On the second derivative of some kinds of Bent functions

Xinyang Zhang
School of Mathematics and Systems Science
Beihang University
Beijing, China
sydney_1995@sina.com

Meng Zhou
School of Mathematics and Systems Science
Beihang University
Beijing, China
zhoumeng1613@hotmail.com

Abstract. Bent function plays an important role in cryptography. It opposes an optimum resistance to linear and differential cryptanalysis. We point out that for some kinds of bent functions, such as Maiorana-McFarland functions and functions with algebraic degree less than three, they are weak in second-order differential cryptanalysis. Thus when constructing bent functions we should use other methods and avoid these functions. Furthermore, a bent function can split into four bent pieces if and only if, the corresponding second-order differential of its dual function is 1.

Keywords-bent function; second derivative; differential cryptanalysis; Hamming distance; Walsh spectrum

I. INTRODUCTION

In the mathematical field of combinatorics, a bent function is a special type of Boolean function. Defined and named in the 1960s by Oscar Rothaus in research not published until 1976([1]), bent functions are so called because they are as different as possible from all linear and affine functions. They have been extensively studied for their applications in cryptography, but have also been applied to spread spectrum, coding theory, and combinatorial design. The definition can be extended in several ways, leading to different classes of generalized bent functions keeping many of the useful properties of the original.

In cryptography, higher-order differential cryptanalysis is a generalization of differential cryptanalysis, an attack against block ciphers. Developed in 1994 by Lars Knudsen([2]), the technique has been applied to a number of ciphers. Whereas ordinary differential cryptanalysis analyzes the differences between two texts, the higher-order variant considers differences between differences, etc. It has been shown to be more powerful than a first-order attack in some cases (see KN-Cipher).

II. BASIC KNOWLEDGE

At first we give the definition of Walsh transform for Boolean functions, which is one of the most important tools for researching the cryptography of Boolean functions.

Denote B_n Boolean functions of n variables.

Definition 2.1. (Walsh transform) Assume $f(x) \in B_n$. The Walsh transform of $f(x)$ is an integer valued function on F_2^n,

$$W_f(a) = \sum_{x \in F_2^n} (-1)^{f(x)+a \cdot x}, a \in F_2^n$$

in which $\cdot$ means the inner product between vectors in F_2^n. $W_f(a)$ is called the Walsh spectrum of $f(x)$ on a.

Obviously, the Walsh transform of $f(x)$ can also be considered as discrete Fourier transform of $(-1)^{f(x)}$.

The nonlinearity of a Boolean function is also an integer, which describes the minimal distance to linear and affine functions.

Definition 2.2.(Nonlinearity) Assume $f(x) \in B_n$, let

$$NL(f) = \min_{l(x) \in B_n} d_H(f(x), l(x))$$

in which

$$l(x) = a \cdot x + b, a \in F_2^n, b \in F_2$$

means affine function and

$$d_H(f(x), l(x)) = \left| \{x \in F_2^n \mid f(x) \neq l(x)\} \right|$$

means the hamming distance between $f(x)$ and $l(x)$, then we call $NL(f)$ the nonlinearity of function $f(x)$.

It is easy to prove some property for Walsh transform.

Proposition 2.1. The inverse transform of Walsh transform is

$$(-1)^{f(x)} = \frac{1}{2^n} \sum_{a \in F_2^n} W_f(a)(-1)^{a \cdot x}.$$

Proposition 2.2. $W_f(a) = 2^n - 2d_H(f(x), a \cdot x)$. Especially, $W_f(0) = 2^n - 2d_H(f(x), 0)$. $W_f(0)$ is also denoted $\mathrm{F}(f)$.

Thus

$$NL(f) = 2^{n-1} - \frac{1}{2}\max_{a\in F_2^n}\left|W_f(a)\right|$$

This equality implies the relationship between the Walsh spectrum and the nonlinearity of a Boolean function. The next equality will imply the correlation between the Walsh spectrum values.

Proposition 2.3. (Parseval) If $f(x)\in B_n$, then

$$\sum_{a\in F_2^n} W_f^2(a) = 2^{2n}.$$

it is easy to know the average value of $W_f^2(a)$ is 2^n, so $\max_{a\in F_2^n}\left|W_f(a)\right| \ge 2^{n/2}$, and then we get an upper bound of $NL(f)$ for $f\in B_n$:

$$NL(f) \le 2^{n-1} - 2^{n/2-1}.$$

Definition 2.3. $f(x)\in B_n$ is called bent function, if $NL(f) = 2^{n-1} - 2^{n/2-1}$.

