New Constructions of p-ary Bent Sequences [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

In this paper, using bent functions defined on the finite field, we generalized the construction method of the family of p-ary bent sequences with balanced and optimal correlation property introduced by Kumar and Moreno for an odd prime p [3], called a *generalized p-ary bent sequence*. It turns out that the family of balanced p-ary sequences with optimal correlation property introduced by Moriuchi and Imamura [6] is a special case of the generalized p-ary bent sequences.

1. Introduction

Rothaus [8] introduced a *binary bent function*, which is a mapping from m-tuple binary vector space to $\{0, 1\}$ and various different classes of binary bent functions have been found [1][2][4]. Using the binary bent functions, Olsen, Scholtz, and Welch [7] constructed a *bent sequence*, which has the balance property and meets the asymptotic lower bound on the correlation values by Welch [9]. Expanding alphabet size from binary to q-ary case, Kumar, Scholtz, and Welch [4] introduced a *generalized bent function* mapping from q-ary vector space to the set of integers modulo q. For an odd prime p, Kumar and Moreno [3] defined a family of p-ary bent sequences by applying the construction method of binary bent sequences to p-ary bent functions and they also introduced the p-ary bent function $tr_1^m(b \cdot x^{p^{rc}+1})$ defined in the finite field F_{p^m} with p^m elements, $c|m, b \in F_{p^m}^*$, which was used to construct the balanced p-ary sequences with optimal correlation property by Moriuchi and Imamura [6].

In this paper, using bent functions defined on the finite field, we generalized the construction method of the family of p-ary bent sequences with balanced and optimal correlation property introduced by Kumar and Moreno for an odd prime p [3], called a *generalized p-ary bent sequence*. It turns out that the family of balanced p-ary sequences with optimal correlation property introduced by Moriuchi and Imamura [6] is a special case of the generalized p-ary bent sequences.

2. Preliminaries

Let $\mathbf{S}$ be the family of M p-ary sequences of period $N = p^n - 1$ for an odd prime p given by

$$\mathbf{S} = \{s_i(t) \mid 0 \le i \le M-1, 0 \le t \le N-1\}.$$

The correlation function of the sequences $s_i(t)$ and $s_j(t)$ in $\mathbf{S}$ is written as

$$R_{i,j}(\tau) = \sum_{t=0}^{N-1} \omega^{s_i(t+\tau) - s_j(t)} \quad (1)$$

where $0 \le i, j \le M-1$, $0 \le \tau \le N-1$. Maximum magnitude of the correlation values is defined as

$$R_{max} = \max_{0 \le i,j \le M-1, 0 \le \tau \le N-1} |R_{i,j}(\tau)|$$

except for the case of $i = j$ and $\tau = 0$.

A family of p-ary sequences of period $p^n - 1$ is said to have optimal correlation property if R_{max} is equal to $p^{\frac{n}{2}} + 1$.

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 the function $f(\underline{x})$ is defined as

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

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

Definition 1 [Kumar, Scholtz, and Welch [4]] : 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 m-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.

Let F_{p^m} be a 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 a mapping from F_{p^m} to its subfield

[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.

F_{p^k} defined as [5] $\mathrm{tr}_k^m(x) = \sum_{i=0}^{e-1} x^{p^{ki}}$, where x is an element in F_{p^m}.

Olsen, Scholtz, and Welch [7] 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} with p^m elements to F_p can be generalized as follows:

Definition 2 [Olsen, Scholtz, and Welch [7]] : Let $f(x)$ be a function from F_{p^m} to F_p. Then the *trace transform* of $f(x)$ and its inverse transform are defined by

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

□

Now, a function $f(x)$ defined on F_{p^m} is called a generalized bent function if the trace transform of $f(x)$ only takes the values of unit magnitude.

