New Family of p-ary Sequences with Optimal Correlation Property [1]

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

Tor Helleseth
Department of Informatics
University of Bergen, N-5020
Bergen, Norway
Email: Tor.Helleseth@ii.uib.no

Abstract

For an odd prime p and an integer $n = (2m+1)k$, a new family of p-ary sequences with optimal correlation property is constructed using the p-ary Helleseth-Gong sequences with ideal autocorrelation. Period of the sequences is $p^n - 1$ and the size of family is p^n. It is also derived that the linear span of the sequences in the family is $(m+2)\cdot n$ except the m-sequence in the family. The maximum nontrivial correlation value R_{max} does not exceed $1 + \sqrt{p^n}$, which means the optimal correlation property in terms of Welch's lower bound.

1. Introduction

In the wireless communication systems employing code-division multiple access(CDMA) scheme, a signature sequence is assigned to each user, which makes it possible to distinguish his signal from that of the other users. In design of sequences for CDMA system, the most important property of the sequences is low periodic correlation between all pairs of distinct sequences and large family size. For an odd prime p, families of p-ary sequences of period $p^n - 1$ with optimal correlation property have been found, where the optimality of correlation values means that maximum magnitude of out-of-phase autocorrelation and crosscorrelation values of any pairs of sequences of period $p^n - 1$ in the family is upper bounded by $R_{max} = p^{\frac{n}{2}} + 1$.

In this paper, for an odd prime p and integers n, m and k such that $n = (2m+1)k$, a new family of p-ary sequences of period $p^n - 1$ with optimal correlation property is constructed using the p-ary Helleseth-Gong sequences with ideal autocorrelation, where the size of the sequence family is p^n. That is, the maximum nontrivial correlation value R_{max} of all pairs of distinct sequences in the family does not exceed $p^{\frac{n}{2}}+1$, which means the optimal correlation property in terms of Welch's lower bound. It is also derived that the linear span of the sequences in the family is $(m+2)\cdot n$ except for the m-sequence in the family.

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

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

where ω is p-th root of unity, $0 \le i, j \le M-1$, and $0 \le \tau \le N-1$. 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} doesn't exceed $p^{\frac{n}{2}} + 1$.

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

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

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

Definition 1 [Kumar, Scholtz and Welch [4]] : A function $f(\underline{x})$ from V_z^n 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 value of unit magnitude for any $\underline{\lambda} \in V_z^n$. □

[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.

In this paper, we assume that the integer z is odd prime p. Thus, V_p^n 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^n to F_p.

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

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

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

□

The elements x and λ in F_{p^n} can be related to the elements $\underline{x}$ and $\underline{\lambda}$ in V_p^n as follows:

$$\begin{aligned} x &= \sum_{i=1}^{n} x_i \cdot \alpha_i \quad \Rightarrow \quad \underline{x} = (x_1, x_2, x_3, \cdots, x_n) \\ \lambda &= \sum_{i=1}^{n} \lambda_i \cdot \alpha_i \quad \Rightarrow \quad \underline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_n) \end{aligned}$$

where x_i and λ_i are in F_p and $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n\}$ is some basis of F_{p^n} over F_p. By replacing x in F_{p^n} by $\underline{x}$ in V_p^n, the function $f(x)$ from F_{p^n} to F_p makes the corresponding function $f(\underline{x})$ from V_p^n to F_p. It was known that 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 $f(\underline{x})$. Therefore, the function $f(x)$ is a generalized bent function from F_{p^n} to F_p if and only if the corresponding function $f(\underline{x})$ is a generalized bent function from V_p^n to F_p.