Notice that $NL(f)$ is a positive integer, so if $f(x)\in B_n$ is a bent function, then n must be even. On the other hand, when n is even, then $f(x)$ is bent if and only if $\max_{a\in F_2^n}\left|W_f(a)\right| = 2^{n/2}$. Thus we have the theorem below, which is somewhere another definition of bent functions.

Theorem 2.1. Assume $f(x)\in B_n$, then $f(x)$ is bent if and only if $\left|W_f(a)\right| = 2^{n/2}$ for all $a\in F_2^n$.

Part Ⅳ will show, for all positive even n, bent function of n variables is surely exist.

Since all the Walsh spectrum values of a bent function $f(x)\in B_n$ is $\pm 2^{n/2}$, $W_f(a)$ naturally implies a Boolean function.

Definition 2.4. Assume $f(x)\in B_n$ is a bent function.

The dual bent function of $f(x)$ is defined as:

$$\tilde{f}(a) = \begin{cases} 0, W_f(a) = 2^{n/2}; \\ 1, W_f(a) = -2^{n/2}, \end{cases}$$

or in short, $W_f(a) = 2^{n/2}(-1)^{\tilde{f}(x)}$.

According to Proposition 2.1, it is easy to prove:

Theorem 2.2. Assume $f(x)\in B_n$ is a bent function. The dual function $\tilde{f}(x)$ is also bent and $\tilde{\tilde{f}} = f$.

Besides the dual property, Theorem 2.1 also means for bent functions, the Hamming distance to all affine functions is either $2^{n-1} + 2^{n/2-1}$ or $2^{n-1} - 2^{n/2-1}$. Especially, if $d_H(f,l) = 2^{n-1} + 2^{n/2-1}$, then $d_H(f,l+1) = 2^{n-1} - 2^{n/2-1}$ and vice versa. This shows that every bent functions has distance $2^{n-1} + 2^{n/2-1}$ to half of all affine functions and distance $2^{n-1} - 2^{n/2-1}$ to another half.

Beside linear cryptanalysis, bent function is also best under differential cryptanalysis.

Denote $D_b f(x) = f(x+b) + f(x)$, which is called the derivative of $f(x)$ in the direction of b.

Definition 2.5. $f(x)\in B_n$ is called balanced when $\mathrm{F}(f) = 0$, which means the preimage of 0 and 1 are both 2^{n-1}.

Lemma 2.1. $W_f^2(a) = \sum_{b\in F_2^n} \mathrm{F}(D_b f)(-1)^{a\cdot b}$.

Proof.

$$\begin{aligned} W_f^2(a) &= \sum_{x\in F_2^n}(-1)^{f(x)+a\cdot x}\sum_{y\in F_2^n}(-1)^{f(y)+a\cdot y} \\ &= \sum_{x\in F_2^n}(-1)^{f(x)+a\cdot x}\sum_{b\in F_2^n}(-1)^{f(x+b)+a\cdot(x+b)} \\ &= \sum_{x\in F_2^n}\sum_{b\in F_2^n}(-1)^{f(x)+f(x+b)+a\cdot b} \\ &= \sum_{b\in F_2^n}(-1)^{a\cdot b}\sum_{x\in F_2^n}(-1)^{f(x)+f(x+b)} \\ &= \sum_{b\in F_2^n}\mathrm{F}(D_b f)(-1)^{a\cdot b}. \end{aligned}$$

Theorem 2.3. Assume n is even. $f(x)\in B_n$ is bent if and only if for all $b\in F_2^n\setminus\{0\}$, $D_b f(x)$ is balanced.

Proof. If for all $b\in F_2^n\setminus\{0\}$, $\mathrm{F}(D_b f) = 0$, then $W_f^2(a) = \mathrm{F}(0) = 2^n$ for any $a\in F_2^n$, thus by Theorem 2.1, $f(x)$ is bent. Conversely, if $f(x)$ is bent, then for any $a\in F_2^n$, $\sum_{b\in F_2^n}\mathrm{F}(D_b f)(-1)^{a\cdot b} = 2^n$. According to the theory of discrete Fourier inverse transform, we have $\mathrm{F}(D_b f) = 0$ when $b\ne 0$.

