New Constructions of Low Correlation Sequences with High Linear Complexity [⋆]

Hai Xiong[1], Chao Li[1], Qingping Dai[1], and Shaojing Fu[2]

[1]Department of Mathematics and System Science, Science College; [2] Computer College; National University of Defence Technology, Changsha, China 410073

xiong.hai@163.com,lichao_nudt@sina.com,qpdai@nudt.edu.cn,shaojing1984@yahoo.cn

Abstract. In this paper, we propose a new concept named similar-bent function and we present two general methods to construct balanced sequences with low correlation by using similar-bent functions and orthogonal similar-bent functions. We find that the bent sequence sets are special cases of our construction. We also investigate the linear complexity of the new constructed sequences. If a suitable similar-bent function is given, the sequences constructed by it can have high linear complexity. As examples, we construct two new low correlation sequence sets. One constructed based on Dobbertin's iterative function is asymptotically optimal with respect to Welch's bound and the other one is constructed based on Kasami function whose sequences have a high linear complexity.

Index Terms—similar-bent function, low correlation, binary sequence, p-ary sequence

1 Introduction

Low correlation magnitude, balanceness and high linear complexity are some important randomness criteria for sequences. The good pseudo-random sequences are widely used in the engineering applications such as CDMA systems. How to construct the sequences with randomness properties is an interesting problem in application.

Many sequence sets with low correlation have been reported[1-9]. However, only a few sequence sets can attain the Welch's bound or Sidelnokiv's bound , for example the Kasami sequences[1], the Gold sequences[2], the Sidelnikov sequences[3], the bent sequences[4], and the Gold-like sequences[6].

The binary bent functions are Boolean functions on even number of variables whose Hamming distance to the affine function space is maximum. They have wide applications in communication, coding and cryptography, etc[10]. Olsen et al.[4] constructed a family of binary sequences with optimal correlation based on binary bent functions. Kumar et al.[11] generalized binary bent functions to p-ary bent functions and they[5] used these functions to construct p-ary bent sequences.

[⋆] The work was supported by the Natural Science Foundation of China (No:60803156, No:61070215). And the authors would like to thank the associate professor Longjiang Qu for his constructive comments.

In this paper, we propose a new concept named similar-bent function, the maximum absolute value of whose walsh spectrum is small. We find that the similar-bent functions and orthogonal similar-bent functions can also be used to construct low correlation sequence sets. Then we present two methods to construct balanced sequence sets with low correlation. In the first method, we use similar-bent function to construct low correlation sequence set. However, in the second method, we need orthogonal similar-bent function. The binary bent sequences[4] and p-ary bent sequences[5] are the special cases of the first construction. When the form of the similar-bent function is given, we get a formula to compute the linear complexity of the new constructed sequences. Of course, the formula is also valid for bent sequences. As examples, we construct two sequence sets based on Dobbertin's iterative function and Kasami function. The set constructed by Dobbertin's iterative function has the parameters $(2^n-1, 2^{\frac{n}{2}}, 2^{\frac{n}{2}}+2^{\frac{3n}{8}+\frac{3}{2}}+2^{\frac{n}{4}+1})$, which is asymptotically optimal with respect to Welch's bound. The other one is a $(2^n-1, 2^{\frac{n}{2}}, 2^{\frac{n}{2}+1}+1)$ low correlation sequence set, whose sequences have a high linear complexity $n+n2^{\frac{n-2}{4}}$.

2 Preliminaries

In this section we firstly review some notations and well known results, then we introduce the similar-bent functions.

2.1 Notations

Some notations throughout this paper are defined as follows:

- p is a prime;
- $\omega = \exp(\frac{2\pi\sqrt{-1}}{p})$;
- m is a positive integer and $n = 2m$;
- For a finite field $\mathbb{F}_{p^k}$, $\mathbb{F}_{p^k}^*$ denotes $\mathbb{F}_{p^k} \setminus \{0\}$;
- α is a primitive element of $\mathbb{F}_{p^n}$ and β is a primitive element of $\mathbb{F}_{p^m}$;
- For two positive integers $k|l$, the trace function $Tr_k^l(x)$ from $\mathbb{F}_{p^l}$ to $\mathbb{F}_{p^k}$ is defined by $Tr_k^l(x) = \sum_{i=0}^{\frac{l}{k}-1} x^{p^{ik}}$;
- For a positive integer $s = \sum_{i=0}^{m-1} s_i p^i$ where $0 \le s_i < p$, let $M(s) = \prod_{i=0}^{m-1}(s_i+1)$ and $w(s) = \sum_{i=o}^{k-1} s_i$, where $w(s)$ is called the p-adic weight of s;
- For a p-ary periodic sequence u, its linear complexity, denoted by $LC(u)$, is the length of the shortest linear feedback shift register (LFSR) that can generate it.
- For a complex number c, $\overline{c}$ denotes the conjugate number of c.

