A Composition Construction of Bent-Like Boolean Functions from Quadratic Polynomials

ZENG Xiangyong and HU Lei
State Key Laboratory of Information Security
(Graduate School of Chinese Academy of Sciences)
Beijing, 100039, China
e-mail: {xyzeng2002, gnuleihu}@sina.com

September 26, 2003

Abstract: In this paper, we generalize the composition construction of Khoo et al. for highly nonlinear Boolean functions ([1]). We utilize general quadratic forms instead of the trace map in the construction. The construction composes an n-variable Boolean function and an m-variable quadratic form over F_{2^n} to get an nm-variable Boolean function with beautiful spectrum property and a doubled algebraic degree. Especially, the method is suitable to construct functions with 3-valued spectra (bent-like functions) or ones with better spectra (near-bent functions). Our proof technique is based on classification of quadratic forms over finite fields and enumeration of solutions of quadratic equations. We also prove the p-ary analogy of these results for odd prime p.

Keywords: bent-like function, bent function, near-bent function, algebraic degree, 3-valued spectrum, quadratic form

1 Introduction

Boolean functions used in cryptosystems are required to have good cryptographic properties, such as balancedness, high nonlinearity and high algebraic degree, to ensure the systems are resistant against linear cryptanalysis ([2]). Besides, it is a desirable property that a Boolean function has 3-valued spectra. This property provides a protection against the soft output joint attack ([3]).

A framework unifies such cryptographic properties is to introduce the concept of near-bent function. Except balancedness, such a function behaves like a bent function, that is, it has 3-valued spectra and high nonlinearity close to the upper bound on nonlinearity, and may have high algebraic degree. It is important to study near-bent functions since bent functions are not balanced and can't be directly used in a cryptosystem.

There is an intrinsic relation between near-bent functions and bent functions. Bent functions can be constructed from near-bent functions ([4]), and vice versa. Another important aspect to study bent and near-bent functions is that the theory is closely related to combinatorics ([5-7]) and communication ([8-15]) in some useful fields such as difference set, partial spread, and sequences with low cross correlation.

Recently, Khoo et al. present a new construction for highly nonlinear Boolean functions from the theory of geometric sequence ([1, 15]). Their functions are cryptographically good and do not have a weakness shared by Boolean functions constructed by concatenating linear functions ([16]). They use a composition construction idea originated from GMW-sequences in communication ([17]). Essentially, they utilize in their construction a special quadratic form, which can be derived from a trace map between finite fields.

In this paper, we generalize their idea to utilize general quadratic forms. Our generalization can obtain a larger class of functions than that in Khoo et al.'s method. On the other hand, our method not only can construct usual binary near-bent functions, but also p-ary functions ([18-22,10]) for any prime p. In addition, our method constructs a larger class of functions than near-bent functions, called bent-like functions. On the other hand, our proof method is completely different with that of Khoo et al. It is direct and is based on classification of quadratic forms over finite fields and enumeration of solutions of quadratic equations. The proof of Khoo et al. is especially indirect and makes reference to one result of Klapper etc. ([17]), which again makes reference to another one ([23]) whose proof is complicated and very long.

This paper is arranged as follows. We give some definitions and preliminaries in Section 2. In Sections 3-4 we construct binary bent-like and near-bent functions, and discuss the basic construction in Section 3 and extend it to a cascaded construction in Section 4. In section 5, we first show a quadratic form over F_p must be bent-like, and then give the similar construction of p-ary bent-like and near-bent functions for odd p.

2 Preliminaries

Let p be a prime, $q = p^n$, and F_q and F_{q^m} be the finite fields with q and q^m elements, respectively. An n-variable function (over F_p) is a map f from $F_p{}^n$ to F_p. It is usually called a Boolean function if $p = 2$ and a generalized Boolean function if $p > 2$.

Taking a basis $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ of F_q over F_p, an n-tuple $(a_1, a_2, \cdots, a_n)$ over F_p uniquely represents an element of F_q, $a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$. Under this representation and its induced representation, we always assume in this paper that F_q is the domain of any n-variable function f, and $F_q{}^m$ is the domains of nm-variable functions.

Let $(\beta_1, \beta_2, \cdots, \beta_n)$ be the dual basis of $(\alpha_1, \alpha_2, \cdots, \alpha_n)$, i.e., $\mathrm{Tr}(\alpha_i\beta_i) = 1$ and $\mathrm{Tr}(\alpha_i\beta_j) = 0$ for $i \neq j$, where Tr is the trace map from F_q to F_p. Then the usual dot product of two n-tuples $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ over F_p is $\mathrm{Tr}(\alpha\beta)$, where

$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$ and $\beta = b_1\beta_1 + b_2\beta_2 + \cdots + b_n\beta_n$. As a consequence, the dot product of two nm-tuples $(a_{1,1}, a_{1,2}, \cdots, a_{m,n})$ and $(b_{1,1}, b_{1,2}, \cdots, b_{m,n})$ over F_p is $\mathrm{Tr}(u_1v_1 + \cdots + u_mv_m)$, where $u_i = a_{i,1}\alpha_1 + a_{i,2}\alpha_2 + \cdots + a_{i,n}\alpha_n$ and $v_i = b_{i,1}\beta_1 + \cdots + b_{i,n}\beta_n$. In this paper, we will study the nm-variable functions over F_p with good Walsh spectra, and we always make such a convention that the input variables of the functions are written as $(x_1, x_2, \cdots, x_m)$ where each $x_i \in F_q$ corresponds to an n-dimensional vector $(x_{i,1}, x_{i,2}, \cdots, x_{i,n})$ over F_p by $x_i = x_{i,1}\alpha_1 + x_{i,2}\alpha_2 + \cdots + x_{i,n}\alpha_n$ under the representation derived from the basis $(\alpha_1, \alpha_2, \cdots, \alpha_n)$, whilst the input variables of the Walsh spectra of the functions are written as $(\lambda_1, \lambda_2, \cdots, \lambda_m)$ where each $\lambda_i \in F$ corresponds to an n-dimensional vector $(\lambda_{i,1}, \lambda_{i,2}, \cdots, \lambda_{i,n})$ over F_p by $\lambda_i = \lambda_{i,1}\beta_1 + \cdots + \lambda_{i,n}\beta_n$ under the representation derived from the basis $(\beta_1, \beta_2, \cdots, \beta_n)$.

An n-variable function f over F_p has a unique polynomial expression of the form $f(x) = \sum_{s=0}^{q-1} a_s x^s$ ($x, a_s \in F_q$) and a unique algebraic expression of the form $f(x_1, \cdots, x_n) = \sum_{i_1=0}^{p-1} \cdots \sum_{i_n=0}^{p-1} c_{i_1,\cdots,i_n} x_1^{i_1} \cdots x_n^{i_n}$ ($x_1, \cdots, x_n, c_{i_1,\cdots,i_n} \in F_p$). The algebraic degree of f is defined as $\deg(f) = \max\{i_1 + \cdots + i_n : c_{i_1,\cdots,i_n} \neq 0\}$, and it is equal to $\max\{\mathrm{Wh}_p(s) : a_s \neq 0\}$ ([24]), where $\mathrm{Wh}_p(s)$ is the sum of the coefficients of the p-adic expression of s.