The trace transform pair of a function $\mathrm{tr}_1^k(f(\underline{x}))$ from $V_{p^k}^e$ to F_p can be modified into the trace transform defined in the intermediate field as follows:

Definition 3 : Let $m = ek$. Let $f(\underline{x})$ be a function from $V_{p^k}^e$ to F_{p^k}. Then the *modified trace transform* of $\mathrm{tr}_1^k(f(\underline{x}))$ and its inverse transform are defined as

$$\begin{aligned} F_M(\underline{\lambda}) &= \frac{1}{\sqrt{p^m}} \sum_{\underline{x} \in V_{p^k}^e} \omega^{\mathrm{tr}_1^k(f(\underline{x})) - \mathrm{tr}_1^k(\underline{\lambda} \cdot \underline{x}^T)}, \\ &\quad \text{all } \underline{\lambda} \in V_{p^k}^e \\ \omega^{\mathrm{tr}_1^k(f(\underline{x}))} &= \frac{1}{\sqrt{p^m}} \sum_{\underline{\lambda} \in V_{p^k}^e} F(\underline{\lambda}) \cdot \omega^{\mathrm{tr}_1^k(\underline{\lambda} \cdot \underline{x}^T)}, \\ &\quad \text{all } \underline{x} \in V_{p^k}^e. \end{aligned}$$

□

Then, it is possible to construct a p-ary bent function defined on F_{p^m} as in the following theorem[10].

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

$$f(x) = \mathrm{tr}_1^m(\sum_{i=0}^{k} a_i \cdot x^{1+p^i}) \tag{2}$$

is bent if

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

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

3. New Constructions of p-ary Bent Sequences

Kumar and Moreno extended the binary bent sequences by Olsen, Scholtz, and Welch into p-ary bent sequences by using p-ary bent functions defined on the m-tuple p-ary vector space V_p^m as in the following theorem.

Theorem 2 [Kumar and Moreno [3]]: Let p be an odd prime and m be an integer. Let $n = 2m$ and α be a primitive element of F_{p^n}. Let $f(\cdot)$ be a p-ary bent function on V_p^m. Let $L(x) = (\mathrm{tr}_1^n(\beta_1 \sigma x), \mathrm{tr}_1^n(\beta_2 \sigma x), \cdots, \mathrm{tr}_1^n(\beta_m \sigma x))$, where $\sigma \in F_{p^n} \backslash F_{p^m}$ and $\{\beta_1, \beta_2, \cdots, \beta_m\}$ be a basis of F_{p^m} over F_p. Let $\delta \in F_{p^m}^*$. Then a family of *p-ary bent sequences* is defined as

$$\begin{aligned} \mathbf{S} &= \{s_\eta(t) \mid \eta \in F_{p^m},\ 0 \leq t \leq p^n - 2\} \\ s_\eta(t) &= f(L(\alpha^t)) + \mathrm{tr}_1^n((\eta \cdot \sigma + \delta)\alpha^t) \end{aligned}$$

where magnitude of their correlation values is upper bounded by $p^m + 1$ and $|\mathbf{S}| = p^m$. □

The construction of a family of p-ary bent sequences can be generalized as follows:

Theorem 3 : Let p be an odd prime and let m, e, k be integers. Let $n = 2m = 2ek$ and α be a primitive element of F_{p^n}. Let $f(\cdot)$ be a p-ary bent function on $V_{p^k}^e$. Let $L(x) = (\mathrm{tr}_k^n(\beta_1 \sigma x), \mathrm{tr}_k^n(\beta_2 \sigma x), \cdots, \mathrm{tr}_k^n(\beta_e \sigma x))$, where $\sigma \in F_{p^n} \backslash F_{p^m}$ and $\{\beta_1, \beta_2, \cdots, \beta_e\}$ is a basis of F_{p^m} over F_{p^k}. Let $\delta \in F_{p^m}^*$. Then a family of *p-ary generalized bent sequences* is defined as

$$\begin{aligned} \mathbf{S} &= \{s_\eta(t) \mid \eta \in F_{p^m},\ 0 \leq t \leq p^n - 2\} \\ s_\eta(t) &= f(L(\alpha^t)) + \mathrm{tr}_1^n((\eta \cdot \sigma + \delta)\alpha^t) \end{aligned}$$

where magnitude of their correlation values is upper bounded by $p^m + 1$ and $|\mathbf{S}| = p^m$. □

Similar to the proof of the binary bent sequence in [9], the above theorem can be proved by using the modified trace transform defined in Definition 3. We begin with a lemma.

