International Symposium on Information Theory and its Applications, ISITA2008
Auckland, New Zealand, 7-10, December, 2008

New Construction of $p-$ary Sequence Family With Large Linear Span

Young-Sik Kim†, Jung-Soo Chung‡, and Jong-Seon No‡

† Samsung Electronics, Co., Ltd.
Yongin, Gyeonggi-do, 446-711, Korea
E-mail: mypurist@gmail.com

‡ Department of EECS, INMC
Seoul National University
Seoul 151-744, Korea
E-mail: integer@ccl.snu.ac.kr, jsno@snu.ac.kr

Abstract

In this paper, we propose a method to construct sequence family $\mathcal{S}_r = \{\mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^t) + \mathrm{tr}_m^n(b\alpha^{dt})]^r) \mid b \in F_{p^n},\ 0 \le t < p^n - 1\}$ with large linear span from a sequence family $\mathcal{S}_1$, where $\gcd(r, p^m - 1) = 1$. Let $T = (p^n - 1)/(p^m - 1)$. If $dT \equiv T \bmod p^n - 1$, the correlation distributions of families $\mathcal{S}_r$ are the same. Two examples of decimation factor d satisfying the condition $dT \equiv T \bmod p^n - 1$ are given and the linear span of the ternary sequences in $\mathcal{S}_r$ with $d = 2p^m - 1$ is derived for some cases.

1. Introduction

Pseudo-noise (PN) sequences with large linear span play an important role in the secure communication and cryptographic applications. Since the linear span of sequences is related to the difficulty of prediction for next values using the previous values, it is desirable to make PN sequences with large linear span for secure communications.

For a long time, many sequence families with good correlation property are proposed. In this paper, we propose a method to construct sequence family $\mathcal{S}_r$ with large linear span from a sequence family $\mathcal{S}_1$. If $dT \equiv T \bmod p^n - 1$, the correlation distributions of families $\mathcal{S}_r$ are the same for some r where $\gcd(r, p^m - 1) = 1$ and $n = em$. Two examples of decimation factor d satisfying the condition $dT \equiv T \bmod p^n - 1$ are suggested and the linear span of the ternary sequences in $\mathcal{S}_r$ with $d = 2p^m - 1$ is derived for some cases.

2. Correlation Distribution of p-ary Sequences Family

This work was supported by the IT R&D program of MKE/IITA [2008-F-007-01, Intelligent Wireless Communication Systems in 3 Dimensional Environment] and the MEST, the MKE, and the MOLAB, Korea, through the fostering project of the Laboratory of Excellency.

Let p be an odd prime and F_{p^n} be the finite field with p^n elements. The trace function $\mathrm{tr}_m^n(\cdot)$ from F_{p^n} to F_{p^m} is defined as $\mathrm{tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{p^{mi}}$ where $x \in F_{p^n}$ and $m|n$. Let α be a primitive element of F_{p^n}. Then a p-ary m-sequence $s(t)$ of period $p^n - 1$ can be written in terms of the trace function as $s(t) = \mathrm{tr}_1^n(\alpha^t)$ where $0 \le t < p^n - 1$.

The cross-correlation function of $s_{b_1}(t)$ and $s_{b_2}(t)$ at shift τ is defined as

$$C_{b_1,b_2}(\tau) = \sum_{t=0}^{p^n-2} \omega^{s_{b_1}(t+\tau) - s_{b_2}(t)} \tag{1}$$

where ω is a primitive complex p-th root of unity.

A sequence family $\mathcal{S}_1$ can be defined as

$$\mathcal{S}_1 = \{s_b(t) \mid b \in Z,\ 0 \le t < p^n - 1\}$$

where $s_b(t) = \mathrm{tr}_1^m(\mathrm{tr}_m^n(\alpha^t) + \mathrm{tr}_m^n(b\alpha^{dt}))$ and Z is a subset of F_{p^n}. The above definition can be generalized as

$$\mathcal{S}_r = \{s_b(t) \mid b \in Z,\ 0 \le t < p^n - 1\} \tag{2}$$

where $s_b(t) = \mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^t) + \mathrm{tr}_m^n(b\alpha^{dt})]^r)$ and $\gcd(r, p^m - 1) = 1$.

Let $T = (p^n - 1)/(p^m - 1)$. If $dT \equiv T \bmod p^n - 1$, the correlation distribution of $\mathcal{S}_r$ and $\mathcal{S}_1$ is the same as in the following theorem.