Let $n = ek$ and e, k be integers. A basis $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_e\}$ of F_{p^n} over F_{p^k} is said to be a *trace-orthogonal basis* if

$$\mathrm{tr}_k^n(\alpha_i \cdot \alpha_j) = \begin{cases} a_i, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases}$$

where $a_i \in F_{p^k}^*$. It is known that for any positive integer e and odd prime p, there exists a trace-orthogonal basis of F_{p^n} over F_{p^k} [9]. The elements x and λ in F_{p^n} can be related to the elements $\underline{x}$ and $\underline{\lambda}$ in the e-dimensional vector space $V_{p^k}^e$ over the finite field F_{p^k} as follows:

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

$$\lambda = \sum_{i=1}^{e} \lambda_i \cdot \alpha_i \quad \Rightarrow \quad \underline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_e) \qquad (2)$$

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

$$\mathrm{tr}_k^n(\lambda \cdot x) = \sum_{i=1}^{e} a_i \cdot \lambda_i \cdot x_i. \qquad (3)$$

Let $\lambda_i^{'} = a_i \cdot \lambda_i$ for $i, 1 \le i \le e$ and $\underline{\lambda}^{'} = (\lambda_1^{'}, \lambda_2^{'}, \lambda_3^{'}, \cdots, \lambda_e^{'})$. Then the relation in (3) can be rewritten as

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

Suppose that using (1) and (2), a function $f(x)$ from F_{p^n} to F_{p^k} is related to the corresponding function $f(\underline{x})$ from $V_{p^k}^e$ to F_{p^k}. Then the trace transform in Definition 2 can be modified into the trace transform defined in the intermediate field as follows.

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

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

□

It is clear that the trace transform of a function $\mathrm{tr}_1^k(f(\underline{x}))$ from $V_{p^k}^e$ to F_p is related to the trace transform $F(\lambda)$ of the corresponding function $\mathrm{tr}_1^k(f(x))$ from F_{p^n} to F_p as follows

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

That is, the set of the trace transform values of the function $\mathrm{tr}_1^k(f(\underline{x}))$ is the same as that of the corresponding function $\mathrm{tr}_1^k(f(x))$. Therefore, if the trace transform of the function $\mathrm{tr}_1^k(f(x))$ or $\mathrm{tr}_1^k(f(\underline{x}))$ only takes the value of unit magnitude, the functions $\mathrm{tr}_1^k(f(x))$ and $\mathrm{tr}_1^k(f(\underline{x}))$ become generalized bent functions.

Let $Q(x)$ be a quadratic form from F_{p^n} to F_{p^k}. Using (1), the quadratic form $Q(x)$ can be expressed as

$$Q(\underline{x}) = \sum_{i=1}^{e} \sum_{j=1}^{e} b_{ij} x_i x_j \qquad (4)$$

where $b_{ij} \in F_{p^k}$. It is known from Dickson [1] that for an odd integer ρ, any quadratic form can be transformed into a canonical form by linear transformation as follows

$$Q(\underline{x}) = \sum_{i=1}^{\rho} r \cdot x_i^2 \qquad (5)$$

where $\rho \le e$ and $r = 1$ or a quadratic nonresidue in F_{p^k}. Then the rank of the quadratic function $Q(\underline{x})$

from $V_{p^k}^e$ to F_{p^k} is ρ. It is clear that the rank of $Q(x)$ and the corresponding function $Q(\underline{x})$ in (4) and (5) are the same. From Definition 3, we easily derived the following lemma.

Lemma 1 : $\mathrm{tr}_1^k(Q(\underline{x}))$ is a quadratic p-ary bent function from $V_{p^k}^e$ to F_p if and only if the quadratic function $Q(\underline{x})$ from $V_{p^k}^e$ to F_{p^k} has full rank e. □

Helleseth and Gong introduced new p-ary sequences with ideal autocorrelation, which are referred to as Helleseth-Gong(HG) sequences [2] as in the following theorem:

