Relationships between Bent Functions and Complementary Plateaued Functions

Yuliang Zheng[1] and Xian-Mo Zhang[2]

[1] School of Comp & Info Tech, Monash University, McMahons Road, Frankston, Melbourne, VIC 3199, Australia. E-mail: yuliang@pscit.monash.edu.au
URL: http://www.pscit.monash.edu.au/links/

[2] School of Info Tech & Comp Sci, the University of Wollongong, Wollongong NSW 2522, Australia. E-mail: xianmo@cs.uow.edu.au

Abstract. We introduce the concept of complementary plateaued functions and examine relationships between these newly defined functions and bent functions. Results obtained in this paper contribute to the further understanding of profound secrets of bent functions. Cryptographic applications of these results are demonstrated by constructing highly nonlinear correlation immune functions that possess no non-zero linear structures.

Key Words:

Plateaued Functions, Complementary Plateaued Functions, Bent Functions, Cryptography

1 Introduction

Bent functions achieve the maximum nonlinearity and satisfy the propagation criterion with respect to every non-zero vector. These functions, however, are neither balanced nor correlation immune. Furthermore they exist only when the number of variables is even. All these properties impede the direct applications of bent functions in cryptography. They also indicate the importance of further understanding the characteristics of bent functions in the construction of Boolean functions with cryptographically desirable properties. This extends significantly a recent paper by Zheng and Zhang [12] where a new class of functions called plateaued functions were introduced. In particular, (i) we introduce the concept of complementary plateaued functions; (ii) we establish relationships between bent and complementary plateaued functions; (iii) we show that complementary plateaued functions provide a new avenue to construct bent functions; (iv) we prove a new characteristic property of non-quadratic bent functions by the use of complementary plateaued functions; (v) As an application, we construct balanced, highly nonlinear correlation immune functions that have no non-zero linear structures.

2 Boolean Functions

Definition 1. *We consider functions from V_n to $GF(2)$ (or simply functions on V_n), V_n is the vector space of n tuples of elements from $GF(2)$. Usually we write a function f on V_n as $f(x)$, where $x = (x_1, \dots, x_n)$ is the variable vector in V_n. The* truth table *of a function f on V_n is a $(0,1)$-sequence defined by $(f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{2^n-1}))$, and the* sequence *of f is a $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \dots, (-1)^{f(\alpha_{2^n-1})})$, where $\alpha_0 = (0, \dots, 0, 0)$, $\alpha_1 = (0, \dots, 0, 1)$, ..., $\alpha_{2^{n-1}-1} = (1, \dots, 1, 1)$. The* matrix *of f is a $(1,-1)$-matrix of order 2^n defined by $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$ where $\oplus$ denotes the addition in $GF(2)$. f is said to be* balanced *if its truth table contains an equal number of ones and zeros.*

Given two sequences $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$, their *component-wise product* is defined by $\tilde{a} * \tilde{b} = (a_1 b_1, \cdots, a_m b_m)$. In particular, if $m = 2^n$ and $\tilde{a}$, $\tilde{b}$ are the sequences of functions f and g on V_n respectively, then $\tilde{a} * \tilde{b}$ is the sequence of $f \oplus g$ where $\oplus$ denotes the addition in $GF(2)$.

Let $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$ be two sequences or vectors, the *scalar product* of $\tilde{a}$ and $\tilde{b}$, denoted by $\langle \tilde{a}, \tilde{b} \rangle$, is defined as the sum of the component-wise multiplications. In particular, when $\tilde{a}$ and $\tilde{b}$ are from V_m, $\langle \tilde{a}, \tilde{b} \rangle = a_1 b_1 \oplus \cdots \oplus a_m b_m$, where the addition and multiplication are over $GF(2)$, and when $\tilde{a}$ and $\tilde{b}$ are $(1,-1)$-sequences, $\langle \tilde{a}, \tilde{b} \rangle = \sum_{i=1}^{m} a_i b_i$, where the addition and multiplication are over the reals.

An *affine* function f on V_n is a function that takes the form of $f(x_1, \dots, x_n) = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \dots, n$. Furthermore f is called a *linear* function if $c = 0$.

A $(1,-1)$-matrix A of order m is called a *Hadamard* matrix if $AA^T = mI_m$, where A^T is the transpose of A and I_m is the identity matrix of order m. A Sylvester-Hadamard matrix of order 2^n, denoted by H_n, is generated by the following recursive relation

$$H_0 = 1, \ H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}, \ n = 1, 2, \dots.$$

Let ℓ_i, $0 \le i \le 2^n - 1$, be the i row of H_n. It is known that ℓ_i is the sequence of a linear function $\varphi_i(x)$ defined by the scalar product $\varphi_i(x) = \langle \alpha_i, x \rangle$, where α_i is the ith vector in V_n according to the ascending alphabetical order.

The *Hamming weight* of a $(0,1)$-sequence ξ, denoted by $HW(\xi)$, is the number of ones in the sequence. Given two functions f and g on V_n, the *Hamming distance* $d(f,g)$ between them is defined as the Hamming weight of the truth table of $f(x) \oplus g(x)$.

The equality in the following lemma is called Parseval's equation (Page 416 [4]).

Lemma 1. *Let f be a function on V_n and ξ denote the sequence of f. Then*

$$\sum_{i=0}^{2^n-1} \langle \xi, \ell_i \rangle^2 = 2^{2n}$$

where ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$.

Definition 2. *The* nonlinearity *of a function f on V_n, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e., $N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \varphi_i)$ where φ_1, φ_2, ..., $\varphi_{2^{n+1}}$ are all the affine functions on V_n.*

The following characterizations of nonlinearity will be useful (for a proof see for instance [5]).

Lemma 2. *The nonlinearity of f on V_n can be expressed by*

$$N_f = 2^{n-1} - \frac{1}{2}\max\{|\langle \xi, \ell_i \rangle|, 0 \leq i \leq 2^n - 1\}$$

where ξ is the sequence of f and ℓ_0, ..., ℓ_{2^n-1} are the rows of H_n, namely, the sequences of linear functions on V_n.

The nonlinearity of functions on V_n is upper bounded by $2^{n-1} - 2^{\frac{1}{2}n-1}$.

Definition 3. *Let f be a function on V_n. For a vector $\alpha \in V_n$, denote by $\xi(\alpha)$ the sequence of $f(x \oplus \alpha)$. Thus $\xi(0)$ is the sequence of f itself and $\xi(0) * \xi(\alpha)$ is the sequence of $f(x) \oplus f(x \oplus \alpha)$. Set*

$$\Delta_f(\alpha) = \langle \xi(0), \xi(\alpha) \rangle,$$

the scalar product of $\xi(0)$ and $\xi(\alpha)$. $\Delta_f(\alpha)$ is also called the auto-correlation *of f with a shift α.*

We can simply write $\Delta_f(\alpha)$ as $\Delta(\alpha)$ if no confusion takes place.