2.2 Sequence and Sequence Set

Let $u = (u_0, u_1, \cdots, u_{N-1})$ be a sequence of period N over $\mathbb{F}_p$. Let $N_x = |\{i : u_i = x, 0 \le i \le N-1\}|$, then u is called balanced if $\max_{x\in\mathbb{F}_p} N_x - \min_{x\in\mathbb{F}_p} N_x \le 1$.

The cross-correlation function of two p-ary periodic sequences $u = (u_0, u_1, \cdots, u_{N-1})$ and $v = (v_0, v_1, \cdots, v_{N-1})$ is defined by

$$C_{u,v}(\tau) = \sum_{i=0}^{N-1} \omega^{u_i - v_{i+\tau}},\ \tau \in Z_N.$$

If the sequences u and v are identical, then it is called the autocorrelation function of sequence u, and we denote it by $C_u(\tau)$.

Let u be a p-ary sequence with period N such that $N|p^m - 1$. Let $f(x) = \sum_{i=1}^{p^m-1} c_i x^i \in \mathbb{F}_{p^m}[x]$ be a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. Then $f(x)$ is called the polynomial representation of the sequence u, if $f(x)$ satisfies $f(\beta^i) = u_i$ for $0 \le i < p^m - 1$.

The following results link the linear complexity of the sequence with its polynomial representation.

Lemma 1. *[10, Theorem 6.3] Let u be a sequence with period $N|p^m - 1$ and $f(x) = \sum_{i=1}^{p^m-1} c_i x^i$ be its polynomial representation. Then $LC(u) = w(f)$, where $w(f) = |\{c_i \ne 0 | 1 \le i \le p^m - 1\}|$.*

Lemma 2. *[10, Theorem 3.17] Let $f(x) = \sum_{i=0}^{p^m-1} c_i x^i \in \mathbb{F}_{p^m}[x]$ be a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. Let $g(x) = f(Tr_m^n(x))$. Then $w(g) = \sum_{c_i \ne 0} M(i)$, where $w(g)$ is the number of the nonzero coefficients of $g(x)$.*

Let V be a sequence set containing K sequences with period N. Let θ_V denote the upper bound of the maximum out-of-phase autocorrelation and cross-correlation magnitude. Then the set V is called an (N, K, θ_V) sequence set. Usually, we say that V is a low correlation sequence set if $\theta_V \le c\sqrt{N}$ where c is a small constant.

The following lower bound of the maximum correlation magnitude of a sequence set is due to Welch[12].

Lemma 3. *Let V be a sequence set containing K sequences with period N. Let $\theta_V = \max\{|C_{u,v}(\tau)| : u, v \in V, 0 \le \tau \le N-1,$ and $\tau \ne 0$ if $u = v\}$. Then*

$$\frac{\theta_V^2}{N} \ge \frac{N(K-1)}{NK-1}.$$

For a low correlation sequence set V with parameters (N, K, θ_V). If $K \ge \sqrt{N}$ and $\lim_{N\to\infty} \frac{\theta_V}{\sqrt{N}} = 1$, then we call that the set V is asymptotically optimal with respect to Welch's bound.

2.3 Two-Tuple Balance Function

Let $f(x)$ be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ with $f(0)=0$. Let $T_f(\lambda)$ be a set defined as follows

$$T_f(\lambda)=\{(f(x),f(\lambda x))|x\in\mathbb{F}_{p^n}\},\ \text{for}\ \lambda\in\mathbb{F}_{p^n}.$$

$f(x)$ is a 2-tuple balance function if it satisfies the following two conditions:
(1) For $\lambda\notin\mathbb{F}_{p^m}$, any pair $(u,v)\in\mathbb{F}_{p^m}^2$ occurs once in $T_f(\lambda)$.
(2) For $1\neq\lambda\in\mathbb{F}_{p^m}^*$, there exists some $v\neq 1$ such that (u,vu) occurs p^m times in $T_f(\lambda)$ for every $u\in\mathbb{F}_{p^m}$.

Zierler had the following result on the two-tuple balance function.

Lemma 4. *[10, Theorem 5.7] $Tr_m^n(x)$ is a two-tuple balance function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$.*

2.4 Similar-Bent Function

Let $f(x)$ and $g(x)$ be two functions from $\mathbb{F}_{p^k}$ to $\mathbb{F}_p$. Then their correlation function is defined by

$$C_{f,g}(\lambda)=\sum_{x\in\mathbb{F}_{p^k}}\omega^{f(x)-g(\lambda x)},\ \lambda\in\mathbb{F}_{p^k}.$$

We call that $f(x)$ is an orthogonal function if $C_{f,f}(\lambda)=0$ holds for all $\lambda\neq 1$.

