Front. Electr. Electron. Eng. 2012, 7(3): 308–311
DOI 10.1007/s11460-012-0205-z

RESEARCH ARTICLE

Pinhui KE, Shengyuan ZHANG

New classes of sequence families with low correlation by using multiplicative and additive characters

Abstract For an odd prime p, a new sequence family of period p^m-1, size $(M-1)p^{mr}$ is proposed using multiplicative and additive characters. The upper bound for the maximum magnitude of nontrivial correlations of the sequence family is derived using well-known character sums. The upper bound is shown to be $(r+1)\sqrt{p^m}+3$, which meets the Welch bound asymptotically.

Keywords finite field, character sum, correlation, polyphase sequence, Welch bound

1 Introduction

In wireless communications, sequences with low correlation are widely used to distinguish multiple users or channels with low mutual-access interference (MAI) [1]. To maximize the achievable data rate, polyphase sequence sets with a variety of lengths and alphabet sizes are more desirable than binary sequence sets for most wireless mobile communication systems employing adaptive modulation schemes. In addition, a large number of distinct sequences may be needed for supporting user requirements that rapidly increase.

A sequence $S=\{s(t)\}$ is called a polyphase sequence with alphabet q if $s(t)$ is a qth root of unity for all t. Let $F=\{s_1,s_2,...,s_M\}$ be a set of M cyclically distinct polyphase sequence with period N, where $s_i=\{s_i(t)\}$ for $1\leqslant i\leqslant M$. The *periodic cross correlation* function between sequence s_i and s_j at the shift phase τ is given by

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

Received February 15, 2012; accepted July 16, 2012

Pinhui KE (✉), Shengyuan ZHANG
Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China
E-mail: keph@fjnu.edu.cn

If $s_i=s_j$, we call it the *periodic autocorrelation* function of sequence s_i at the shift phase τ, and it is denoted as $R_{s_i}(\tau)$. Let $R_{\max}(F)$ be the maximal correlation of F, i.e.,

$$R_{\max}(F)=\max|R_{s_i,s_j}(\tau)|$$

for any $0\leqslant\tau\leqslant N-1$ if $1\leqslant i\neq j\leqslant M$ and $0<\tau\leqslant N-1$ if $i=j$. The sequence family F is said to have *low correlation* if $R_{\max}(F)\leqslant v\sqrt{N}$ for a small constant v. There exist many designs of sequence families that meet this asymptotic bound with equality. Readers may refer to Refs. [1,2] for an overview on this topic.

In Ref. [3], polyphase sequence families with low correlation were constructed from the shift and addition of the power residue sequence (Sidelnikov sequence, respectively) and its constant multiple sequences, whose maximum correlation were shown to be upper bounded by $2\sqrt{L}+5$ or $3\sqrt{L}+4$ ($2\sqrt{L}+6$ or $3\sqrt{L}+5$ for sequence families from Sidelnikov sequence, respectively), where L is the period of the constructed sequences. In Ref. [4], more generalized constructions were considered by the addition of multiple cyclic shifts of power residue and Sidelnikov sequences, which can be represented by multiplicative character. Recently, sequence family of prime period p, family size $(p-2)p^r$, and maximum correlation at most $(r+1)\sqrt{p}+2$ was obtained by using multiplicative and additive characters in Ref. [5].

In this paper, we generalize the constructions in Ref. [5] to the general finite field. Our constructions are also based on multiplicative character and additive character. However, instead of using the traditional multiplicative character directly, we use it in a way similar to the one use in the construction of Sidelnikov sequence. Before presenting our constructions, we review some related definitions and properties of finite field.

Let p be a prime and $q=p^m$, where m is a positive integer. Let F_q be a finite field containing q elements. Given $a\in F_q$, an *additive character* of F_q is a homomorphism mapping from additive group $(F_q,+)$ to $(C^*,\cdot)$ defined by

$$\varphi_a(x) = e^{\frac{2\pi\sqrt{-1}}{p}\mathrm{Tr}(ax)},$$

where Tr is the trace function of F_q over F_p, i.e.,

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{m-1}}.$$

In the case $a = 0$, we call φ_0 trivial additive character; otherwise, we call it nontrivial. *Multiplicative character* of F_q is another useful tool in this paper. Let ξ be a generator for the cyclic group $(F_q^*, \cdot)$, where $F_q^* = F_q \backslash \{0\}$. For an integer a, a multiplicative character of F_q is a homomorphism mapping from cyclic group $(F_q^*, \cdot)$ to $(C^*, \cdot)$ defined by

