**Far East Journal of Applied Mathematics**
Volume 40, Number 1, 2010, Pages 33-42
Published Online: April 22, 2010
This paper is available online at http://www.pphmj.com


# ON PERFECT NONLINEAR FUNCTIONS

**BIN WEN and CHUNYAN JI**

Department of Mathematics
Changshu Institute of Technology
Suzhou 215006, P. R. China
e-mail: wenbin9903@yahoo.com.cn

**Abstract**

Functions with high nonlinearity, e.g., perfect nonlinear functions and bent functions, have been an instrumental tool not only in algebra and finite geometries but also in combinatorics, coding theory and cryptography as well. In this paper, we study perfect nonlinear functions, especially properties of the derivative of the components of the perfect nonlinear functions. As a result, some sufficient and necessary conditions have been presented to judge when a function is a perfect nonlinear function, and hope these conditions are useful in constructing new perfect nonlinear functions.

## 1. Introduction

Let $p$ be an odd prime number and $q = p^m$. A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is called *perfect nonlinear* or *planar* if for each $a \in \mathbb{F}_q^*$, the *derivative function* $D_a f = f(x + a) - f(x)$ is a permutation on $\mathbb{F}_q$. Much attention has been paid to these functions recently as they are widely used in communication theory and cryptography. For a survey on perfect nonlinear functions (and, more generally, highly nonlinear functions), we refer to [2, 6].

2010 Mathematics Subject Classification: 94C10.

Keywords and phrases: perfect nonlinear function, derivative function, Walsh transform.

Received December 24, 2009

Up to now, all known perfect nonlinear functions from $\mathbb{F}_q$ to $\mathbb{F}_q$ were affine equivalents to one of the following functions (strictly speaking, this list is not complete, since every semifield of odd order gives a perfect nonlinear function):

(1) $f_1 = x^2$ (folklore);

(2) $f_2 = x^{p^d+1}$, where $d \geq 0$ and $2 \nmid \frac{m}{(m,d)}$ (Dembowski and Ostrom [4]);

(3) $f_3 = x^{10} \pm x^6 - x^2$, where $p = 3$ and $2 \nmid m$ (Coulter and Matthews [3] and Ding and Yuan [5]);

(4) $f_4 = x^{\frac{3^k+1}{2}}$, where $p = 3$, $2 \nmid k$ and $(m, k) = 1$ (Coulter and Matthews [3]);

(5) $f_5 = x^{p^s+1} - u^{p^k-1}x^{p^k+p^{2k}+s}$ in $\mathbb{F}_{p^{3k}}$, where $\gcd(k, 3) = 1$, $k - s \equiv 0 \pmod 3$, $s \neq k$ and $k/(k, s)$ is odd, and $u$ is a generator of $\mathbb{F}_{p^{3k}}^*$ (Zha et al. [7]).

From the above list, we see that only a few classes of perfect nonlinear functions are known. So, it is necessary to construct new PN functions. On the other hand, only a few properties of perfect nonlinear functions are known. Therefore, we explore more properties of perfect nonlinear functions, especially the properties of the derivative of the components of the perfect nonlinear functions. These properties constitute sufficient and necessary conditions for judging when a function is perfect nonlinear. Although we have not been able to construct new perfect nonlinear functions, we try to give some sufficient and necessary conditions to judge when a function is perfect nonlinear, and hope these conditions are useful in constructing new perfect nonlinear functions.

## 2. Characterizations of Perfect Nonlinear Functions

To begin with, we state some preparatory knowledge that will be used in this section.

Let $q = p^m$ be a power of an odd prime $p$, where $m$ is an arbitrary positive integer. Write Tr for the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$ defined by

$$\mathrm{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{m-1}}.$$

Let $f$ be a function on $\mathbb{F}_q$. The linear combinations of the coordinates of $f$ are the functions $f_\lambda(x) = \mathrm{Tr}(\lambda(x))$, $\lambda \in \mathbb{F}_q$, where $f_0 = 0$. The functions $f_\lambda(x)$ are called the *components of f*. Let $\varphi_a(x) = \mathrm{Tr}(ax)$ be a linear function over $\mathbb{F}_q$.

Now we define a transform on functions from $\mathbb{F}_q$ into $\mathbb{F}_p$ which will be used for the component functions of those defined from $\mathbb{F}_q$ into itself. Let $g$ be a function from $\mathbb{F}_q$ into $\mathbb{F}_p$. The *Walsh transform* of $g$ (see [1]) is defined by

$$W(g) = \sum_{x \in \mathbb{F}_q} \varepsilon_p^{g(x)}, \quad \varepsilon_p = e^{2\pi i/p}.$$

With the preparations above, we are now ready to present a full characterization of perfect nonlinear functions by means of the derivatives and the sum of square indicators of their functions.