For a function $f(x)$ from $\mathbb{F}_{p^k}$ to $\mathbb{F}_p$, its walsh transformation is a complex-valued function over $\mathbb{F}_{p^k}$, which is defined by

$$W_f(\lambda)=\sum_{x\in\mathbb{F}_{p^k}}\omega^{Tr_1^k(\lambda x)-f(x)},\ \lambda\in\mathbb{F}_{p^k}.$$

The linearity of f is $\max_{\lambda\in\mathbb{F}_{p^m}}|W_f(\lambda)|$, denoted by $LS(f)$. We call $f(x)$ a bent function if $LS(f)=\sqrt{p^k}$. If $p=2$, we know that the walsh transformation of $f(x)$ is an integer-valued function. So there doesn't exist bent function when $p=2$ and k is an odd integer. And at this time we call $f(x)$ a near bent function if $W_f(\lambda)\in\{0,\pm 2^{\frac{k+1}{2}}\}$ holds for all $\lambda\in\mathbb{F}_{p^k}$.

Definition 1. *Let $f(x)$ be a function from $\mathbb{F}_{p^k}$ to $\mathbb{F}_p$. If there exists a constant c which is independent of k such that $LS(f)\leq\sqrt{cp^k}$, then we call $f(x)$ a **similar-bent** function.*

It is clear that bent functions and near bent functions are subclasses of similar-bent functions. And the well known Gold function, Kasami function, Welch function and Niho function etc.[13] are examples of orthogonal similar-bent functions. Their definitions are given in the follows. We can see more results about the constructions of bent functions and near bent functions in the papers [14-15].

Let k be an odd integer and $f(x) = Tr_1^k(x^d)$ be a function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$. If $d = 2^i + 1$ with $\gcd(i, k) = 1$ and $1 \leq i \leq \frac{k-1}{2}$, then we call that $f(x)$ is Gold function. If $d = 2^{2i} - 2^i + 1$ with $\gcd(i, k) = 1$ and $1 \leq i \leq \frac{k-1}{2}$, then we call that $f(x)$ is Kasami function. If $d = 2^{\frac{k-1}{2}} + 3$, then we call that $f(x)$ is Welch function. If $d = 2^i + 2^{\frac{i}{2}} - 1$ with $i = \frac{k-1}{2}$ be an even integer or $d = 2^i + 2^{\frac{3i+1}{2}} - 1$ with $i = \frac{k-1}{2}$ be an odd integer, then we call that $f(x)$ is Niho function.

Another interesting class of similar-bent functions are the Dobbertin's iterative functions, which is a class of balanced Boolean functions with high nonlinearity presented in 1995[16].

Dobbertin's Construction: Let k be an odd integer and $l = 2^t \cdot k \geq 4$ such that $t \geq 1$. The Boolean function $f(x, y)$ over $\mathbb{F}_2^l$ is defined by

$$f(x,y) = \begin{cases} f_0(x,y), \text{ if } x \neq 0; \\ g_1(y), \text{ if } x = 0, \end{cases} \tag{1}$$

where $x, y \in \mathbb{F}_2^{\frac{l}{2}}$, $f_0(x, y)$ is a l-variable normal bent function and $g_1(y)$ is generated by an iterative procedure as

$$g_i(x,y) = \begin{cases} f_{i+1}(x,y), \text{ if } x \neq 0; \\ g_{i+1}(y), \text{ if } x = 0, \end{cases} \tag{2}$$

where $x, y \in \mathbb{F}_2^{\frac{l}{2^{i+1}}}$ The process stops at $i = t - 1$. And $g_t(y)$ be a balanced k-variable Boolean function with $LS(g_t) \leq 2^{\frac{k+1}{2}}$.

3 Some Lemmas

In this section, we give some lemmas which are important for our constructions.

Lemma 5. *Let $f(x)$ be a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. Let $h_1(x) = Tr_1^n(\gamma_1 x) + f(Tr_m^n(x))$, $h_2(x) = Tr_1^n(\gamma_2 x) + f(Tr_m^n(x))$, where $\gamma_1 \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}$, $\varepsilon \in \mathbb{F}_{p^m}$, and $\gamma_2 = \gamma_1 + \varepsilon$. Then the two functions $h_1(x)$ and $h_2(x)$ have the following correlation magnitude distribution:*

$$|C_{h_1(x),h_2(x)}(\lambda)| = \begin{cases} p^n, & \text{when } \lambda = 1 \text{ and } \varepsilon = 0; \\ 0, & \text{when } \lambda = 1 \text{ and } \varepsilon \neq 0; \\ 0, & \text{when } 1 \neq \lambda \in \mathbb{F}_{p^m}^*; \\ \leq LS(f)^2, & \text{when } \lambda \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}. \end{cases} \tag{3}$$

Proof. It is trivial to verify the first identity. In the following, we assume that $\varepsilon \neq 0$ or $\lambda \neq 1$.