Lemma 1 : Let $n = 2m = 2ek$, where m, e and k are positive integers. Let $L(x)$ be an onto linear mapping from F_{p^n} to $V_{p^k}^e$ and $f(\underline{x})$ a function from $V_{p^k}^e$ to F_p. Then, the trace transform of the function $f(L(x))$ is given as

$$F(\lambda) = \begin{cases} 0, & \lambda \notin \mathrm{range}(L^*) \\ p^{\frac{m}{2}} \cdot F_M(\underline{u}), & \lambda \in \mathrm{range}(L^*),\ L^*(\underline{u}) = \lambda \end{cases}$$

where $F_M(\underline{u})$ is the modified trace transform of $f(\underline{x})$ defined in Definition 3.

Proof : Using the definition of trace transform, the trace transform of the function $f(L(x))$ can be easily

expressed as

$$\begin{aligned} & F(\lambda) \\ = & \frac{1}{\sqrt{p^n}} \sum_{x\in F_{p^n}} \omega^{f(L(x))-\mathrm{tr}_1^n(\lambda\cdot x)} \\ = & \frac{1}{\sqrt{p^n}} \sum_{x\in F_{p^n}} \frac{1}{\sqrt{p^m}} \cdot \sum_{\underline{u}\in V_{p^k}^e} F_M(\underline{u}) \cdot \omega^{\mathrm{tr}_1^k(L(x)\cdot \underline{u}^T)} \\ & \times \omega^{-\mathrm{tr}_1^n(\lambda\cdot x)} \\ = & \frac{1}{\sqrt{p^{n+m}}} \sum_{\underline{u}\in V_{p^k}^e} F_M(\underline{u}) \sum_{x\in F_{p^n}} \omega^{\mathrm{tr}_1^k(L(x)\cdot \underline{u}^T)-\mathrm{tr}_1^n(\lambda\cdot x)}. \end{aligned}$$

From the adjoint of linear mapping $L(x)$, we have

$$\mathrm{tr}_1^k(L(x)\cdot \underline{u}^T) = \mathrm{tr}_1^k(\mathrm{tr}_k^n(x\cdot L^*(\underline{u}))).$$

Thus the trace transform of the function $f(L(x))$ can be rewritten as follows:

$$F(\lambda) = \frac{1}{\sqrt{p^{n+m}}} \sum_{\underline{u}\in V_{p^k}^e} F_M(\underline{u}) \cdot \sum_{x\in F_{p^n}} \omega^{\mathrm{tr}_1^n((L^*(\underline{u})-\lambda)\cdot x)}.$$

Clearly, the inner sum of the above equation is equal to p^n when $\lambda = L^*(\underline{u})$ and otherwise it is equal to zero. Therefore, if $\lambda \in \mathrm{range}(L^*)$, then we have

$$\begin{aligned} F(\lambda) &= \frac{1}{\sqrt{p^{n+m}}} \cdot p^n \cdot F_M(\underline{u}), \quad \text{when } \lambda = L^*(\underline{u}) \\ &= p^{\frac{m}{2}} \cdot F_M(\underline{u}). \end{aligned}$$

For $\lambda \notin \mathrm{range}(L^*)$, there is no $\underline{u}$ in $V_{p^k}^e$ such that $\lambda = L^*(\underline{u})$. Thus $F(\lambda) = 0$.

□

From the definition of the linear mapping $L(x)$, for any $\underline{u} \in V_{p^k}^e$, we have the following relationship

$$L(x)\cdot \underline{u}^T = \mathrm{tr}_k^n(\zeta\cdot\sigma\cdot x)$$

where $\underline{u} = (u_1, u_2, \cdots, u_e)$ and

$$\zeta = \sum_{i=1}^{e} \beta_i u_i.$$

Clearly, as $\underline{u}$ varies over $V_{p^k}^e$, ζ covers all elements in F_{p^m}, that is,

$$\{\zeta \mid \underline{u} \in V_{p^k}^e\} = F_{p^m}.$$

Thus we have the range of L^* as

$$\mathrm{range}(L^*) = \{\zeta\cdot\sigma \mid \zeta \in F_{p^m}\}. \tag{3}$$

Proof of Theorem 3: The trace transform of $s_\eta(x)$ can be written as

$$\hat{S}_\eta(\lambda) = \frac{1}{\sqrt{p^n}} \sum_{x\in F_{p^n}} \omega^{f(L(x))-\mathrm{tr}_1^n((\lambda-\eta\sigma-\delta)\cdot x)}.$$