$$\chi_a(\xi^t) = e^{\frac{2\pi\sqrt{-1}}{q-1}at}.$$

It is convenient to assume that $\chi_a(0) = 0$. Given two characters χ_a and χ_b, one can form the product $\chi_a\chi_b$ by setting

$$\chi_a\chi_b(g) = \chi_a(g)\chi_b(g)$$

for all $g \in F_q^*$. It is well known that the set of characters of $(F_q^*, \cdot)$ forms a cyclic group under the multiplication of characters. The *order* of a multiplicative character χ_a is thus defined to be the least positive integer d such that $\chi_a^d(g) = 1$ for any $g \in F_q^*$.

Following bounds on character sums will be useful in the estimation of the correlation function of sequence families.

Lemma 1 [6] Let χ be a nontrivial multiplicative character of F_q of order M, and φ be a nontrivial additive character of F_q. Suppose that $f \in F_q[x]$ is not, up to a nonzero multiplicative constant, an Mth power in $F_q[x]$. Then, for any polynomial $g \in F_q[x]$, we have

$$\left|\sum_{x\in F_q} \chi\Big(f(x)\Big)\varphi\Big(g(x)\Big)\right| \leqslant \Big(\deg(g) + d - 1\Big)\sqrt{q},$$

where d is the number of distinct roots of f in its splitting field over F_q.

Lemma 2 [7] Let φ be a nontrivial additive character of F_q, and let $f \in F_q[x]$ be of degree $n \geqslant 1$ with $\gcd(n,p) = 1$. Then,

$$\left|\sum_{x\in F_q} \varphi\Big(f(x)\Big)\right| \leqslant (n-1)\sqrt{q}.$$

2 New constructions

Let F_q be a finite field with q elements, where $q = p^m$, p is an odd prime and m is a positive integer. Assume M is a positive integer satisfying $M|(q-1)$, let χ be a multiplicative character of F_q^* with order M. Let φ be a nontrivial additive character of F_q and ξ be a generator of $(F_q^*, \cdot)$. Given integer r, $0 \leqslant r \leqslant p-2$, denote

$$C^r = \{(a;b_r,b_{r-1},...,b_1) | 1 \leqslant a \leqslant M-1, \text{ and } b_i \in F_q \text{ for } 1 \leqslant i \leqslant r\}.$$

Let $c = (a;b_r,b_{r-1},...,b_1) \in C^r$, the sequence s^c is then given by

$$s^c(t) = \chi^a(\xi^t + 1)\varphi\left(\sum_{i=1}^{r} b_i(\xi^t)^i\right)$$

for $0 \leqslant t \leqslant q-2$. For $r = 0,1,...,p-2$, define the sequence family Γ_r^* to be

$$\Gamma_r^* = \{s^c | c \in C^r\}.$$

It is obvious that each sequence in Γ_r^* has period $q-1$ and takes on values that are Mpth roots of unity except for one element per period. In the following, we will determine its maximum nontrivial correlation and its family size, which turns out to be approximately good with respect to Welch bound.

Theorem 1 Let Γ_r^* be the sequence family defined above. Then, we have

$$R_{\max}(\Gamma_r^*) \leqslant (r+1)\sqrt{q} + 1.$$

Proof. Given two sequences s^c and $s^{c'}$ in Γ_r^*, by assuming that $c = (a;b_r,b_{r-1},...,b_1)$ and $c' = (a';b_{r'},b_{r-1'},...,b_{1'})$, we have

$$s^c(t) = \chi^a(\xi^t + 1)\varphi\Big(\sum_{i=1}^{r} b_i(\xi^t)^i\Big),$$

$$s^{c'}(t) = \chi^{a'}(\xi^t + 1)\varphi\Big(\sum_{i=1}^{r} b_{i'}(\xi^t)^i\Big).$$

