On p-ary Bent Functions Defined on Finite Fields [1]

*Young-Sik Kim [O], *Ji-Woong Jang, *Jong-Seon No and **Tor Helleseth
*School of Electrical Engineering and Computer Science, Seoul National University
**Department of Informatics, University of Bergen
Email: jsno@snu.ac.kr

Abstract

It is known that a bent function corresponds to a perfect nonlinear function, which makes it difficult to do the differential cryptanalysis in DES and in many other block ciphers. In this paper, for an odd prime p, quadratic p-ary bent functions defined on finite fields are given from the families of p-ary sequences with optimal correlation property. And quadratic p-ary bent functions, that is, perfect nonlinear functions from the finite field F_{p^m} to its prime field F_p are constructed by using the trace functions.

1. Introduction

Rothaus introduced bent functions defined on the m-tuple binary vector space into $\{0,1\}$ [14]. A Boolean function defined on the m-tuple binary vector space becomes a bent function if its Fourier coefficients only take the values $+1$ or -1, which corresponds to the maximum Hamming distance from the linear Boolean functions. From the good Fourier transform properties, they have been used in the many areas such as cryptology, constructions of families of binary sequences with optimal correlation property [13], and error correcting codes.

A function from F_{q^m} to F_q is called a *perfect nonlinear function* if the number of solutions $x \in F_{q^m}$ of $f(x+a) - f(x) = b$ for $a \in F_{q^m}^*, b \in F_q$ is exactly q^{m-1}. Dembowski and Ostrom introduced a *Dembowski-Ostrom polynomial* [2][3], which sometimes gives rise to a planar polynomial. Nyberg [11] introduced a mapping with differential k-uniformity, which is the important property for the differential cryptanalysis in DES and in many other block ciphers. He also proved that the perfect nonlinear function is bent[11]. Helleseth introduced the some power mappings with low differential uniformity[5][6] and many other highly nonlinear mappings are introduced by Carlet and Ding[1].

In this paper, for an odd prime p, quadratic p-ary bent functions defined on finite fields are given from the families of p-ary sequences with optimal correlation property. And quadratic p-ary bent functions, that is, perfect nonlinear functions from the finite field F_{p^m} to its prime field F_p are constructed by using the trace functions.

2. Preliminaries

Let z be an integer and V_z^m be an m-dimensional vector space over the set of integers modulo z, J_z. Let $\omega = e^{j\frac{2\pi}{z}}$, $j = \sqrt{-1}$. Let $f(\underline{x})$ be a function from V_z^m to J_z. The Fourier transform of $f(\underline{x})$ and its inverse transform are defined as

$$F(\underline{\lambda}) = \frac{1}{\sqrt{z^m}} \sum_{\underline{x} \in V_z^m} \omega^{f(\underline{x}) - \underline{\lambda}\cdot\underline{x}^T}, \quad \text{all } \underline{\lambda} \in V_z^m$$

$$\omega^{f(\underline{x})} = \frac{1}{\sqrt{z^m}} \sum_{\underline{\lambda} \in V_z^m} F(\underline{\lambda}) \cdot \omega^{\mathrm{tr}_1^m(\underline{\lambda}\cdot\underline{x}^T)}, \quad \text{all } \underline{x} \in V_z^m$$

where $\underline{x}^T$ denotes transpose of $\underline{x}$. Then a generalized bent function is defined as:

Definition 1 [Kumar, Scholtz, and Welch [8]] : A function $f(\underline{x})$ from V_z^m to J_z is said to be a *generalized bent function* if the Fourier coefficients $F(\underline{\lambda})$ of $f(\underline{x})$ only take the values of unit magnitude for any $\underline{\lambda} \in V_z^m$. ◇

In this paper, it is only considered that the integer z is an odd prime p. Thus, V_p^m is the n-dimensional vector space over the finite field F_p with p elements and $f(\underline{x})$ is a function from V_p^m to F_p. A bent function from V_p^m to F_p is called a p-ary bent function instead of a generalized bent function in this paper.

Let F_{p^m} be the finite field with p^m elements. Let $m = ek > 1$ for some positive integers e and k. Then a trace function $\mathrm{tr}_k^m(\cdot)$ is the mapping from F_{p^m} to its subfield F_{p^k} defined by [10] $\mathrm{tr}_k^m(x) = \sum_{i=0}^{e-1} x^{p^{ki}}$, where x is an element in F_{p^m}.