At the last of this part, the theorem below point out the bent functions, after affine transform, is still bent.

Lemma 2.2. Assume $f(x)\in B_n$, $A\in F_2^{n\times n}$ is an invertible matrix, $b\in F_2^n$, $l(x)$ is an affine Boolean function of n variables and $g(x) = f(Ax+b) + l(x)$. In the case of $l(x) = c^T x$, $W_g(a) = (-1)^{b^T y}W_f(y)$; or $l(x) = c^T x + 1$, then $W_g(a) = (-1)^{b^T y+1}W_f(y)$, in which $y = A^{-1T}(a+c)$.

Proof. In the case of $l(x) = c^T x$,

$$
\begin{aligned}
&W_g(a)\\
&=\sum_{x\in F_2^n}(-1)^{f(Ax+b)+c^Tx+a^Tx}\\
&=\sum_{x\in F_2^n}(-1)^{f(x)+(a+c)^T(A^{-1}x+A^{-1}b)}\\
&=\sum_{x\in F_2^n}(-1)^{f(x)+y^T(x+b)}\\
&=(-1)^{b^Ty}\sum_{x\in F_2^n}(-1)^{f(x)+y^Tx}.
\end{aligned}
$$

In the case of $l(x)=c^Tx+1$, the prove is similar.

According to Theorem 2.1, it is easy to get:

Theorem 2.4. Assume $f(x)$ is a bent function of n variables, $A\in F_2^{n\times n}$ is an invertible matrix, $b\in F_2^n$ and $l(x)$ is an affine Boolean function of n variables, then $g(x)=f(Ax+b)+l(x)$ is also bent. Furthermore, the dual function of $g(x)$ is $\tilde{g}(a)=\tilde{f}(y)+b^Ty$ and $\tilde{g}(a)=\tilde{f}(y)+b^Ty+1$ in which $y=A^{-1T}(a+c)$, in the case of $l(x)=c^Tx$ and $l(x)=c^Tx+1$ respectively.

III. Dual Bent Function and Restriction

The properties of bent functions on F_2^n, such as the Walsh spectrum and differentials, are clear right now. Then it is natural to ask: how about its restriction on half of F_2^n ? Since half of F_2^n is isomorphic with F_2^{n-1}, the largest proper even dimension subspace is quarter, which is isomorphic to F_2^{n-2}. Is there a property "almost bent" for n odd? If the restriction of a bent function on quarter of F_2^n is "bent", how about the other three quarter? Furthermore, is there any relationship between restriction and second differential, which seems not obvious?

This part will give a positive answer to all these questions.

Definition 3.1. Assume $f(x)\in B_n$, if there exists $\lambda\in\mathbb{N}$ such that $W_f(a)\in\{0,\lambda,-\lambda\}$ for every $a\in F_2^n$, then $f(x)$ is called plateaued functions(or three-valued functions), which λ is called the altitude of $f(x)$.

According to Parseval relation, $\lambda=2^m$ with $m\geq n/2$. The equivalence requires n even, this case is the bent function. While n odd, the minimal m can reach is $(n+1)/2$. This kind of $f(x)$ is called semi-bent functions.

According to Lemma 2.2, plateaued and semi-bent property, similar with bent, is also affine invariant.

According to Theorem 2.4, the definition of plateaued, bent and semi-bent functions, are easy to generalized on Boolean function restricted on a subspace (or an affine subspace).

Definition 3.2. Assume $f(x)\in B_n$ and $E\subseteq F_2^n$ a subspace of dimension m. $f\big|_{u+E}$ is called plateaued(resp. bent, semi-bent) if there exists an isomorphism $\sigma:E\to F_2^m$, such that $g(y)=f(u+\sigma^{-1}(y))$ is plateaued(resp. bent, semi-bent) in B_m. At here, "there exists" is in fact equal with "for all".

Theorem 3.1. Assume $f(x,x_{n+1})\in B_{n+1}$. Denote $f_0(x)=f(x,0)$ and $f_1(x)=f(x,1)$, then the Walsh spectrum of $f(x,x_{n+1})$ is:

$$
\begin{cases}
W_f(a,0)=W_{f_0}(a)+W_{f_1}(a)\\
W_f(a,1)=W_{f_0}(a)-W_{f_1}(a)
\end{cases}.
$$

Especially, if both $f_0(x)$ and $f_1(x)$ are bent on F_2^n, then $f(x,x_{n+1})$ is semi-bent on F_2^{n+1}.