**Theorem 2.1.** *Let* $f : \mathbb{F}_q \to \mathbb{F}_q$ *be a function and* $f_\lambda(x) = \mathrm{Tr}(\lambda f(x))$ *be components of* $f(x)$ *for* $\lambda \in \mathbb{F}_q$. *Then for any* $a \in \mathbb{F}_q^*$, *we have*

$$\sum_{\lambda \in \mathbb{F}_q} |W(D_a f_\lambda)|^2 \geq q^2.$$

*Moreover, f is a perfect nonlinear function if and only if*

$$\sum_{\lambda \in \mathbb{F}_q} |W(D_a f_\lambda)|^2 = q^2.$$

**Proof.**

$$\sum_{\lambda \in \mathbb{F}_q} |W(D_a f_\lambda)|^2$$

$$= \sum_{\lambda \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \varepsilon_p^{\mathrm{Tr}[\lambda(f(x+a)-f(x))]-\mathrm{Tr}[\lambda(f(y+a)-f(y))]}$$

$$= \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \sum_{\lambda \in \mathbb{F}_q} \varepsilon_p^{\mathrm{Tr}[\lambda(f(x+a)-f(x))]-\mathrm{Tr}[\lambda(f(y+a)-f(y))]}$$

$$= q|\{(x, y) | f(x+a) - f(x) = f(y+a) - f(y)\}|$$

$$= q^2 + q\left|\{(x, y)|\, f(x+a) - f(x) = f(y+a) - f(y),\ x \neq y\}\right|$$

$$\geq q^2.$$

If $f$ is a perfect nonlinear function, then

$$\left|\{(x, y)|\, f(x+a) - f(x) = f(y+a) - f(y),\ x \neq y\}\right| = 0.$$

Hence

$$\sum_{\lambda \in \mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2 = q^2.$$

Conversely, if

$$\sum_{\lambda \in \mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2 = q^2,$$

then

$$\left|\{(x, y)|\, f(x+a) - f(x) = f(y+a) - f(y),\ x \neq y\}\right| = 0.$$

Hence, $D_a f$ is a permutation on $\mathbb{F}_q$ and $f$ is a perfect nonlinear function on $\mathbb{F}_q$. □

**Theorem 2.2.** *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function and*

$$V(f_\lambda) = \sum_{a \in \mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2$$

*be a square sum indicator of the components $f_\lambda$ of $f$. Then we have*

$$\sum_{\lambda \in \mathbb{F}_q^*} V(f_\lambda) \geq q^2(q-1).$$

*Moreover, $f$ is a perfect nonlinear function if and only if*

$$\sum_{\lambda \in \mathbb{F}_q^*} V(f_\lambda) = q^2(q-1).$$

**Proof.**

$$\sum_{\lambda \in \mathbb{F}_q^*} V(f_\lambda) = \sum_{\lambda \in \mathbb{F}_q^*} \sum_{a \in \mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2$$

$$= \sum_{\lambda \in \mathbb{F}_q} \sum_{a \in \mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2 - \sum_{a \in \mathbb{F}_q} |\, W(D_a f_0)\,|^2$$

$$= \sum_{a\in\mathbb{F}_q^*}\sum_{\lambda\in\mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2 - \sum_{a\in\mathbb{F}_q} |\, W(D_a f_0)\,|^2 + \sum_{\lambda\in\mathbb{F}_q} |\, W(D_0 f_\lambda)\,|^2$$

$$\geq q^2(q-1).$$

If $f$ is a perfect nonlinear function, then

$$\sum_{\lambda\in\mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2 = q^2.$$

Hence

$$\sum_{\lambda\in\mathbb{F}_q^*} V(f_\lambda) \geq q^2(q-1).$$

Conversely, suppose that

$$\sum_{\lambda\in\mathbb{F}_q^*} V(f_\lambda) \geq q^2(q-1).$$

By Theorem 2.1, for any $a \in \mathbb{F}_q^*$, we have

$$\sum_{\lambda\in\mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2 \geq q^2. \tag{1}$$

Also,

$$\sum_{\lambda\in\mathbb{F}_q^*} V(f_\lambda) = \sum_{\lambda\in\mathbb{F}_q^*}\sum_{a\in\mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2$$

$$= \sum_{a\in\mathbb{F}_q^*}\sum_{\lambda\in\mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2.$$

Hence

$$\sum_{a\in\mathbb{F}_q^*}\sum_{\lambda\in\mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2 = q^2(q-1).$$

By inequality (1), we have

$$\sum_{\lambda\in\mathbb{F}_q} |\, W(D_a f_\lambda)\,|^2 = q^2.$$

Therefore, $f$ is a perfect nonlinear function. □

For perfect nonlinear power functions, we have the following holds.

