A New Large Family of Binary Sequences with Large Linear Span and Low Correlation

Jun Chen[1,2], Yun Chen[2]

[1]School of Information Science and Technology, Southwest Jiaotong University, Sichuan, China
[2]Department of Computer Science, Chengdu University of Information and Technology, Sichuan, China
chenjun@cuit.edu.cn, chy@cuit.edu.cn

Abstract - Let n, m and r be three positive integers such that $n = 2m$ and $\gcd(r, 2^m - 1) = 1$, a new family $S^{(r)}$ of $2^{5n/2}$ binary sequences of period $2^n - 1$ is proposed. The presented family takes 7-valued out-of-phase atuo- and cross-correlation values $-2^{n/2} - 1$, -1, $2^{n/2} - 1$, $2 \cdot 2^{n/2} - 1$, $3 \cdot 2^{n/2} - 1$, $4 \cdot 2^{n/2} - 1$ and $5 \cdot 2^{n/2} - 1$. For $r = (2^{m-1} - 1)/7$ and $m \equiv 1 \bmod 3$, it is proved that the linear span of sequences in $S^{(r)}$ is $n \cdot l^{(n-2)/6}/2$, where l = 2, 3, 4, 5, 6, 7, and the distribution of linear span of sequences in $S^{(r)}$ is determined.

Index Terms - Sequence, Family size, Linear span, Low correlation.

I. Introduction

Binary pseudo-noise sequences family with low correlation, large size and large linear span is important for code-division multiple-access (CDMA) communication systems [1]. In CDMA systems, several users share the same bandwidth, and each user is assigned a distinct spreading sequence. To distinguish each user and minimize mutual interference, we must have low crosscorrelation between distinct sequences. Furthermore, we must also have low autocorrelation between a sequence and its shift time version in order to acquire the accurate phase information at the receiver. Large family size is required to support a large number of distinct users, and the larger size of the sequences, the higher capacity of the systems. To resist attacks from the application of Berlekamp-Massey algorithm, the sequences should also have large linear span. Families of sequences with optimal correlation such as Kasami sequences [2], bent function sequences [3] and Gold sequences [4] have been found. Later on, other binary sequences families with low correlation are proposed, and some of them have large family size [5-9] or large linear span [10-12].

Quadratic functions and homogeneous functions over finite fields are useful tools for design of sequences with low correlation. The later are specially used to design *d*-form sequences. Applying lifting idea to sets of *d*-form sequence, new families of sequences are found [10-12]. Some of them have large linear span [10-12]. Zeng [9] presented a large family by lifting the sequences which combines Niho sequences [13] and Helleseth sequences [14].

In this paper, for $n = 2m$, and r relatively prime to $2^{n/2} - 1$, we construct a new large family $S^{(r)}$ of binary sequences by using a new 2-form function which is an extension of the 2-form function in [14]. The presented family has 7-valued nontrivial correlation values $-2^{n/2} - 1$, -1, $2^{n/2} - 1$, $2^{n/2+1} - 1$, $3 \cdot 2^{n/2} - 1$, $2^{n/2+2} - 1$ and $5 \cdot 2^{n/2} - 1$. The sequences in $S^{(1)}$ are constructed from a new 2-form function, and those in $S^{(r)}$ are lifting of $S^{(1)}$. For $r = (2^{n/2-1} - 1)/7$ and $n \equiv 2 \bmod 6$, the exact linear span of sequences in $S^{(r)}$ is proved to be $n \cdot l^{(n-2)/6}/2$, where $l = 2, 3, 4, 5, 6, 7$ and the distribution of linear span of sequences in $S^{(r)}$ is deteremined.

This paper is organized as follows. Section 2 gives some preliminaries. Section 3 constructs the sequences family $S^{(r)}$ and determines its correlation values and the liner span of its sequences. Section 4 concludes the study.

In order to help the reader to understand the relationship between the new large family of sequences and the previously known large families of sequences, we summarize the relationship among these families with large family sizes in Table 1.