Let $\omega = e^{i2\pi/p}$ be a primitive complex p-th root of unity. The Walsh transform of an n-variable function $f : F_q \to F_p$ is a complex function W_f defined over F_q and defined by $W_f(\lambda) = \sum_{x \in F_q} \omega^{f(x) - \mathrm{Tr}(\lambda x)}$ for $\lambda \in F_q$, or equivalently, defined over $F_p{}^n$ and defined by $W_f(\lambda) = \sum_{x \in F_p{}^n} \omega^{f(x) - \lambda \cdot x}$ for $\lambda \in F_p{}^n$, where x is a vector of $F_p{}^n$. The values of W_f are called the spectra of f.

Definition 1: $f: F_q \to F_p$ is called a bent-like function if $|W_f(\lambda)|$ is 0 or p^u for any $\lambda \in F_q$, where $2u$ is a fixed integer. f is called a bent function if $|W_f(\lambda)| = p^{n/2}$ for any $\lambda \in F_q$. A bent-like function is called a near-bent function if $u = (n+1)/2$ when $p > 2$, and $u = (n+1)/2$ for odd n and $u = (n+2)/2$ for even n when $p = 2$.

Remark 1: (i) Parseval's equation $\sum_{\lambda \in F_q} \left|W_f(\lambda)\right|^2 = p^{2n}$ tells us that if $|W_f(\lambda)|$ takes only one nonzero value θ for $\lambda \in F_q$, then θ^2 is a rational number. However, $\theta^2 = |W_f(\lambda)|^2$ is an algebraic integer ([25]), so θ^2 is an integer ([25,26]), and hence divides p^{2n} by Parseval's equation again. So, $\theta = p^u$ for some u with $2u$ being an integer.

(ii) Parseval's equation also says that $u \geq n/2$ for a bent-like function, and that if $u = n/2$ then $|W_f(\lambda)|$ is always nonzero.

(iii) When $p = 2$, the above defined bent-like functions are also called plateaued functions ([27,28,1]) or ones with 3-value spectra ([29-34,1]) since $W_f(\lambda)$ takes one of three values 0, 2^u, and -2^u, and for odd n, the near-bent functions are also called Gold-like ([12,14,15]).

(iv) For $p = 2$, $W_f(\lambda)$ is always an integer. So, u is an integer for a bent-like function, and a bent function exists only when n is even. This is a well known fact. For $p > 2$, u may be a half integer. See [15] and the example in Section 5 (Theorem 3). For results on existence of generalized bent functions, see [20-22].

Definition 2: Let f be an n-variable function over F_p. If the outputs of f at exact $1/p$ of its all possible inputs are a for any element a of F_p, then f is called to be balanced.

Lemma 1: Let f be an n-variable function over F_p. f is balanced if and only if $W_f(0) = 0$.

Proof. It is clear by the fact that $\sum_{i=0}^{p-1} a_i \omega^i = 0$ if and only if $a_0 = a_1 = \cdots = a_{p-1}$, where $a_0, \cdots, a_{p-1}$ are integers.

Bent functions are ones with optimal nonlinearity ([35]), but they are not balanced by Lemma 1 (also a well known fact), so they can't be directly used in the design of cryptosystems. Patterson and Wiedemann show that for odd $n \geq 15$, it is possible to construct functions whose nonlinearity is greater than that obtained by concatenating two bent functions ([36]). Maitra and Sarkar give methods to heuristically modify the Patterson-Wiedemann and bent functions to achieve balanced and still retain nonlinearity higher than the bent concatenation value ([37]). However, the spectra of these modified functions are not considered and maybe they are vulnerable under the soft output joint attack ([3]). One of our purposes is also to obtain balanced Boolean functions with good nonlinearity and we concentrate our attention on studying near-bent functions. Different from their methods, our idea is composing an n-variable near-bent function and a quadratic form over F_{p^n}. See [38] for knowledge of quadratic form over a finite field.

Definition 3: An m-variable quadratic form over F_q is a polynomial over F_q of the form $Q(x_1, \cdots, x_m) = \sum_{i,j=1}^{m} a_{ij} x_i x_j + \sum_{i=1}^{m} b_i x_i + c$, $a_{ij}, b_i, c \in F_q$. It needs not to be homogeneous, i.e., b_i and c may be nonzero. If for any $\beta \in F_q$, the outputs of $Q(x_1, \cdots, x_m)$ at exact $1/q$ of its all possible inputs are β, then Q is called to be balanced. $Q(x_1, \cdots, x_m)$ is called to be non-degenerate if it is not transformed to a quadratic form of fewer variables under any invertible affine transformation over F_q on $(x_1, \cdots, x_m)$.

3 Bent-like functions from quadratic forms

In this section, we assume $p = 2$, and present a construction of bent-like functions, which composes balanced quadratic forms.

Let f be an n-variable Boolean function, and $Q(x_1, \cdots, x_m)$ be an m-variable quadratic form over F_q. Define an nm-variable function g as $f(Q(x_1, \cdots, x_m))$.

Theorem 1: Assume f and $Q(x_1, \cdots, x_m)$ are balanced. Then g is balanced, and the spectra of g take such values: 0 and $\pm q^d W_f(\lambda)$, $\lambda \in F_q^{\ *}$, where d is an integer depending only on $Q(x_1,\cdots,x_m)$.

Proof. Let $\Lambda = (\lambda_1,\cdots,\lambda_m) \in F_q^{\ m}$. Then

$$W_g(\Lambda) = \sum_{(x_1,\cdots,x_m)\in F_q^{\ m}} (-1)^{\mathrm{Tr}(\lambda_1 x_1+\cdots+\lambda_m x_m)+f(Q(x_1,\cdots,x_m))} .$$

By applying an invertible affine transformation on $(x_1,x_2,\cdots,x_m)$ ([38]), $\lambda_1 x_1+\cdots+\lambda_m x_m$ and $Q(x_1,\cdots,x_m)$ can be transformed into $d_1 x_1+\cdots+d_m x_m+d_0$ and $Q'(x_1,\cdots,x_m)+c_0$, respectively, where $Q'(x_1,\cdots,x_m)$ is of one of the following (pairwisely affinely non-equivalent) forms:

i) $x_1x_2+x_3x_4+\cdots+x_{2t-1}x_{2t}$ $(t \ge 1)$;

ii) $x_1x_2+x_3x_4+\cdots+x_{2t-1}x_{2t}+x_{2t+1}$ $(t \ge 1)$;

iii) $x_1x_2+x_3x_4+\cdots+x_{2t-1}x_{2t}+x_{2t+1}^2$ $(t \ge 0)$;

iv) $x_1x_2+x_3x_4+\cdots+x_{2t-3}x_{2t-2}+x_{2t-1}^2+x_{2t}$ $(t \ge 1)$;

v) $x_1x_2+x_3x_4+\cdots+x_{2t-1}x_{2t}+x_{2t+1}^2+x_{2t+1}$ $(t \ge 0)$;

vi) $(x_1x_2+x_3x_4+\cdots+x_{2t-1}x_{2t})+\alpha x_{2t-1}^2+\alpha x_{2t}^2$ $(t \ge 1)$;

vii) $(x_1x_2+x_3x_4+\cdots+x_{2t-1}x_{2t})+\alpha x_{2t-1}^2+\alpha x_{2t}^2+x_{2t+1}$ $(t \ge 1)$,

where $\alpha \in F_q$ satisfies $\mathrm{Tr}(\alpha)=1$. Since Q is balanced, so is Q'. By Lemma 3 in Appendix, $Q'(x_1,\cdots,x_m)$ should be one of Cases ii), iii), iv), and vii).