When $\lambda \in \mathbb{F}_{p^m}^*$, we have

$$h_2(\lambda x) = Tr_1^m(\lambda Tr_m^n(\gamma_1 x) + \lambda\varepsilon Tr_m^n(x)) + f(\lambda Tr_m^n(x)).$$

Since $\gamma_1 \notin \mathbb{F}_{p^m}$ and $Tr_m^n(x)$ is a two-tuple balance function, we get

$$\begin{aligned} C_{h_1(x),h_2(x)}(\lambda) &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{h_1(x)-h_2(\lambda x)} \\ &= \sum_{u,v\in\mathbb{F}_{p^m}} \omega^{Tr_1^m(u)+f(v)-Tr_1^m(\lambda u+\lambda\varepsilon v)-f(\lambda v)} \\ &= \sum_{v\in\mathbb{F}_{p^m}} \omega^{-Tr_1^m(\lambda\varepsilon v)+f(v)-f(\lambda v)} \sum_{u\in\mathbb{F}_{p^m}} \omega^{Tr_1^m((1-\lambda)u)} \\ &= 0. \end{aligned}$$

When $\lambda \notin \mathbb{F}_{p^m}$, then $\lambda\gamma_2$ and λ can be expressed as $\lambda\gamma_2 = b_{00}\gamma_1 + b_{01}, \lambda = b_{10}\gamma_1 + b_{11}$, where $b_{ij}(0 \leq i,j \leq 1) \in \mathbb{F}_{p^m}$ and $b_{10} \neq 0$. So we have

$$h_2(\lambda x) = Tr_1^m(b_{00}Tr_m^n(\gamma_1 x) + b_{01}Tr_m^n(x)) + f(b_{10}Tr_m^n(\gamma_1 x) + b_{11}Tr_m^n(x)).$$

Hence

$$\begin{aligned} C_{h_1(x),h_2(x)}(\lambda) &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{h_1(x)-h_2(\lambda x)} \\ &= \sum_{u,v\in\mathbb{F}_{p^m}} \omega^{Tr_1^m(u)+f(v)-Tr_1^m(b_{00}u+b_{01}v)-f(b_{10}u+b_{11}v)} \\ &= \sum_{v\in\mathbb{F}_{p^m}} \omega^{-Tr_1^m(b_{01}v)+f(v)} \sum_{u\in\mathbb{F}_{p^m}} \omega^{-f(b_{10}u+b_{11}v)+Tr_1^m((1-b_{00})u)} \\ &= \sum_{v\in\mathbb{F}_{p^m}} \omega^{-Tr_1^m(b_{01}v)+f(v)} \sum_{w\in\mathbb{F}_{p^m}} \omega^{-f(w)+Tr_1^m((1-b_{00})b_{10}^{-1}w-(1-b_{00})b_{10}^{-1}b_{11}v)} \\ &= \sum_{v\in\mathbb{F}_{p^m}} \omega^{-Tr_1^m((b_{01}+(1-b_{00})b_{10}^{-1}b_{11})v)+f(v)} \sum_{w\in\mathbb{F}_{p^m}} \omega^{-f(w)+Tr_1^m((1-b_{00})b_{10}^{-1}w)} \\ &= \overline{W_f(b_{01}+(1-b_{00})b_{10}^{-1}b_{11})}W_f((1-b_{00})b_{10}^{-1}). \end{aligned}$$

The result thus follows. □

Lemma 6. *Let $f(x)$ be an orthogonal function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$, $h_1(x) = Tr_1^n(\gamma_1 x) + f(Tr_m^n(x))$ and let $h_2(x) = Tr_1^n(\gamma_2 x) + f(Tr_m^n(x))$, where $\gamma_1 \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}$, $\varepsilon \in \mathbb{F}_{p^m}$ and $\gamma_2 = \varepsilon\gamma_1$. Then the two functions $h_1(x)$ and $h_2(x)$ have the following correlation magnitude distribution:*

$$|C_{h_1(x),h_2(x)}(\lambda)| = \begin{cases} p^n, & \text{when } \lambda = 1 \text{ and } \varepsilon = 1; \\ 0, & \text{when } \lambda = 1 \text{ and } \varepsilon \neq 1; \\ 0, & \text{when } 1 \neq \lambda \in \mathbb{F}_{p^m}^*; \\ \leq LS(f)^2, & \text{when}\lambda \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}. \end{cases} \tag{4}$$

Proof. This proof is similar to the proof of Lemma 5. We also assume that $\varepsilon \neq 1$ or $\lambda \neq 1$ in the following.

