2^n-2} is a differentially 4-uniform permutation [18]; its instance for $n=8$ is used as a major component of the AES S-box [9].

The Dobbertin function is the only APN power function whose nonlinearity and Walsh coefficients remain unknown. In 2000, it was proven that it is not AB and that all its Walsh coefficients are divisible by $2^{\frac{2n}{5}}$, but not all of them are divisible by $2^{\frac{2n}{5}+1}$ [5]. During the last twenty years, no more progress has been made. In this work, we present two observations which may stimulate future advances in the study of this problem. In the first one, we show that the Dobbertin exponent can be represented as $\frac{2^{2m}+2^m+1}{2^m+1}$, $\frac{2^{3m}+2^{2m}+1}{2^{2m}+1}$, $\frac{2^{3m}+2^m+1}{2^{3m}+1}$ and $\frac{2^{2m}+2^m+1}{2^{4m}+1}$, that is, as fractions of cubic and quadratic exponents. We also show that such a representation is optimal, in the sense that it is impossible to represent the exponent of the Dobbertin function as a fraction of two quadratic exponents. The second observation is a conjecture giving a full description of the Walsh spectrum of the Dobbertin function.

2 On the exponent of the Dobbertin function

It is known that the exponent of the Kasami function in the case n odd can be represented as $2^{2i}-2^i+1=\frac{2^{3i}+1}{2^i+1}$, that is, the function can be expressed as the composition of a quadratic power function with the inverse of another quadratic power function. As shown in [7], this property gives a simple explanation of the AB-ness of the Kasami function for n odd. Here we study whether a similar property can be derived for the Dobbertin exponent.

Recall that the exponents d and d' of the functions x^d and $x^{d'}$ over $\mathbb{F}_{2^n}$ are in the same cyclotomic coset if $d'=2^k d \mod (2^n-1)$ for some non-negative integer k. Power functions with exponents in the same cyclotomic coset have the same extended Walsh spectrum, and the same differential uniformity. In particular, if one of them is APN (AB), then the second is also APN (AB). This means that we are free to choose any

representatives from the cyclotomic coset of a power function. We use this below to find an alternative representation for the Dobbertin APN function.

Lemma 1. *For any positive integer m the following equivalences are true:*

$$\begin{aligned}\sum_{i=1}^{4} 2^{im} - 1 &\equiv 2^{2m+1}\frac{2^{2m}+2^m+1}{2^m+1} \mod (2^{5m}-1)\\ &\equiv 2^{m+1}\frac{2^{3m}+2^{2m}+1}{2^{2m}+1} \mod (2^{5m}-1)\\ &\equiv 2^{m+1}\frac{2^{3m}+2^m+1}{2^{3m}+1} \mod (2^{5m}-1)\\ &\equiv 2^{m+1}\frac{2^{2m}+2^m+1}{2^{4m}+1} \mod (2^{5m}-1).\end{aligned}$$

Proof. Consider the first congruence. We first prove that 2^m+1 is invertible modulo $2^{5m}-1$, i.e. that $\gcd(2^m+1, 2^{5m}-1) = 1$. This follows from

$$\gcd(2^k+1, 2^l-1) = \begin{cases} 1, & \text{if } l/\gcd(l,k) \text{ is odd;} \\ 2^{\gcd(m,k)}+1, & \text{if } l/\gcd(l,k) \text{ is even.}\end{cases} \tag{1}$$

Indeed, since $\gcd(m, 5m) = m$, we have $\gcd(2^m+1, 2^{5m}-1) = 1$.
For simplicity, denote 2^m by y. It remains to check the equivalence $(y+1)(y^4+y^3+y^2+y-1) \equiv 2y^2(y^2+y+1) \mod (y^5-1)$ which is straightforward. Indeed, computing the left-hand side of this equivalence, we get
$(y+1)(y^4+y^3+y^2+y-1) = y^5+2y^4+2y^3+2y^2-1 \equiv 2y^4+2y^3+2y^2 \mod (y^5-1)$.
This proves the first statement of the lemma.

