PAPER

New Constructions of *p*-ary Bent Sequences*

Young-Sik KIM[†a)], ***Student Member***, **Ji-Woong JANG**[†b)], **Jong-Seon NO**[†c)], ***and*** **Tor HELLESETH**[††d)], ***Nonmembers***

SUMMARY In this paper, using p-ary bent functions defined on vector space over the finite field F_{p^k}, we generalized the construction method of the families of p-ary bent sequences with balanced and optimal correlation properties introduced by Kumar and Moreno for an odd prime p [3], called *generalized p-ary bent sequences*. It turns out that the family of balanced p-ary sequences with optimal correlation property introduced by Moriuchi and Imamura [8] is a special case of the newly constructed generalized p-ary bent sequences.

key words: *bent sequences, generalized bent functions, optimal correlation, p-ary bent sequences*

1. Introduction

Rothaus [10] introduced a *bent function*, which is a Boolean function from m-tuple binary vector space to $\{0, 1\}$ and its Fourier coefficients only take the values $+1$ or -1. Various different classes of bent functions have been found [1], [4]. Using the bent functions, Olsen, Scholtz, and Welch [9] constructed *bent sequences*, which have the balance property and meet the asymptotic lower bound on the correlation values by Welch [12]. Lempel and Cohn [5] also introduced bent sequences by extending the result of Olsen, Scholtz, and Welch. 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, there have been research results on the families of p-ary sequences of period $p^n - 1$ with optimal correlation property. The optimality of correlation values means that maximum magnitude of out-of-phase autocorrelation and crosscorrelation values of any sequences of period $p^n - 1$ in the family is upper bounded by $R_{max} = p^{\frac{n}{2}} + 1$. Families of p-ary sequences with optimal correlation property have been introduced by Sidelnikov and by Kumar and Moreno [3]. Liu and Komo [7] constructed p-ary Kasami sequences with optimal correlation property by expanding alphabet size from binary to p-ary case. But those sequences don't have balance property. Moriuchi and Imamura constructed a family of balanced p-ary sequences with optimal correlation property using the p-ary bent sequences by Kumar and Moreno. The families of p-ary sequences with optimal correlation property are listed in Table 1.

Table 1 Families of p-ary sequences with optimal correlation property. In the first column, K&M represents Kumar and Moreno case. And in the first row, B means balance property.

Family	Period	n	Size	$R_{\max}$	B
Sidelnikov	$p^n - 1$	even or odd	p^n	$p^{\frac{n}{2}} + 1$	no
K&M	$p^n - 1$	ek, e:odd	p^n	$p^{\frac{n}{2}} + 1$	no
Kasami	$p^n - 1$	even, $2m$	p^m	$p^{\frac{n}{2}} + 1$	no
Moriuchi	$p^n - 1$	even, $2m$	p^m	$p^{\frac{n}{2}} + 1$	yes
Bent	$p^n - 1$	even, $2m$	p^m	$p^{\frac{n}{2}} + 1$	yes

In this paper, we introduce the modified trace transform of the function from vector space over the finite field F_{p^k} to the finite field F_p. Using the modified trace transform and p-ary bent functions defined on vector space over F_{p^k}, we generalized the construction method of the family of p-ary bent sequences with balanced and optimal correlation properties introduced by Kumar and Moreno for an odd prime p [3], called *generalized p-ary bent sequences*. It turns out that the family of balanced p-ary sequences with optimal correlation property introduced by Moriuchi and Imamura [8] is a special case of the newly constructed generalized p-ary bent sequences.

2. *p*-ary Bent Functions Defined on Finite Fields

Let z be an integer and V_z^m be the 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

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

where $\underline{x}^T$ stands for transpose of $\underline{x}$ and $\underline{\lambda} \cdot \underline{x}^T$ denotes the inner product of the two row vectors $\underline{\lambda}$ and $\underline{x}$. Kumar, Scholtz, and Welch defined the generalized bent function as follows:

Definition 1: [Kumar, Scholtz, and Welch [4]] A function

Manuscript received April 25, 2003.
Manuscript revised September 5, 2003.
Final manuscript received October 22, 2003.