When $\lambda \in \mathbb{F}_{p^m}^*$, we have

$$h_2(\lambda x) = Tr_1^m(\lambda\varepsilon Tr_m^n(\gamma_1 x)) + f(\lambda Tr_m^n(x)).$$

Note that $f(x)$ is orthogonal, thus

$$\begin{aligned} C_{h_1(x),h_2(x)}(\lambda) &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{h_1(x)-h_2(\lambda x)} \\ &= \sum_{u,v\in\mathbb{F}_{p^m}} \omega^{Tr_1^m(u)+f(v)-Tr_1^m(\lambda\varepsilon u)-f(\lambda v)} \\ &= \sum_{v\in\mathbb{F}_{p^m}} \omega^{f(v)-f(\lambda v)} \sum_{u\in\mathbb{F}_{p^m}} \omega^{Tr_1^m((1-\lambda\varepsilon)u)} \\ &= 0. \end{aligned}$$

When $\lambda \notin \mathbb{F}_{p^m}$, then $\lambda\gamma_2$ and λ can be expressed as $\lambda\gamma_2 = b_{00}\gamma_1 + b_{01}, \lambda = b_{10}\gamma_1 + b_{11}$, where $b_{ij}(0 \leq i, j \leq 1) \in \mathbb{F}_{p^m}$ and $b_{10} \neq 0$. So we have

$$h_2(\lambda x) = Tr_1^m(b_{00}Tr_m^n(\gamma_1 x) + b_{01}Tr_m^n(x)) + f(b_{10}Tr_m^n(\gamma_1 x) + b_{11}Tr_m^n(x)).$$

Hence

$$\begin{aligned} C_{h_1(x),h_2(x)}(\lambda) &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{h_1(x)-h_2(\lambda x)} \\ &= \overline{W_f(b_{01} + (1-b_{00})b_{10}^{-1}b_{11})}W_f((1-b_{00})b_{10}^{-1}). \end{aligned}$$

We finish the proof. □

4 Construction Based On Similar-Bent Function

Construction I: Let $f(x)$ be a similar-bent function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ and $LS(f) \leq \sqrt{cp^m}$. For any given $\gamma \in \mathbb{F}_{p^n} \backslash \mathbb{F}_{p^m}$, then we can construct a sequence set $V^I_{f,\gamma} = \{s_\varepsilon | \varepsilon \in \mathbb{F}_{p^m}\}$, where the sequence $s_\varepsilon = (s_{\varepsilon,0}, s_{\varepsilon,1}, \cdots)$ is defined by

$$s_{\varepsilon,i} = Tr^n_1((\gamma + \varepsilon)\alpha^i) + f(Tr^n_m(\alpha^i)). \tag{5}$$

Theorem 1. *Let $V^I_{f,\gamma}$ be the sequence set defined in Construction I. Then $V^I_{f,\gamma}$ is a $(p^n - 1, p^m, cp^m + 1)$ low correlation sequence set.*

Proof. Let $h_\varepsilon(x) = Tr^n_1((\gamma+\varepsilon)x)+f(Tr^n_m(x))$ for $\varepsilon \in \mathbb{F}_{p^m}$. Then $h_\varepsilon(x)$ is the polynomial representation of the sequence s_ε. For any two sequence $s_{\varepsilon_1}, s_{\varepsilon_1} \in V^I_{f,\gamma}$, we have that

$$C_{s_{\varepsilon_1}, s_{\varepsilon_2}}(\tau) = C_{h_{\varepsilon_1}(x), h_{\varepsilon_2}(x)}(\alpha^\tau) - 1.$$

Then ones can get the following results from Lemma 5.

(1) If $\varepsilon_1 \neq \varepsilon_2$, then $|C_{\varepsilon_1,\varepsilon_2}(\tau)| \leq LS(f)^2 + 1 \leq cp^m + 1$ holds for all $0 \leq \tau < p^n - 1$;
(2) If $\varepsilon_1 = \varepsilon_2$, then $|C_{\varepsilon_1,\varepsilon_2}(\tau)| \leq LS(f)^2 + 1 \leq cp^m + 1$ holds for all $0 < \tau < p^n - 1$.