TABLE 1 Comparison of Binary Sequences with Large Family Sizes

Family of sequences	n	period	family size	$R_{\max}$	linear span (minimal, maximal)
Chang et al.[5]	odd	$2^n - 1$	2^{2n}	$2^{\frac{n+3}{2}} - 1$	$(n, 3n)$
Rothaus [6]	odd	$2^n - 1$	$2^{2n} + 2^n + 1$	$2^{\frac{n+3}{2}} - 1$	$(n, 3n)$
Yu and Gong $S_e(2)$ [7]	even	$2^n - 1$	2^{2n}	$2^{\frac{n}{2}+2} - 1$	$(\frac{n(n-3)}{2}, \frac{n(n+1)}{2})$
Zhou et al. S_1^k [8]	odd	$2^n - 1$	2^{2n}	$2^{\frac{n+3}{2}} - 1$	$(\frac{n(n-3)}{2}, \frac{n(n+1)}{2})$
Construction 2 in [9]	even	$2^n - 1$	$2^{\frac{5n}{2}}$	$5 \cdot 2^{\frac{n}{2}} - 1$	unknown
Sequences we study	$n \equiv 2 \bmod 6$	$2^n - 1$	$2^{\frac{5n}{2}}$	$5 \cdot 2^{\frac{n}{2}} - 1$	$(\frac{n2^{\frac{n-2}{6}}}{2}, \frac{n7^{\frac{n-2}{6}}}{2})$

II. Preliminary

Assume $S = \{\{s_h(t) \mid 0 \le t \le N-1\} \mid 1 \le h \le M\}$ be a family of M binary sequences of period N. The periodic correlation function between two sequences $\{s_h(t)\}$ and $\{s_l(t)\}$ in S is defined by

$$R_{h,l}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_h(t) + s_l(t+\tau)}, 0 \le \tau < N-1.$$

The correlation value $R_{h,l}(\tau)$ is called nontrival periodic correlation function if $h \ne l$ or $\tau \ne 0$.

The maximum nontrival periodic correlation value $R_{\max}$ is defined by

$$R_{\max} = \max\{|R_{h,l}(\tau)| \, | \, h \neq l \text{ or } \tau \neq 0\}$$

Let n, m, e be three positive integers such that $n = me$, $e \geq 2$. The trace function $tr_m^n(\cdot)$ is the mapping from the finite field $GF(2^n)$ to its subfield $GF(2^m)$ defined by $tr_m^n(x) = \sum_{k=0}^{e-1} x^{2^{mk}}$, where x is an element in $GF(2^n)$. The trace function satisfies the following properties:

1) $tr_m^n(ax+by) = atr_m^n(x) + btr_m^n(y)$, for all $a,b \in GF(2^m)$ and $x, y \in GF(2^n)$.

2) $tr_m^n(x^{2^m}) = tr_m^n(x)$, for all $x \in GF(2^n)$.

3) $tr_1^n(x) = tr_1^m[tr_m^n(x)]$, for all $x \in GF(2^n)$.

We refer the readers to [15] for detailed the properties of the trace function.

Lemma 1 ([13]) For any $\sigma \in GF(2^m)$, we have

$$\sum_{x \in GF(2^n)} (-1)^{tr_1^n(\sigma x)} = \begin{cases} 0 & for\ \sigma \neq 0 \\ 2^n & for\ \sigma = 0. \end{cases}$$

III. A New Family Of Binary Sequences

Let n, m be two positive integers such that $n = 2m$ and α be a primitive element of finite field $GF(2^n)$, and γ_v, $\gamma_u \in GF(2^n)$, $\eta_w \in GF(2^m)$, $\gcd(r, 2^m - 1) = 1$.