Olsen, Scholtz, and Welch [13] introduced a *trace transform* for a function from F_{2^m} to F_2. Then the trace transform for a function from the finite field F_{p^m} to F_p can be generalized as follows:

Definition 2 [Olsen, Scholtz, and Welch [13]] : Let $f(x)$ be a function from F_{p^m} to F_p. Then the *trace*

[1] This work was supported in part by BK21 and ITRC program of the Korean Ministry of Information and Communications and the Norwegian Research Council.

transform of $f(x)$ and its inverse transform are defined by

$$F(\lambda) = \frac{1}{\sqrt{p^m}} \sum_{x \in F_{p^m}} \omega^{f(x) - \mathrm{tr}_1^m(\lambda \cdot x)}, \quad \text{all } \lambda \in F_{p^m}$$

$$\omega^{f(x)} = \frac{1}{\sqrt{p^m}} \sum_{\lambda \in F_{p^m}} F(\lambda) \cdot \omega^{\mathrm{tr}_1^m(\lambda \cdot x)}, \quad \text{all } x \in F_{p^m}.$$

◇

It was defined by Nyberg[12] that a function is said to be *differentially k-uniform* if the maximum number of solutions $x \in F_q$ of $f(x+a) - f(x) = b$, for $a \in F_q^*, b \in F_q$ is k. Nyberg generalized the perfect nonlinear functions introduced by Meier and Staffelbach as follows.

Definition 3 [Nyberg [11]] : A function $f(\underline{x})$ from V_z^m to J_z is perfect nonlinear if for all $\underline{w} \in V_z^m, \underline{w} \neq 0$ and $k \in J_z$

$$f(\underline{x}) = f(\underline{x} + \underline{w}) + k$$

is satisfied for exactly z^{m-1} values of $\underline{x} \in V_z^m$. ◇

Thus the perfect nonlinear function is differentially q^{m-1}-uniform. Nyberg also proved the relationship between perfect nonlinear functions and bent functions as follows.

Theorem 1 [Nyberg [11]] : A perfect nonlinear function from V_z^m to J_z is bent. The converse is true if z is a prime. ◇

In the following section, we introduce p-ary bent functions from F_{p^m} to F_p, which correspond to functions with differential p^{m-1}-uniformity, that is, perfect nonlinear functions. The perfect nonlinearity is the important property for the differential cryptanalysis in DES and in many other block ciphers.

3. Construction of p-ary Bent Functions Defined on Finite Fields

Let α be a primitive element of the finite field F_{p^m}. By replacing x in F_{p^m} by α^t, a function $f(\alpha^t)$ from $F_{p^m}^*$ to F_p can be considered as a p-ary sequence of period $p^m - 1$.

From the Welch's lower bound on the crosscorrelation values[16], the maximum magnitude of the crosscorrelation values of two p-ary sequences of period $p^m - 1$ are lower bounded by $p^{\frac{m}{2}} + 1$ and they are said to have optimal correlation property.

From the p-ary sequences proposed by Sidelnikov, we have the p-ary bent functions defined on F_{p^m} as

$$f_b(x) = \mathrm{tr}_1^m(b \cdot x^2), \quad \text{for any } b \in F_{p^m}^*.$$

Kumar and Moreno introduced p-ary sequences with optimal correlation, which give us the p-ary bent functions defined on F_{p^m} as

$$f_b(x) = \mathrm{tr}_1^m(b \cdot x^{p^{kr}+1}), \quad \text{for any } b \in F_{p^m}^*$$

where e is an odd integer, $m = ek$, and r is an integer such that $1 \leq r \leq e-1, gcd(r,e) = 1$. The p-ary Kasami sequences also give us the p-ary bent functions defined on F_{p^m} given by

$$f_b(x) = \mathrm{tr}_1^k(b \cdot x^T), \quad b \in F_{p^m}^*$$

where $m = 2k$ and $T = p^k + 1$.

Further, it is possible to construct a p-ary bent function defined on F_{p^m} as in the following theorem.

Theorem 2 : Let $m = 2k$ or $2k+1$. Let $a_i \in F_p$. The quadratic p-ary function $f(x)$ from F_{p^m} to F_p given by

$$f(x) = \mathrm{tr}_1^m(\sum_{i=0}^{k} a_i \cdot x^{1+p^i}) \tag{1}$$

is bent, that is, perfect nonlinear if

$$\sum_{i=0}^{k} a_i \cdot (\epsilon^{il} + \epsilon^{-il}) \neq 0, \quad \text{for all } l, 0 \leq l \leq m-1 \tag{2}$$

where $\epsilon = e^{j\frac{2\pi}{m}}$ is an m-th root of unity.