The other three equivalences are proven in the same way. A justification that $2^{2m}+1$, $2^{3m}+1$ and $2^{4m}+1$ are invertible modulo $2^{5m}-1$ easily follows from (1). The corresponding congruences are then straightforward to check. □

Lemma 2. *Let m be a positive integer. Then, for any positive integers j, l, r such that $1 \le j, l, r < 5m$, the following inequivalence holds:*

$$\left(\sum_{i=1}^{4} 2^{im} - 1\right)(2^j+1) \not\equiv 2^l + 2^r \mod (2^{5m}-1). \tag{2}$$

Proof. We shall show that for any $1 \le j < 5m$, the 2-weight of the left-hand side of (2) is always strictly greater then 2. The cases $j \in \{m, 2m, 3m, 4m\}$ are covered in Lemma 1 when the 2-weight of $\left(\sum_{i=1}^{4} 2^{im} - 1\right)(2^j+1)$ equals 3. We thus consider the remaining 5 cases

1. $1 \leq j < m$,
2. $j = m + j', 1 \leq j' < m$,
3. $j = 2m + j', 1 \leq j' < m$,
4. $j = 3m + j', 1 \leq j' < m$,
5. $j = 4m + j', 1 \leq j' < m$.

In all of these cases, the 2-weight of $\left(\sum_{i=1}^{4} 2^{im} - 1\right)(2^j + 1)$ is equal to $m + 6$. Indeed, for $1 \leq j < m$ we get

$$\left(\sum_{i=1}^{4} 2^{im} - 1\right)(2^j + 1) \equiv (\sum_{i=1}^{4} 2^{im+j} - 2^j + \sum_{i=1}^{4} 2^{im} - 1) \mod (2^{5m} - 1).$$

Hence,

$$wt\left(\left(\sum_{i=1}^{4} 2^{im} - 1\right)(2^j + 1)\right) = wt\big(\sum_{i=1}^{4} 2^{im+j} + \sum_{i=2}^{4} 2^{im}\big) + wt\big(2^m - 2^j - 1\big) = 7 + (m-1) = m+6.$$

Similarly, for $j = m + j', 1 \leq j' < m$:

$$\begin{aligned}\left(\sum_{i=1}^{4} 2^{im} - 1\right)(2^j + 1) &= \left(\sum_{i=1}^{4} 2^{im} - 1\right)(2^{m+j'} + 1) = \sum_{i=2}^{5} 2^{im+j'} - 2^{m+j'} + \sum_{i=1}^{4} 2^{im} - 1 \\ &\equiv \big(\sum_{i=2}^{4} 2^{im+j'} - 2^{m+j'} + \sum_{i=1}^{4} 2^{im} + 2^{j'} - 1\big) \mod (2^{5m} - 1).\end{aligned}$$

Therefore,

$$\begin{aligned}wt\left(\left(\sum_{i=1}^{4} 2^{im} - 1\right)(2^j + 1)\right) &= wt\left(\sum_{i=2}^{4} 2^{im+j'} - 2^{m+j'} + \sum_{i=1}^{4} 2^{im} + 2^{j'} - 1\right) \\ &= wt(\sum_{i=2}^{4} 2^{im+j'} + 2^{4m} + 2^{3m} + 2^m) + wt(2^{2m} - 2^{m+j'}) \\ &\quad + wt(2^{j'} - 1) = 6 + (m - j') + j' = 6 + m.\end{aligned}$$

The remaining cases are proven in the exact same way. □

The following corollary is a straightforward consequence of Lemma 1 and Lemma 2.

Corollary 1. *Let x^d be a power function defined over the field $\mathbb{F}_{2^{5m}}$ with $d = 2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$. Then x^d is equivalent to power functions with the exponents $\frac{2^{2m}+2^m+1}{2^m+1}$, $\frac{2^{3m}+2^{2m}+1}{2^{2m}+1}$, $\frac{2^{3m}+2^m+1}{2^{3m}+1}$ and $\frac{2^{2m}+2^m+1}{2^{4m}+1}$. Furthermore, these representations are optimal, in the sense that x^d is inequivalent to any power function whose exponent is a fraction of two quadratic exponents.*

3 A conjecture about the Walsh spectrum of the Dobbertin function

In order to get information about the form of the Walsh spectrum of the Dobbertin function, we performed experiments over the fields $\mathbb{F}_{2^{5m}}$ for $m \leq 7$. Below, we present computational data in two tables for n odd and n even, respectively.