We have

$$W_g(\Lambda) = (-1)^{\mathrm{Tr}(d_0)} \sum_{(x_1,\cdots,x_m)\in F_q^{\ m}} (-1)^{\mathrm{Tr}(d_1x_1+\cdots+d_mx_m)+f(Q'(x_1,\cdots,x_m)+c_0)}$$

If $\Lambda = (\lambda_1,\cdots,\lambda_m) = (0,\cdots,0)$, then $(d_1,\cdots,d_m) = (0,\cdots,0)$, and

$$\begin{aligned} W_g(\Lambda) &= (-1)^{\mathrm{Tr}(d_0)} \sum_{(x_1,\cdots,x_m)\in F_q^{\ m}} (-1)^{f(Q'(x_1,\cdots,x_m)+c_0)} \\ &= (-1)^{\mathrm{Tr}(d_0)} q^{m-1} \sum_{z\in F_q} (-1)^{f(z+c_0)} = 0 \end{aligned}$$

since f and Q' are balanced. By Lemma 1, g is balanced. Below we assume that

$\Lambda=(\lambda_1,\cdots,\lambda_m)\neq(0,\cdots,0)$ and $(d_1,\cdots,d_m)\neq(0,\cdots,0)$. For $y,z\in F_q$, let $\delta_{y,z}$ be the number of $(x_1,\cdots,x_m)\in F_q{}^m$ satisfying both that $d_1x_1+\cdots+d_mx_m=y$ and $Q'(x_1,\cdots,x_m)=z$. Then

$$W_g(\Lambda)=(-1)^{\mathrm{Tr}(d_0)}\sum_{y,z\in F_q}\delta_{y,z}(-1)^{\mathrm{Tr}(y)}(-1)^{f(z+c_0)}.$$

Now we need the following lemma.

Lemma 2: For a fixed $\Lambda\neq 0$,

(a) If $\delta_{y,z}$ is independent on y, then $W_g(\Lambda)=0$.

(b) Assume there exist integers N_1,N_2,d,d', independent on y and z, such that

$$\delta_{y,z}=\begin{cases}N_1+N_2 & \text{if } y=dz+d'\\ N_1 & \text{if } y\neq dz+d'\end{cases}$$

Then $W_g(\Lambda)=\pm N_2W_f(d)$.

(c) Assume there exist integers N_1,N_2,d,d', independent on y and z, such that

$$\delta_{y,z}=\begin{cases}N_1+N_2 & \text{if } y=d\sqrt{z}+d'\\ N_1 & \text{if } y\neq d\sqrt{z}+d'\end{cases}$$

Then $W_g(\Lambda)=\pm N_2W_f(d^2)$.

(d) For any constant N,

$$W_g(\Lambda)=(-1)^{\mathrm{Tr}(d_0)}\sum_{y,z\in F_q}(\delta_{y,z}-N)(-1)^{\mathrm{Tr}(y)}(-1)^{f(z+c_0)}.$$

Proof. We use the fact that $\sum_{y\in F_q}(-1)^{\mathrm{Tr}(y)}=0$. So, (d) is trivial.

(a) We have

$$W_g(\Lambda)=(-1)^{\mathrm{Tr}(d_0)}\sum_{z\in F_q}\delta_{y,z}(-1)^{f(z+c_0)}\sum_{y\in F_q}(-1)^{\mathrm{Tr}(y)}=0.$$

(b) We have

$$\begin{aligned}W_g(\Lambda)&=(-1)^{\mathrm{Tr}(d_0)}\sum_{\substack{y,z\in F_q\\ y=dz+d'}}N_2(-1)^{\mathrm{Tr}(y)}(-1)^{f(z+c_0)}\\ &=(-1)^{\mathrm{Tr}(d_0)}\sum_{z\in F_q}N_2(-1)^{\mathrm{Tr}(dz+d')}(-1)^{f(z+c_0)}\\ &=(-1)^{\mathrm{Tr}(d_0)}\sum_{z\in F_q}N_2(-1)^{\mathrm{Tr}(dz-dc_0+d')}(-1)^{f(z)}\\ &=(-1)^{\mathrm{Tr}(d_0-dc_0+d')}N_2W_f(d).\end{aligned}$$

(c) Similarly as (b), we have

$$\begin{aligned} W_g(\Lambda) &= (-1)^{\mathrm{Tr}(d_0-dc_0+d')}\sum_{z\in F_q} N_2(-1)^{\mathrm{Tr}(d\sqrt{z})}(-1)^{f(z)} \\ &= (-1)^{\mathrm{Tr}(d_0-dc_0+d')}\sum_{z\in F_q} N_2(-1)^{\mathrm{Tr}(d^2 z)}(-1)^{f(z)} \\ &= (-1)^{\mathrm{Tr}(d_0-dc_0+d')}W_f(d^2). \end{aligned}$$

Continue the proof of Theorem 1. Note that $\delta_{y,z}$ is the number of the solutions $(x_1,\cdots,x_m)\in F_q{}^m$ of the system of equations

$$\begin{cases} d_1x_1+\cdots+d_mx_m = y & (1) \\ Q'(x_1,\cdots,x_m)=z & (2) \end{cases}$$

Let $x_1,\cdots,x_u$ be the all variables which appear in the expression of $Q'(x_1,\cdots,x_m)$, that is, $u=2t$ for iv), and $u=2t+1$ for ii), iii), and vii). If there exists a subscript $i>u$ such that $d_i\neq 0$, then by taking values of $x_1,\cdots,x_u$ satisfying (2), arbitrarily taking values for $x_{u+1},x_{u+2},\cdots,x_{i-1},x_{i+1},x_{i+2},\cdots,x_m$ and then taking a uniquely determined value for x_i to make (1) holds, we are easy to know that $\delta_{y,z}$ is equal to the product of q^{m-u-1} and the number of solutions $(x_1,x_2,\cdots,x_u)$ of Equation (2), and $\delta_{y,z}$ is independent on y. Thus, by Lemma 2 (a), $W_g(\Lambda)=0$.

Below we assume that $d_{u+1}=\cdots=d_m=0$. Then the system of equations (1) and (2) is degenerately on the variables $x_1,x_2,\cdots,x_u$. Let $\delta'_{y,z}$ be the number of the solutions $(x_1,\cdots,x_u)\in F_q{}^u$ of this degenerated system of equations, then $\delta_{y,z}=q^{m-u}\delta'_{y,z}$.

If $d_u=0$, then by taking values of $x_1,x_2,\cdots,x_{u-1}$ satisfying (1) and taking a uniquely determined value of x_u satisfying (2), we have $\delta'_{y,z}=q^{u-2}$ and $\delta_{y,z}=q^{m-2}$, then by Lemma 2 (a) again, $W_g(\Lambda)=0$.

Assume $d_u\neq 0$. Then

$$x_u = c_1x_1+\cdots+c_{u-1}x_{u-1}+y/d_u,$$

where $c_i = d_i / d_u$. Replacing x_u in (2) by $c_1 x_1 + \cdots + c_{u-1} x_{u-1} + y / d_u$, the degenerated system of equations becomes a single equation on variables $x_1, x_2, \cdots, x_{u-1}$, which has a form of one of the following:

$$\sum_{i=1}^{t} x'_{2i-1}\, x'_{2i} = z + y / d_u + \sum_{i=1}^{t} c_{2i-1} c_{2i} \tag{3}$$

$$\sum_{i=1}^{t} (x_{2i-1} x_{2i} + c_{2i-1}{}^2 x_{2i}{}^2 + c_{2i}{}^2 x_{2i}{}^2) = z + (y / d_u)^2 \tag{4}$$

$$\sum_{i=1}^{t-1} x'_{2i-1}\, x'_{2i} + x^2_{2t-1} + c_{2t-1} x_{2t-1} = z + y / d_u + \sum_{i=1}^{t-1} c_{2i-1} c_{2i} \tag{5}$$

$$\sum_{i=1}^{t} x'_{2i-1}\, x'_{2i} + \alpha x'^2_{2t-1} + \alpha x'^2_{2t} = z + y / d_u + \alpha c^2_{2t-1} + \alpha c^2_{2t} + \sum_{i=1}^{t} c_{2i-1} c_{2i} \tag{6}$$

corresponding to Cases ii), iii), iv), and vii), respectively, where $x'_{2i-1} = x_{2i-1} + c_{2i}$ and $x'_{2i} = x_{2i} + c_{2i-1}$ ($1 \le i \le t$) in (3), (5), and (6).