Proof.

$$
\begin{aligned}
&W_f(a,a_{n+1})\\
&=\sum_{(x,x_{n+1})\in F_2^{n+1}}(-1)^{f(x,x_{n+1})+a^Tx+a_{n+1}x_{n+1}}\\
&=\sum_{x\in F_2^{n+1}}(-1)^{f(x,0)+a^Tx}+\sum_{x\in F_2^{n+1}}(-1)^{f(x,1)+a^Tx+a_{n+1}}\\
&=W_{f_0}(a)+(-1)^{a_{n+1}}W_{f_1}(a).
\end{aligned}
$$

The second statement is easy to prove.

Corollary 3.1. If $f(x,x_{n+1})$ in Theorem 3.1 is bent, then both $f_0(x)$ and $f_1(x)$ are semi-bent functions on F_2^n. Furthermore, for every $a\in F_2^n$, one of $W_{f_0}(a)$ and $W_{f_1}(a)$ is $\pm 2^{(n+1)/2}$ while the other is 0.

Corollary 3.2. If $f(x,x_{n+1})$ in Theorem 3.1 is semi-bent and one of $f_0(x)$ and $f_1(x)$ is bent, then another is also bent.

Theorem 3.2.([3]) Let n and m be two even positive integers. Let f be a Boolean function on $F_2^{n+m}=F_2^n\times F_2^m$ such that, for any element y of F_2^m, the function $f_y:x\mapsto f(x,y)$ on F_2^n is bent. Then f is bent if and only if, for any element s of F_2^n, the function $\varphi_s:y\mapsto\tilde{f}_y(s)$ is bent on F_2^m. In this case, the dual of f is $\tilde{f}(s,t)=\tilde{\varphi}_s(t)$.

Theorem 3.3. Assume $f(x)\in B_n$ is bent and $E\subseteq F_2^n$ a subspace of dimension $n-2$. The conditions below are equivalent:

(1) There exists $u\in F_2^n$ such that $f\big|_{u+E}$ is bent;

(2) For every $u\in F_2^n$, $f\big|_{u+E}$ is bent;

(3) Let $E^{\perp}=\{0,a,b,a+b\}$, then $D_aD_b\tilde{f}(x)=1$.

Proof. Let σ be an isomorphism on F_2^n which $\sigma(E)=\{x\in F_2^n : x_{n-1}=x_n=0\}$. Obviously $\sigma\big|_E$ is an isomorphism from E to F_2^{n-2}. Consider Boolean function $g(y)=f(\sigma^{-1}(y))$ on F_2^n.

(1) $\Leftrightarrow$ (2): If $u\neq 0$, we can consider $f(x+u)$. So without losing generality, let $u=0$. Since $f_{0,0}=f\big|_E$ is bent, then $g_{0,0}=g(y)\big|_{y_{n-1}=y_n=0}$ is bent on F_2^{n-2}. According to Theorem 2.4, $g(y)$ is bent on F_2^n. According to Corollary 3.1, both $g(y)\big|_{y_{n-1}=0}$ and $g(y)\big|_{y_{n-1}=1}$ are semi-bent on F_2^{n-1}. $g(y)\big|_{y_n=0}$ and $g(y)\big|_{y_n=1}$ are in the same way. According to Corollary 3.2, $g_{0,1}=g(y)\big|_{y_{n-1}=0,y_n=1}$ is bent on F_2^{n-2}. Thus $f_{0,1}=f\big|_{\sigma^{-1}(0,\cdots,0,1)+E}$ is bent and vice versa, since

$$\begin{aligned} g_{0,1} &= g(y_1,\cdots y_{n-2},0,1)\\ &= f(\sigma^{-1}(0,\cdots 0,1)+\sigma^{-1}(y_1,\cdots y_{n-2},0,0)). \end{aligned}$$

$g_{1,0}=g(y)\big|_{y_{n-1}=1,y_n=0}$ and $g_{1,1}=g(y)\big|_{y_{n-1}=y_n=1}$ are in the same way, corresponding $f_{1,0}=f\big|_{\sigma^{-1}(0,\cdots 0,1,0)+E}$ and $f_{1,1}=f\big|_{\sigma^{-1}(0,\cdots 0,1,1)+E}$ respectively. These are all the four $u+E\subseteq F_2^n$.