The family $S^{(r)}$ of binary sequences is defined by

$$S^{(r)} = \{s_{u,v,w} \,|\, 1 \leq u, v \leq 2^n, 1 \leq w \leq 2^m\},$$

where

$$s_{u,v,w} = \{s_{u,v,w}(t) \,|\, 0 \leq t \leq 2^n - 2\}$$

and

$$s_{u,v,w}(t) = tr_1^m\{[tr_m^{2m}(\alpha^{2t} + \gamma_u \alpha^{2(2^{m+1}-1)t} + \gamma_v \alpha^{(3\cdot 2^m - 1)t}) + \eta_w \alpha^{(2^m+1)t}]^r\}.$$

A. Correlation Values and Size of Family $S^{(r)}$

Theorem 1 For any pair of sequences s_{u_1,v_1,w_1} and s_{u_2,v_2,w_2} in $S^{(r)}$, the possible nontrivial periodic correlation function is given by

$$R_{(u_1,v_1,w_1),(u_2,v_2,w_2)}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_{u_1,v_1,w_1}(t) + s_{u_2,v_2,w_2}(t+\tau)} \qquad (1)$$

$$\in \{-2^m - 1, -1, 2^m - 1, 2^{m+1} - 1, 3\cdot 2^m - 1, 2^{m+2} - 1, 5\cdot 2^m - 1\}$$

Proof: Let $T = 2^m + 1$. For any t, $0 \leq t \leq 2^n - 2$, we can write

$$t = t_1 T + t_2,\ 0 \leq t_1 \leq 2^m - 2,\ 0 \leq t_2 \leq T - 1.$$

Because α^T is a primitive element of the finite field $GF(2^m)$, so is α^{rT}. Notice that $\alpha^{T^2 t_1} = \alpha^{2Tt_1}$ and that

$$tr_m^{2m}(\alpha^{2(t_1T+t_2)} + \gamma_u \alpha^{2(2^{m+1}-1)(t_1T+t_2)} + \gamma_v \alpha^{(3\cdot 2^m-1)(t_1T+t_2)}) + \eta_w \alpha^{(2^m+1)(t_1T+t_2)} = \alpha^{2t_1T}[tr_m^{2m}(\alpha^{2t_2} + \gamma_u \alpha^{2(2^{m+1}-1)t_2} + \gamma_v \alpha^{(3\cdot 2^m-1)t_2}) + \eta_w \alpha^{(2^m+1)t_2}],$$

one can express the t-th item $s_{u,v,w}(t)$ of sequence $s_{u,v,w}$ in the form

$$s_{u,v,w}(t) = tr_1^m\{\alpha^{2t_1rT}[(tr_m^{2m}(\alpha^{2t_2} + \gamma_u \alpha^{2(2^{m+1}-1)t_2} + \gamma_v \alpha^{(3\cdot 2^m-1)t_2}) + \eta_w \alpha^{(2^m+1)t_2})]^r\}.$$

By applying Lemma 1, (1) reduces to

$$\begin{aligned} R_{(u_1,v_1,w_1),(u_2,v_2,w_2)}(\tau) &= \sum_{t_2=0}^{T-1} \sum_{t_1}^{2^m-2} (-1)^{tr_1^m[\alpha^{2rt_1T} f_1(t_2,\tau)]} \\ &= \sum_{t_2=0}^{T-1} [\sum_{x \in GF(2^m)} (-1)^{tr_1^m[x f_1(t_2,\tau)]} - 1] \\ &= -T + 2^m \cdot X_1(\tau), \end{aligned} \qquad (2)$$

where we define

$$\begin{aligned} f_1(t_2,\tau) = [&tr_m^{2m}(\alpha^{2(t_2+\tau)} + \gamma_{u_2} \alpha^{2(2^{m+1}-1)(t_2+\tau)} + \gamma_{v_2} \alpha^{(3\cdot 2^m-1)(t_2+\tau)}) \\ &+ \eta_{w_2} \alpha^{(2^m+1)(t_2+\tau)}]^r + [tr_m^{2m}(\alpha^{2t_2} + \gamma_{u_1} \alpha^{2(2^{m+1}-1)t_2} \\ &+ \gamma_{v_1} \alpha^{(3\cdot 2^m-1)t_2}) + \eta_{w_1} \alpha^{(2^m+1)t_2}]^r, 0 \leq t_2 \leq T-1 \end{aligned} \qquad (3)$$

and $X_1(\tau) = |\{t_2 \,|\, 0 \leq t_2 \leq T-1, f_1(t_2,\tau) = 0\}|$.