For Case ii), by Lemma 3 in Appendix,

$$\delta'_{y,z} = \begin{cases} q^{2t-1} - q^{t-1} + q^{t} & \text{if } z + y / d_u = \sum_{i=1}^{t} c_{2i-1} c_{2i} \\ q^{2t-1} - q^{t-1} & \text{if } z + y / d_u \ne \sum_{i=1}^{t} c_{2i-1} c_{2i} \end{cases}$$

and by Lemma 2 (b), $W_g(\Lambda) = \pm q^{m-2t-1} q^{t} W_f(d_u) = \pm q^{m-t-1} W_f(d_u)$.

For Case iii), by Lemma 4 in Appendix,

$$\delta'_{y,z} = \begin{cases} q^{2t-1} \pm q^{t-1} \mp q^{t} & \text{if } z + (y / d_u)^2 = 0 \\ q^{2t-1} \pm q^{t-1} & \text{if } z + (y / d_u)^2 \ne 0 \end{cases}$$

and by Lemma 2(c), $W_g(\Lambda) = \pm q^{m-2t-1} q^{t} W_f(d'') = \pm q^{m-t-1} W_f(d'')$.

For Case iv), if $c_{2t-1} = 0$ then $\delta'_{y,z} = q^{2t-2}$ and $W_g(\Lambda) = 0$ by Lemma 2(a). Suppose $c_{2t-1} \ne 0$. Replacing x'_i by $c_{2t-1} x''_i$ ($1 \le i \le 2t-2$) and replacing x'_{2t-1} by $c_{2t-1} x''_{2t-1}$, (5) become

$$\sum_{i=1}^{t-1} x''_{2i-1}\, x''_{2i} + x''^2_{2t-1} + x''_{2t-1} = (z + y / d_u + \sum_{i=1}^{t-1} c_{2i-1} c_{2i}) / c^2{}_{2t-1}.$$

By Lemma 3, we have

$$\delta'_{y,z} = q^{2t-2} + q^{t-1}(-1)^{\mathrm{Tr}(a)} \ , \ \delta_{y,z} = q^{m-2} + q^{m-t-1}(-1)^{\mathrm{Tr}(a)} \ ,$$

where $a = (z + y/d_u + \sum_{i=1}^{t-1} c_{2i-1}c_{2i})/c^2{}_{2t-1}$. By Lemma 2(d),

$$W_g(\Lambda) = \pm q^{m-t-1} \sum_{y,z\in F_q} (-1)^{\mathrm{Tr}(y+a)}(-1)^{f(z+c_0)}$$

$$= \begin{cases} 0 & \text{if } d_u c^2{}_{2t-1} \neq 1 \\ \pm q^{m-t} W_f(c_{2t-1}{}^{-2}) & \text{if } d_u c^2{}_{2t-1} = 1 \end{cases}$$

For Case vii), by Lemma 3,

$$\delta'_{y,z} = \begin{cases} q^{2t-1} - q^{t-1} + q^t & \text{if } z + y/d_u = \alpha c_{2t-1}^2 + \alpha c_{2t}^2 + \sum_{i=1}^{t} c_{2i-1}c_{2i} \\ q^{2t-1} - q^{t-1} & \text{otherwise} \end{cases}$$

and by Lemma 2(b) again, $W_g(\Lambda) = \pm q^{m-2t-1} q^t W_f(d_u) = \pm q^{m-t-1} W_f(d_u)$. This completes the proof.

Remark 2: (1) As noted in Introduction, our proof technique is direct and is based on enumeration of solutions of quadratic forms over a finite field. Khoo et al. prove their conclusion by using a result on crosscorrelation of sequences.

(2) Our result is different with that of Khoo et al. in three aspects: a) The quadratic form used in [1] is $\mathrm{Tr}_{q^m/q}(x^{q^k+1})$, where $\mathrm{Tr}_{q^m/q}$ is the trace map from F_{q^m} to F_q. The form is homogeneous, and is special among homogeneous forms, while the form in our construction is any (balanced) and may be not homogeneous; b) The index m in [1] is assumed to be odd, while in ours m can be even; c) The quadratic form used in [1,17] is non-degenerate and is equivalent to only one case, Case iii) in Theorem 1, while ours can be any balanced form.

Corollary 1: Assume f and $Q(x_1,\cdots,x_m)$ are balanced and Q is non-degenerate. Then the spectrum set of $f(Q(x_1,\cdots,x_m))$ is $\{\pm q^{[m/2]} W_f(\lambda) : \lambda \in F_q\}$.

Corollary 2: Assume f is balanced and the spectra of f are 3-valued: 0 and $\pm 2^{(n+l)/2}$, where l is an integer satisfying $l \geq 1$ and $l = n(\mathrm{mod}\, 2)$, and assume $Q(x_1,\cdots,x_m)$ is balanced and non-degenerate. Then the spectra of $f(Q(x_1,\cdots,x_m))$ are also 3-valued: 0 and $\pm 2^{[m/2]n+(n+l)/2}$. Furthermore, if m is odd, then the nonzero spectrum values of $f(Q(x_1,\cdots,x_m))$ are $\pm 2^{(nm+l)/2}$, and consequently, $f(Q(x_1,\cdots,x_m))$ is near-bent if and only if also is f ; while if m is even, the nonzero spectrum values are $\pm 2^{(nm+n+l)/2}$.

Remark 3: When m is even, $f(Q(x_1,\cdots,x_m))$ can't be a near-bent function. It is an interesting phenomenon that in study of bent-like functions, we usually obtain better conclusion in the case of m being odd than that of m being even.

Theorem 2: Assume $m \geq 2$. Then $\deg f(Q(x_1,\cdots,x_m)) = 2\deg(f)$.

Proof. Let $\{\gamma_1,\cdots,\gamma_m\}$ be a basis of the field F_{q^m} over F_q . Let $f(x) = \sum_{s=0}^{q-1} a_s x^s$ be the polynomial expression of f . Set $X = x_1\gamma_1 + \cdots + x_m\gamma_m$. Since $Q(x_1,\cdots,x_m)$ is quadratic, it can be written as $Q(x_1,\cdots,x_m) = \sum_{t\in S} c_t X^t$, where

$$S = \{0, q^u, q^v + q^{v+w} : 0 \leq u < m, 0 \leq v < v+w < m\},$$

and there exists a subscript t of the form $q^v + q^{v+w}$ such that $c_t \neq 0$.