Based on Tables 2 and 3, we conjecture that the Walsh spectrum of the Dobbertin function x^d, where $d = 2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$ over $\mathbb{F}_{2^{5m}}$ has the following possible forms depending on the parity of m:

- $\{0, 2^{2m}(2^m+1), \pm 2^{5k-2}, \pm a \cdot 2^{2m} \mid 1 \leq a \leq k \cdot (k+1), a \text{ odd}\}$ for $m = 2k-1, k \in \mathbb{N}$;
- $\{0, -2^{2m}(2^m+1), \pm 2^{5k}, \pm 2^{5k+1}, \pm a \cdot 2^{2m} \mid 1 \leq a \leq k \cdot (k+2), a \text{ odd}\}$ for $m = 2k, k \in \mathbb{N}$.

Moreover, $W_F(u, v)$ takes the maximum absolute value $2^{2m}(2^{m+1}+1)$ only once, for $u = v = 1$: for even m, we have $\min W_F(u, v) = -2^{2m}(2^{m+1}+1)$, and for odd m, we have $\max W_F(u, v) = 2^{2m}(2^m+1)$. Hence, the nonlinearity of the Dobbertin function should be $2^{5m-1} - 2^{2m-1}(2^m+1)$.

Table 2

Walsh coefficients of the Dobbertin function over $\mathbb{F}_{2^{5m}}$ with $m = 2k-1$, $1 \leq k \leq 4$

$n = 5, m = 1, k = 1$	$n = 15, m = 3, k = 2$	$n = 25, m = 5, k = 3$	$n = 35, m = 7, k = 4$
0	0	0	0
$12 = 2^2(2^1+1)$	$576 = 2^6(2^3+1)$	$33792 = 2^{10}(2^5+1)$	$2113536 = 2^{14}(2^7+1)$
$\pm 8 = \pm 2^3$	$\pm 64 = \pm 2^6$	$\pm 1024 = \pm 2^{10}$	$\pm 16384 = \pm 2^{14}$
$\pm 4 = \pm 2^2$	$\pm 256 = \pm 2^8$	$\pm 8192 = \pm 2^{13}$	$\pm 262144 = \pm 2^{18}$
	$\pm 192 = \pm 3 \cdot 2^6$	$\pm 3072 = \pm 3 \cdot 2^{10}$	$\pm 49152 = \pm 3 \cdot 2^{14}$
	$\pm 320 = \pm 5 \cdot 2^6$	$\pm 5120 = \pm 5 \cdot 2^{10}$	$\pm 81920 = \pm 5 \cdot 2^{14}$
		$\pm 7168 = \pm 7 \cdot 2^{10}$	$\pm 114688 = \pm 7 \cdot 2^{14}$
		$\pm 9216 = \pm 9 \cdot 2^{10}$	$\pm 147456 = \pm 9 \cdot 2^{14}$
		$\pm 11264 = \pm 11 \cdot 2^{10}$	$\pm 180224 = \pm 11 \cdot 2^{14}$
			$\pm 212992 = \pm 13 \cdot 2^{14}$
			$\pm 245760 = \pm 15 \cdot 2^{14}$
			$\pm 278528 = \pm 17 \cdot 2^{14}$
			$\pm 311296 = \pm 19 \cdot 2^{14}$

Table 3

Walsh coefficients of the Dobbertin function over $\mathbb{F}_{2^{5m}}$ with $m = 2k$, $1 \leq k \leq 3$