Let $X_2(\tau) = |\{t \,|\, f_1(t,\tau) = 0, 0 \leq t \leq 2^n - 2\}|$. Notice that $f_1(t+T,\tau) = \alpha^{2rT} f_1(t,\tau)$, we have $X_1(\tau) = X_2(\tau)/(2^m - 1)$, so only $X_2(\tau)$ must be count.

Next, define

$$\begin{aligned} f_2(t,\tau) = &tr_m^{2m}(\alpha^{2(t+\tau)} + \gamma_{u_2} \alpha^{2(2^{m+1}-1)(t+\tau)} + \gamma_{v_2} \alpha^{(3\cdot 2^m-1)(t+\tau)}) \\ &+ \eta_{w_2} \alpha^{(2^m+1)(t+\tau)} + tr_m^{2m}(\alpha^{2t} + \gamma_{u_1} \alpha^{2(2^{m+1}-1)t} \\ &+ \gamma_{v_1} \alpha^{(3\cdot 2^m-1)t}) + \eta_{w_1} \alpha^{(2^m+1)t}, 0 \leq t \leq 2^n - 2. \end{aligned}$$

Since $\gcd(r, 2^m - 1) = 1$, we have $f_1(t,\tau) = 0 \Leftrightarrow f_2(t,\tau) = 0$. Thus in order to calculate $X_2(\tau)$, it suffices to count the number of zeros of the function $f_2(t,\tau) = 0$ as t varies over the range 0 to $2^n - 2$.

Letting $y = \alpha^{(2^m-1)t}$, we can change the function $f_2(t,\tau) = 0$ into

$$\begin{aligned} &(\gamma_{u_1} + \gamma_{u_2} \alpha^{2(2^{m+1}-1)\tau}) y^6 + (\gamma_{v_1} + \gamma_{v_2} \alpha^{(3\cdot 2^m-1)\tau}) y^5 \\ &+ (1 + \alpha^{2^{m+1}\tau}) y^4 + (\eta_{w_1} + \eta_{w_2} \alpha^{(2^m+1)\tau}) y^3 + (1 + \alpha^{2\tau}) y^2 \\ &+ (\gamma_{v_1}^{2^m} + \gamma_{v_2}^{2^m} \alpha^{(3-2^m)\tau}) y + (\gamma_{u_1}^{2^m} + \gamma_{u_2}^{2^m} \alpha^{(4-2^{m+1})\tau}) = 0 \end{aligned} \qquad (4)$$

It is easy to see that not all coefficients of the polynomial in y in (4) vanish simultaneously if $(u_1,v_1,w_1) \neq (u_2,v_2,w_2)$ or $\tau \neq 0$. In addition, the coefficients of the polynomial in y in (4) lie in finite field $GF(2^n)$, therefore the polynomial in y in

(4) has 0, 1, 2, …, or 6 different roots over $GF(2^n)$ for its degree is at most six [9]. Thus depending upon whether the roots of the polynomial in y in (4) can be expressed as (2^m-1) th powers in finite field $GF(2^n)$, the possible values of $X_2(\tau)$ are 0, 2^m-1, $2(2^m-1)$, $3(2^m-1)$, $4(2^m-1)$, $5(2^m-1)$, or $6(2^m-1)$. So we have $X_1(\tau)=0$, 1, 2, 3, 4, 5, or 6. And Theorem 1 immediately follows from (2).