Proof : We have to prove that the trace transform

$$F(\lambda) = \frac{1}{\sqrt{p^m}} \sum_{x \in F_{p^m}} \omega^{\sum_{i=0}^{k} \mathrm{tr}_1^m(a_i \cdot x^{1+p^i}) - \mathrm{tr}_1^m(\lambda \cdot x)}$$

has the unit magnitude for all $\lambda \in F_{p^m}$. Let $y_l = x^{p^{l-1}}$. Then we have

$$\sum_{i=0}^{k} \mathrm{tr}_1^m(a_i \cdot x^{1+p^i}) = \sum_{i=0}^{k} a_i \mathrm{tr}_1^m(x^{1+p^i})$$
$$= \sum_{i=0}^{k} a_i \sum_{l=1}^{m} (x^{1+p^i})^{p^{l-1}} = \sum_{i=0}^{k} a_i \sum_{l=1}^{m} x^{p^{l-1}+p^{l+i-1}}$$
$$= \sum_{i=0}^{k} a_i \sum_{l=1}^{m} y_l y_{l+i} = G(y_1, y_2, \cdots, y_m)$$

where $G(y_1, y_2, \cdots, y_m)$ is a quadratic function on $V_{p^m}^m$.

In a similar way to the proof in [7], let $\{\mu_1, \mu_2, \cdots, \mu_m\}$ and $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ be a pair of dual basis of F_{p^m} over F_p, that is,

$$\mathrm{tr}_1^m(\gamma_i \cdot \mu_l) = \begin{cases} 1, & \text{if } i = l, \\ 0, & \text{otherwise.} \end{cases}$$

Using the basis $\{\mu_1, \mu_2, \cdots, \mu_m\}$, we have

$$\underline{x} = (x_1, x_2, \cdots, x_m)^T, \text{ whenever } x = \sum_{i=1}^{m} x_i \mu_i \in F_{p^m}$$

and from the dual basis,

$$x_i = \mathrm{tr}_1^m(x\gamma_i), \ 1 \leq i \leq m.$$

Then we have the relations

$$\underline{x} = A\underline{y}, \ \underline{y} = B\underline{x}$$

where

$$A = \begin{bmatrix} \gamma_1 & \gamma_1^p & \gamma_1^{p^2} & \cdots & \gamma_1^{p^{m-1}} \\ \gamma_2 & \gamma_2^p & \gamma_2^{p^2} & \cdots & \gamma_2^{p^{m-1}} \\ & & \cdots & & \\ \gamma_m & \gamma_m^p & \gamma_m^{p^2} & \cdots & \gamma_m^{p^{m-1}} \end{bmatrix}$$

$$B = \begin{bmatrix} \mu_1 & \mu_2 & \mu_3 & \cdots & \mu_m \\ \mu_1^p & \mu_2^p & \mu_3^p & \cdots & \mu_m^p \\ \mu_1^{p^2} & \mu_2^{p^2} & \mu_3^{p^2} & \cdots & \mu_m^{p^2} \\ & & \cdots & & \\ \mu_1^{p^{m-1}} & \mu_2^{p^{m-1}} & \mu_3^{p^{m-1}} & \cdots & \mu_m^{p^{m-1}} \end{bmatrix}.$$

By replacing x in (1) by $\sum_{i=1}^m x_i\mu_i$, the quadratic function defined on V_p^m is given as

$$H(\underline{x}) = f(\sum_{i=1}^m x_i\mu_i).$$

Then we have

$$G(\underline{y}) = G(B\underline{x}) = H(\underline{x}).$$

If there exist common nonzero solutions to the set of equations $\frac{\partial H(x_1,\cdots,x_m)}{\partial x_l} = 0$ for all l, $H(x_1, x_2, \cdots, x_m)$ is said to be *singular*.

From the Deligne's theorem [4], if $H(\underline{x})$ is nonsingular, then

$$|\sum_{\underline{x}\in V_p^m} \omega^{H(\underline{x})+L(\underline{x})}| \le p^{\frac{m}{2}}$$

where $L(\underline{x})$ is any linear function on V_p^m. From the Parseval theorem, we have

$$|\sum_{\underline{x}\in V_p^m} \omega^{H(\underline{x})+L(\underline{x})}| = p^{\frac{m}{2}}$$

which means that $F(\lambda)$ has the unit magnitude for all $\lambda \in F_{p^m}$.