Theorem 1 [Helleseth and Gong [2]]: Let n, m and k be positive integers such that $n = (2m+1)k$. Let $s, 1 \le s \le 2m$ be a positive integer such that $gcd(2m+1, s) = 1$. Let p be an odd prime and α be a primitive element in F_{p^n}. Let $b_0 = 1$ and $b_{ls} = (-1)^l$. Let $q = p^k$ and $u_0 = \frac{b_0}{2}$ and $u_l = b_{2l} = b_{2m+1-2l}$ for $l = 0, 1, 2, \cdots, m$. Then the Helleseth-Gong sequences of period $p^n - 1$ given by

$$s(t) = \mathrm{tr}_1^n(\sum_{l=0}^{m} u_l \cdot \alpha^{\frac{q^{2l}+1}{2}t}) \tag{6}$$

have the ideal autocorrelation property. □

Let $F_{p^n}^* = F_{p^n} \backslash \{0\}$ and $x = \alpha^t$. Then the Helleseth-Gong sequences in (6) can also be written as

$$\mathrm{tr}_1^n(\sum_{l=0}^{m} u_l \cdot x^{\frac{q^{2l}+1}{2}}), \qquad x \in F_{p^n}^*.$$

Let $h(x)$ be the Helleseth-Gong polynomial defined by

$$h(x) = \sum_{l=0}^{m} u_l \cdot x^{\frac{q^{2l}+1}{2}}, \quad x \in F_{p^n}.$$

Then the Helleseth-Gong sequences in (6) can be rewritten as

$$s(t) = \mathrm{tr}_1^n(h(\alpha^t)), \quad 0 \le t \le p^n - 2.$$

We can construct the new p-ary sequence using the Helleseth-Gong sequence as follows

$$\begin{aligned} s_b(t) &= \mathrm{tr}_1^n(\alpha^t) + \mathrm{tr}_1^n(h(b \cdot \alpha^{2t})) \\ &= \mathrm{tr}_1^n(\alpha^t + \sum_{l=0}^{m} u_l \cdot b^{\frac{q^{2l}+1}{2}} \cdot \alpha^{(q^{2l}+1)t}) \end{aligned} \tag{7}$$

where $b \in F_{p^n}$. It is clear that the sequences in (7) have period of $p^n - 1$.

3. New family of p-ary Sequences with optimal correlation and large linear span

Using the new p-ary sequence defined in (7), a family of p-ary sequences with family size p^n and optimal correlation property can be constructed as follows:

Theorem 2 : Let $s_b(t)$ be the p-ary sequence defined in (7). Then the family of p-ary sequences given by

$$\mathbf{S} = \{s_b(t) \mid b \in F_{p^n},\ 0 \le t \le p^n - 2\}$$

has the optimal correlation property with $R_{max} = p^{\frac{n}{2}} + 1$.

Proof: The crosscorrelation function of two p-ary sequences $s_{b_i}(x)$ and $s_{b_j}(x)$ in $\mathbf{S}$ can be rewritten as

$$\begin{aligned} R_{ij}(\tau) &+ 1 \\ &= \sum_{t=0}^{p^n-2} w^{s_{b_i}(t+\tau) - s_{b_j}(t)} + 1 \\ &= \sum_{x \in F_{p^n}} w^{\mathrm{tr}_1^n(c \cdot x + h(b_i \cdot c^2 \cdot x^2) - x - h(b_j \cdot x^2))} \end{aligned} \tag{8}$$

where $c = \alpha^\tau \in F_{p^n}^*$. Then the proof can be classified into the following three cases.
Case (i) $c = 1$, $b_i = b_j$:
It is clear that $R_{ij}(\tau) = p^n - 1$.
Case (ii) $c \neq 1$, $b_i c^2 = b_j$:
It is also clear that $R_{ij}(\tau) = -1$.
Case (iii) $b_i c^2 \neq b_j$:
The condition excludes the case of $b_i = b_j = 0$. Thus we will prove it for $b_j \neq 0$ because the proof of the case for $b_i \neq 0$ is similar to that for $b_j \neq 0$.