Definition 4. *Let f be a function on V_n. We say that f satisfies the* propagation criterion with respect to α *if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function, where $x = (x_1, \ldots, x_n)$ and α is a vector in V_n. Furthermore f is said to satisfy the* propagation criterion of degree k *if it satisfies the propagation criterion with respect to every non-zero vector α whose Hamming weight is not larger than k (see [6]).*

The *strict avalanche criterion (SAC)* [9] is the same as the propagation criterion of degree one.

Obviously, $\Delta(\alpha) = 0$ if and only if $f(x) \oplus f(x \oplus \alpha)$ is balanced, i.e., f satisfies the propagation criterion with respect to α.

Definition 5. *Let f be a function on V_n. α in V_n is called a* linear structure *of f if $|\Delta(\alpha)| = 2^n$ (i.e., $f(x) \oplus f(x \oplus \alpha)$ is a constant).*

For any function f, $\Delta(\alpha_0) = 2^n$, where α_0 is the zero vector on V_n. It is easy to verify that the set of all linear structures of a function f form a linear subspace of V_n, whose dimension is called the *linearity of f*. It is also well-known that if f has non-zero linear structure, then there exists a nonsingular $n \times n$ matrix B

over $GF(2)$ such that $f(xB) = g(y) \oplus h(z)$, where $x = (y, z)$, $y \in V_p$, $z \in V_q$, g is a function on V_p and g has no non-zero linear structure, and h is a linear function on V_q. Hence q is equal to the linearity of f.

The following lemma is the re-statement of a relation proved in Section 2 of [2].

Lemma 3. *Let f be a function on V_n and ξ denote the sequence of f. Then*

$$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))H_n = (\langle\xi, \ell_0\rangle^2, \langle\xi, \ell_1\rangle^2, \ldots, \langle\xi, \ell_{2^n-1}\rangle^2)$$

where α_j is the binary representation of an integer j, $j = 0, 1, \ldots, 2^n - 1$ and ℓ_i is the ith row of H_n.

There exist a number of equivalent definitions of correlation immune functions [1, 3]. It is easy to verify that the following definition is equivalent to Definition 2.1 of [1]:

Definition 6. *Let f be a function on V_n and let ξ be its sequence. Then f is called a* kth-order correlation immune function *if and only if $\langle\xi, \ell\rangle = 0$ for every ℓ, the sequence of a linear function $\varphi(x) = \langle\alpha, x\rangle$ on V_n constrained by $1 \le HW(\alpha) \le k$.*

For convenience sake in this paper we give the following statement.

Lemma 4. *Let f be a function on V_n and let ξ be its sequence. Then $\langle\xi, \ell_i\rangle = 0$, where ℓ_i is the ith row of H_n, if and only if $f(x) \oplus \langle\alpha_i, x\rangle$ is balanced, where α_i is the binary representation of integer i, $i = 0, 1, \ldots, 2^n - 1$.*

In fact, ℓ_i is the sequence of linear function $\varphi(x) = \langle\alpha_i, x\rangle$. This proves Lemma 4. Due to Lemma 4 and Definition 6, we conclude

Lemma 5. *Let f be a function on V_n and let ξ be its sequence. Then f is a* kth-order correlation immune function *if and only if $f(x) \oplus \langle\alpha, x\rangle$ where α is any vector in V_n, constrained by $1 \le HW(\alpha) \le k$.*

Definition 7. *A function f on V_n is called a* bent function *[7] if $\langle\xi, \ell_i\rangle^2 = 2^n$ for every $i = 0, 1, \ldots, 2^n - 1$, where ℓ_i is the ith row of H_n.*

A bent function on V_n exists only when n is even, and it achieves the maximum nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$. From [7] we have the following:

Theorem 1. *Let f be a function on V_n. The following statements are equivalent: (i) f is bent, (ii) the nonlinearity of f, N_f, satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$, (iii) $\Delta(\alpha) = 0$ for any non-zero α in V_n, (iv) the matrix of f is an Hadamard matrix.*

Bent functions have following properties [7]:

Proposition 1. *Let f be a bent function on V_n and ξ denote the sequence of f. Then (i) the degree of f is at most $\frac{1}{2}n$, (ii) for any nonsingular $n \times n$ matrix B over $GF(2)$ and any vector $\beta \in V_p$, $g(x) = f(xB \oplus \beta)$ is a bent function, (iii) for any affine function ψ on V_n, $f \oplus \psi$ is a bent function, (iv) $2^{-\frac{1}{2}n}\xi H_n$ is the sequence of a bent function.*

The following is from [10] (called Theorem 18 in that paper).

Lemma 6. *Let f be a function on V_n ($n \geq 2$), ξ be the sequence of f, and p is an integer, $2 \leq p \leq n$. If $\langle \xi, \ell_j \rangle \equiv 0 \pmod{2^{n-p+2}}$, where ℓ_j is the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$, then the degree of f is at most $p - 1$.*

3 Plateaued Functions

3.1 rth-order Plateaued Functions

The concept of plateaued functions was first introduced in [12]. In addition to the concept, the same paper also studies the existence, properties and construction methods of plateaued functions.

Notation 1. *Let f be a function on V_n and ξ denote the sequence of f. Set $\Im_f = \{i | \langle \xi, \ell_i \rangle \neq 0, \ 0 \leq i \leq 2^n - 1\}$ where ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$.*

We will simply write $\Im_f$ as $\Im$ when no confusion arises.

Definition 8. *Let f be a function on V_n and ξ denote the sequence of f. If there exists an even number r, $0 \leq r \leq n$, such that $\#\Im = 2^r$ and each $\langle \xi, \ell_j \rangle^2$ takes the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$, then f is called a* rth-order plateaued function *on V_n. f is also called a* plateaued function *on V_n if we ignore the particular order r.*

Due to Parseval's equation, the condition $\#\Im = 2^r$ can be obtained from the condition "each $\langle \xi, \ell_j \rangle^2$ takes the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$". For convenience sake, however, both conditions are mentioned in Definition 8.

The following can be immediately obtained from Definition 8.

Proposition 2. *Let f be a function on V_n. We conclude (i) if f is a rth-order plateaued function then r must be even, (ii) f is an nth-order plateaued function if and only if f is bent, (iii) f is a 0th-order plateaued function if and only if f is affine.*

The next result is a consequence of Theorem 3 of [8].

Proposition 3. *A partially-bent function is a plateaued function.*

However, it is important to note that the converse of Proposition 3 has been shown to be false [12].

3.2 $(n-1)$th-order Plateaued Functions on V_n

Following the general results on rth-order plateaued functions on V_n [12], in this paper we examine in greater depth the properties and construction methods of $(n-1)$th-order plateaued functions on V_n. These properties will be useful in research into bent functions.