Theorem 2 The family size of sequences $S^{(r)}$ is $2^{5n/2}$.

Proof: For proving Theorem 2, we assume that the conclusion to be false, i.e., there exists a nonnegative integer τ ($0 \le \tau \le 2^n-2$) such that $s_{u_1,v_1,w_1}(t)=s_{u_2,v_2,w_2}(t+\tau)$, where $0 \le t \le 2^n-2$ and $(u_1,v_1,w_1)\neq(u_2,v_2,w_2)$. From the hypothesis above, we can obtain that the correlation value $R_{(u_1,v_1,w_1),(u_2,v_2,w_2)}(\tau)$ is

$$R_{(u_1,v_1,w_1),(u_2,v_2,w_2)}(\tau)=\sum_{t=0}^{2^n-2}(-1)^{s_{u_1,v_1,w_1}(t)+s_{u_2,v_2,w_2}(t+\tau)}=2^n-1.$$

From Theorem 1, we know that is a contradiction. Thus we are done.

B. Linear Spans of Sequences in $S^{(r)}$

To obtain an exact expression on linear span of sequences in $S^{(r)}$, we assume in this subsection that $r=(2^{m-1}-1)/7$ and $m\equiv 1 \bmod 3$. Key [16] showed that the linear span $LS(s_{u,v,w})$ of a sequence $s_{u,v,w}$ in $S^{(r)}$ can be determined by expanding the t-th item $s_{u,v,w}(t)$ of $s_{u,v,w}$ as a polynomial in α^t and counting the number of monomials with nonzero coefficient in the polynomial.

Let $x=\alpha^t$ and $y=x^{2^m-1}$, and use $s_{u,v,w}(x)$ to denote

$$s_{u,v,w}(x)=tr_1^m\{[tr_m^{2m}(x^2+\gamma_u x^{2(2^{m+1}-1)}+\gamma_v x^{(3\cdot 2^m-1)})+\eta_w x^{(2^m+1)}]^r\}.$$

Then

$$s_{u,v,w}(x)=tr_1^m\{[tr_m^{2m}(x^2+\gamma_u x^{2(2^{m+1}-1)}+\gamma_v x^{(3\cdot 2^m-1)})+\eta_w x^{(2^m+1)}]^r\}$$

$$=\sum_{k=0}^{m-1}\{x^2y^{-2}[\gamma_u y^6+\gamma_v y^5+y^4+\eta_w y^3+y^2+\gamma_v^{2^m}y+\gamma_u^{2^m}]\}^{2^k r}.$$

Letting

$$\Delta_k(x)=\{x^2y^{-2}[\gamma_u y^6+\gamma_v y^5+y^4+\eta_w y^3+y^2+\gamma_v^{2^m}y+\gamma_u^{2^m}]\}^{2^k r},$$

we have the following lemma.

Lemma 2 For different k, the monomials appearing with nonzero coefficient in the expansion of $\Delta_k(x)$ are disjointed.

Proof: Since $y=x^{2^m-1}$, we first reduce all exponents modulo 2^m-1. Then y becomes 1, so each nonzero monomial occurring in the expansion of $\Delta_k(x)$ has a degree congruent to $2\cdot 2^k r$ modulo 2^m-1.If there is a monomial which appears simultaneously in both expansion $\Delta_k(x)$ and $\Delta_{k'}(x)$ with nonzero coefficients, then its degree is congruent to $2^{k+1}r \equiv 2^{k'+1}r \bmod 2^m-1$.Since $\gcd(r,2^m-1)=1$, one has $2^{k+1}=2^{k'+1}$, and $k=k'$.This completes the proof of Lemma 2.

Let $\Gamma_{u,v,w}(y)=(\gamma_u y^6+\gamma_v y^5+y^4+\eta_w y^3+y^2+\gamma_v^{2^m}y+\gamma_u^{2^m})^r$.