**Lemma 2.3.** *Let* $f = x^d$ *be a power function on* $\mathbb{F}_q$. *If f is a perfect nonlinear function, then* $\gcd(d, q-1) = 2$.

**Proof.** We consider the number of the solutions of the equation

$$(x+a)^d - x^d = b, \quad a \in \mathbb{F}_q^*, \quad b \in \mathbb{F}_q.$$

Let $a = 1$ and $b = 0$. Then

$$(x+1)^d - x^d = 0,$$

which is equivalent to $x^d = 1, \quad x \neq 1$.

Let $\alpha$ be a generator of $\mathbb{F}_q^*$ and $x = \alpha^t, \quad t \in \mathbb{Z}_{q-1}$. Then

$$|\{x \in \mathbb{F}_q \,|\, x^d = 1, \ x \neq 1\}| = |\{t \in \mathbb{Z}_{q-1}^* \,|\, dt \equiv 0 (\mathrm{mod}\, q-1)\}|.$$

The number of the solutions of $dt \equiv 0 (\mathrm{mod}\, q-1)$ in $\mathbb{Z}_{q-1}^*$ is $\gcd(d, q-1) - 1$. If $f$ is a perfect nonlinear function, then

$$|\{x \in \mathbb{F}_q \,|\, x^d = 1, \ x \neq 1\}| = \gcd(d, q-1) - 1 = 1.$$

We have $\gcd(d, q-1) = 2$. □

**Theorem 2.4.** *Let* $f = x^d$ *be a power function on* $\mathbb{F}_q$ *and* $\alpha$ *be a generator of* $\mathbb{F}_q^*$. *Then* $W(D_a f_\lambda) = W(D_a f_{\lambda\alpha^d})$ *for any* $a, \lambda \in \mathbb{F}_q^*$. *Moreover, we have*

$$V(f_\lambda) = q^2 + s\sum_{i=1}^{u-1} |W(D_1 f_{\lambda\alpha^{id}})|^2$$

*and*

$$\sum_{\lambda \in \mathbb{F}_q} |W(D_a f_\lambda)|^2 = \frac{1}{s}\sum_{j=0}^{s-1} V(f_{\alpha^j}),$$

*where* $s = \gcd(d, q-1), \ u = (q-1)/s$.

**Proof.**

$$W(D_a f_\lambda) = \sum_{x\in\mathbb{F}_q} \varepsilon_p^{\mathrm{Tr}[\lambda(f(x+a)-f(x))]}$$

$$= \sum_{x\in\mathbb{F}_q} \varepsilon_p^{\mathrm{Tr}[\lambda((x+a)^d - x^d)]}$$

$$= \sum_{x\in\mathbb{F}_q} \varepsilon_p^{\mathrm{Tr}\left[\lambda\alpha^d\left(\left(\frac{x}{a}+1\right)^d - \left(\frac{x}{a}\right)^d\right)\right]}$$

$$= \sum_{x\in\mathbb{F}_q} \varepsilon_p^{\mathrm{Tr}[\lambda\alpha^d((x+1)^d - x^d)]}$$

$$= W(D_1 f_{\lambda\alpha^d}).$$

$$V(f_\lambda) = \sum_{a\in\mathbb{F}_q} |W(D_a f_\lambda)|^2$$

$$= q^2 + \sum_{a\in\mathbb{F}_q^*} |W(D_a f_\lambda)|^2$$

$$= q^2 + \sum_{a\in\mathbb{F}_q^*} |W(D_1 f_{\lambda\alpha^d})|^2$$

$$= q^2 + \sum_{i=0}^{q-2} |W(D_1 f_{\lambda\alpha^d})|^2$$

$$= q^2 + \sum_{i=0}^{u-1} |W(D_1 f_{\lambda\alpha^{id}})|^2 + \sum_{i=u}^{2u-1} |W(D_1 f_{\lambda\alpha^{id}})|^2 + \sum_{i=2u}^{3u-1} |W(D_1 f_{\lambda\alpha^{id}})|^2$$

$$+ \cdots + \sum_{i=(s-1)u}^{su-1} |W(D_1 f_{\lambda\alpha^{id}})|^2$$

$$= q^2 + \sum_{i=0}^{u-1} |W(D_1 f_{\lambda\alpha^{id}})|^2 + \sum_{i=0}^{u-1} |W(D_1 f_{\lambda\alpha^{(i+u)d}})|^2$$

$$+\cdots+\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{(i+(s-1)u)d}})|^2$$

$$=q^2+\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{id}})|^2+\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{id}})|^2$$

$$+\cdots+\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{id}})|^2$$

$$=q^2+s\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{id}})|^2. \tag{2}$$