Proposition 4. *Let p be a positive odd number and g be a $(p-1)$th-order plateaued function on V_p. Then*

(i) the nonlinearity of g, N_g, satisfies $N_g = 2^{p-1} - 2^{\frac{1}{2}(p-1)}$,
(ii) the degree of g is at most $\frac{1}{2}(p+1)$,
(iii) g has at most one non-zero linear structure,
(iv) for any nonsingular $p \times p$ matrix B over $GF(2)$ and any vector $\beta \in V_p$, $h(y) = g(yB \oplus \beta)$ is also a $(p-1)$th-order plateaued function, where $y \in V_p$,
(v) for any affine function ψ on V_p, $g \oplus \psi$ is also a $(p-1)$th-order plateaued function on V_p.

Proof. Due to Lemmas 2 and 6, (1) and (ii) are obvious. We now prove (iii). Applying Lemma 3 to function g, we have

$$(\Delta(\beta_0), \Delta(\beta_1), \ldots, \Delta(\beta_{2^p-1}))H_p = (\langle\xi, e_0\rangle^2, \langle\xi, e_1\rangle^2, \ldots, \langle\xi, e_{2^p-1}\rangle^2)$$

where β_j is the binary representation of an integer j, $j = 0, 1, \ldots, 2^p - 1$ and e_i is the ith row of H_p. Multiplying the above equality by itself, we obtain $2^p \sum_{j=0}^{2^p-1} \Delta^2(\beta_j) = \sum_{j=0}^{2^p-1} \langle\xi, e_1\rangle^4$. Note that $\Delta(\beta_0) = 2^p$ and that g is a $(p-1)$th-order plateaued function on V_p. Hence $2^p(2^{2p} + \sum_{j=1}^{2^p-1} \Delta^2(\beta_j)) = 2^{3p+1}$. It follows that $\sum_{j=1}^{2^p-1} \Delta^2(\beta_j) = 2^{2p}$. This proves that g has at most one non-zero linear structure and hence (iii) is true. (iv) and (v) are easy to verify. □

Theorem 2. *Let p be a positive odd number and g be a $(p-1)$th-order plateaued function on V_p that has no non-zero linear structure. Then there exists a nonsingular $2^p \times 2^p$ matrix B over $GF(2)$, such that $h(y) = g(yB)$, where $y \in V_p$, is a $(p-1)$th-order plateaued function on V_p and also a 1st-order correlation immune function.*

Proof. Set $\Omega = \{\beta | \beta \in V_p, \langle\xi, e_\beta\rangle = 0\}$, where e_β is identified with e_i and β is the binary representation of an integer i, $0 \le i \le 2^p - 1$.

Since $\#\Omega = 2^{p-1}$, the rank of Ω, denoted $rank(\Omega)$, satisfies $rank(\Omega) \ge p-1$. We now prove $rank(\Omega) = p$. Assume that $rank(\Omega) = p-1$. Since $\#\Omega = 2^{p-1}$, Ω is identified with a $(p-1)$-dimensional linear subspace of V_p. Recall that we can use a nonsingular affine transformation on the variables to transform a linear subspace into any other linear subspace with the same dimension. Without loss of the generality, we assume that Ω is composed of $\beta_0, \beta_1, \ldots, \beta_{2^{p-1}-1}$, where each β_j is the binary representation of an integer j, $0 \le j \le 2^p - 1$. By using Lemma 3, we have

$$(\langle \xi, e_0 \rangle^2, \langle \xi, e_1 \rangle^2, \ldots, \langle \xi, e_{2^p-1} \rangle^2) H_p = 2^p(\Delta_g(\beta_0), \Delta_g(\beta_1), \ldots, \Delta_g(\beta_{2^p-1}))$$

and hence

$$(0, 0, \ldots, 0, 2^{p+1}, 2^{p+1}, \ldots, 2^{p+1}) H_p = 2^p(\Delta_g(\beta_0), \Delta_g(\beta_1), \ldots, \Delta_g(\beta_{2^p-1}))$$

where the number of zeros is equal to 2^{p-1}. By using the construction of H_p and comparing the terms in the above equality, we find that $\Delta_g(\beta_{2^{p-1}}) = -2^p$. That is, $\beta_{2^{p-1}}$ is a non-zero linear structure of g. This contradicts the assumption in the proposition, that g has no non-zero linear structure. This proves $rank(\Omega) = p$. Hence we can choose p linearly independent vectors $\gamma_1, \ldots, \gamma_p$ from Ω.

Let μ_j denote the vector in V_p, whose jth term is one and all other terms are zeros, $j = 1, \ldots, p$. Define a $p \times p$ matrix B over $GF(2)$, such that $\gamma_j B = \mu_j$, $j = 1, \ldots, p$. Set $h(y) = g(yB^T)$, where $y \in V_p$ and B^T is the transpose of B. Due to (iv) of Proposition 4, $h(y)$ is a $(p-1)$th-order plateaued function on V_p. Next we prove that $h(y)$ is a 1st-order correlation immune function.

Note that $h(y) \oplus \langle \mu_j, y \rangle = g(yb^T) \oplus \langle \mu_j, y \rangle = g(z) \oplus \langle \mu_j, z(B^T)^{-1} \rangle$ where $z = yB^T$.

On the other hand,

$$\langle \mu_j, z(B^T)^{-1} \rangle = z(B^T)^{-1}\mu_j^T = z(B^{-1})^T \mu_j^T = z(\mu_j B^{-1})^T = z\gamma_j^T = \langle z, \gamma_j \rangle$$

It follows that $h(y) \oplus \langle \mu_j, y \rangle = g(z) \oplus \langle \gamma_j, z \rangle$ where $z = yB^T$.

Note that e_{γ_j} is the sequence of linear function $\psi_{\gamma_j} = \langle \gamma_j, y \rangle$. Since $\gamma_j \in \Omega$, $\langle \xi, e_{\gamma_j} \rangle = 0$. Due to Lemma 4, $g(z) \oplus \langle \gamma_j, z \rangle$ is balanced. Hence $h(y) \oplus \langle \mu_j, y \rangle$ is balanced. By using Lemma 5, we have proved that $h(y)$ is a 1st-order correlation immune function. □

Theorem 3. *Let p be a positive odd integer and g be a $(p-1)$th-order plateaued function on V_p. If g has a non-zero linear structure, then there exists a non-singular $2^p \times 2^p$ matrix B over $GF(2)$, such that $g(yB) = cx_1 \oplus h(z)$ where $y = (x_1, x_2, \ldots, x_p)$, $z = (x_2, \ldots, x_n)$, each $x_j \in GF(2)$ and the function h is a bent function on V_{p-1}.*