By Lemma 2, the linear span is determined by counting the number of nonzero monomials in *x* occurring in the expansion of $\Delta_k(x)$ for each *k*. This number is obviously equal to the number of nonzero monomials in *y* occurring in the expansion of $\Gamma_{u,v,w}(y)$. It implies that the linear span $LS(s_{u,v,w})$ is

$$LS(s_{u,v,w})=m\cdot|\{\text{monomials in }\Gamma_{u,v,w}(y)\}|.$$

Lemma 3 The degree of each nonzero monomial in *y* in the expansion of $\Gamma_{u,v,w}(y)$ is distinct.

Proof: Since $r=(2^{m-1}-1)/7=1+8+\mathrm{L}+8^{(m-4)/3}$, one has

$$\Gamma_{u,v,w}(y)=(\gamma_u y^6+\gamma_v y^5+y^4+\eta_w y^3+y^2+\gamma_v^{2^m}y+\gamma_u^{2^m})^r$$
$$=\prod_{i=0}^{(m-4)/3}(\gamma_u y^6+\gamma_v y^5+y^4+\eta_w y^3+y^2+\gamma_v^{2^m}y+\gamma_u^{2^m})^{8^i}.$$

Then the degree of monomial in *y* in expansion of $\Gamma_{u,v,w}(y)$ can be expressed as $e=\sum_{i=0}^{(m-4)/3}e_i 8^i$, where $e_i\in\{0,1,\cdots,6\}$. It is obviously that the exponent of *y* is the base-8 represent- ation of some positive integer, and because the maximum exponent $6(2^{m-1}-1)/7$ of *y* is less than $2^{m-1}-1$, the degree of each *y* is distinct. This completes the proof of Lemma 3.

Lemma 4 The possible number of nonzero monomials appearing in the expansion of $\Gamma_{u,v,w}(y)$ is $l^{(m-1)/3}$, where *l* = 2,3,4,5,6,7.

Proof: From Lemma 3, the expansion of $\Gamma_{u,v,w}(y)$ is a product of (*m*-1)/3 expression of *y*, and each exponent of *y* is different. Obviously, when $\gamma_u\cdot\gamma_v\cdot\eta_w\neq 0$, there are $7^{(m-1)/3}$ nonzero monomials in the expansion of term $\Gamma_{u,v,w}(y)$. when $\eta_w=0$ and $\gamma_u\cdot\gamma_v\neq 0$, there are $6^{(m-1)/3}$ nonzero monomials in the expansion of $\Gamma_{u,v,w}(y)$. when $\eta_w\neq 0$ and either γ_u or γ_v equals to zero, the number of nonzero monomials appearing in the expansion of $\Gamma_{u,v,w}(y)$ is $5^{(m-1)/3}$. when $\eta_w=0$ and either $\gamma_u=0$ or $\gamma_v=0$, there are $4^{(m-1)/3}$ nonzero monomials in the expansion of $\Gamma_{u,v,w}(y)$. when $\eta_w\neq 0$ and both $\gamma_u=0$ and $\gamma_v=0$, there are $3^{(m-1)/3}$ monomials in the expansion of terms $\Gamma_{u,v,w}(y)$. when $\eta_w=0$, $\gamma_u=0$ and $\gamma_v=0$, there are $2^{(m-1)/3}$ nonzero monomials in the expansion of $\Gamma_{u,v,w}(y)$. The proof ends.

Combining Lemma 2, 3, 4, we have the following Theorem.

Theorem 3: The linear span of sequence $s_{u,v,w}$ in $S^{(r)}$ is given by

$$LS(s_{u,v,w}) = n \cdot l^{(n-2)/6} / 2, \ l = 2,3,4,5,6,7.$$

Proof: Since $n = 2m$, we have $LS(s_{u,v,w}) = m \cdot l^{(m-1)/3}$ $= n \cdot l^{(n-2)/6} / 2$, where $l = 2,3,4,5,6,7$. Thus we are done.