Theorem 1 Let $n = em$ and $T = (p^n - 1)/(p^m - 1)$. Let d be a positive integer such that $dT \equiv T \bmod p^n - 1$. The cross-correlation distribution of $\mathcal{S}_r$ is the same as that of $\mathcal{S}_1$.

Proof: Note that the cross-correlation of $s_{b_1}(t)$ and $s_{b_2}(t)$ can be written as

$$C_{b_1,b_2}(\tau) = \sum_{t=0}^{p^n-2} \omega^{\mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^{t+\tau}) + \mathrm{tr}_m^n(b_1\alpha^{d(t+\tau)})]^r)} \times \omega^{-\mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^t) + \mathrm{tr}_m^n(b_2\alpha^{dt})]^r)}. \tag{3}$$

Let t_1 and t_2 be the digits in the base-T expansion of t, $0 \le t < p^n - 1$. That is, $t = t_1 T + t_2$, where $0 \le t_1 < p^m - 1$ and $0 \le t_2 < T$. From $dT = T \bmod p^n - 1$, (3) can be rewritten as

$$C_{b_1,b_2}(\tau) = \sum_{t_2=0}^{T-1} \sum_{t_1=0}^{p^m-2} \omega^{\mathrm{tr}_1^m(\alpha^{rTt_1} h_r(t_2,\tau,b_1,b_2))} = -T + \sum_{t_2=0}^{T-1} \sum_{\beta \in F_{p^m}} \omega^{\mathrm{tr}_1^m(\beta h_r(t_2,\tau,b_1,b_2))} \quad (4)$$

where $h_r(t_2,\tau,b_1,b_2) = [\mathrm{tr}_m^n(\alpha^{t_2+\tau}) + \mathrm{tr}_m^n(b_1\alpha^{d(t_2+\tau)})]^r - [\mathrm{tr}_m^n(\alpha^{t_2}) + \mathrm{tr}_m^n(b_2\alpha^{dt_2})]^r$. If $h_r(t_2,\tau,b_1,b_2)) \neq 0$, the inner sum is vanished. Otherwise, the inner sum is p^m. Thus, we have to count the number of t_2 satisfying $h_r(t_2,\tau,b_1,b_2) = 0$.

Let $K_r(\tau,b_1,b_2)$ be the number of t_2, $0 \le t_2 < T$, satisfying $h_r(t_2,\tau,b_1,b_2) = 0$. Since $(r, p^m - 1) = 1$, $K_r(\tau,b_1,b_2)$ is the same as the number of t_2, $0 \le t_2 < T$, satisfying

$$\mathrm{tr}_m^n(\alpha^{t_2+\tau}) + \mathrm{tr}_m^n(b_1\alpha^{d(t_2+\tau)}) = \mathrm{tr}_m^n(\alpha^{t_2}) + \mathrm{tr}_m^n(b_2\alpha^{dt_2}) \quad (5)$$

that is, $K_1(\tau,b_1,b_2)$. Thus, (4) can be rewritten as

$$C_{b_1,b_2}(\tau) = (K_1(\tau,b_1,b_2) - 1)p^{2k} - 1. \quad (6)$$

Therefore, the correlation distribution of a pair of sequences in $\mathcal{S}_r$ is the same as that in $\mathcal{S}_1$. □

Two examples for the above theorem are given as follows.

Corollary 2 Let $p^m \not\equiv 2 \bmod 3$. For $n = 2m$ and $d = 2p^m - 1$, the correlation distribution of a pair of sequences in $\mathcal{S}_r$ is the same as that in $\mathcal{S}_1$.

Proof: Since we have

$$dT = 2(p^n - 1) + p^m + 1 \equiv T \bmod p^n - 1$$

the proof is done from Theorem 1. □

Corollary 3 [2] Let $n = 4k$ and $d = (p^{2k}+1/2)^2$. The correlation distribution of a pair of sequences in $\mathcal{S}_r$ is the same as that in $\mathcal{S}_1$.

Proof: Since $p^{2k} + 3 \equiv 0 \bmod 4$, we have

$$dT = \Big(\frac{p^{2k}+3}{4}\Big)(p^n - 1) + T \equiv T \bmod p^n - 1.$$

Therefore, the statement is proved from Theorem 1. □

3. Linear Span of Ternary Sequences

Now we will derive the linear span of ternary sequences in $\mathcal{S}_r$ with $d = 2p^m - 1$ for some special cases of r. From Blahut's theorem [1], it is known that the linear complexity of sequence $s_b(t)$ in $\mathcal{S}_r$ can be determined by deriving the number of nonzero terms in

$$s_b(t) = \sum_{j=0}^{p^n-2} c_j \alpha^{jt}, \quad c_j \in F_p.$$

Let $n = 2m$ and $d = 2p^m - 1$. Inner trace of $s_b(t)$ in (2) can be rewritten as

$$\mathrm{tr}_m^n(\alpha^t + b\alpha^{dt}) = \alpha^{p^m t} + b^{p^m}\alpha^{p^m dt} + \alpha^t + b\alpha^{dt}. \quad (7)$$