Since $\frac{n}{k}$ is an odd integer, it is clear that a quadratic nonresidue in F_{p^k} is also a quadratic nonresidue in F_{p^n}. Thus b_i and b_j can be expressed as $b_i = r_i \cdot a_i^2$ and $b_j = r_j \cdot a_j^2$, where $a_i, a_j \in F_{p^n}$ and r_i and r_j are 1 or quadratic nonresidue in F_{p^k}. We assume that $b_j \neq 0$ and thus $a_j \neq 0$. Let $u = \frac{a_i}{a_j} \cdot c$ and $y = a_j \cdot x$. Then the crosscorrelation function in (8) can be rewritten as

$$\begin{aligned} R_{ij}(\tau) &+ 1 \\ &= \sum_{x \in F_{p^n}} w^{\mathrm{tr}_1^n(h(r_i \cdot a_i^2 \cdot c^2 \cdot x^2) - h(r_j \cdot a_j^2 \cdot x^2)) + \mathrm{tr}_1^n((c-1) \cdot x)} \\ &= \sum_{y \in F_{p^n}} w^{\mathrm{tr}_1^n(h(r_i \cdot u^2 \cdot y^2) - h(r_j \cdot y^2)) + \mathrm{tr}_1^n(\frac{c-1}{a_j} \cdot y)}. \end{aligned}$$

Using the property that for $r \in F_{p^k}$, $h(rx) = rh(x)$, we have

$$\begin{aligned} & R_{ij}(\tau) + 1 \\ &= \sum_{y \in F_{p^n}} w^{\mathrm{tr}_1^n(r_i \cdot h(u^2 \cdot y^2) - r_j \cdot h(y^2)) + \mathrm{tr}_1^n(\frac{c-1}{a_j} \cdot y)} \\ &= \sum_{y \in F_{p^n}} w^{\mathrm{tr}_1^k(\mathrm{tr}_k^n(r_i \cdot h(u^2 \cdot y^2) - r_j \cdot h(y^2)))} \qquad (9) \\ &\quad \cdot w^{\mathrm{tr}_1^n(\frac{c-1}{a_j} \cdot y)}. \qquad (10) \end{aligned}$$

Let $Q(y)$ be the quadratic function defined by

$$\begin{aligned} Q(y) &= \mathrm{tr}_k^n(r_i \cdot h(u^2 \cdot y^2) - r_j \cdot h(y^2)) \\ &= \mathrm{tr}_k^n(\sum_{l=0}^{m} u_l \cdot [r_i \cdot u^{q^{2l}+1} - r_j] \cdot y^{q^{2l}+1}) \\ &= r_j \cdot \mathrm{tr}_k^n(\sum_{l=0}^{m} u_l \cdot [\frac{r_i}{r_j} \cdot u^{q^{2l}+1} - 1] \cdot y^{q^{2l}+1}). \end{aligned}$$

Then (10) corresponds to the trace transform of the quadratic function $\mathrm{tr}_1^k(Q(y))$ from F_{p^n} to F_p defined in Definition 2. If the quadratic function $\mathrm{tr}_1^k(Q(y))$ is a p-ary bent function, then we have $|R_{ij}(\tau)+1| = p^{\frac{n}{2}}$. From Definition 3 and Lemma 1, if $Q(y)$ has full rank, then $\mathrm{tr}_1^k(Q(y))$ is bent. Thus it is sufficient to show that $Q(y)$ has full rank $2m+1$.