(2) $\Leftrightarrow$ (3): Consider the matrix of σ, denoted by A. According to Theorem 2.4, $\tilde{g}(x)=\tilde{f}(A^Tx)$. Since $E^{\perp}=A^T(AE)^{\perp}=A^T\{y\in F_2^n : y_1=\cdots=y_{n-2}=0\}$, then $D_aD_b\tilde{f}(x)=\sum_{i,j}\tilde{g}(y_1,\cdots y_{n-2},y_{n-1}+i,y_n+j)$, in which $x=A^T(y_1,\cdots,y_n)^T$. Thus for all $(y_1,\cdots,y_{n-2})\in F_2^{n-2}$, $\tilde{g}(y_1,\cdots,y_{n-2},i,j)$ is bent on F_2^2, since the sum of four value is always 1. According to Theorem 3.2, all the $g_{i,j}$ are bent on F_2^{n-2}. All the deductions above are invertible.

IV. Second Derivative of Maiorana-McFarland Functions

Definition 4.1.([4], [5]) The Maiorana-McFarland functions(in short M-M functions) is defined as $f(x,y)=x\cdot\pi(y)+g(y)$ on $F_2^n=\{(x,y)\,|\,x,y\in F_2^{n/2}\}$ with n even, in which π is a permutation on $F_2^{n/2}$ and g is any Boolean function of variables $n/2$ and $\cdot$ means the inner product between vectors in $F_2^{n/2}$.

Proposition 4.1. M-M function f is bent.

Proof. For any $(a_1,a_2)\in F_2^n$,

$$\begin{aligned} &W_f(a_1,a_2)\\ &=\sum_{x\in F_2^{n/2}}\sum_{y\in F_2^{n/2}}(-1)^{x\cdot\pi(y)+g(y)+a_1\cdot x+a_2\cdot y}\\ &=\sum_{y\in F_2^{n/2}}(-1)^{a_2\cdot y+g(y)}\sum_{x\in F_2^{n/2}}(-1)^{x\cdot(a_1+\pi(y))}\\ &=2^{n/2}(-1)^{a_2\cdot\pi^{-1}(a_1)+g(\pi^{-1}(a_1))}=\pm 2^{n/2} \end{aligned}$$

thus f is bent.

Corollary 4.1. The dual bent function of function $f(x,y)=x\cdot\pi(y)+g(y)$ is:

$$\tilde{f}(a_1,a_2)=a_2\cdot\pi^{-1}(a_1)+g(\pi^{-1}(a_1)).$$

By Theorem 2.2, the derivatives $D_bf(x,y)$ on all $b\in F_2^n\setminus\{0\}$ are balanced, however, the construction itself implies the weakness when difference again for some b.

Theorem 4.1. Suppose $a,b\in F_2^{n/2}\times\{0\}\subseteq F_2^n$, then $D_aD_bf(x,y)=0$.

Proof. Denote $a=(a_1,0)$ and $b=(b_1,0)$, in which $a_1,b_1\in F_2^{n/2}$, then

$$\begin{aligned} &D_aD_bf(x,y)\\ &=D_a(b_1\cdot\pi(y))\\ &=0. \end{aligned}$$

V. Second Derivative of Bent Functions Algebraic Degree Less Than Three

In general, second-order differential cryptanalysis is effective only for functions degree less than 2(i.e. constant, linear, and quadratic functions). However, for bent functions, which are best under (first-order) differential cryptanalysis, the degree it can effectively attack can be enlarged to less than 3.

Lemma 5.1. If the degree of $f(x)\in B_n$ is less than k+1, then for all $b\in F_2^n\setminus\{0\}$, the degree of $D_bf(x)$ is less than k.

Theorem 5.1. If the degree of bent function $f(x)\in B_n$ is less than 3, then for any $b\in F_2^n\setminus\{0\}$, there exists $a\in F_2^n\setminus\{0,b\}$ such that $D_aD_bf(x)=1$.