Suppose $p^m \equiv -1 \pmod 4$. Then $\gcd((p^m - 1)/2, 2(p^m + 1)) = 1$ and the primitive element α of $F_{p^{2m}}$ can be written as $\alpha = \beta\gamma$ with $\beta^{(p^m-1)/2} = 1$ and $\gamma^{2(p^m+1)} = 1$. And we have

$$d = 2p^m - 1 = \begin{cases} 1 \bmod \frac{1}{2}(p^m - 1) \\ -3 \bmod 2(p^m + 1). \end{cases}$$

Note that $\beta^{p^m} = \beta$ and $\gamma^{p^m} = -\gamma^{-1}$. Then (7) can be written as

$$\begin{aligned} &\mathrm{tr}_m^n(\alpha^t + b\alpha^{dt}) \\ &\quad = \beta^t(-1)^t\gamma^{-t} + b^{p^m}\beta^t(-1)^t\gamma^{3t} + \beta^t\gamma^t + b\beta^t\gamma^{-3t} \\ &\quad = \beta^t\gamma^{-3t}(b^{p^m}(-1)^t\gamma^{6t} + \gamma^{4t} + (-1)^t\gamma^{2t} + b). \end{aligned}$$

Let $y = (-1)^t\gamma^{2t}$ and $x = \beta^t\gamma^{-3t}$. Note that $x^{p^m-1} = \beta^{p^m t}\gamma^{-3p^m t}/\beta^t\gamma^{-3t} = (-1)^t\gamma^{6t} = y^3$. And $y^{p^m} = y^{-1}$. Then we have

$$\mathrm{tr}_m^n(\alpha^t + b\alpha^{dt}) = x(b^{p^m}y^3 + y^2 + y + b) = xg(y)$$

where $g(y) = b^{p^m}y^3 + y^2 + y + b$.

Suppose $p^m \equiv 1 \pmod 4$. Then $\gcd(2(p^m - 1), (p^m + 1)/2) = 1$ and the primitive element α of $F_{p^{2m}}$ can be written as $\alpha = \beta\gamma$ with $\beta^{2(p^m-1)} = 1$ and $\gamma^{(p^m+1)/2} = 1$. And we have

$$d = 2p^m - 1 = \begin{cases} 1 \bmod 2(p^m - 1) \\ -3 \bmod \frac{1}{2}(p^m + 1). \end{cases}$$

Note that $\beta^{p^m} = -\beta$ and $\gamma^{p^m} = \gamma^{-1}$. Similarly, (7) can be written as

$$\mathrm{tr}_m^n(\alpha^t + b\alpha^{dt}) = x(b^{p^m}y^3 + y^2 + y + b) = xg(y).$$

The exponent r in (2) can be expanded as

$$r = \sum_{i=1}^{w} a_i p^{l_i}, \qquad 1 \le a_i \le p - 1 \quad (8)$$

where l_i's are distinct integers in the range $0 \le l_i < m$ for all i and w is the Hamming weight of r, that is, the number of nonzero exponents in the p-adic expansion of r. Without loss of generality, we can assume that $0 = l_1 < l_2 < l_3 < \cdots < l_w < m$. Let R_1 and R_2 be the number of $a_i = 1$ and $a_i = 2$, respectively. Then, we can derive the linear complexity of ternary sequences for some special case.

Then, a sequence in $\mathcal{S}_r$ can be written as

$$s_b(t) = \mathrm{tr}_1^m(x^r[g(y)]^r) = \sum_{s=0}^{2k-1} x^{rp^s}[g(y)]^{rp^s}. \quad (9)$$

For $p \neq 3$, we have $p^m \equiv 1 \bmod 3$. Note that the summands in (9) can be expanded as

$$x^r[g(y)]^r = \sum_{l=0}^{2r} c_l x^{\frac{(p^m-1)l}{3}+r}$$

where $c_l \in F_{p^n}$. The right-hand side is raised with two distinct powers p^{s_i} and p^{s_j}, where $0 \le s_i < s_j \le m-1$. If there are overlapped terms with the same power of x between $x^{rp^{s_i}}[g(y)]^{rp^{s_i}}$ and $x^{rp^{s_j}}[g(y)]^{rp^{s_j}}$, we have

$$(\frac{p^m-1}{3}l_1 + r)p^s \equiv \frac{p^m-1}{3}l_2 + r \bmod p^n - 1 \quad (10)$$

where $s = s_j - s_i$, $0 < s \le m-1$. Then (10) can be rewritten as

$$(p^s - 1)r \equiv 0 \bmod \frac{p^m-1}{3}$$

which is a contradiction because $\gcd(r, (p^m-1)/3) = 1$ and $(p^m-1)/3 - (p^s-1) \ge (p^{m-1}(p-3)+1)/3 > 0$.