Combining Lemma 2, 3, 4 and Theorem 3, the linear span of sequences in $S^{(r)}$ has the following distribution.

$$LS(s_{u,v,w}) = \begin{cases} n \cdot 2^{(n-2)/6} / 2, & 1 \text{ time} \\ n \cdot 3^{(n-2)/6} / 2, & 2^{n/2} - 1 \text{ times} \\ n \cdot 4^{(n-2)/6} / 2, & 2(2^n - 1) \text{ times} \\ n \cdot 5^{(n-2)/6} / 2, & 2(2^{n/2} - 1)(2^n - 1) \text{ times} \\ n \cdot 6^{(n-2)/6} / 2, & (2^n - 1)^2 \text{ times} \\ n \cdot 7^{(n-2)/6} / 2. & (2^n - 1)^2 (2^{n/2} - 1) \text{ times} \end{cases}$$

IV. Conclusion

In this paper, a new family of binary sequences *S* with large size is proposed. This sequence family has maximum nontrivial correlation value $5 \cdot 2^{n/2} - 1$, maximum linear span $n \cdot 7^{(n-2)/6} / 2$ and family size $2^{5n/2}$. Compared with several previously known large families of binary sequences, this new sequence family not only has large size and low correlation, but also large linear span. And it can be a candidate in some applications where the family size and linear span are more important than the correlation value. In addition, it is a very interest in calculating the linear span of the sequence for a general value of parameter *r*, and it is an open problem to determine the distribution of correlation values of this sequence family.

References

[1] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications Handbook, McGraw Hill, 2001.

[2] Kasami T. Weight distribution of Bose-Chaudhuri-Hocquenghem codes , Combinatorial Mathematics and Its Applications, Chapel Hill, NC: Univ. North Carolina Press, 1969.

[3] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions, IEEE Trans. Inf. Theory, vol.14, no.1, pp.154-156, 1968.

[4] J. D. Olsen, R. A. Scholt, and L. R. Welch, Bent function sequences, IEEE Trans. Inf. Theory, vol.IT-28, no.6, pp.858-864, 1982.

[5] A. Chang, et al. "On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code", IEEE Trans. Inf. Theory, vol.46, no.2, pp.680-687, Mar. 2000.

[6] O. S.Rothaus. "Modified Gold codes", IEEE Trans. Inf. Theory, vol.39, no.2, pp.654-656, Mar. 1993.

[7] N. Y. Yu and G. Gong. A new binary sequence family with low correlation and large size,

[8] Z. C. Zhou and X. H. Tang. New families of binary sequences with low correlation and large size, IEICE Trans. Fundamentals vol. E92-A, no.1, pp.291-297, 2009.

[9] Fanxin Zeng. "Two classes of large families of sequences with low correlation", IEEE Proceedings of IWSDA'97, pp.56-60.

[10] J. S. No and P. V. Kumar. A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span, IEEE Trans. Inf. Theory, vol.35, no.2, pp.371-379, 1989.

[11] A. Klapper, d-form sequences: Familes of sequences with low correlation values and large linear spans, IEEE Trans. Inf. Theory, vol. 41, no.2, pp.654-656, 1995.

[12] X. Y. Zeng, L. HU and W. F. Jiang. A family of binary sequences with 4-valued optimal out-of-phase correlation and large linear span, IEICE Trans. Fundamentals, vol. E89-A, no.7, 2006.

[13] Niho Y. Multivalued Cross-Correlation Functions between Two Maximal Linear Recursive Sequences, Ph. D. dissertation, Univ. Southern Calif., Los Angeles, 1972.

[14] T. Helleseth. Some results about the cross-correlation fuction between two maximal linear sequences. Discrete Mathmatics, 16(3): 209-232, 1976.

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

[16] E L. Key, "An analysis of the structure and complexity of non-linear binary sequence generators", IEEE Trans. Theory, vol. IT-22, pp. 732-736, 1976.