[†]The authors are with School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-742, Korea.

[††]The author is with Department of Informatics, University of Bergen, N-5020 Bergen, Norway.

a) E-mail: kingsi@ccl.snu.ac.kr
b) E-mail: stasera@ccl.snu.ac.kr
c) E-mail: jsno@snu.ac.kr
d) E-mail: Tor.Helleseth@ii.uib.no

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

$f(\underline{x})$ 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, we assume 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 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 a mapping from F_{p^m} to its subfield F_{p^k} defined as [6]

$$\mathrm{tr}_k^m(x) = \sum_{i=0}^{e-1} x^{p^{ki}}$$

where x is an element in F_{p^m}.

Olsen, Scholtz, and Welch [9] introduced *trace transform* for a function from F_{2^m} to F_2. Then the trace transform for a function from F_{p^m} to F_p can be generalized as follows:

Definition 2: [Olsen, Scholtz, and Welch [9]] 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

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

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

□

A basis $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_e\}$ of F_{p^m} over F_{p^k} is said to be a *trace-orthogonal basis* if

$$\mathrm{tr}_k^m(\alpha_i \alpha_l) = \begin{cases} a_i, & \text{if } i = l \\ 0, & \text{otherwise} \end{cases}$$

where $a_i \in F_{p^k} \backslash \{0\}$. It is known that for any positive integer e and an odd prime p, there exists a trace-orthogonal basis of F_{p^m} over F_{p^k} [11]. Let $V_{p^k}^e$ be the e-dimensional vector space over F_{p^k}. The elements x and λ in F_{p^m} can be determined from the elements $\underline{x}$ and $\underline{\lambda}$ in $V_{p^k}^e$ by the relations

$$x = \sum_{i=1}^{e} x_i \alpha_i \quad \Rightarrow \quad \underline{x} = (x_1, x_2, x_3, \cdots, x_e)$$

$$\lambda = \sum_{i=1}^{e} \lambda_i \alpha_i \quad \Rightarrow \quad \underline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_e)$$

where x_i and λ_i are in F_{p^k}. If we choose the basis as a trace-orthogonal basis, then we have the relation

$$\mathrm{tr}_k^m(\lambda x) = \sum_{i=1}^{e} a_i \lambda_i x_i. \tag{2}$$

Let $\lambda_i' = a_i \lambda_i$ for $i, 1 \le i \le e$ and $\underline{\lambda}' = (\lambda_1', \lambda_2', \lambda_3', \cdots, \lambda_e')$. Then the relation in Eq. (2) can be rewritten as

$$\mathrm{tr}_k^m(\lambda x) = \sum_{i=1}^{e} \lambda_i' x_i = \underline{\lambda}' \cdot \underline{x}^T.$$

For $k = 1$, by replacing x in F_{p^m} by $\underline{x}$ in V_p^m, the function $f(x)$ from F_{p^m} to F_p makes the corresponding function $f(\underline{x})$ from V_p^m to F_p. Therefore, the set of the trace transform values of the function $f(x)$ is the same as that of the Fourier coefficients of the corresponding function $f(\underline{x})$. If the trace transform values of the function $f(x)$ only take the values of unit magnitude, the corresponding function $f(\underline{x})$ becomes the generalized bent function. 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.