It is already known that the rank of the quadratic function $Q(y)$ becomes ρ if $q^{2m+1-\rho}$ is the number of solutions $z \in F_{p^n}$, satisfying $Q(y+z) = Q(y)$ for all $y \in F_{p^n}$. Let $a_l = u_l \cdot [\frac{r_i}{r_j} \cdot u^{q^{2l}+1} - 1]$. Then we have

$$\mathrm{tr}_k^n(\sum_{l=0}^{m} a_l \cdot (y+z)^{q^{2l}+1}) = \mathrm{tr}_k^n(\sum_{l=0}^{m} a_l \cdot y^{q^{2l}+1}),$$

which can be modified into

$$\mathrm{tr}_k^n(\sum_{l=0}^{m} a_l \cdot (y^{q^{2l}} z + y z^{q^{2l}}) + \sum_{l=0}^{m} a_l \cdot z^{q^{2l}+1}) = 0.$$

Raising the first term to the $q^{2m+1-2l}$ power, we have

$$\mathrm{tr}_k^n(y \cdot [\sum_{l=0}^{m} a_l^{q^{2m+1-2l}} \cdot z^{q^{2m+1-2l}} + \sum_{l=0}^{m} a_l \cdot z^{q^{2l}}] + \sum_{l=0}^{m} a_l \cdot z^{q^{2l}+1}) = 0,$$

which is equivalent to

$$\sum_{l=0}^{m} a_l^{q^{2m+1-2l}} \cdot z^{q^{2m+1-2l}} + \sum_{l=0}^{m} a_l \cdot z^{q^{2l}} = 0 \quad (11)$$

$$\mathrm{tr}_k^n(\sum_{l=0}^{m} a_l \cdot z^{q^{2l}+1}) = 0.$$

The equation (11) can be rewritten as

$$\sum_{l=0}^{m} u_l \cdot \{(\frac{r_i}{r_j} \cdot u^{(q^{2l}+1)q^{2m+1-2l}} - 1) \cdot z^{q^{2m+1-2l}} + (\frac{r_i}{r_j} \cdot u^{(q^{2l}+1)} - 1) \cdot z^{q^{2l}}\} = 0$$

and thus, we have

$$\sum_{l=0}^{2m} b_l \cdot (\frac{r_i}{r_j} \cdot u^{(q^{2l}+1)} - 1) \cdot z^{q^{2l}} = 0$$

where $u_0 = \frac{b_0}{2}$, $u_l = b_{2l} = b_{2m+1-2l}$. To prove that the rank of $Q(y)$ is $\rho = 2m+1$, we have to show that the equation

$$\sum_{l=0}^{2m} b_l \cdot (\frac{r_i}{r_j} \cdot (\frac{a_i}{a_j} \cdot c)^{q^{2l}+1} - 1) \cdot z^{q^{2l}} = 0$$

has $z = 0$ as its only solution for any $\frac{r_i}{r_j} \cdot (\frac{a_i}{a_j} \cdot c)^2 \neq 1$, which is already proved in [2]. From the condition, it clear that $\frac{r_i}{r_j} \cdot (\frac{a_i}{a_j} \cdot c)^2 = \frac{b_i c^2}{b_j} \neq 1$ and thus we prove the theorem. □

The linear span of the p-ary sequences introduced by Sidelnikov and Kumar and Moreno [3] is given as $2n$ except for the m-sequence in the family but the linear span of the new p-ary sequences $s_b(t)$ in Theorem 2 is derived as in the following theorem.

Theorem 3 : The linear span of the sequence $s_b(t)$ for $b \in F_{p^n}^*$ defined in Theorem 2 is $(m+2) \cdot n$.

Proof: For $d_i = q^{2i}+1, 0 \leq i \leq m$ in (7), $gcd(d_i, p^n - 1) = 2$. It is clear that α^{d_i} doesn't belong to any subfield of F_{p^n}. Thus the coset of α^2 in F_{p^n} has size n and so does the element α^{d_i}. Therefore, the linear span of $s_b(x)$ is $(m+2) \cdot n$.

References

[1] L.E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover, New York 1958.

[2] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation function," preprint, 2001.

[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] F.J. McWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes,* New York: North-Holland, 1977.

[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] 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.

[10] M.K. Simon, J.K. Omura, R.A. Scholtz and B.K. Levitt, *Spread Spectrum Communications*, vol. 1, Computer Science Press, Rockville, MD, 1985.

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