Proof. Since g has a non-zero linear structure, there exists a nonsingular $2^p \times 2^p$ matrix B over $GF(2)$, such that $g^*(y) = g(yB) = cx_1 \oplus h(z)$ where $y = (x_1, x_2, \ldots, x_p)$, $z = (x_2, \ldots, x_n)$ and h is a function on V_{p-1}. We only need to prove that h is bent. Without loss of generality, assume that $c = 1$. Then we have $g^*(y) = x_1 \oplus h(z)$. Let η denote the sequence of h. Hence the sequence of g^*, denoted by ξ, satisfies $\xi = (\eta, -\eta)$. Let e_i denote the ith row of H_{p-1}. From the structure of Sylvester-Hadamard matrices, (e_i, e_i) is the ith row of H_p, denoted by ℓ_i, $i = 0, 1, \ldots, 2^{p-1} - 1$, and $(e_i, -e_i)$ is the $(2^{p-1} + i)$th row of H_p, denoted by $\ell_{2^{p-1}+i}$, $i = 0, 1, \ldots, 2^{p-1} - 1$. Obviously

$$\langle \xi, \ell_i \rangle = 0, \ i = 0, 1, \ldots, 2^{p-1} - 1 \tag{1}$$

Since g^* is a $(p-1)$th-order plateaued function on V_p, (1) implies

$$\langle \xi, \ell_{2^{p-1}+i} \rangle = \pm 2^{\frac{1}{2}(p+1)}, \ i = 0, 1, \ldots, 2^{p-1} - 1 \tag{2}$$

Note that $\langle \xi, \ell_{2^{p-1}+i} \rangle = 2\langle \eta, e_i \rangle$, $i = 0, 1, \ldots, 2^{p-1} - 1$. From (2), $\langle \eta, e_i \rangle = \pm 2^{\frac{1}{2}(p-1)}$, $i = 0, 1, \ldots, 2^{p-1} - 1$. This proves that h is a bent function on V_{p-1}. □

4 Complementary $(n-1)$th-order Plateaued Functions on V_n

To explore new properties of bent functions, we propose the following new concept.

Definition 9. *Let p be a positive odd number and g_1, g_2 be two functions on V_p. Denote the sequences of g_1 and g_2 by ξ_1 and ξ_2 respectively. Then g_1 and g_2 are said to be* complementary $(p-1)$th-order plateaued functions *on V_p if they are $(p-1)$th-order plateaued functions on V_p, and satisfy the property that $\langle \xi_1, e_i \rangle = 0$ if and only if $\langle \xi_2, e_i \rangle \neq 0$, and $\langle \xi_1, e_i \rangle \neq 0$ if and only if $\langle \xi_2, e_i \rangle = 0$.*

The following Lemma can be found in [11]:

Lemma 7. *Let $k \geq 2$ be a positive integer and $2^k = a^2 + b^2$ where $a \geq b \geq 0$ and both a and b are integers. Then $a^2 = 2^k$ and $b = 0$ when k is even, and $a^2 = b^2 = 2^{k-1}$ when n is odd.*

Proposition 5. *Let p be a positive odd number and g_1, g_2 be two functions on V_p. Denote the sequences of g_1 and g_2 by ξ_1 and ξ_2 respectively. Then g_1 and g_2 are complementary $(p-1)$th-order plateaued functions on V_p if and only if $\langle \xi_1, e_i \rangle^2 + \langle \xi_2, e_i \rangle^2 = 2^{p+1}$, where e_i is the ith row of H_p, $i = 0, 1, \ldots, 2^p - 1$.*

Proof. The necessity is obvious. We now prove the sufficiency. We keep using all the notations in Definition 9. Assume that $\langle \xi_1, e_i \rangle^2 + \langle \xi_2, e_i \rangle^2 = 2^{p+1}$, where e_i is the ith row of H_p, $i = 0, 1, \ldots, 2^p - 1$. Since $p+1$ is even, by using Lemma 7, we conclude $\langle \xi_1, e_i \rangle^2 = 2^{p+1}$ or 0, $i = 0, 1, \ldots, 2^p - 1$. Similarly $\langle \xi_2, e_i \rangle^2 = 2^{p+1}$ or 0, $i = 0, 1, \ldots, 2^p - 1$. It is easy to see that g_1 and g_2 are complementary $(p-1)$th-order plateaued functions on V_p. □

Theorem 4. *Let p be a positive odd number and g_1, g_2 be two functions on V_p. Then g_1 and g_2 are complementary $(p-1)$th-order plateaued functions on V_p if and only if for every non-zero vector β in V_p, $\Delta_{g_1}(\beta) = -\Delta_{g_2}(\beta)$.*

Proof. Applying Lemma 3 to function g_1 and g_2, we obtain

$$\begin{aligned} &(\Delta_{g_1}(\beta_0) + \Delta_{g_2}(\beta_0), \Delta_{g_1}(\beta_1) + \Delta_{g_2}(\beta_1), \ldots, \Delta_{g_1}(\beta_{2^p-1}) + \Delta_{g_2}(\beta_{2^p-1}))H_p \\ &= (\langle \xi_1, e_0 \rangle^2 + \langle \xi_2, e_0 \rangle^2, \langle \xi_1, e_1 \rangle^2 + \langle \xi_2, e_1 \rangle^2, \ldots, \langle \xi_1, e_{2^p-1} \rangle^2 + \langle \xi_2, e_{2^p-1} \rangle^2) \end{aligned} \tag{3}$$

where β_i is the binary representation of integer i and e_i is the ith row of H_p, $i = 0, 1, \ldots, 2^p - 1$.

Assume that g_1 and g_2 are complementary $(p-1)$th-order plateaued functions on V_p. From (3), we have

$$(\Delta_{g_1}(\beta_0) + \Delta_{g_2}(\beta_0), \Delta_{g_1}(\beta_1) + \Delta_{g_2}(\beta_1), \ldots, \Delta_{g_1}(\beta_{2^p-1}) + \Delta_{g_2}(\beta_{2^p-1}))H_p$$
$$= (2^{p+1}, 2^{p+1}, \ldots, 2^{p+1}) \quad (4)$$

or

$$(\Delta_{g_1}(\beta_0) + \Delta_{g_2}(\beta_0), \Delta_{g_1}(\beta_1) + \Delta_{g_2}(\beta_1), \ldots, \Delta_{g_1}(\beta_{2^p-1}) + \Delta_{g_2}(\beta_{2^p-1}))$$
$$= 2(1, 1, \ldots, 1)H_p$$

Comparing the jth terms in the two sides of the above equality, we have $\Delta_{g_1}(\beta) + \Delta_{g_2}(\beta) = 2^{p+1}$, for $\beta = 0$, and $\Delta_{g_1}(\beta) + \Delta_{g_2}(\beta) = 0$, for $\beta \neq 0$.

Conversely, assume that $\Delta_{g_1}(\beta) + \Delta_{g_2}(\beta) = 0$, for $\beta \neq 0$. From (3), we have

$$(2^{p+1}, 0, \ldots, 0)H_p$$
$$= (\langle \xi_1, e_0 \rangle^2 + \langle \xi_2, e_0 \rangle^2, \langle \xi_1, e_1 \rangle^2 + \langle \xi_2, e_1 \rangle^2, \ldots, \langle \xi_1, e_{2^p-1} \rangle^2 + \langle \xi_2, e_{2^p-1} \rangle^2)$$

It follows that $\langle \xi_1, e_i \rangle^2 + \langle \xi_2, e_i \rangle^2 = 2^{p+1}$, $i = 0, 1, \ldots, 2^p - 1$. This proves that g_1 and g_2 are complementary $(p-1)$th-order plateaued functions on V_p. □

By using Theorem 4, we conclude

Proposition 6. *Let p be a positive odd number and g_1, g_2 be complementary $(p-1)$th-order plateaued functions on V_p. Then*

(i) β is a non-zero linear structure of g_1 if and only if β is a non-zero linear structure of g_2,
(ii) one and only one of g_1 and g_2 is balanced.