Let $f(\underline{x})$ be a function from $V_{p^k}^e$ to F_p. Then the trace transform pair of a function $f(\underline{x})$ 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. Then the *modified trace transform* of $f(\underline{x})$ and its inverse transform are defined as

$$F_M(\underline{\lambda}) = \frac{1}{\sqrt{p^m}} \sum_{\underline{x} \in V_{p^k}^e} \omega^{f(\underline{x}) - \mathrm{tr}_1^k(\underline{\lambda} \cdot \underline{x}^T)}, \forall \underline{\lambda} \in V_{p^k}^e \tag{3}$$

$$\omega^{f(\underline{x})} = \frac{1}{\sqrt{p^m}} \sum_{\underline{\lambda} \in V_{p^k}^e} F_M(\underline{\lambda}) \omega^{\mathrm{tr}_1^k(\underline{\lambda} \cdot \underline{x}^T)}, \forall \underline{x} \in V_{p^k}^e.$$

□

Similarly to the case of $k = 1$, the trace transform $F(\lambda)$ defined in Eq. (1) of the function $f(x)$ is related to the modified trace transform defined in Eq. (3) as follows

$$F(\lambda) = F_M(\underline{\lambda}').$$

That is, the set of the trace transform values $F(\lambda)$ for $\lambda \in F_{p^n}$ is the same as that of $F_M(\underline{\lambda}')$ for $\underline{\lambda}' \in V_{p^k}^e$.

Let $f(x)$ be a function from F_{p^m} to F_p. From the definition of the trace transform defined in Definition 2, it is clear that if magnitude of the crosscorrelation values of the sequence $f(\alpha^t)$ and the m-sequence $\mathrm{tr}_1^m(\alpha^t)$ is upper-bounded by $p^{\frac{m}{2}} + 1$, then the function $f(x)$ becomes a p-ary bent function defined on F_{p^m}. Therefore, from the families of p-ary sequences with optimal correlation property listed in Table 1, p-ary bent functions defined on F_{p^m} can be given as in the followings.

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

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

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

$$f_b(x) = \mathrm{tr}_1^m(b\, x^{p^{kr}+1}), \quad \text{for any } b \in F_{p^m}^* \tag{4}$$

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

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

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

Further, it is possible to construct a p-ary bent function defined on F_{p^m} as in the following theorem [2].

Theorem 4: [Kim, Jang, No, and Helleseth [2]] 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

$$f(x) = \mathrm{tr}_1^m\left(b\sum_{i=0}^{k} a_i x^{1+p^i}\right) \tag{5}$$

is bent if

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

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

Using the above theorem, the several examples of quadratic p-ary bent functions defined on the finite field are given as follows.

Example 5: For $p = 3$ and $m = 5$, the functions defined on F_{3^5} given by

$$\mathrm{tr}_1^5(x^2 + x^4 + 2x^{10})$$
$$\mathrm{tr}_1^5(x^2 + 2x^4 + x^{10})$$

are bent and for $p = 3$ and $m = 7$, the functions defined on F_{3^7} given by

$$\mathrm{tr}_1^7(x^2 + x^4)$$
$$\mathrm{tr}_1^7(x^2 + x^4 + x^{10} + x^{28})$$
$$\mathrm{tr}_1^7(x^2 + x^4 + x^{10} + 2x^{28})$$
$$\mathrm{tr}_1^7(x^2 + x^4 + 2x^{10} + x^{28})$$
$$\mathrm{tr}_1^7(x^2 + 2x^4 + x^{10} + x^{28})$$

are bent. □

Using p-ary bent functions introduced in this section, construction methods of p-ary bent sequences will be generalized and even though different p-ary bent functions can be transformed into the same form, it will be shown that the different p-ary bent functions generates the inequivalent p-ary bent sequences in the following section.

3. New Constructions of *p*-ary Bent Sequences

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

$$\mathbf{S} = \{s_i(t) \mid 0 \le i \le M-1, 0 \le t \le p^n - 2\}.$$

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

$$R_{i,l}(\tau) = \sum_{t=0}^{p^n-2} \omega^{s_i(t+\tau) - s_l(t)} \tag{6}$$

where $0 \le i, l \le M-1, 0 \le \tau \le p^n - 2$. Maximum magnitude of the correlation values is defined as

$$R_{max} = \max_{0\le i,l\le M-1, 0\le\tau\le p^n-2} |R_{i,l}(\tau)|$$

except for the case of $i = l$ 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 $p^{\frac{n}{2}} + 1$.