Now we have to check the nonsingularity of $H(\underline{x})$. Since we have

$$\frac{\partial H}{\partial \underline{x}} = \begin{bmatrix} \frac{\partial H}{\partial x_1} \\ \frac{\partial H}{\partial x_2} \\ \cdots \\ \frac{\partial H}{\partial x_m} \end{bmatrix} = B^T \frac{\partial G}{\partial \underline{y}},$$

it is sufficient to prove the nonsingularity of $G(\underline{y})$.

Differentiating $G(\cdot)$, we obtain

$$\frac{\partial G(y_1,\cdots,y_m)}{\partial y_l} = \sum_{i=0}^k a_i \left(y_{l+i} + y_{l-i}\right).$$

If there exists no common nonzero solution to the set of equations $\frac{\partial G(y_1,\cdots,y_m)}{\partial y_l} = 0$ for all l, that is, $\sum_{i=0}^k a_i \left(y_{l+i} + y_{l-i}\right) \neq 0$ for all l, then $G(y_1, y_2, \cdots, y_m)$ is nonsingular.

Thus, in order for $G(y_1, y_2, \cdots, y_m)$ to be nonsingular, the circulant matrix over F_p for $m = 2k+1$ given by

$$\begin{bmatrix} 2a_0 & a_1 & \cdots & a_k & a_k & a_{k-1} & \cdots & a_1 \\ a_1 & 2a_0 & \cdots & a_{k-1} & a_k & a_k & \cdots & a_2 \\ a_2 & a_1 & \cdots & a_{k-2} & a_{k-1} & a_k & \cdots & a_3 \\ & & \cdots & & \cdots & & \cdots & \\ a_2 & a_3 & \cdots & a_{k-1} & a_{k-2} & a_{k-3} & \cdots & a_1 \\ a_1 & a_2 & \cdots & a_k & a_{k-1} & a_{k-2} & \cdots & 2a_0 \end{bmatrix}$$

or the circulant matrix over F_p for $m = 2k$ given by

$$\begin{bmatrix} 2a_0 & a_1 & \cdots & 2a_k & a_{k-1} & a_{k-2} & \cdots & a_1 \\ a_1 & 2a_0 & \cdots & a_{k-1} & 2a_k & a_{k-1} & \cdots & a_2 \\ a_2 & a_1 & \cdots & a_{k-2} & a_{k-1} & 2a_k & \cdots & a_3 \\ & & \cdots & & \cdots & & \cdots & \\ a_2 & a_3 & \cdots & a_{k-2} & a_{k-3} & a_{k-4} & \cdots & a_1 \\ a_1 & a_2 & \cdots & a_{k-1} & a_{k-2} & a_{k-3} & \cdots & 2a_0 \end{bmatrix}$$

should have full rank.

It is known [9] that the determinant of the circulant matrix $C = [c_0, c_1, \cdots, c_{m-1}]$ is given as

$$D = \prod_{l=0}^{m-1} h(\epsilon^l)$$

where $h(x) = \sum_{i=0}^{m-1} c_i \cdot x^i$ and ϵ is an m-th root of unity.

Thus, the full rank of the matrices in the theorem is guaranteed if

$$\sum_{i=0}^k a_i \cdot (\epsilon^{il} + \epsilon^{-il}) \neq 0, \quad \text{for all } l, 0 \le l \le m-1.$$

◇

Using Theorem 2, we can have quadratic p-ary bent functions as follows.

Corollary 1 : Let I be an index set such that $gcd(p, |I|) = 1$. Let m be an positive integer such that $gcd(m, |I|) = 1$. Then the quadratic p-ary function $f(x)$ from F_{p^m} to F_p given by

$$f(x) = \sum_{i\in I} \mathrm{tr}_1^m(x^{p^i+1})$$

is *bent*.

Proof : Let x be an element of the set $E = \{e^{j\frac{2\pi l}{m}} | 0 \le l \le m-1\}$. Then the condition in (2) is written as

$$\sum_{i\in I} (\delta^i + \delta^{-i}) \neq 0, \quad \text{for all } \delta \in E. \tag{3}$$

From $gcd(p, |I|) = 1$ and $gcd(m, |I|) = 1$, it is easy to check that (3) is satisfied.