Proof. (i) can be obtained from Theorem 4.

(ii) We keep using the notations in Definition 9. From Proposition 5, $\langle \xi_1, e_0 \rangle^2 = 2^{p+1}$ if and only if $\langle \xi_2, e_0 \rangle^2 = 0$, and $\langle \xi_1, e_0 \rangle^2 = 0$ if and only if $\langle \xi_2, e_0 \rangle^2 = 2^{p+1}$. Note that e_0 is the all-one sequence hence $\langle \xi_j, e_0 \rangle = 0$ implies g_j is balanced. Hence one and only one of g_1 and g_2 is balanced. □

Proposition 7. *Let p be a positive odd number and g_1, g_2 be complementary $(p-1)$th-order plateaued functions on V_p. For any $\beta, \gamma \in V_p$, set $g_1^*(y) = g_1(y \oplus \beta)$ and $g_2^*(y) = g_2(y \oplus \gamma)$. Then $g_1^*(y)$ and $g_2^*(y)$ are complementary $(p-1)$th-order plateaued functions on V_p.*

Proof. Since g_1, g_2 are complementary $(p-1)$th-order plateaued functions on V_p, from Theorem 4, for any non-zero vector α in V_p, $\Delta_{g_1}(\alpha) = -\Delta_{g_2}(\alpha)$. On the other hand, it is easy to verify $\Delta_{g_2^*}(\alpha) = \Delta_{g_2}(\alpha)$, where α is any vector in V_p. Hence for any non-zero vector β in V_p, $\Delta_{g_1}(\alpha) = -\Delta_{g_2^*}(\alpha)$. Again, by using Theorem 4, we have proved that g_1, g_2^* are complementary $(p-1)$th-order plateaued functions on V_p. By the same reasoning, we can prove that g_1^* and g_2^* are complementary $(p-1)$th-order plateaued functions on V_p. □

Now fix β, i.e., fix g_1^* in Proposition 7, and let γ be arbitrary. We can see that there exist more than one function that can team up with g_1^* to form complementary $(p-1)$th-order plateaued functions on V_p. This shows that the relationship of complementary $(p-1)$th-order plateaued functions on V_p is not a one-to-one correspondence.

Theorem 5. *Let p be a positive odd number and ξ_1, ξ_2 be two $(1,-1)$ sequences of length 2^p. Set $\eta_1 = 2^{-\frac{1}{2}(p+1)}(\xi_1+\xi_2)H_p$ and $\eta_2 = 2^{-\frac{1}{2}(p+1)}(\xi_1-\xi_2)H_p$. Then ξ_1 and ξ_2 are the sequences of complementary $(p-1)$th-order plateaued functions on V_p if and only if η_1 and η_2 are the sequences of complementary $(p-1)$th-order plateaued functions on V_p.*

Proof. Assume that ξ_1 and ξ_2 are the sequences of complementary $(p-1)$th-order plateaued functions on V_p respectively. It can be verified straightforwardly that both η_1 and η_2 are $(1,-1)$ sequences. Hence both η_1 and η_2 are the sequences of functions on V_p.

Furthermore we have

$$\eta_1 H_p = 2^{\frac{1}{2}(p+1)}(\frac{1}{2}(\xi_1+\xi_2)),\ \ \eta_2 H_p = 2^{\frac{1}{2}(p+1)}(\frac{1}{2}(\xi_1-\xi_2)) \tag{5}$$

Note that both $\frac{1}{2}(\xi_1+\xi_2)$ and $\frac{1}{2}(\xi_1-\xi_2)$ are $(0,1,-1)$ sequences. From (5), $\langle \eta_1, e_i\rangle$ and $\langle \eta_2, e_i\rangle$, where e_i is the ith row of H_p, $i=0,1,\ldots,2^p-1$, take the value of $\pm 2^{\frac{1}{2}(p+1)}$ or 0 only. On the other hand, it is easy to see that the ith term of $\frac{1}{2}(\xi_1 \pm \xi_2)$ is non-zero if and only if the ith term of $\frac{1}{2}(\xi_1 \mp \xi_2)$ is zero. This proves that $\langle \eta_1, e_i\rangle \neq 0$ if and only if $\langle \eta_2, e_i\rangle = 0$, also $\langle \eta_1, e_i\rangle = 0$ if and only if $\langle \eta_2, e_i\rangle \neq 0$, $i=0,1,\ldots,2^p-1$. By using Proposition 5 η_1 and η_2 are the sequences of complementary $(p-1)$th-order plateaued functions on V_p.

Conversely, Assume that η_1 and η_2 are the sequences of complementary $(p-1)$th-order plateaued functions on V_p. Note that $\xi_1 = 2^{-\frac{1}{2}(p+1)}(\eta_1+\eta_2)H_p$ and $\xi_2 = 2^{-\frac{1}{2}(p+1)}(\eta_1-\eta_2)H_p$. Inverse the above deduction, we have proved that ξ_1 and ξ_2 are the sequences of complementary $(p-1)$th-order plateaued functions on V_p.

□

In Section 5, we will prove that the existence of complementary $(n-2)$th-order plateaued functions on V_{n-1} is equivalent to the existence of bent functions on V_n.

5 Relating Bent Functions on V_n to Complementary $(n-2)$th-order Plateaued Functions on V_{n-1}

Lemma 8. *Let n be a positive even number and f be a function on V_n. Denote the sequence of f by $\xi = (\xi_1, \xi_2)$, where both ξ_1 and ξ_2 are of length 2^{n-1}. Let ξ_1 and ξ_2 be the sequences of functions f_1 and f_2 on V_{n-1} respectively. Then f is bent if and only if f_1 and f_2 are complementary $(n-2)$th-order plateaued functions on V_{n-1}.*

Proof. Obviously, $\xi H_n = (\langle \xi, \ell_0 \rangle, \langle \xi, \ell_1 \rangle, \ldots, \langle \xi, \ell_{2^n-1} \rangle)$ where ℓ_j is the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$. Hence

$$(\xi_1, \xi_2) \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix} = (\langle \xi, \ell_0 \rangle, \langle \xi, \ell_1 \rangle, \ldots, \langle \xi, \ell_{2^n-1} \rangle) \tag{6}$$

For each j, $0 \le j \le 2^{n-1}-1$, comparing the jth terms in the two sides of equality (6), also comparing the $2^{n-1} + j$ terms in the two sides of the equality, we find

$$\langle \xi_1, e_j \rangle + \langle \xi_2, e_j \rangle = \langle \xi, \ell_j \rangle, \ \ \langle \xi_1, e_j \rangle - \langle \xi_2, e_j \rangle = \langle \xi, \ell_{2^{n-1}+j} \rangle \tag{7}$$

e_j is the jth row of H_{n-1}, $j = 0, 1, \ldots, 2^{n-1} - 1$.