The balance property of the p-ary sequences is defined as follows.

Definition 6: Let $\{s(t)\}$ be a p-ary sequence of period $p^n - 1$ over F_p for some integer n. Let N_b be the number of occurrences of an element b in a period of the sequence. Then the p-ary sequence $\{s(t)\}$ is said to have the *balance property* if

$$N_b = \begin{cases} p^{n-1}, & \text{if } b \in F_p^* \\ p^{n-1} - 1, & \text{if } b = 0. \end{cases}$$

□

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 7: [Kumar and Moreno [3]] Let p be an odd prime and m be a positive 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

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

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

By using p-ary bent functions from $V_{p^k}^e$ to F_p defined in the previous section, it is possible to construct a family of p-ary bent sequences. Thus the construction of a family of p-ary bent sequences can be generalized as follows:

Theorem 8: Let p be an odd prime and let m, e, k be positive 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 *generalized p-ary bent sequences* is defined as

$$\mathbf{S} = \{s_\eta(t) \mid \eta \in F_{p^m},\ 0 \le t \le p^n - 2\}$$
$$s_\eta(t) = f(L(\alpha^t)) + \mathrm{tr}_1^n((\eta\sigma + \delta)\alpha^t) \tag{7}$$

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

Similarly to the proof of the generalized binary bent sequence in [12], the above theorem can be proved by using the modified trace transform defined in Definition 3. We begin with a lemma.

Lemma 9: 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

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

where L^* denotes an adjoint of $L(\cdot)$ [9].

Proof : The trace transform of the function $f(L(x))$ can be expressed as

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

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

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

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

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

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 $\lambda \in \text{range}(L^*)$, then we have

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

For $\lambda \notin \text{range}(L^*)$, 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

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

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

$$\text{range}(L^*) = \{\zeta\sigma \mid \zeta \in F_{p^m}\}. \tag{8}$$

Proof of Theorem 8: The trace transform of $s_\eta(x)$ can be written as

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

From Lemma 9, we can calculate the trace transform of $s_\eta(x)$ as follows.

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

where $F_M(\underline{u})$ is the modified trace transform of $f(\underline{x})$. From Eq. (8), the range of L^* has the property as follows.

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

Let

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

Then, the set H is the same for all sequences in the family of the sequences **S**.

It is well-known that the equation $x^2 + x + w = 0$ for $w \in F_{p^m}$ has a root σ_0 in $F_{p^n} \backslash F_{p^m}$, 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 $\phi \neq 0$, $| H \cap H\alpha^\tau | = 1$. 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 $\phi = 0$, $| H \cap H\alpha^\tau | = 0$. Then we proved that for $1 \leq \tau \leq p^n - 2$ and a primitive element $\alpha \in F_{p^n}$,

$$| H \cap H\alpha^{\tau} | \le 1. \tag{9}$$

Since $F_M(\underline{u})$ of the bent function $f(\underline{x})$ on $V_{p^k}^e$ takes on the values $+1$ or -1, the trace transform of the sequence $s_\eta(x)$ can be given as

$$\hat{S}_\eta(\lambda) = \begin{cases} 0, & \text{for } \lambda \notin H \\ \pm p^{\frac{m}{2}}, & \text{for } \lambda \in H. \end{cases} \tag{10}$$

The crosscorrelation of the sequences $s_{\underline{y}}(t)$ and $s_{\underline{z}}(t)$ in Eq. (6) 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

$$\begin{aligned} R_{yz}(\tau) &= -1 + \sum_{x \in F_{p^n}} \omega^{s_{\underline{y}}(x) - s_{\underline{z}}(x\alpha^{\tau})} \\ &= -1 + \sum_{\lambda \in F_{p^n}} \hat{S}_{\underline{y}}(\lambda) \hat{S}^*_{\underline{z}}(\lambda\alpha^{\tau}). \end{aligned}$$

From Eq. (9) and Eq. (10), the correlation function can be derived as

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

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

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

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 $\mathbf{S}$.