Let $d=ks$. Since $q-1=us$ and $s=\gcd(q-1, d)=\gcd(us, ks)$, we have $\gcd(u, k)=1$. Therefore, equation (2) becomes

$$V(f_\lambda)=q^2+s\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{iks}})|^2=q^2+\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{is}})|^2.$$

Hence

$$V(f_\lambda)=q^2+s\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{is}})|^2,$$

and

$$V(f_\lambda)-q^2=s\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{is}})|^2.$$

Let $\lambda=\alpha^j$, $0\le j\le s-1$. Then

$$V(f_{\alpha^j})-q^2=s\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{j+is}})|^2.$$

And

$$\sum_{j=0}^{s-1}(V(f_{\alpha^j})-q^2)=s\sum_{j=0}^{s-1}\sum_{i=0}^{u-1}|W(D_1 f_{\lambda\alpha^{j+is}})|^2.$$

Moreover, let $a = \alpha^l$. Then

$$\sum_{x\in\mathbb{F}_q^*} |W(D_a f_\lambda)|^2 = \sum_{x\in\mathbb{F}_q^*} |W(D_1 f_{\lambda\alpha^d})|^2$$

$$= \sum_{i=0}^{s-1}\sum_{j=0}^{u-1} |W(D_1 f_{\alpha^{j+is}\alpha^{lks}})|^2$$

$$= \sum_{i=0}^{s-1}\sum_{j=0}^{u-1} |W(D_1 f_{\alpha^{i+(j+lk)s}})|^2$$

$$= \sum_{i=0}^{s-1}\sum_{j=0}^{u-1} |W(D_1 f_{\alpha^{i+js}})|^2.$$

Therefore

$$\sum_{j=0}^{s-1}(V(f_{\alpha^j}) - q^2) = s\sum_{\lambda\in\mathbb{F}_q^*} |W(D_a f_\lambda)|^2.$$

Namely

$$\sum_{\lambda\in\mathbb{F}_q} |W(D_a f_\lambda)|^2 = \frac{1}{s}\sum_{j=0}^{s-1} V(f_{\alpha^j}).$$ □

**Corollary 2.5.** *Let* $f = x^d$ *be a perfect nonlinear function on* $\mathbb{F}_q$ *and* $\alpha$ *be a generator of* $\mathbb{F}_q^*$. *Then*

$$V(f_1) + V(f_\alpha) = 2q^2.$$

**Proof.** Since $f$ is a perfect nonlinear function, we have $\gcd(d, q-1) = 2$ by Lemma 2.3. Hence, by Theorem 2.4, we have

$$2\sum_{\lambda\in\mathbb{F}_q} |W(D_a f_\lambda)|^2 = \sum_{j=0}^{1} V(f_{\alpha^j}) = V(f_1) + V(f_0).$$

Also, by Theorem 2.1, $f$ is a perfect nonlinear function if and only if

$$\sum_{\lambda \in \mathbb{F}_q} | W(D_a f_\lambda) |^2 = q^2.$$

Hence, we have

$$V(f_1) + V(f_\alpha) = 2q^2.$$

## References


[1] T. P. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, On almost perfect nonlinear functions over $\mathbb{F}_2^n$, IEEE Tans. Inform. Theory 52 (2006), 4160-4170.

[2] C. Carlet and C. Ding, Highly nonlinear mappings, J. Complexity 20 (2004), 205-244.

[3] R. S. Coulter and R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II, Des. Codes Cryptogr. 10 (1997), 167-184.

[4] P. Dembowski and T. G. Ostrom, Planes of order *n* with colineation groups of order *n*, Math. Z. 103 (1968), 239-258.

[5] C. Ding and J. Yuan, A family of skew Hadamard difference sets, J. Combin. Theory Ser. A 113 (2006), 1526-1535.

[6] K. Nyberg, Differentially uniform mapping for cryptography, Advances in Cryptology EURO-CRYPT'93, Lecture Notes in Computer Science, 765, T. Helleseth, ed., Springer-Verlag, New York, 1994, pp. 55-64.

[7] Z. Zha, G. Kyureghyan and X. Wang, Perfect nonlinear binomials and their semifields, Finite Fields Appl. 15 (2009), 125-133.