Assume that f is bent. From Theorem 1, $|\langle \xi, \ell_j \rangle| = 2^{\frac{1}{2}n}$ and $|\langle \xi, \ell_{2^{n-1}+j} \rangle| = 2^{\frac{1}{2}n}$, $j = 0, 1, \ldots, 2^{n-1} - 1$.

Due to (7), $|\langle \xi_1, e_j \rangle + \langle \xi_2, e_j \rangle| = |\langle \xi_1, e_j \rangle - \langle \xi_2, e_j \rangle| = 2^{\frac{1}{2}n}$. This causes $\langle \xi_1, e_j \rangle = 2^{\frac{1}{2}n}$ and $\langle \xi_2, e_j \rangle = 0$ otherwise $\langle \xi_1, e_j \rangle = 0$ and $\langle \xi_2, e_j \rangle = 2^{\frac{1}{2}n}$. This proves that f_1 and f_2 are complementary $(n-2)$th-order plateaued functions on V_{n-1}.

Conversely, assume that f_1 and f_2 are complementary $(n-2)$th-order plateaued functions on V_{n-1}. From Proposition 5, for each i, $0 \le i \le 2^{n-1} - 1$, $\langle \xi_1, e_i \rangle$ and $\langle \xi_1, e_i \rangle$ take the value of $\pm 2^{\frac{1}{2}n}$ or 0 only. Furthermore $\langle \xi_1, e_i \rangle = 0$ implies $\langle \xi_2, e_i \rangle \ne 0$, and $\langle \xi_1, e_i \rangle \ne 0$ implies $\langle \xi_2, e_i \rangle = 0$. From (7), $\langle \xi, \ell_j \rangle = \pm 2^{\frac{1}{2}n}$ and $\langle \xi, \ell_{2^{n-1}+j} \rangle \pm 2^{\frac{1}{2}n}$, $j = 0, 1, \ldots, 2^{n-1} - 1$. Due to Theorem 1, f is bent.

□

Lemma 8 can be briefly restated as follows:

Theorem 6. *Let n be a positive even number and f be a function on V_n. Then f is bent if and only if the two functions on V_{n-1}, $f(0, x_2, \ldots, x_n)$ and $f(1, x_2, \ldots, x_n)$, are complementary $(n-2)$th-order plateaued functions on V_{n-1}.*

Proof. It is easy to verify that $f(x_1, \ldots, x_n) = (1 \oplus x_1) f(0, x_2, \ldots, x_n) \oplus x_1 f(1, x_2, \ldots, x_n)$. Set $f_1(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n)$ and $f_2(x_2, \ldots, x_n) = f(1, x_2, \ldots, x_n)$. Denote the sequences of f_1 and f_2 by ξ_1 and ξ_2 respectively. Obviously, the sequence of f, denoted by ξ, satisfies $\xi = (\xi_1, \xi_2)$. By using Lemma 8, we have proved the theorem. □

Due to Theorem 6, the following proposition is obvious.

Proposition 8. *Let n be a positive even number and f be a function on V_n. Then f is bent if and only if the two functions on V_{n-1},*
$f(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n)$ and
$f(x_1, \ldots, x_{j-1}, 1, x_{j+1}, \ldots, x_n)$ are complementary $(n-2)$th-order plateaued functions on V_{n-1}. $j = 1, \ldots, n$.

The following theorem follows Theorem 6 and Proposition 7.

Theorem 7. *Let n be a positive even number and f be a function on V_n. Write $x = (x_1, \ldots, x_n)$ and $y = (x_2, \ldots, x_n)$ where $x_j \in GF(2)$, $j = 1, \ldots, n$. Set $f_1(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n)$ and $f_2(x_2, \ldots, x_n) = f(1, x_2, \ldots, x_n)$. Then f is bent if and only if $g(x) = (1 \oplus x_1)f_1(y \oplus \gamma_1) \oplus x_1 f_2(y \oplus \gamma_2)$ is bent, where γ_1 and γ_2 are any two vectors in V_{n-1}.*

By using Theorem 5 and Lemma 8, we conclude

Theorem 8. *Let $\xi = (\xi_1, \xi_2)$ be a $(1, -1)$ sequence of length 2^n, where both ξ_1 and ξ_2 are of length 2^{n-1}. Then ξ is the sequence of a bent function if and only if $2^{-\frac{1}{2}n}((\xi_1 + \xi_2)H_{n-1},\ (\xi_1 - \xi_2)H_{n-1})$ is the sequence of a bent function.*

Theorems 6, 7 and 8 represent new characterisations of bent functions. In addition, Theorems 7 and 8 provide methods of constructing new bent function from known bent functions.

6 Non-quadratic Bent Functions

Definition 10. *Let f be a function on V_n and W be an r-dimensional linear subspace of W. From linear algebra, V_n can be divided into 2^{n-r} disjoint* cosets *of W:*

$$V_n = U_0 \cup U_1 \cup \cdots \cup U_{2^{n-r}-1}$$

where $U_0 = W$, $\#U_j = 2^r$, $j = 0, 1, \ldots, 2^{n-r} - 1$, and for any two vectors γ and β in V_n, β and γ belong to the same coset U_j if and only if $\beta \oplus \gamma \in W$. The partition is unique if the order of the cosets is ignored. Each U_j can be expressed as $U_j = \gamma_j \oplus W$ where γ_j is a vector in V_n and $\gamma_j \oplus W$ denotes $\{\gamma_j \oplus \alpha | \alpha \in W\}$ however γ_j is not unique. For a coset $U = \gamma \oplus W$, define a function g on W such that $g(\alpha) = f(\gamma \oplus \alpha)$ for every $\alpha \in W$. Then g is called the restriction of f to coset $\gamma \oplus W$. *In particular, the* restriction of f to linear subspace W *is a function h on W such that $h(\alpha) = f(\alpha)$ for every $\alpha \in W$.*

Proposition 9. *Let f be a bent function on V_n and W be an arbitrary $(n-1)$-dimensional linear subspace. Let V_n divided into two disjoint cosets: $V_n = W \cup U$. Then the restriction of f to linear subspace W, f_W, and the restriction of f to coset U, f_U, are complementary $(n-2)$th-order plateaued functions on V_{n-1}.*

Proof. In fact, $W^* = \{(0, x_2, \ldots, x_n) | x_2, \ldots, x_n \in GF(2)\}$ forms an $(n-1)$-dimensional linear subspace and $U^* = \{(1, x_2, \ldots, x_n) | x_2, \ldots, x_n \in GF(2)\}$ is a coset of W. By using a nonsingular linear transformation on the variables, we can transform W into W^* and U into U^* simultaneously.. By using Theorem 6, we have proved the Proposition. □

Proposition 9 shows that the restriction of f to any $(n-1)$-dimensional linear subspace is still cryptographically strong.