Let $b(x) = \sum_{i=1}^{r} b_i x^i$ and $b'(x) = \sum_{i=1}^{r} b_{i'} x^i$. For τ, $0 \leqslant \tau \leqslant q-2$,

$$\begin{aligned} &R_{s^c,s^{c'}}(\tau) \\ &= \sum_{t=0}^{q-2} \chi^a(\xi^t + 1)\varphi\Big(b(\xi^t)\Big)\overline{\chi^{a'}(\xi^{t+\tau} + 1)}\,\overline{\varphi\Big(b'(\xi^{t+\tau})\Big)} \\ &= \sum_{x\in F_q^*} \chi\Big((x+1)^a \cdot (\theta x + 1)^{M-a'}\Big)\varphi\Big(b(x) - b'(\theta x)\Big) \\ &= \sum_{x\in F_q^*} \chi\Big(f(x)\Big)\varphi\Big(g(x)\Big), \end{aligned} \tag{1}$$

where $\theta = \xi^\tau$, $f(x) = (x+1)^a \cdot (\theta x + 1)^{M-a'}$, and $g(x) = b(x) - b'(\theta x)$. To estimate the correlation between s^c and $s^{c'}$ at τ, we divide it into following cases.

1) If $c = c'$, only nontrivial autocorrelation of s^c need to be considered, that is, $\theta \neq 1$. Then, $f(x)$ has two distinct roots. Thus, $f(x)$ cannot be a Mth power. Moreover, $g(x)$ has degree at most r. By Lemma 1,

$$|R_{s^c}(\tau)| = \left|\sum_{x \in F_q} \chi\Big(f(x)\Big)\varphi\Big(g(x)\Big) - 1\right| \leqslant (r+1)\sqrt{q} + 1.$$

2) If $c \neq c'$ and $f(x) = h(x)^M$ for some $h(x) \in F_q[x]$, we have $a = a'$ and $\theta = 1$. By $c \neq c'$ and $a = a'$, we have $(b_r,...,b_1) \neq (b_r,...,b_{1'})$. Hence, $g(x) = b(x) - b'(x)$ is a polynomial with degree at least 1 and at most r. Furthermore, by assumption $r \leqslant p-2$, we have $\gcd\Big(\deg\Big(g(x)\Big), q\Big) = 1$. By applying Lemma 2, we have

$$\Big|R_{s^c,s^{c'}}(\tau)\Big| = \left|\sum_{x \in F_q} \varphi\Big(g(x)\Big) - 1\right| \leqslant (r-1)\sqrt{q} + 1.$$

3) If $c \neq c'$ and $f(x) \neq h(x)^M$ for any $h(x) \in F_q[x]$, then, $f(x)$ has at most two distinct roots and $g(x)$ has degree at most r. By applying Lemma 2 again, we have

$$\Big|R_{s^c,s^{c'}}(\tau)\Big| = \left|\sum_{x \in F_q} \chi\Big(f(x)\Big)\varphi\Big(g(x)\Big) - 1\right| \leqslant (r+1)\sqrt{q} + 1.$$

Combining above cases, the proof is thus completed. □

By Theorem 1, sequences in Γ_r^* are cyclically distinct. Hence, the family size of Γ_r^* is $(M-1)q^r$. Note that each sequence in Γ_r^* has one 0 per period. Similar to Ref. [5], we can modify sequences in Γ_r^* to be polyphase sequences by changing these zeros. Technologically, we can define $\chi(0) = 1$ instead of $\chi(0) = 0$. Let us denote the new sequence as $\hat{s}^c$ and the corresponding sequence family as Γ_r. It is easily seen from Eq. (1) that for all $\hat{s}^c$ and $\hat{s}^{c'}$ in Γ_r,

$$R_{\hat{s}^c,\hat{s}^{c'}}(\tau) = R_{s^c,s^{c'}}(\tau) + \varphi\Big(b(-1)\Big)\overline{\chi^{a'}(-\theta+1)}\,\overline{\varphi\Big(b'(-\theta)\Big)} + \chi^a(-\theta^{-1}+1)\varphi\Big(b(-\theta^{-1})\Big)\overline{\varphi\Big(b'(-1)\Big)}.$$

Therefore,

$$|R_{\hat{s}^c,\hat{s}^{c'}}(\tau)| \leqslant |R_{s^c,s^{c'}}(\tau)| + 2.$$

Corollary 1 Let Γ_r be the sequence family defined above. Then we have

$$R_{\max}(\Gamma_r) \leqslant (r+1)\sqrt{q} + 3.$$

Several known classes of sequence families with low correlation and large family size are compared in Table 1. In Table 1, the alphabet size M is a factor of period L or $L-1$. When we compare it with the sequence families given in Refs. [3,4,8], new constructed sequence family possesses the same period and maximum correlation magnitude, a larger family size if we let r equal to 1 or 2, but a larger alphabet size. Similarly, compared with the sequence family in Ref. [9], new sequence family has a lower maximum correlation magnitude, but a lager alphabet size. Hence, for the new construction, the increase of the family size is at the cost of faster increase of the alphabet size in general. However, in applications, the