$n = 10, m = 2, k = 1$	$n = 20, m = 4, k = 2$	$n = 30, m = 6, k = 3$
0 $-80 = -2^4(2^2 + 1)$ $\pm 16 = \pm 2^4$ $\pm 32 = \pm 2^5$ $\pm 64 = \pm 2^6$ $\pm 48 = \pm 3 \cdot 2^4$	0 $-4352 = -2^8(2^4 + 1)$ $\pm 256 = \pm 2^8$ $\pm 1024 = \pm 2^{10}$ $\pm 2048 = \pm 2^{11}$ $\pm 768 = \pm 3 \cdot 2^8$ $\pm 1280 = \pm 5 \cdot 2^8$ $\pm 1792 = \pm 7 \cdot 2^8$	0 $-266240 = -2^{12}(2^6 + 1)$ $\pm 4096 = \pm 2^{12}$ $\pm 32768 = 2^{15}$ $\pm 65536 = \pm 2^{16}$ $\pm 12288 = \pm 3 \cdot 2^{12}$ $\pm 20480 = \pm 5 \cdot 2^{12}$ $\pm 28672 = \pm 7 \cdot 2^{12}$ $\pm 36864 = \pm 9 \cdot 2^{12}$ $\pm 45056 = \pm 11 \cdot 2^{12}$ $\pm 53248 = \pm 13 \cdot 2^{12}$ $\pm 61440 = \pm 15 \cdot 2^{12}$

Acknowledgments

This research was supported by the Trond Mohn foundation (TMS). The authors would like to thank Tor Helleseth for useful discussions.

References

[1] T. Beth and C. Ding, "On almost perfect nonlinear permutations", Advances in Cryptology, Eurocrypt'93, Lecture Notes in Comput.Sci., vol. 765, 1993, pp. 65–76.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", J. Cryptol., vol. 4, no. 1, 1991, pp. 3–72.

[3] L. Budaghyan. "Construction and Analysis of Cryptographic Functions", Springer Verlag, 2015.

[4] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: A proof of Welsh conjecture", IEEE Trnas. Inf. Theory, vol. 46, no. 1, 2000, pp. 4–8.

[5] A. Canteaut, P. Charpin, and H. Dobbertin, "Weight divisibility by cyclic codes, highly nonlinear functions on $\mathbb{F}_2^n$, and crosscorelation of maximum-weight sequences", SIAM Journal of Discrete Mathematics, vol. 13, no. 1, 2000, pp. 105–138.

[6] C. Carlet. "Vectorial (multi-output) Boolean Functions for Cryptography", Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 398-469, 2010.

[7] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptography", Design, Codes and Cryptography, vol. 15, no. 2, 1998, pp.125–156.

[8] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis", Advances in Cryptology, Eurocrypt'94, Lecture Notes in Comput.Sci., vol. 950, 1995, pp. 356–365.

[9] J. Daemen and V. Rijmen. The Design of Rijndael. Springer Verlag, 2002.

[10] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case", IEEE Trnas. Inf. Theory, vol. 45, no. 4, 1999, pp. 1271–1275.

[11] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case", Inf. and Comput., vol. 151, 1999, pp. 57–72.

[12] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5", Proceedings of Finite Fields and Applications Fq5, Augsburg, Germany, Springer, 2000, pp. 113–121.

[13] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorellation functions", IEEE Transactions on Information Theory, no. 14, 1968, pp. 154–156.

[14] H. Hollman and Q. Xiang, "A proof of Welch and Niho conjectures on crosscorellation of binary m-sequences ", Finite Fields and Their Applications, no. 7, 2001, pp. 253–286.

[15] T. Kasami, "The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes", Information and Control, no. 18, 1971, pp. 369–394.

[16] G. Lachaud and J. Wolfmann, "The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes", IEEE Trans. Inform. Theory, vol. 36, 1990, pp. 686-692.

[17] M. Matsui, "Linear cryptanalysis methods for DES cipher", Advances in Cryptology, Eurocrypt'93, Lecture Notes in Comput.Sci., vol. 65, 1993, pp. 386–397.

[18] K. Nyberg, "Differentially uniform mappings for cryptography", Advances in Cryptology, Eurocrypt'93, Lecture Notes in Comput.Sci., vol. 765, 1993, pp. 55–64.