We now prove the following characteristic property of quadratic bent functions.

Lemma 9. *Let f be a bent function on V_n. Then for any $(n-1)$-dimensional linear subspace W, the restriction of f to W has a non-zero linear structure if and only if f is quadratic.*

Proof. Let f be quadratic and W be an arbitrary $(n-1)$-dimensional linear subspace. Since $n-1$ is odd, the restriction of f to W, denoted by g, is not bent. Hence due to (iii) of Theorem 1, there exists a non-zero vector β in W, such that $g(y) \oplus g(y \oplus \beta)$ is not balanced. On the other hand, since g is also quadratic, $g(y) \oplus g(y \oplus \beta)$ is affine. It is easy to see that any non-balanced affine function must be constant. This proves that β is a non-zero linear structure of g.

We now prove the converse: "if for any $(n-1)$-dimensional linear subspace W, the restriction of f to W has a non-zero linear structure, then f is quadratic" by induction on the dimension n.

Let $n = 2$. Bent functions on V_2 must be quadratic. For $n = 4$, from (i) of Proposition 1, bent functions on V_4 must be quadratic.

Assume that the converse is true for $4 \leq n \leq k-2$ where k is even. We now prove the converse for $n = k$.

Let f be a bent function on V_k such that for any $(k-1)$-dimensional linear subspace W the restriction of f to W has a non-zero linear structure.

It is easy to see that f can be expressed as $f(x) = x_1 g(y) \oplus h(y)$ where $y = (x_2, \ldots, x_k)$, both g and h are functions on V_{k-1}. From Theorem 6, $f(0, x_2, \ldots, x_k) = h(y)$ and $f(1, x_2, \ldots, x_k) = g(y) \oplus h(y)$ are complementary $(k-2)$th-order plateaued functions on V_{k-1}.

Since $\{(0, x_2, \ldots, x_k) | x_2, \ldots, x_k \in GF(2)\}$ forms a $(k-1)$-dimensional linear subspace, due to the assumption about f: "the restriction of f to any $(k-1)$-dimensional linear subspace has a non-zero linear structure", $f(0, x_2, \ldots, x_k) = h(y)$ has a non-zero linear structure. Without loss of generality, we can assume that the vector β in V_{k-1}, $\beta = (1, 0, \ldots, 0)$, is the non-zero linear structure of $h(y)$. It is easy to see $h(y) = cx_2 \oplus b(z)$ where c is a constant in $GF(2)$, $z = (x_3, \ldots, x_k)$ and $b(z)$ is a function on V_{k-2}. Without loss of generality, we assume that $c = 1$. From Theorem 3, $b(z)$ is a bent function on V_{k-2}.

It is easy to see $\Delta_h(\beta) = -2^{k-1}$. From Theorem 4, $\beta = (1, 0, \ldots, 0)$ is also a linear structure of $g(y) \oplus h(y)$ and $\Delta_{g \oplus h} = 2^{k-1}$. Hence $g(y) \oplus h(y)$ can be expressed as $g(y) \oplus h(y) = dx_2 \oplus p(z)$, where $z = (x_3, \ldots, x_k)$. Due to Theorem 3, $p(z)$ is a bent function on V_{k-2}. Since $\Delta_{g \oplus h}(\beta) = 2^{k-1}$, $d = 0$. Hence $g(y) = h(y) \oplus p(z) = x_2 \oplus b(z) \oplus p(z)$ and hence

$$f(x) = x_1(x_2 \oplus b(z) \oplus p(z)) \oplus x_2 \oplus b(z) \tag{8}$$

Since $\{(x_1, 0, x_3, \ldots, x_k)|x_1, x_3, \ldots, x_k \in GF(2)\}$ forms a $(k-1)$-dimensional linear subspace, $f(x_1, 0, x_3, \ldots, x_k)$ is the restriction of f to this $(k-1)$-dimensional linear subspace. Due to the assumption about f, $f(x_1, 0, x_3, \ldots, x_k)$ has a non-zero linear structure, denoted by γ, $\gamma \in V_{k-1}$. From (8),
$f'(u) = f(x_1, 0, x_3, \ldots, x_n) = x_1(b(z) \oplus p(z)) \oplus b(z)$, where $u \in V_{k-1}$ and $u = (x_1, x_3, x_4, \ldots x_k)$.

There exist two cases of γ.

Case 1: $\gamma = (0, \mu)$ where $\mu \in V_{k-2}$. Since $\gamma \neq 0$, μ is non-zero. It is easy to see $f'(u) \oplus f'(u \oplus \gamma) = x_1(b(z) \oplus b(z \oplus \mu) \oplus p(z) \oplus p(z \oplus \mu)) \oplus b(z) \oplus b(z \oplus \mu)$.

Since $f'(u) \oplus f'(u \oplus \gamma)$ is a constant, $b(z) \oplus b(z \oplus \mu) \oplus p(z) \oplus p(z \oplus \mu) = 0$ and $b(z) \oplus b(z \oplus \mu) = c'$, where c' is constant. On the other hand, since $b(z)$ is bent and $\mu \neq 0$, $b(z) \oplus b(z \oplus \mu)$ is balanced and hence it is not constant. This is a contradiction. This proves that Case 1 cannot take place.

Case 2: $\gamma = (1, \nu)$ where $\nu \in V_{k-2}$ and ν is not necessarily non-zero. It is easy to see $f'(u) \oplus f'(u \oplus \gamma) = x_1(b(z) \oplus b(z \oplus \nu) \oplus p(z) \oplus p(z \oplus \nu)) \oplus b(z) \oplus p(z \oplus \nu)$.

Since $f'(u) \oplus f'(u \oplus \gamma)$ is a constant, $b(z) \oplus b(z \oplus \nu) \oplus p(z) \oplus p(z \oplus \nu) = 0$ and $b(z) \oplus p(z \oplus \nu) = c''$, where c'' is constant, and hence $b(z \oplus \nu) \oplus p(z) = c''$. From (8),

$$f(x) = x_1x_2 \oplus x_1(b(z) \oplus b(z \oplus \nu) \oplus c'') \oplus x_2 \oplus b(z) \tag{9}$$

We now turn to the restriction of f to another $(k-1)$-dimensional linear subspace. Write $U^* = \{(x_3 \ldots, x_k)|\, x_3, \ldots, x_k \in GF(2)\}$ and $U_* = \{(x_1, x_2)|x_1, x_2 \in GF(2)\}$. Hence U^* is a $(k-2)$-dimensional linear subspace and U_* is a 2-dimensional linear subspace, and $V_k = (U_*, U^*)$, where $(X, Y) = \{(\alpha, \beta)|\alpha \in X, \beta \in Y\}$.

Let Λ denote an arbitrary $(k-3)$-dimensional linear subspace in U^*. Hence (U_*, Λ) is a $(k-1)$-dimensional linear subspace.