Let $s = 2^{s_1} + \cdots + 2^{s_u}$ be the binary expression of s , $1 \leq s < 2^n$, $0 \leq s_1 < \cdots < s_u < n$. Then

$$\begin{aligned} f(Q(x_1,\cdots,x_m)) &= \sum_{s=0}^{q-1} a_s (\sum_t c_t X^t)^s \\ &= a_0 + \sum_{s=1}^{q-1} a_s \sum_{t_1\in S}\cdots\sum_{t_u\in S} c_{t_1}{}^{2^{s_1}} \cdots c_{t_u}{}^{2^{s_u}} X^{2^{s_1}t_1+\cdots+2^{s_u}t_u} \end{aligned}$$

It is easy to show that if $2^{s_1}t_1 + \cdots + 2^{s_u}t_u = 2^{s_1'}t_1' + \cdots + 2^{s_v'}t_v'$, then $s = s'$, $u = v$, and $(t_1,\cdots,t_u) = (t_1',\cdots,t_v')$, where $s' = 2^{s_1'} + \cdots + 2^{s_v'}$ is the binary expression of s' , $1 \leq s' < 2^n$, $0 \leq s_1' < \cdots < s_v' < n$, and also to show that $Wh_2(2^{s_1}t_1 + \cdots + 2^{s_u}t_u) = Wh_q(t_1) + \cdots + Wh_q(t_u)$, where $Wh_q(0) = 0$, $Wh_q(q^u) = 1$, and $Wh_q(q^u + q^{u+v}) = 2$. So,

$$\begin{aligned} \deg f(Q) = \max\{&Wh_q(t_1) + \cdots + Wh_q(t_u) : 1 \leq u = Wh_2(s) \leq \deg f, t_1,\cdots,t_u \in S\} \\ &= 2\deg f. \end{aligned}$$

4 Recursively composed bent-like functions

Similar as the construction of cascaded GMW sequences ([17]), we recursively compose bent-like functions in this section.

Set $q_0 = q = 2^n$, $q_i = q_{i-1}^{m_i}$, $1 \le i \le l.$ Let $g_0 : F_q \to F_2$ be an n-variable Boolean function, and $Q_i(x_1, \cdots, x_{m_i}) : F_{q_i} \to F_{q_{i-1}}$ be an m_i-variable quadratic form over $F_{q_{i-1}}$. Define recursively the functions

$$g_i(x) = g_{i-1}(Q_i(x_1, \cdots, x_{m_i})), 1 \le i \le l.$$

By Theorems 1-2 and Corollary 2 we have

Corollary 3: Assume f and $Q_i(x_1, \cdots, x_{m_i})$ with $m_i \ge 2$ are balanced.

(i) g_l is balanced, and $\deg g_l = 2^l \deg f$.

(ii) The spectra of g_l take the values 0 and $\pm q_0^{e_1} q_1^{e_2} \cdots q_{l-1}^{e_l} W_f(\lambda)$, $\lambda \in F_q^*$, where $e_i \ge [m_i / 2]$ is an integer depending only on $Q_i(x_1, \cdots, x_{m_i})$.

(iii) Assume all Q_i are non-degenerate. Then the spectra of g_l take the values 0 and $\pm q_0^{[m_1/2]} q_1^{[m_2/2]} \cdots q_{l-1}^{[m_l/2]} W_f(\lambda)$, where $\lambda \in F_q^*$. In particular, when all $m_i (1 \le i \le l)$ are odd, the spectra of g_l take values 0 and $\pm q^{\frac{m_1 m_2 \cdots m_l - 1}{2}} W_f(\lambda)$, $\lambda \in F_q^*$. Furthermore, if f is near-bent, then also is g_l.

5 A generalization to p-ary bent-like functions

In this section we assume p is odd and generalize the above results to p-ary bent-like functions. First, we show that any quadratic polynomial $h(x_1, \cdots, x_n)$ over F_p is bent-like. The similar result is well known for $p = 2$. Further, we characterize when $h(x_1, \cdots, x_n)$ is bent or near-bent. Second, we show that a composition of a bent-like function and a quadratic form is also bent-like, and as a consequence, there is also a GMW-like construction of bent-like functions for odd p. These are a generalization of the results in Sections 3-4. The proof is similar as Theorem 1. Some proof details will be omitted.

Theorem 3: Let p be odd and $h(x_1,\cdots,x_n)$ be an n-variable quadratic form over F_p. Then

(i) $h(x_1,\cdots,x_n)$ is always bent-like.

(ii) Assume $h(x_1,\cdots,x_n)$ is affinely equivalent to a r-variable non-degenerate quadratic form. Then the nonzero value of $|W_h(\lambda)|$ is either $p^{(2n-r)/2}$ or $p^{(2n-r+1)/2}$.

(iii) $h(x_1,\cdots,x_n)$ is bent if and only if it is equivalent to $\sum_{i=1}^{n-1} x_i^2 + cx_n^2 + c_0$, where $c \in F_q{}^*$, $c_0 \in F_q$.

(iv) If $h(x_1,\cdots,x_n)$ is homogeneous, then the nonzero value of $|W_h(\lambda)|$ is $p^{(2n-r)/2}$, and $h(x_1,\cdots,x_n)$ is bent and near-bent if and only if $r = n$ and $n-1$, respectively.

Proof. Let $x = (x_1,\cdots,x_n)$ denote a row vector. There are an $n \times n$ matrix A, a column vector B and a $c \in F_p$ such that $h(x_1,\cdots,x_n) = xAx^t + xB + c$, where x^t denotes the transpose of x. Then for $\lambda = (\lambda_1,\cdots,\lambda_n) \in F_p{}^n$,

$$\begin{aligned}
|W_h(\lambda)|^2 &= \sum_{x,y\in F_p{}^n} \omega^{\lambda\cdot x - h(x)} \omega^{h(y)-\lambda\cdot y} \\
&= \sum_{x,z\in F_p{}^n} \omega^{\lambda\cdot x - h(x) + h(x+z) - \lambda\cdot(x+z)} \\
&= \sum_{z\in F_p{}^n} \omega^{h(z)-\lambda\cdot z} \sum_{x\in F_p{}^n} \omega^{h(x+z)-h(x)-h(z)} \\
&= \sum_{z\in F_p{}^n} \omega^{h(z)-\lambda\cdot z - c} \sum_{x\in F_p{}^n} \omega^{z(A+A^t)x^t}
\end{aligned}$$

Let $V = \{z \in F_p{}^n : z(A + A^t) = 0\}$ and $\dim_{F_p} V = s$. Since $\sum_{x\in F_p{}^n} \omega^{zx^t} = 0$ for $0 \neq z \in F_p{}^n$, we have

$$|W_h(\lambda)|^2 = p^n \sum_{z\in V} \omega^{h(z)-\lambda\cdot z - c} \quad .$$

$h(x) - c$ is a linear function on V since $h(x+z) - h(x) - h(z) - c = z(A + A^t)z^t = 0$, and so, $\sum_{z\in V} \omega^{h(z)-\lambda\cdot z-c} = p^s$ or 0. Thus, $|W_h(\lambda)| = p^{(n+s)/2}$ or 0, and $h(x_1, x_2,\cdots,x_n)$ is bent-like.

By applying an invertible affine transformation over F_p on $(x_1,\cdots,x_n)$ ([38]), $h(x_1,\cdots,x_n)$ is transformed into $h'(x_1,\cdots,x_n)+c_0$, where $h'(x_1,\cdots,x_n)$ is of one of the following (pairwisely affinely non-equivalent) forms:

i) $\sum_{i=1}^{r} x_i^2$ $(1 \le r \le n)$;

ii) $\sum_{i=1}^{r-1} x_i^2 + z_0 x_r^2$ (r being even and $2 \le r \le n$);

iii) $\sum_{i=1}^{r-1} x_i^2 + x_r$ $(2 \le r \le n)$;

iv) $\sum_{i=1}^{r-2} x_i^2 + z_0 x_{r-1}^2 + x_r$ (r being odd and $3 \le r \le n$),

where z_0 is a non-square element in F_q^*.