The theorem then follows. □

Theorem 2. *Let $V^I_{f,\gamma}$ be the sequence set defined in Construction I. Then all the sequences in the set $V^I_{f,\gamma}$ are balanced.*

Proof. Let $h_\varepsilon(x)$ be the function as defined in the proof of Theorem 1. We only need to prove that the function $h_\varepsilon(x)$ is balanced for any given $\varepsilon \in \mathbb{F}_{p^m}$. Note that $Tr^n_m(x)$ is a two-tuple-balance function, we have

$$\sum_{x \in \mathbb{F}_{p^n}} \omega^{h_\varepsilon(x)} = \sum_{u,v \in \mathbb{F}_{p^m}} \omega^{Tr^m_1(u)+f(v)} = 0 = \sum_{i=0}^{p-1} N_i \omega^i,$$

where N_i denotes $\#\{x \in \mathbb{F}_{p^n} | h_\varepsilon(x) = i\}$. Since $\{1, \omega^1, \cdots, \omega^{p-2}\}$ are linear independent in $Z[\omega]$, we have $N_0 = N_1 = \cdots = N_{p-1}$. The proof is now finished. □

Theorem 3. *Let $f(x) = \sum_{i=1}^{p^m-1} c_i x^i$ be a similar-bent function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$, and $V^I_{f,\gamma}$ be the sequence set defined in Construction I. Then all of the sequences in the set $V^I_{f,\gamma}$ have the same linear complexity $n + \sum_{w(i)>1, c_i \neq 0} M(i)$, where $w(i)$ denotes the p-adic weight of i.*

Proof. For any given sequence $s_\varepsilon \in V^I_{f,\gamma}$, let $h_\varepsilon(x) = Tr^n_1((\gamma+\varepsilon)x) + f(Tr^n_m(x))$ be its polynomial representation. According to Lemma 1, we only need to prove that $w(h_\varepsilon(x)) = n + \sum_{w(i)>1,c_i\neq 0} M(i)$.

Let $f_1(x) = \sum_{j=0}^{m-1} c_{p^j} x^{p^j}$ and $f_2(x) = \sum_{w(i)>1} c_i x^i$. Then we have

$$\begin{aligned} h_\varepsilon(x) &= Tr^n_1((\gamma+\varepsilon)x) + f(Tr^n_m(x)) \\ &= Tr^n_1((\gamma+\varepsilon)x) + f_1(Tr^n_m(x)) + f_2(Tr^n_m(x)) \\ &= \sum_{j=0}^{m-1} \left[Tr^n_m((\gamma+\varepsilon+c_{p^j}^{p^{m-j}})x)\right]^{p^j} + f_2(Tr^n_m(x)). \end{aligned}$$

Note that Lemma 2 and $\gamma+\varepsilon+c_{p^j}^{p^{m-j}} \neq 0$ holds for $0 \leq j \leq m-1$, thus

$$\begin{aligned} w(h_\varepsilon(x)) &= \sum_{j=0}^{m-1} M(p^j) + w(f_2(x)) \\ &= 2m + \sum_{w(i)>1,c_i\neq 0} M(i) \\ &= n + \sum_{w(i)>1,c_i\neq 0} M(i). \end{aligned}$$

We are done. □

Olsen, Scholtz, and Welch[4] constructed a family of binary sequences called bent sequences. Subsequently, Kumar, Scholtz and Welch[5] generalized this construction to p-ary sequence. Their results are introduced in the following theorem.

Theorem 4. *Let $n = 2m$ and α be a primitive element of $\mathbb{F}_{p^n}$. Let $(\eta_1, \eta_2, \cdots, \eta_m)$ be a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ and $\gamma \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}$. Let $f(x_1, x_2, \cdots, x_m)$ be a bent function from $\mathbb{F}_p^m$ to $\mathbb{F}_p$. Let $e_i = (e_{i,1}, \cdots, e_{i,m})$ run through over all the elements of $\mathbb{F}_p^m$ as i varies between 1 and p^m. Then a family of binary sequences is defined by*

$$V = \{s_{e_i}(t) | 1 \leq i \leq p^m\},$$

where $s_{e_i}(t) = f(tr^n_1(\eta_1\alpha^t), \cdots, tr^n_1(\eta_m\alpha^t)) + \sum_{j=1}^m e_{i,j} tr^n_1(\eta_j\alpha^t) + tr^n_1(\gamma\alpha^t)$. The size of the family is p^m and the bound of the correlation magnitude is p^m+1.

There are few reports about the linear complexity of bent sequences. Kumar and Scholtz[17] researched the linear complexity of the binary bent sequences. They have the following results.

Theorem 5. *Let $k > 1$ be a positive integer, $n = 2m = 4k$ and $2 < d \leq k$. Let $f(x_1, x_2, \cdots, x_m)$ be a bent function from $\mathbb{F}_2^m$ to $\mathbb{F}_2$ with algebraic degree d. Let u be a bent sequence constructed by using $f(x)$. Then the linear complexity of u satisfies the following equation*

$$LC(u) \leq \sum_{i=1}^{d-1} \binom{n}{i} + \binom{m}{d} 2^d - \sum_{i=1}^{\lfloor (d-1)/2 \rfloor} \binom{m}{i}.$$

And there exist bent sequences constructed by using bent function of algebraic degree d, whose linear complexity can achieve the lower bound

$$LC(u) \geq \binom{m}{d} 2^d + \frac{1}{2} \sum_{i=2}^{d-1} \binom{m}{i} 2^i + n.$$

The above bent function can also be regarded as defined over $\mathbb{F}_{p^m}$ because $\mathbb{F}_{p^m}$ and $\mathbb{F}_p^m$ are isomorphic. In Construction I, if f is a binary bent(p-ary bent) function, then we get binary bent (p-ary bent) sequences. Thus our construction includes bent sequences as subclasses. But if the function f in Construction I is not a bent function, we may get new sequence sets. The following is an example.