Proof. Since $f(x)$ is bent, then by Theorem 2.3, $\mathrm{F}(D_bf)=0$. By Lemma 2.1,

$\sum_{a\in F_2^n} \mathrm{F}(D_aD_bf) = \mathrm{F}^2(D_bf) = 0$. By Lemma 5.1, D_aD_bf for all $a \in F_2^n$ are affine functions. Thus, $\mathrm{F}(D_aD_bf)$ can only be three values: 2^n when $D_aD_bf = 0$, -2^n when $D_aD_bf = 1$, and 0 else. $\mathrm{F}(D_0D_bf) = \mathrm{F}(0) = 2^n$, so for satisfying the equality of $\sum_{a\in F_2^n} \mathrm{F}(D_aD_bf) = 0$, there exists $a \in F_2^n$, such that $\mathrm{F}(D_aD_bf) = -2^n$, which means $D_aD_bf = 1$. Obviously, $a \notin \{0, b\}$.

On the other hand, this weakness in second differential can be used on constructing new bent functions. According to, $D_aD_bf(x) = 1$ implies all the four $\tilde{f}\big|_{u+E}$ is bent in which $u \in F_2^n$ and $E = \{a, b\}^{\perp}$. Hence we have:

Theorem 5.2. If the degree of bent function $f(x) \in B_n$ is less than 3, then the dual function $\tilde{f}(x)$ can be split into four bent $\tilde{f}\big|_{u+E}$ on four pieces of $u + E$ in F_2^n, in which $E \subseteq F_2^n$ is a subspace of dimension $n-2$. Furthermore, the choice of E is at least $(2^n - 1)/3$.

Proof. Consider the bijection between E and $E^{\perp} \setminus \{0\} \subseteq F_2^n$, since every $E^{\perp} \setminus \{0\}$ has exactly three elements and every $b \in F_2^n \setminus \{0\}$ is belong to at least one of $E^{\perp} \setminus \{0\}$, then the proof is trivial.

VI. Conclusion

From our result, when constructing bent functions, we should use some other methods and avoid these functions. Some other known primary constructions of bent functions are:

partial spreads class([5],[6]);

trace of power functions on F_2^n ([5],[7],[8]);

γ_F of almost bent functions([9]);

restrictions of functions on a hyperplane([10]).

Acknowledgment

This work was partly supported by Chinese National Natural Science Foundation project 11271040.

References

[1] O. S. Rothaus， "On "Bent" funcions," Journal of Combinatorial Theory, Series A , vol. 20(3), May. 1976, pp. 300-305, doi:10.1016/0097-3165(76)90024-8.

[2] L. R. Knudsen, "Truncated and Higher Order Differentials," Fast Software Encryption: Second International Workshop. Leuven, Belgium, LNCS 1008, Springer Press, Dec.1994, pp. 196-211, doi:10.1007/3-540-60590-8_16.

[3] Y. Crama, P. L. Hammer, "Boolean Models and Methods in Mathematics, Computer Science, and Engineering," Cambridge University Press, London, 2010.

[4] R. L. McFarland, "A family of difference sets in non-cyclic groups," Journal of Combinatorial Theory, Series A, vol. 15(1), July 1973, pp. 1-10, doi:10.1016/0097-3165(73)90031-9

[5] J. F. Dillon, "Elementary Hadamard difference sets," Ph. D. Thesis, University of Maryland, 1974.

[6] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," Fast Software Encryption: Second International Workshop. Leuven, Belgium, LNCS 1008, Springer Press, Dec.1994, pp. 61-74, doi: 10.1007/3-540-60590-8_5.

[7] J. F. Dillon, H. Dobbertin, "New cyclic diffenence sets with singer parameters," Finite Fields and Their Applications, vol. 10(3), July 2004, pp: 342-389, doi:10.1016/j.ffa.2003.09.003.

[8] P. Langevin, G. Leander, "Monomial Bent functions and stickelberger's theorem," Finite Fields and Their Applications, vol. 14(3), July 2008, pp. 727-742, doi:10.1016/j.ffa.2007.12.001.

[9] C. Carlet, P. Charpin, V. Zinoviev, "Codes, Bent functions and permutations suitable for DES-like cryptosystems," Designs, Codes and Cryptography, vol. 15(2), Nov. 1998, pp. 125-156, doi: 10.1023/A:1008344232130.

[10] J. F. Dillon, G. McGuire, "Near bent functions on a hyperplane," Finite Fields and Their Applications, vol. 14(3), July 2008, pp. 715-720, doi:10.1016/j.ffa.2007.11.001.