From Lemma 1, we can calculate the trace transform as follows.

$$\hat{S}_\eta(\lambda) = \begin{cases} p^{\frac{m}{2}} \cdot F_M(\underline{u}), & \text{for } \lambda-\eta\sigma-\delta \in \mathrm{range}(L^*) \\ & \quad : L^*(\underline{u}) = \lambda-\eta\sigma-\delta, \\ 0, & \text{for } \lambda-\eta\sigma-\delta \notin \mathrm{range}(L^*) \end{cases}$$

where $F_M(\underline{u})$ is the modified trace transform of $f(\underline{x})$. From (3), the range of L^* has the property as follows.

$$\begin{aligned} \mathrm{range}(L^*)+\eta\sigma+\delta &= \{\zeta\cdot\sigma \mid \zeta\in F_{p^m}\}+\eta\sigma+\delta \\ &= \{\zeta\cdot\sigma \mid \zeta\in F_{p^m}\}+\delta \\ &= \mathrm{range}(L^*)+\delta \\ &= \{\zeta\cdot\sigma+\delta \mid \zeta\in F_{p^m}\}. \end{aligned}$$

Let

$$H = \mathrm{range}(L^*)+\eta\sigma+\delta = \{\zeta\cdot\sigma+\delta \mid \zeta\in F_{p^m}\}.$$

Then, the set H is the same for all sequences in the family of the sequences $\mathbf{S}$.

It is well-known that the equation $x^2+x+w=0$ has a root, σ_0, which generates F_{p^n} over F_{p^m}. That is,

$$F_{p^n} = \{\phi\sigma_0+\psi \mid \phi,\psi\in F_{p^m}\}.$$

Then α^τ can be written in the form $\alpha^\tau = \phi\sigma_0+\psi$. Now an element, z, in $H\cap H\alpha^\tau$ can be written in two ways

$$z = \zeta_1\sigma_0+\delta$$

and

$$\begin{aligned} z &= \alpha^\tau(\zeta_2\sigma_0+\delta) \\ &= (\phi\sigma_0+\psi)(\zeta_2\sigma_0+\delta) \\ &= \phi\zeta_2\sigma_0^2+(\phi\delta+\psi\zeta_2)\sigma_0+\psi\delta \\ &= (-\phi\zeta_2+\phi\delta+\psi\zeta_2)\sigma_0+\psi\delta-\phi\zeta_2 w. \end{aligned}$$

From the uniqueness of such representations, it follows that

$$\zeta_1 = -\phi\zeta_2+\phi\delta+\psi\zeta_2$$

and

$$\delta = \psi\delta-\phi\zeta_2 w.$$

If $\phi \neq 0$, the second equation can be solved for ζ_2 and then the first equation evaluated for ζ_1. Therefore if $\phi\neq 0$, $\mid H\cap H\alpha^\tau \mid = 1$. If $\phi = 0$, then ψ must equal 1 for a solution to exist since $\delta\neq 0$. This implies that $\alpha^\tau = 1$ which contradicts the fact that α is primitive and $0<\tau<p^n-1$. Therefore if $\phi=0$, $\mid H\cap H\alpha^\tau \mid = 0$. Then we proved that for $1\le\tau\le p^n-2$ and a primitive element $\alpha\in F_{p^n}$,

$$\mid H\cap H\alpha^\tau \mid \le 1. \tag{4}$$

Since we already assumed that $F_M(\underline{u})$ takes on the values $+1$ or -1, the trace transform of the sequence $s_\eta(x)$ can be given as

$$\hat{S}_\eta(\lambda) = \begin{cases} 0, & \text{for } \lambda\notin H \\ \pm p^{\frac{m}{2}}, & \text{for } \lambda\in H. \end{cases} \tag{5}$$

The crosscorrelation of the sequences $s_{\underline{y}}(t)$ and $s_{\underline{z}}(t)$ in (1) can be written as

$$R_{yz}(\tau) = -1+\sum_{x\in F_{p^n}} \omega^{s_{\underline{y}}(x)-s_{\underline{z}}(x\alpha^\tau)}.$$

Now we can prove the theorem for the following two cases.