Let $f''(y)$ denote the restriction of f to (U_*, Λ), where $y \in (U_*, \Lambda)$. Hence y can be expressed as $y = (x_1, x_2, v)$ with $v = (v_1, \ldots, v_{k-2}) \in \Lambda$, where $v_1, \ldots, v_{k-2} \in GF(2)$ but not arbitrary because Λ is a proper subset of V_{k-2}.

From (9), $f''(y)$ can be expressed as $f''(y) = x_1x_2 \oplus x_1(b'(v) \oplus b''(v) \oplus a) \oplus x_2 \oplus b'(v)$, where $b'(v)$ denotes the restriction of $b(z)$ to Λ and $b''(v)$ denotes the restriction of $b(z \oplus \nu)$ to Λ.

From the assumption about f, f'' has a non-zero linear structure γ', $\gamma' \in (U_*, \Lambda)$. Write $\gamma' = (a_1, a_2, \tau)$ where $\tau \in \Lambda$. Since $\gamma' = (a_1, a_2, \tau)$ is a non-zero linear structure of f'', it is easy to verify $a_1 = a_2 = 0$. This proves $\gamma' = (0, 0, \tau)$. Since γ' is non-zero, $\tau \neq 0$.

Hence $f''(y) \oplus f''(y \oplus \gamma') = x_1(b'(v) \oplus b'(v \oplus \tau) \oplus b''(v) \oplus b''(v \oplus \tau)) \oplus b'(v) \oplus b'(v \oplus \tau)$. Since $f''(y) \oplus f''(y \oplus \gamma')$ is constant, $b'(v) \oplus b'(v \oplus \tau) \oplus b''(v) \oplus b''(v \oplus \tau) = 0$ and $b'(v) \oplus b'(v \oplus \tau)$ is constant. Hence τ is a non-zero linear structure of $b'(v)$. This proves that for any $(n-3)$-dimensional linear subspace Λ, the restriction of $b(z)$ to Λ, i.e., $b'(v)$, has a non-zero linear structure. On the other hand, since $b(z)$ is a bent function on V_{k-2}, due to the induction assumption, $b(z)$ is quadratic. Hence $b(z) \oplus b(z \oplus \nu)$ must be affine. From (9), we have proved $f(x) = x_1x_2 \oplus x_1(b(z) \oplus b(z \oplus \nu) \oplus a) \oplus x_2 \oplus b(z)$ is quadratic when $n = k$. □

Due to the low algebraic degree, quadratic functions are not cryptographically desirable, although some of them are highly nonlinear.

The following is an equivalent statement of Lemma 9.

Theorem 9. *Let f be a bent function on V_n. Then f is non-quadratic if and only if there exists an $(n-1)$-dimensional linear subspace W such that the restriction of f to W, f_W, has no non-zero linear structure.*

Theorem 9 is an interesting characterization of non-quadratic bent functions.

7 New Constructions of Cryptographic Functions

The relationships among a bent function on V_n and complementary $(n-2)$th-order plateaued functions on V_{n-1} are helpful to design cryptographic functions from bent functions. In fact, from Theorem 6, any bent function on V_n can be "split" into complementary $(n-2)$th-order plateaued functions on V_{n-1}.

We prefer non-quadratic bent functions as they are useful to obtain complementary plateaued functions that have no non-zero linear structures.

Let f be a non-quadratic bent function on V_n. By using Theorem 9, we can find an $(n-1)$-dimensional subspace W such that the restriction of f to W, f_W, has no non-zero linear structure. For any vector $\alpha \in V_n$ with $\alpha \notin W$, we have $(\alpha \oplus W) \cap W = \emptyset$ and $V_n = W \cup (\alpha \oplus W)$. From Proposition 9, the restriction of f to $\alpha \oplus W$, $f_{\alpha \oplus W}$, and f_W are complementary $(n-2)$th-order plateaued functions on V_{n-1}. Due to (i) of Proposition 6, $f_{\alpha \oplus W}$ has no non-zero linear structure. Due to (ii) of Proposition 6, one and only one of f_W and $f_{\alpha \oplus W}$ is balanced. From Propositions 4, we can see that both f_W and $f_{\alpha \oplus W}$ are highly nonlinear.

Furthermore, by using Theorem 2, we can use a nonsingular linear transformation on the variables to transform the balanced f_W or $f_{\alpha \oplus W}$ into another $(n-2)$th-order plateaued function g on V_{n-1}. The resultant function is a 1st-order correlation immune function. Obviously g is still balanced and highly nonlinear, and it does not have non-zero linear structure.

We note that there is a more straightforward method to construct a balanced, highly nonlinear function on any odd dimensional linear space, by "concatenating" known bent functions. For example, let f be a bent function on V_k, we can set $g(x_1, \ldots, x_{k+1}) = x_1 \oplus f(x_2, \ldots, x_{k+1})$. Then g is a balanced, highly nonlinear function on V_{k+1}, where $k+1$ is odd. Let η and ξ denote the sequences of g and f respectively. It is easy to see $\eta = (\xi, -\xi)$ and hence η is a concatenations of ξ and $-\xi$. We call this method *concatenating* bent functions. A major problem of this method is that f contains a non-zero linear structure $(1, 0, \ldots, 0)$.

In contrast, the method of "splitting" a bent function we discussed earlier allows us to obtain functions that do not have non-zero linear structure.

8 Conclusions

We have identified relationships between bent functions and complementary plateaued functions, and discovered a new characteristic property of bent functions. Furthermore we have proved a necessary and sufficient condition of non-quadratic bent functions. Based on the new results on bent functions, we have proposed a new method for constructing balanced, highly nonlinear and correlation immune functions that have no non-zero linear structures.

9 Acknowledgement

The second author was supported by a Queen Elizabeth II Fellowship (227 23 1002).

References

1. P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In *Advances in Cryptology - CRYPTO'91*, volume 576, Lecture Notes in Computer Science, pages 87–100. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
2. Claude Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3:135–145, 1993.
3. Xiao Guo-Zhen and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, 1988.
4. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.
5. W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434, Lecture Notes in Computer Science, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.
6. B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, volume 437, Lecture Notes in Computer Science, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
7. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.
8. J. Wang. The linear kernel of boolean functions and partially-bent functions. *System Science and Mathematical Science*, 10:6–11, 1997.
9. A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, volume 219, Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, Berlin, Heidelberg, New York, 1986.
10. Y. Zheng X. M. Zhang and Hideki Imai. Duality of boolean functions and its cryptographic significance. In *Advances in Cryptology - ICICS'97*, volume 1334, Lecture Notes in Computer Science, pages 159–169. Springer-Verlag, Berlin, Heidelberg, New York, 1997.
11. X. M. Zhang and Y. Zheng. Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors. *Design, Codes and Cryptography*, 7(1/2):111–134, 1996. special issue dedicated to Gus Simmons.
12. Y. Zheng and X. M. Zhang. Plateaued functions. In *Advances in Cryptology - ICICS'99*, volume 1726, Lecture Notes in Computer Science, pages 284–300. Springer-Verlag, Berlin, Heidelberg, New York, 1999.