If $p = 3$, it is clear that $3^{n-1} \equiv 1/3 \bmod 3^n - 1$. Therefore, from

$$(3^{n-1}(p^m-1)l_1 + r)p^{s_j} \equiv (3^{n-1}(p^m-1)l_2 + r)p^{s_i} \bmod p^n - 1,$$

we have

$$(p^s - 1)r \equiv 0 \bmod p^m - 1.$$

which is a contradiction because $p^m > p^s$.

Therefore, the exponents of x occurring in the expansion of any two terms $x^{rp^{s_i}}[g(y)]^{rp^{s_i}}$ and $x^{rp^{s_j}}[g(y)]^{rp^{s_j}}$ in the above sum are distinct. Thus, the linear complexity of the sequence is exactly m times the number of distinct power of x (having nonzero coefficients) in the expansion of (9).

Now, we have to count the number of terms in the expansion of the function $[g(y)]^r$. Using (8), $[g(y)]^r$ can be rewritten as

$$[g(y)]^r = \prod_{i=1}^{w} g_i(y)$$

where $g_i(y) = [b^{p^{m+l_i}}y^{3p^{l_i}} + y^{2p^{l_i}} + y^{p^{l_i}} + b^{p^{l_i}}]^{a_i}$.

By counting the number of non-zero terms in $g_i(y)$, the linear span of sequences in $\mathcal{S}_r$ can be derived. In the following theorem, we will derive the linear span of ternary sequences in $\mathcal{S}_r$ with $d = 2p^m - 1$ for some special cases.

Theorem 4 Let $l_{i+1} > l_i + 1$ and $d = 2p^m - 1$ where $p^m \not\equiv 2 \bmod 3$. The linear span L of ternary sequences in the family $\mathcal{S}_r$ is given as

$$L = \begin{cases} 2^{R_1} \cdot 3^{R_2}, & \text{if } b' = 0 \\ 4^{R_1} \cdot 5^{R_2}, & \text{if } b' = 1 \\ 4^{R_1} \cdot 6^{R_2}, & \text{if } b' = \alpha^{\frac{3^m-1}{2}} \\ 4^{R_1} \cdot 7^{R_2}, & \text{otherwise} \end{cases}$$

where R_j $(j = 1, 2)$ is the number of coefficients in (8) satisfying $a_i = j$.

Proof: Let $b^{p^{l_i}} = b'$ and $y^{p^{l_i}} = z$. We will use $g(z)$ instead of $g(y)$. If $a_i = 1$, we have

$$g(z) = \begin{cases} z^2 + z, & \text{if } b' = 0 \\ b'^{3^m}z^3 + z^2 + z + b', & \text{otherwise.} \end{cases}$$

If $a_i = 2$, $g(z)$ can be expanded as $g(z) = b'^{2\cdot 3^m}z^6 + 2b'^{3^m}z^5 + (2b'^{3^m}+1)z^4 + 2(b'^{3^m+1}+1)z^3 + (2b'+1)z^2 + 2b'z + b'^2$. Therefore, we can count the number of terms $g(z)$ as

$$\text{The number of terms of } g(z) = \begin{cases} 3, & \text{if } b' = 0 \\ 5, & \text{if } b' = 1 \\ 6, & \text{if } b' = \alpha^{\frac{3^m-1}{2}} \\ 7, & \text{otherwise.} \end{cases}$$

□

References

[1] R. E. Blahut, "Transform techniques for error control codes," *IBM J. Res. Develop.*, vol. 23, pp. 299–315, 1979.

[2] E.-Y. Seo, Y.-S. Kim, J.-S. No, and D.-J. Shin, "Cross-correlation distribution of p-ary m-sequence of period $p^{4k} - 1$ and its decimated sequences by $((p^{2k}+1)/2)^2$," to be published in *IEEE Trans. Inf. Theory*, July 2008.

[3] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, pp. 209–232, 1976.