It is clear that $s = n-r$ for Cases i) and ii) and $s = n-r+1$ for Cases iii) and iv). So, the nonzero value of $|W_h(\lambda)|$ is $p^{(2n-r)/2}$ for Cases i) and ii) and is $p^{(2n-r+1)/2}$ for Cases iii) and iv). In the last two cases, $h(x_1,x_2,\cdots,x_n)$ is not bent. If $h(x_1,\cdots,x_n)$ is homogeneous, then we can easily show that $h'(x_1,\cdots,x_n)$ can't be of the form iii) or iv), and thus, it is one of the former two cases.

Remark 4: Given an n-variable quadratic form $h(x_1,\cdots,x_n)$ over F_p, we can transform $h(x_1,\cdots,x_n)$ to one of the standard forms in i)-iv) in Theorem 3 by a series of concrete elementary transformations ([38]), and so, it is easy to judge whether $h(x_1,\cdots,x_n)$ is bent or near-bent by Theorem 3. Conversely, from a proper standard form we can obtain a quadratic form with known r by using an affine transformation, especially, obtain a bent or near-bent quadratic form.

Theorem 4: Assume p is odd, f and $Q(x_1,\cdots,x_m)$ are balanced. Suppose $Q(x_1,\cdots,x_m)$ is affinely equivalent to a non-degenerate quadratic form with odd number of variables. Then the absolute values of the spectra of $f(Q(x_1,\cdots,x_m))$ take the values 0 and $q^d\,|W_f(\lambda)|$,

$\lambda \in F_q^*$, where d is an integer depending only on $Q(x_1,\cdots,x_m)$.

Proof. Suppose $Q(x_1,\cdots,x_m)$ is affinely equivalent to $Q'(x_1,\cdots,x_r)+c_0$ and $Q'(x_1,\cdots,x_r)$ is of one of the forms i)-iv) in Theorem 3. (Note that: Here $x_1,\cdots,x_m$ are variables taking their values in F_{p^n}.) Since $Q(x_1,\cdots,x_m)$ and $Q'(x_1,\cdots,x_r)$ are balanced, by Lemma 5 in Appendix, $Q'(x_1,\cdots,x_r)$ should be one of Cases iii) (r being odd) and iv). The remaining proof is highly similar as that of Theorem 1 and should use the enumeration results listed in Lemma 6 in Appendix. We omit the details of the proof.

Remark 5: Unlike in the case $p=2$, the number r of variables of the non-degenerate quadratic form equivalent to $Q(x_1,\cdots,x_m)$ should be assumed to be odd in Theorem 4. If r is even, the analogy result doesn't hold.

Corollary 4: Assume f and $Q(x_1,\cdots,x_m)$ are balanced, m is odd, and Q is non-degenerate. Then the absolute values of the spectra of $f(Q(x_1,x_2,\cdots,x_m))$ take the values $q^{[m/2]}|W_f(\lambda)|$ ($\lambda \in F_q$).

Corollary 5: Let $p>2$, $q_0=q=p^n$, $q_i=q_{i-1}^{m_i}$, m_i be odd, $1\le i\le l$. Assume $g_0:F_q\to F_p$ is balanced, and $Q_i(x_1,\cdots,x_{m_i}):F_{q_i}\to F_{q_{i-1}}$ is a balanced and non-degenerate quadratic form over $F_{q_{i-1}}$. For $1\le i\le l$, recursively define an $nm_1\cdots m_i$-variable function

$$g_i(x)=g_{i-1}(Q_i(x_1,\cdots,x_{m_i})),1\le i\le l.$$

Then g_l is balanced, and $|W_{g_l}(\Lambda)|$ ($\Lambda\in F_{q_l}$) is 0 or takes a value of the form $q^{\frac{m_1m_2\cdots m_l-1}{2}}|W_f(\lambda)|$, $\lambda\in F_q^*$. Furthermore, if g_0 is bent-like (or near-bent, respectively), then also is g_l.

The p-ary analogy of Theorem 2 doesn't hold in general. However, we can similarly prove the following

Theorem 5: Assume $m \geq 2$ and assume in the polynomial expression $\sum_{s=0}^{q-1} a_s x^s$ of f there is an s such that $Wh_p(s) = \deg f$ and $s = p^{s_1} + \cdots + p^{s_u}$, $1 \leq s < 2^n$, $0 \leq s_1 < \cdots < s_u < n$, then $\deg f(Q(x_1, \cdots, x_m)) = 2\deg(f)$.

Acknowledgement: This work is supported by the National Natural Science Foundation of China (90104034) and the High Technology Research and Development (863) Program of China (2002AA141020).

References

[1] K. Khoo and G. Gong, New constructions for resilient and highly nonlinear Boolean functions. CACR Technical Report, CORR 2003-11, 2003, available at http://www.cacr.math.uwaterloo.ca/.

[2] Matsui M. Linear cryptanalysis method for DES cipher. LNCS 765, Eurocrypt’93, 1994, 386-397.

[3] Leveiller S., Zemor G., Guillot P. and Boutros J. A new cryptanalytic attack for PN-generators filtered by a Boolean function. Proceedings of Selected Areas of Cryptography-SAC’2002, 2002.

[4] Hu L., Pei D.Y. and Feng D.G. Construction of a class of bent functions (in Chinese). Journal of the Graduate School of the Chinese Academy of Sciences, Vol.19, No.2, 2002, 103-106.

[5] Rothaus O. On bent functions. J. combin. Theory Ser. A, Vol. 20, 1976, 300-305.

[6] Dillion J. Elementary Hadamard difference sets. Ph.D. dissertation, Univ. Maryland, College Park, 1974.

[7] Carlet C. Generalized partial spreads. IEEE Trans. Inform. Theory, vol.41, No.5, 1995, 1482 –1487.

[8] Olsen J., Scholtz R. and Welch L. Bent-function sequences. IEEE Trans. Inform. Theory, vol.28, No.6, 1982, 858 –864.

[9] Lempel A. and Cohn M. Maximal families of bent sequences. IEEE Trans. Inform. Theory, vol.28, No.6, 1982, 865 –868.

[10] Kumar P. On bent sequences and generalized bent functions (Ph.D. thesis abstr.). IEEE Trans. Inform. Theory, vol.30, No.2, 1984, 450–450.

[11] No J.G., Gil M. and Shin D. Generalized construction of binary bent sequences with optimal correlation property. IEEE Trans. Inform. Theory, vol.49, No.7, 2002, 1769 –1780.

[12] Boztas S. and Kumar P.V. Binary sequences with Gold-like correlation but larger line span. IEEE Trans. Inform. Theory, vol.40, No.2, 1994, 532-537.

[13] Helleseth T. and Kumar P.V. Sequences with low cross correlation. Chapter in Handbook of Coding Theory, North-Holland, 1998.

[14] Khoo K. Gong G. and Stinson D.R. A new family of Gold-like sequences. IEEE International symposium on information theory’2002, 2002, 181.

[15] Khoo K. Gong G. and Stinson D.R. Sequences with low cross correlation. CACR Technical

Report, CORR 2003-01, 2003, available at http://www.cacr.math.uwaterloo.ca/.

[16] Carlet C. A larger class of cryptographic Boolean functions via a study of the Maiorana-Mcfarland Construction. LNCS 2442. Berlin: Springer-Verlag. 2002, 549-564.