◇

Using the result of Theorem 2, we can find the p-ary bent functions similar to the bent functions by Kumar and Moreno as follows.

Corollary 2 : Let e be an odd integer and k be an even integer. Let $m = ek$. Let r be an integer such that $1 \leq r \leq e-1, gcd(r,e) = 1$. Then the function on F_{p^m} given by

$$f(x) = \mathrm{tr}_1^m(x^{p^{\frac{m}{2}-kr}+1})$$

is bent. $\diamond$

For $k = 0$, $f(x)$ becomes the bent function from p-ary Kasami sequences.

Let $q = p^m$. Dembowski and Ostrom introduced the Dembowski-Ostrom polynomials[2][3] on F_q defined by

$$f(x) = \sum_{i=0}^{m-1}\sum_{l=0}^{m-1} a_{i,l}x^{p^i+p^l} \tag{4}$$

where $a_{i,l} \in F_q$. It is easy to check that for $a \in F_q^*$, we have

$$\begin{aligned} f(x+a) - f(x) &= \sum_{i=0}^{m-1}\sum_{l=0}^{m-1}(a_{i,l}(x^{p^i}a^{p^l} + x^{p^l}a^{p^i}) \\ &\quad + a_{i,l}a^{p^i+p^l}). \end{aligned}$$

It is known[10] that a p-polynomial is a permutation polynomial if and only if the p-polynomial only has the solution "0". Clearly,

$$\sum_{i=0}^{m-1}\sum_{l=0}^{m-1} a_{i,l}(x^{p^i}a^{p^l} + x^{p^l}a^{p^i})$$

is a p-polynomial and thus $f(x)$ is a planar polynomial if for any $a \in F_q^*$,

$$\sum_{i=0}^{m-1}\sum_{l=0}^{m-1} a_{i,l}(x^{p^i}a^{p^l} + x^{p^l}a^{p^i}) \neq 0, \text{ for all } x \in F_q^*. \tag{5}$$

Using the Dembowski-Ostrom polynomials, we can construct p-ary bent functions defined on F_{p^m} as follows.

Theorem 3 : Let $f(x)$ be the Dembowski-Ostrom polynomial defined in (4) satisfying (5). Then the function $\mathrm{tr}_1^m(f(x))$ from F_{p^m} to F_p is bent. $\diamond$

From the simulation result, the converse of Theorem 3 is not true.

$\diamond$

References

[1] C. Carlet and C. Ding, "Highly nonlinear mappings," Preprint, 2002.

[2] R. Coulter and R.W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Designs, Codes and Cryptography*, vol. 10, pp. 167-184, 1997.

[3] P. Dembowski and T.G. Ostrom, "Planes of order n with collineation groups of order n^2," *Math. Z. 103*, pp. 239-258, 1968.

[4] L.E. Dickson, *Linear groups with exposition of the Galois field theory*, Dover Publications, New York, 1958.

[5] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 475-485, Mar. 1999.

[6] T. Helleseth and D. Sandberg, "Some power mappings with low differential uniformity," *Applicable Algebra in Engineering, Communication and Computing*," vol. 8, pp. 363-370, 1997.

[7] P.V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inform. Theory*, vol. 37, pp. 603-616, May 1991.

[8] P.V. Kumar, R.A. Scholtz, and L.R. Welch, "Generalized bent functions and their properties," *Journal of Combinatorial Theory*, Series A. vol. 40, pp. 90-107, 1985.

[9] P. Lancaster and M. Tismenetsky, *The Theory of Matrices with Applications*, 2nd ed., 1985.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.

[11] K. Nyberg, "Constructions of bent functions and difference sets," *Lecture Notes in Computer Science* 473, Springer-Verlag, pp. 151-160, 1991.

[12] K. Nyberg, "Differentially uniform mappings for cryptography," *Lecture Notes in Computer Science* 765, Springer-Verlag, pp. 55-64, 1994.

[13] J.D. Olsen, R.A. Scholtz, and L.R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. 28, pp. 858-864, Nov. 1982.

[14] O.S. Rothaus, "On bent functions," *Journal of Combinatorial Theory*, Series A. vol. 20, pp. 300-305, 1976.

[15] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," *SIAM J. Comput.*, vol. 9, no. 4, pp. 758-767, Nov. 1980.

[16] L. R. Welch, "Lower bounds on the maximal cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. 20, pp. 396-399, May 1976.