i) $\tau \neq 0$ **:**
Using the Parseval's theorem and the expression of the sequences by the element x in F_{p^n}, the crosscorrelation function can be written as

$$R_{yz}(\tau) = -1 + \sum_{\lambda \in F_{p^n}} \hat{S}_{\underline{y}}(\lambda) \cdot \hat{S}^*_{\underline{z}}(\lambda \alpha^\tau).$$

From (4) and (5), the correlation function can be derived as

$$\begin{aligned} R_{yz}(\tau) &= -1 \pm p^{\frac{m}{2}} \cdot p^{\frac{m}{2}} \cdot \mid H \cap H\alpha^\tau \mid \\ &= \begin{cases} -1, & \text{for } \mid H \cap H\alpha^\tau \mid = 0 \\ -1 \pm p^m, & \text{for } \mid H \cap H\alpha^\tau \mid = 1. \end{cases} \end{aligned}$$

ii) $\tau = 0$ and $\underline{y} \neq \underline{z}$:
The crosscorrelation function can be written as

$$\begin{aligned} R_{yz}(0) &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{tr}_1^k(L(\alpha^t)\cdot(\underline{y}-\underline{z})^T)} \\ &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{tr}_1^n(\eta\sigma\cdot\alpha^t)} = -1 \end{aligned}$$

since $\eta = \sum_{i=1}^{e} \beta_i(y_i - z_i) \neq 0$.

We proved the correlation property of the sequences in the family **S**.

□

Using the p-ary bent function on F_{p^m} defined in Theorem 1, the p-ary bent sequences can also be constructed as follows:

Theorem 4 : Let $n = 2m$, $m = 2k$ or $2k+1$, and $a_i \in F_p$. Let $\sigma \in F_{p^n} \backslash F_{p^m}$ and $\eta \in F_{p^m}$, $\delta \in F^*_{p^m}$. Let $f(\cdot)$ be the quadratic p-ary bent function from F_{p^m} to F_p defined in (2) given by

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

Then a family of p-ary bent sequences is given as

$$\begin{aligned} \mathbf{S} &= \{s_\eta(t) \mid \eta \in F_{p^m},\ 0 \leq t \leq p^n - 2\} \\ s_\eta(t) &= \mathrm{tr}_1^m(\sum_{i=0}^{k} a_i \cdot [\mathrm{tr}_m^n(\sigma\alpha^t)]^{1+p^i}) \\ &\quad + \mathrm{tr}_1^n((\eta \cdot \sigma + \delta)\alpha^t). \end{aligned}$$

□

Using the p-ary bent sequences by Kumar and Moreno defined in [3], Moriuchi and Imamura [6] introduced the family of p-ary sequences with balanced and optimal correlation property given by

$$s_\eta(t) = \mathrm{tr}_1^k(b \cdot [\mathrm{tr}_k^n(\sigma\alpha^t)]^{p^{kr}+1}) + \mathrm{tr}_1^n((\eta \cdot \sigma + \delta)\alpha^t)$$

and it turns out to be a special case of the family of generalized p-ary bent sequences defined in Theorem 4 when $f(\cdot)$ is the p-ary bent function by Kumar and Moreno.

It is clear that the number of terms of p-ary bent sequences defined in Theorem 2 increases as their period increases but it is not true for the p-ary bent sequences in Theorem 4. It is also known that the binary bent sequences exist when n is multiple of 4 but the p-ary bent sequences can be constructed for any even n.

References

[1] C. Carlet, "Two new classes of bent functions," in *Proc. EURO-CRYPT'93 (Lecture Notes in Computer Science 765)*, pp. 77-101, 1994.

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

[3] 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.

[4] 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.

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

[6] T. Moriuchi and K. Imamura, "Balanced nonbinary sequences with good periodic correlation properties obtained from modified Kumar-Moreno sequences," *IEEE Trans. Inform. Theory*, vol. 41, pp. 572-576, Mar. 1995.

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

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

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

[10] Young-Sik Kim, Ji-Woong Jang, Jong-Seon No, and Tor Helleseth, "On p-ary Bent Functions Defined on Finite Fields," *Mathematical Properties of Sequences and Other Combinatorial Structures, The Kluwer International Series in Engineering and Computer Science*, Kluwer Academic Publishers, pp. 65-76, 2003.