[17] Klapper A., Chan A.H. and Goresky M. Cascaded GMW sequences. IEEE Trans. Inform. Theory. Vol. 39, No 1, 1993, 171-183.

[18] Kumar P.V., Schultz R.A. and Welch L.R. Generalized bent functions and their properties. J. combin. Theory Ser. A, Vol. 40, 1985, 90-107.

[19] Ersan A., Ismail S.G. and Masatoshi I. A note of generalized bent functions. Journal of Pure and Applied Algebra. Vol.106, No.1, 1996, 1-9.

[20] Pei D. On non-existence of generalized bent functions. In: LN in pure and applied math, Vol. 141. New York: Decker, 1993, 165-172.

[21] Feng K. Generalized bent functions and ideal class numbers of imaginary quadratic fields. Science in China (series A), Vol. 30, No. 6, 2000, 489-496.

[22] Ma Z., Liu F. and Feng K. New results on non-existence of generalized bent functions (II). Science in China (series A), Vol. 32, No. 1, 2002, 1-9.

[23] Klapper A., Chan A.H. and Goresky M. Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences. Discrete Applied Mathematics. 46 (1993), 1-20.

[24] McWilliams F.J. and Solane N.J. Theory of error-correcting codes. Amsterdam: North-Holland, 1977.

[25] Hecke E. Lecture on the theory of algebra numbers, Vol. 77, Graduate Texts in Mathematics. New York: Springer-Verlag, 1981.

[26] Cohen H. A course in computational algebraic number theory, Vol. 138, Graduate Texts in Mathematics, New York: Springer-Verlag, 1993.

[27] Zheng Y. and Zhang X.M. Relationship between Bent functions and complementary plateaued functions. LNCS 1787. 1999, 60-75.

[28] Zhang X.M. and Zheng Y. On Plateaued Functions. IEEE Trans. on Inform. Theory. Vol. 47, No. 3, 2001, 1215-1223.

[29] Gold R. Maximal Recursive Sequences with 3-valued Recursive Cross–Correlation Functions. IEEE Transactions on Information Theory, January 1968, 154–156.

[30] Kasami T. The weight enumerators for several classes of subcodes of second order binary Reed Muller codes. Information and Control. Vol.18, 1971, 369-394.

[31] Dillon J.F. Multiplicative difference sets via characters. Designs, Code and Cryptography. Vol.17, 1999, 225-235.

[32] Dillon J. and Dobbertin H. New cyclic difference sets with singer parameter. Finite Fields and their Applications, to appear.

[33] Gong G. and Youssef A.M. Cryptographic properties of the Welch-Gong transformation sequence generators. IEEE Trans. on Inform. Theory. Vol. 48, No. 11, 2002, 2837 –2846.

[34] Gong G., Khoo K., Additive autocorrelation of resilient Boolean functions, CACR Technical Report, CORR 2003-21, 2003, available at http://www.cacr.math.uwaterloo.ca/.

[35] Meier W. and Staffelbach O. Nonlinearity criteria for cryptographic functions. LNCS 434. Berlin: Springer-Verlag. 1990, 549-562.

[36] Patterson N.J. and Wiedemann D.H. The covering radius of the $(2^{15},16)$ Reed-Muller code

is at less 16276. IEEE Trans. on Inform. Theory. Vol. IT-29, 1983, 354–356.

[37] Maitra S. and Sarkar P. Modifications of Patterson-Wiedemann functions for cryptographic applications. IEEE Trans. on Inform. Theory. Vol. 48, No. 1, 2002, 278 –284.

[38] Wan Z.X. Geometry of classical groups over finite fields. Bromley: Chartwell-Bratt Ltd， 1993.

[39] Cohen E. Linear and quadratic equations in a Galois field with applications to geometry. Duke. Math. J. Vol. 32, 1965, 633-641.

Appendix: Number of solutions of quadratic forms

Define a function v on F_q as $v(0)=q-1$ and $v(a)=-1$ for any $0\neq a\in F_q$. For $p=2$, we have

Lemma 3 ([38]): Let $Q'(x_1,\cdots,x_u)$ is a quadratic form of one of the forms i)-vii) in Theorem 1, $u=2t$ for i), iv), and vi); and $u=2t+1$ for other 4 cases. Then as an equation of $x_1,x_2,\cdots,x_u$, then numbers ρ_z of solutions of $Q'(x_1,\cdots,x_u)=z$ is $q^{2t-1}+q^{t-1}v(z)$, q^{2t}, q^{2t}, q^{2t-1}, $q^{2t}+q^t(-1)^{Tr(z)}$, $q^{2t-1}-q^{t-1}v(z)$, and q^{2t}, respectively.

Proof. This lemma is proved in [38] for $z=0$. It holds trivially for Cases ii), iii), iv), and vii). For Cases i) and vi), it is easy to check the validation of the lemma by the fact that $Q'(x_1,\cdots,x_u)$ is homogeneous. For Case v), the number is

$$\sum_{c_1,\cdots,c_t\in F_q} n_1(c_1)n_2(c_2)\cdots n_t(c_t)(1+(-1)^{\mathrm{Tr}(c_1+\cdots+c_t+z)})$$

since the number of solutions of the univariable equation ${x^2}_{2t+1}+x_{2t+1}=c_1+\cdots+c_t+z$ is $1+(-1)^{\mathrm{Tr}(c_1+\cdots+c_t+z)}$, where $n_i(c_i)=q+v(c_i)$ is the number of solutions of the equation $x_{2i-1}x_{2i}=c_i$ of two variables. So,

$$\begin{aligned}
&\sum_{c_1,\cdots,c_t\in F_q} n_1(c_1)n_2(c_2)\cdots n_t(c_t)(1+(-1)^{\mathrm{Tr}(c_1+\cdots+c_t+z)})\\
&=\sum_{c_1,\cdots,c_t\in F_q} n_1(c_1)n_2(c_2)\cdots n_t(c_t)+\sum_{c_1,\cdots,c_t\in F_q} n_1(c_1)n_2(c_2)\cdots n_t(c_t)(-1)^{\mathrm{Tr}(c_1+\cdots+c_t+z)}\\
&=\left(\sum_{c_1\in F_q} n_1(c_1)\right)^t+(-1)^{\mathrm{Tr}(z)}\left(\sum_{c_1\in F_q} n_1(c_1)(-1)^{\mathrm{Tr}(c_1)}\right)^t\\
&=q^{2t}+(-1)^{\mathrm{Tr}(z)}q^t
\end{aligned}$$

where we use the facts that $\sum_{c_1\in F} n_1(c_1) = q^2$ and $\sum_{c_1\in F} n_1(c_1)(-1)^{Tr(c_1)} = q$.

Lemma 4: Let $c_1, c_2, \cdots, c_{2t}, z \in F_q$. Then the number of solutions of $2t$-variables equations $\sum_{i=1}^{t}(x_{2i-1}x_{2i} + c_{2i-1}x_{2i-1}^2 + c_{2i}x_{2i}^2) = z$ is $q^{2t-1} + q^{t-1}v(z)(-1)^{Tr(c_1c_2+c_3c_4+\cdots+c_{2t-1}c_{2t})}$.

Proof: If the lemma is proved for $z = 0$, then it is easy to check the validation of the lemma for nonzero z by the fact that the left side of the equation is homogeneous. Assume $z = 0$. First we prove the case of $t = 1$.