Example 1. Let $k > 1$ be an odd integer and $m = 2k$. Let $f(x)$ be the Dobbertin's iterative function[16] from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Let $V_{f,\gamma}^I$ be the sequence set defined in Construction I. According to Theorem 9 in [16], we can get that $\max_{\lambda \in \mathbb{F}_{2^m}} |W_f(\lambda)| \leq 2^k + 2^{\frac{k+1}{2}}$. Then $V_{f,\gamma}^I$ is a $(2^n - 1, 2^m, 2^{\frac{n}{2}} + 2^{\frac{3n}{8}+\frac{3}{2}} + 2^{\frac{n}{4}+1})$ low correlation sequence set. And $V_{f,\gamma}^I$ is asymptotically optimal with respect to Welch's bound.

5 Construction Based On Orthogonal Similar-Bent Function

Construction II: Let $f(x)$ be an orthogonal similar-bent function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ and $LS(f) \leq \sqrt{cp^m}$. For any given $\gamma \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}$, then we can construct a sequence set $V_{f,\gamma}^{II} = \{s_\varepsilon | \varepsilon \in \mathbb{F}_{p^m}\}$, where the sequence $s_\varepsilon = (s_{\varepsilon,0}, s_{\varepsilon,1}, \cdots)$ is defined by

$$s_{\varepsilon,i} = Tr_1^n(\gamma \varepsilon \alpha^i) + f(Tr_m^n(\alpha^i)). \tag{6}$$

The following theorem comes from Lemma 6.

Theorem 6. *Let $V_{f,\gamma}^{II}$ be the sequence set defined in Construction II. Then $V_{f,\gamma}^{II}$ is a $(p^n - 1, p^m, cp^m + 1)$ low correlation sequence set.*

Theorem 7. *Let $V_{f,\gamma}^{II}$ be the sequence set defined in Construction II. Then all the sequences in the set $V_{f,\gamma}^{II}$ are balanceable.*

Proof. Let $h_\varepsilon(x) = Tr_1^n(\gamma\varepsilon x) + f(Tr_m^n(x))$ for $\varepsilon \in \mathbb{F}_{p^m}$. Then $h_\varepsilon(x)$ is the polynomial representation of the sequence s_ε. Note that $f(x)$ is orthogonal, so we have

$$\sum_{x\in\mathbb{F}_{p^n}} \omega^{h_{\mathbf{0}}(x)} = \sum_{x\in\mathbb{F}_{p^n}} \omega^{f(Tr_m^n(x))} = \sum_{v\in\mathbb{F}_{p^m}} p^m \omega^{f(v)} = 0.$$

Then $s_{\mathbf{0}}$ is balanceable. The proof for the other sequences is similar to the proof Theorem 2. □

Theorem 8. *Let $f(x) = \sum_{i=1}^{p^m-1} c_i x^i$ be an orthogonal similar-bent function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$, and $V_{f,\gamma}^{II}$ be the sequence set defined in Construction II. Except for $s_{\mathbf{0}}$, all the other sequences in the set $V_{f,\gamma}^{II}$ have the same linear complexity and their linear complexity is $n + \sum_{w(i)>1, c_i\neq 0} M(i)$, where $w(i)$ denotes the p-adic weight of i. And the linear complexity of $s_{\mathbf{0}}$ is $\sum_{c_i\neq 0} M(i)$.*

Proof. This proof is similar to the proof of Theorem 3. We omit it here. □

As we know, Gold function, Kasami function, Welch function and Niho function etc. are all orthogonal similar-bent functions. We can use these functions to construct sequence sets and get their corresponding parameters. However, the sequences constructed based on Kasami function may have better linear complexity, as the following example shows.

Example 2. Let m be an odd integer, $f(x) = Tr_1^m(ax^d)$ be the Kasami function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, where $d = 2^{2i} - 2^i + 1,\ \gcd(i,m) = 1$. Then $LS(f) = 2^{\frac{m+1}{2}}$. Let $V_{f,\gamma}^{II}$ be the sequence set defined in Construction II. Then $V_{f,\gamma}^{II}$ is a $(2^n-1, 2^m, 2^{m+1}+1)$ low correlation sequence set. The linear complexity of $s_{\mathbf{0}}$ is $m2^{i+1}$, and other sequences' linear complexity is $n+m2^{i+1}$. Especially, if we let $i = \frac{m-1}{2}$, then the linear complexity of these sequences can attain $n + n2^{\frac{n-2}{4}}$ except for $s_{\mathbf{0}}$.