In order to prove the balance property of the sequences $s_\eta(t)$, it is enough to show that $\mathbf{B} = 0$, where $\mathbf{B}$ is defined as

$$\mathbf{B} = \sum_{x \in F_{p^n}} \omega^{s_\eta(t)}. \tag{11}$$

Combining Eq. (7) and Eq. (11), we have

$$\mathbf{B} = \sum_{x \in F_{p^n}} \omega^{f(L(\alpha^t)) - \mathrm{tr}_1^n((-\eta\sigma-\delta)\alpha^t)}.$$

From Eq. (8), $-\eta\sigma - \delta$ cannot belong to the range of L^* since $\delta \neq 0$. From Lemma 9 , it is clear that $\mathbf{B} = 0$. □

As an example, let $m = 2k$, $b \in F_{p^k}^*$, and let u be an positive integer such that $(u, p^k - 1) = 1$. Then the function $\mathrm{tr}_1^k(bx_1x_2^u)$ on $V_{p^k}^2$ is a p-ary bent function. Let $\{\beta_1, \beta_2\}$ be a basis of F_{p^m} over F_{p^k}. Then a p-ary generalized bent sequence with optimal correlation property is given as

$$\begin{aligned} s_\eta(t) &= \mathrm{tr}_1^k(b\,\mathrm{tr}_k^n(\beta_1\sigma\alpha^t)[\mathrm{tr}_k^n(\beta_2\sigma\alpha^t)]^u) \\ &\quad + \mathrm{tr}_1^n((\eta\sigma + \delta)\alpha^t). \end{aligned}$$

Similarly, using the p-ary bent function on F_{p^m} defined in Theorem 4, the p-ary bent sequences can also be constructed as follows:

Theorem 10: 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 in Eq. (5) given by

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

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

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

□

Example 11: For $p = 3$, $n = 8$, $m = 4$, and $k = 2$, the function defined on F_{3^4} given by $\mathrm{tr}_1^4(x^2 + x^4 + 2x^{10})$ is bent from Theorem 4. From Theorem 10, the family of p-ary bent sequences is given as follows,

$$\begin{aligned} \mathbf{S} &= \{s_\eta(t) \mid \eta \in F_{3^4},\ 0 \le t \le 3^8 - 2\} \\ s_\eta(t) &= \mathrm{tr}_1^4([\mathrm{tr}_4^8(\sigma\alpha^t)]^2 + [\mathrm{tr}_4^8(\sigma\alpha^t)]^4 \\ &\quad + 2[\mathrm{tr}_4^8(\sigma\alpha^t)]^{10}) + \mathrm{tr}_1^8((\eta\sigma + \delta)\alpha^t) \end{aligned}$$

where $\sigma \in F_{3^8} \backslash F_{3^4}$, $\eta \in F_{3^4}$, $\delta \in F_{3^4}^*$, and α is a primitive element of F_{3^8}. □

Using the p-ary bent sequences by Kumar and Moreno defined in Eq. (4), Moriuchi and Imamura [8] introduced the family of p-ary sequences with balanced and optimal correlation property given by

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

and it turns out to be a special case of the family of generalized p-ary bent sequences defined in Theorem 10 when $f(\cdot)$ is the p-ary bent function by Kumar and Moreno.

It was known by Sidelnikov that for $m > 1$ and $b \in F_{p^m}^*$, the function $\mathrm{tr}_1^m(b\,x^2)$ on F_{p^m} is a p-ary bent function and thus a p-ary bent sequence with optimal correlation property is given as

$$s_\eta(t) = \mathrm{tr}_1^m(b\,[\mathrm{tr}_m^n(\sigma\alpha^t)]^2) + \mathrm{tr}_1^n((\eta\sigma + \delta)\alpha^t).$$