If $c_1c_2 = 0$, then by an appropriate invertible linear transformation on x_1 and x_2, the equation $x_1x_2 + c_1x_1^2 + c_2x_2^2 = 0$ is transformed to $x_1'x_2' = 0$, which has $2q - 1 = q + v(0)$ solutions. If $c_1c_2 \neq 0$, then the equation $x_1x_2 + c_1x_1^2 + c_2x_2^2 = 0$ always has a full-zero solution. For its nonzero solution, replacing x_1 by c_2x_1, then the equation can be written as $c_1c_2 + x_2/x_1 + (x_2/x_1)^2 = 0$, which has solutions (two different solutions) if and only if $Tr(c_1c_2) = 0$, that is, it has $1 + (-1)^{Tr(c_1c_2)}$ solutions for the variable x_2/x_1. So, the equation $x_1x_2 + c_1x_1^2 + c_2x_2^2 = 0$ has

$$1 + (q-1)(1 + (-1)^{Tr(c_1c_2)}) = q + (-1)^{Tr(c_1c_2)}v(0)$$

solutions.

For general t, we prove the lemma by induction. Assume the lemma in all cases for less than t. Let $N_t(z)$ and $n_t(z)$ be number of solutions of $\sum_{i=1}^{t}(x_{2i-1}x_{2i} + c_{2i-1}x_{2i-1}^2 + c_{2i}x_{2i}^2) = z$ and $x_{2t-1}x_{2t} + c_{2t-1}x_{2t-1}^2 + c_{2t}x_{2t}^2 = z$, respectively. Then the number of solutions of $\sum_{i=1}^{t}(x_{2i-1}x_{2i} + c_{2i-1}x_{2i-1}^2 + c_{2i}x_{2i}^2) = 0$ is equal to

$$\begin{aligned}
&N_{t-1}(0)n_t(0) + \sum_{0\neq a\in F_q} N_{t-1}(a)n_t(a)\\
&= N_{t-1}(0)n_t(0) + (q-1)N_{t-1}(1)n_t(1)\\
&= (q^{2t-3} + q^{t-2}(-1)^{Tr(c_1c_2+c_3c_4+\cdots+c_{2t-3}c_{2t-2})}(q-1)) \cdot (q + (-1)^{Tr(c_{2t-1}c_{2t})}(q-1))\\
&\quad + (q-1)(q^{2t-3} - (-1)^{Tr(c_1c_2+c_3c_4+\cdots+c_{2t-3}c_{2t-2})}q^{t-2}) \cdot (q - (-1)^{Tr(c_{2t-1}c_{2t})})\\
&= q^{2t-1} + q^{t-1}(q-1)(-1)^{Tr(c_1c_2+c_3c_4+\cdots+c_{2t-1}c_{2t})}
\end{aligned}$$

The lemma is proved.

For the case of $p>2$, define a function ε on F_q as $\varepsilon(0)=0$, $\varepsilon(a)=1$ for any $0\neq a\in F_q^{*2}$ and $\varepsilon(a)=-1$ for any $a\notin F_q^{*2}$.

Lemma 5 ([38]): Let $Q'(x_1,\cdots,x_r)$ be a quadratic form over $F_q=F_{p^n}$ of one of the forms i)-iv) in Theorem 3. Let F_q^{*2} denote the set of square elements of F_q^*. Denote numbers of solutions of $Q'(x_1,\cdots,x_r)=z$ by ρ_z. If r is odd, then

(1) Q' is of the form i). If $-1\notin F_q^{*2}$ and $n\equiv 1(\bmod 4)$, then ρ_z is $q^{r-1}-q^{\frac{r-1}{2}}\varepsilon(-z)$. If $n\equiv 3(\bmod 4)$ or $-1\in F_q^{*2}$, then ρ_z is $q^{r-1}+q^{\frac{r-1}{2}}\varepsilon(-z)$.

(2) Q' is of the form iii) or iv), ρ_z is q^{r-1}.

If r is even then

(1) Q' is of the form i). If $(-1)^{\frac{r}{2}}\in F_q^{*2}$, ρ_z is $q^{r-1}+q^{\frac{r}{2}-1}v(z)$. If $(-1)^{\frac{r}{2}}\notin F_q^{*2}$, ρ_z is $q^{r-1}-q^{\frac{r}{2}-1}v(z)$.

(2) Q' is of the form ii). If $(-1)^{\frac{r}{2}}\in F_q^{*2}$, ρ_z is $q^{r-1}-q^{\frac{r}{2}-1}v(z)$. If $(-1)^{\frac{r}{2}}\notin F_q^{*2}$, ρ_z is $q^{r-1}+q^{\frac{r}{2}-1}v(z)$.

(3) Q' is of the form iii), ρ_z is q^{r-1}.

Using Lemma 5 and a result in [39] we can prove the following Lemma 6. The details are omitted.

Lemma 6: Let $Q'(x_1,\cdots,x_r)$ be as in Lemma 5, $r\leq m$. Let $\delta_{y,z}$ be the number of $(x_1,\cdots,x_m)\in F_q{}^m$ satisfying both that $d_1x_1+\cdots+d_mx_m=y$ and $Q'(x_1,\cdots,x_r)=z$. If r is odd then

(1) Q' is of the form i). Let $\beta=\sum_{j=1}^{r}d_j^2$, $\gamma=y^2-z\beta$, then $\delta_{y,z}$ is q^{m-2}, $q^{m-2}\pm\varepsilon(-z)q^{m-\frac{r+3}{2}}$, $q^{m-2}+q^{m-\frac{r+3}{2}}v(\gamma)\varepsilon((-1)^{\frac{r-1}{2}}\beta)$, or $q^{m-2}+q^{m-\frac{r+1}{2}}\varepsilon((-1)^{\frac{r-1}{2}}z)$.

(2) Q' is of the form iii). Then $\delta_{y,z}$ is q^{m-2} or

$$q^{m-2} \pm q^{m-\frac{r+3}{2}} v(z - y/d_r - \sum_{j=1}^{r-1} d_j^2 / 4d_r^2) .$$

(3) Q' is of the form iv). Then $\delta_{y,z}$ is q^{m-2} or

$$q^{m-2} \pm q^{m-\frac{r+3}{2}} v(z - y/d_r - \sum_{j=1}^{r-2} d_j^2 / 4d_r^2 - z_0 d_{r-1}^2 / 4d_r^2) .$$

If r is even then

(1) Q' is of the form i). Let $\beta = \sum_{j=1}^{r} d_j^2$, $\gamma = y^2 - z\beta$, then $\delta_{y,z}$ is q^{m-2} ,

$q^{m-2} \pm v(z) q^{m-\frac{r}{2}-2}$, $q^{m-2} + q^{m-\frac{r}{2}-1} \varepsilon((-1)^{\frac{r}{2}} \gamma)$, or $q^{m-2} + q^{m-\frac{r}{2}-1} v(z) \varepsilon((-1)^{\frac{r}{2}})$.

(2) Q' is of the form ii). Let $\beta = \sum_{j=1}^{r-1} d_j^2 + \frac{d_r^2}{z_0}$, $\gamma = y^2 - z\beta$, Then $\delta_{y,z}$ is q^{m-2} ,

$q^{m-2} + q^{m-\frac{r}{2}-1} \varepsilon((-1)^{\frac{r}{2}} z_0 \gamma)$, or $q^{m-2} + q^{m-\frac{r}{2}-1} v(z) \varepsilon((-1)^{\frac{r}{2}})$.

(3) Q' is of the form iii). Then $\delta_{y,z}$ is q^{m-2} or

$$q^{m-2} \pm q^{m-\frac{r}{2}-1} \varepsilon(y/d_r + \sum_{j=1}^{r-1} d_j^2 / 4d_r^2 - z) .$$