Table 1 Comparison of several classes of sequence families with low correlation and large family size

	period L	alphabet	$R_{\max}$	family size
$\tilde{F}_r$ [3]	p	M	$2\sqrt{L}+5$	$\frac{(M+1)(L+1)}{2}$
F_r [3]	p	M	$3\sqrt{L}+4$	$\frac{(M-1)^2(L-1)}{2}+(M-1)$
F_s [3]	p^m-1	M	$2\sqrt{L+1}+6$	$\frac{(M-1)L}{2}+\left\lfloor\frac{M-1}{2}\right\rfloor$
L [8]	p^m-1	M	$3\sqrt{L+1}+5$	$\frac{(M-1)^2(L-2)}{2}+\frac{M(M-1)}{2}$
V [4]	p^m-1	M	$3\sqrt{L+1}+1$	$(M-1)\cdot\left(\frac{\mathrm{L}}{2}+1\right)$
U [4]	p^m-1	M	$3\sqrt{L+1}+5$	$\frac{M(M-1)(L-1)}{2}+M-1$
$F_o^k(\rho)$ [9]	p^m-1	p	$1+p^{\frac{m+(2\rho-1)e}{2}}$	p^{me}
Ω_r [5]	p	$p(p-1)$	$(r+1)\sqrt{p}+2$	$(p-2)\cdot p^r$
Γ_r (this paper)	p^m-1	Mp	$(r+1)\sqrt{p^m}+3$	$(M-1)\cdot p^{mr}$

alphabet size M is often required to be much smaller than the period L of the sequence, that is, $M \ll L$. Thus, the proper increase of the alphabet size may be acceptable for the gaining of a larger family size by taking small integer M, small prime p, and large integer m. Finally, we have to acknowledge that the individual sequences in the new sequence family may behave not well in balanceness and autocorrelation, which has been verified for several cases.

3 Conclusion

Just as it was pointed out in Ref. [5] that there is a tradeoff between the sequence family size and its maximum correlation, which also serves as a motivation of the constructions presented in this paper. Our constructions can be regarded as a generalization of the constructions in Ref. [5]. By Theorem 1 and Corollary 1, the correlation of the new sequence family meets the Welch bound asymptotically.

Acknowledgements This work was supported in part by the National Natural Science Foundation of China (Grant Nos. 61102093 and 61072080), Natural Science Foundation of Fujian Province (No. 2010J01319), and Key Project of Fujian Provincial Universities — Information Technology Research Based on Mathematics.

References

1. Golomb S W, Gong G. Signal Design for Good Correlation — For Wireless Communication, Cryptography and Radar. Cambridge, U.K.: Cambridge University Press, 2005
2. Helleseth T, Kumar P V, Pless V S, Huffman W C. Sequences with low correlation. In: Handbook of Coding Theory. Amsterdam, Netherlands: Elsevier, 1998
3. Han Y K, Yang K. New M-ary sequence families with low correlation and large size. IEEE Transactions on Information Theory, 2009, 55 (4): 1815–1823
4. Yu N Y, Gong G. New construction of M-ary sequence families with low correlation from the structure of Sidelnikov sequences. IEEE Transactions on Information Theory, 2010, 56(8): 4061–4070
5. Schmidt K U. Sequence families with low correlation derived from multiplicative and additive characters. IEEE Transactions on Information Theory, 2011, 57(4): 2291–2294
6. Niederreiter H, Winterhof A. Incomplete character sums and polynomial interpolation of the discrete logarithm. Finite Fields and Their Applications, 2002, 8(2): 184–192
7. Lidl R, Niederreiter H. Finite Fields (Encyclopedia of Mathematics and Its Applications. vol. 20). 2nd ed. New York, NY: Cambridge University Press, 1997
8. Kim Y S, Chung J S, No J S, Chung H. New families of M-ary sequences with low correlation constructed from Sidelnikov sequences. IEEE Transactions on Information Theory, 2008, 54(8): 3768–3774
9. Zhou Z C, Tang X H. New nonbinary sequence families with low correlation, large size, and large linear span. Applied Mathematics Letters, 2011, 24(7): 1105–1110