Remark 1. We can easily verify that the sequence set $V_{f,\gamma}^{I}$ is different from $V_{f,\gamma}^{II}$ constructed by the same similar-bent function.

6 Conclusion

Based on similar-bent functions and orthogonal similar-bent functions, we give two constructions of low correlation sequence set. And all the new constructed sequences are balanceable. In the first construction, we can get the bent sequences if we choose bent function as the similar-bent function. But we can get new sequence sets if we choose other similar-bent functions. A formula for computing the linear complexity of these sequences is given. If a suitable similar-bent function is chosen, the new sequences can have a high linear complexity. As examples, we give two new sequence sets. One is constructed by Dobbertin's iterative function, which is a $(2^n-1, 2^m, 2^{\frac{n}{2}}+2^{\frac{3n}{8}+\frac{3}{2}}+2^{\frac{n}{4}+1})$ low correlation sequence set and is asymptotically optimal with respect to Welch's bound. The other one is constructed by Kasami function, which is a $(2^n-1, 2^m, 2^{\frac{n}{2}+1}+1)$ low correlation sequence set.

References

1. T. Kasami, Weight Distribution Formular for Some Class of Cyclic Codes Coordinated Science Laboratory, Univ. of Illinos. Urbana. Tech. Rep. R-285(AD 632547). Apr. 1966.
2. R. Gold, "Maximal Recursive Sequences with 3-valued Recursive Coress-correlation Functions," IEEE Trans. Inform. Theory, vol. IT-14, no. 1, pp. 154-156, 1968.
3. V. M. Sidelnikov, "On Mutual Correlation of Sequences," Soviet Math. Dokl., vol. 12, no. 1, pp. 197-201, 1971.
4. J. D. Olsen, R. A. Scholtz, L. R. Welch, "Bent-Function Sequences," IEEE Trans. Inform. Theory, vol. IT-28, no. 6, pp. 858-864, 1982.
5. P. V. Kumar, "On Bent Sequences and Generalized Bent Functions," PH.D. Dissertation, Univ. Southern California, Los Angeles, 1983.
6. S. Boztas, P. V. Kumar, "Binary Sequences with Gold-like Correlaiton but Larger Linear Span," IEEE Trans. Inform. Theory, vol. 40, no. 2, pp. 532-537, 1994.
7. N. Y. Yu, G. Gong, "New Construction of M-Ary Sequence Families with Low Correlation from the Structure of Sidelnikov Sequences," IEEE Trans. Inform. Theory, vol. 56, no. 8, pp. 4061-4070, 2010.
8. Z. C. Zhou, X. H. Tang, "Generalized Modified Gold Sequences," Des. Codes Cryptogr., vol. 60, pp. 241-253, 2011.
9. J. Y. Kim, S. T. Choi, J. S. No, "A New Family of p-Ary Sequences of Period $(p^n-1)/2$ With Low Correlation," IEEE Trans. vol. 57, no. 6, pp. 3825-3830, 2011.
10. S. W. Golomb and G. Gong, "Signal Design for Good Correlation," New York: Cambridge University Press, 2005.
11. P. V. Kumar, R. A. Scholtz, L. R. Welch, "Generalized Bent Functions and Their Properties," J. Comb. Theory, Ser. A, vol. 40, no. 1, pp. 90-107, 1985.
12. L. R. Welch, "Low Bounds on the Maximum Cross Correlation of Signals," IEEE Trans. Inform. Theory, vol. It-20, no. 3, pp. 397-399, 1974.
13. C. Li, L. J. Qu, Y. Zhou, "Security Criteria Analysis of Cryptography Functions," Beijing: Science Press, 2011. (In Chinese)
14. N. N. Tokareva, "Generalization of Bent Functions. A Survey," Journal of Applied and Industrial Mathematics, vol. 5, no. 1, pp. 110-129, 2011.
15. J. F. Dillon, G. M. Guire "Near Bent Functions on A Hyperlane," Finite Fields and Appl. vol. 14, no. 3, pp. 715 - 720, 2008.
16. H. Dobbertin, "Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity," in Workshop on Fast Software Encryption, Springer-Verlag, vol. 1008, pp. 61-74, 1995.
17. P. V. Kumar, R. A. Scholtz, "Bounds on the Linear Span of Bent Sequences," IEEE Trans. Inform. Theory, vol. IT-29, no. 6, pp. 854-862, 1983.