Further, for $m = 2k$, $K = p^k + 1$, and $b \in F_{p^k}^*$, the function

$\mathrm{tr}_1^k(b\,x^K)$ on F_{p^m} from p-ary Kasami sequences is a p-ary bent function and the corresponding p-ary bent sequence is given as

$$s_\eta(t) = \mathrm{tr}_1^k(b\,[\mathrm{tr}_m^n(\sigma\alpha^t)]^K) + \mathrm{tr}_1^n((\eta\sigma + \delta)\alpha^t).$$

It is clear that the number of terms of p-ary bent sequences defined in Theorem 7 increases as their period increases but it is not true for the p-ary bent sequences in Theorem 10. 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," Proc. EUROCRYPT'93 (Lecture Notes in Computer Science 765), pp.77–101, 1994.
[2] Y.-S. Kim, J.-W. Jang, J.-S. No, and T. Helleseth, "On p-ary bent functions defined on finite fields," in Mathematical Properties of Sequences and Other Combinatorial Structures, The Kluwer International Series in Engineering and Computer Science, pp.65–76, Kluwer Academic Publishers, 2003.
[3] P.V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," IEEE Trans. Inf. Theory, vol.37, no.3, pp.603–616, May 1991.
[4] P.V. Kumar, R.A. Scholtz, and L.R. Welch, "Generalized bent functions and their properties," J. Comb. Theory A., vol.40, pp.90–107, 1985.
[5] A. Lempel and M. Cohn, "Maximal families of bent sequences," IEEE Trans. Inf. Theory, vol.28, no.6, pp.865–868, Nov. 1982.
[6] R. Lidl and H. Niederreiter, Finite Fields, vol.20 of Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.
[7] S.-C. Liu and J.F. Komo, "Nonbinary Kasami sequences over $GF(p)$," IEEE Trans. Inf. Theory, vol.38, no.4, pp.1409–1412, July 1992.
[8] T. Moriuchi and K. Imamura, "Balanced nonbinary sequences with good periodic correlation properties obtained from modified Kumar-Moreno sequences," IEEE Trans. Inf. Theory, vol.41, no.2, pp.572–576, March 1995.
[9] J.D. Olsen, R.A. Scholtz, and L.R. Welch, "Bent-function sequences," IEEE Trans. Inf. Theory, vol.28, no.6, pp.858–864, Nov. 1982.
[10] O.S. Rothaus, "On bent functions," J. Comb. Theory A., vol.20, pp.300–305, 1976.
[11] 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.
[12] L.R. Welch, "Lower bounds on the maximal cross correlation of signals," IEEE Trans. Inf. Theory, vol.20, no.3, pp.397–399, May 1974.

Young-Sik Kim received the B.S. and M.S. degrees in the School of Electrical Engineering, Seoul National University, Seoul, Korea, in 2001 and 2003, respectively. Currently, he is a Ph.D. candidate in the School of Electrical Engineering and Computer Science, Seoul National University. His research interests include pseudo random sequences, error-correcting codes, and communications theory.

Ji-Woong Jang received the B.S. and M.S. degrees in the School of Electrical Engineering, Seoul National University, Seoul, Korea, in 2000 and 2002, respectively. Currently, he is a Ph.D. candidate in the School of Electrical Engineering and Computer Science, Seoul National University. His research interests include pseudo random sequences, space-time codes, and communications theory.

Jong-Seon No received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988. He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, Korea, from September 1990 to July 1999. He joined the faculty of the School of Electrical Engineering and Computer Science, Seoul National University, in August 1999, where he is currently an Associate Professor. His area of research interests includes error-correcting codes, sequences, cryptography, space-times codes, LDPC codes, and wireless communication systems.

Tor Helleseth received Cand. Real and Dr. Philos. degrees in mathematics from University of Bergen, Bergen, Norway, in 1971 and 1979, respectively. He was a research assistant at department of mathematics in University of Bergen from 1973 to 1980. He was also a chief headquarter at the Defense in Norway from 1981 to 1984. And he joined the faculty of the Department of Informatics in University of Bergen from 1984.