LETTER

New Family of Polyphase Sequences with Low Correlation from Galois Rings*

Linyan YU[†a)], ***Student Member***, **Pinhui KE**[†b)], ***and*** **Zuling CHANG**[††c)], ***Nonmembers***

SUMMARY In this letter, we give a new construction of a family of sequences of period p^k-1 with low correlation value by using additive and multiplicative characters over Galois rings. The new constructed sequence family has family size $(M-1)(p^k-1)^r p^{kr(e-1)}$ and alphabet size Mp^e. Based on the characters sum over Galois rings, an upper bound on the correlation of this sequence family is presented.

key words: *Galois rings, character sum, correlation, polyphase sequence*

1. Introduction

Pseudorandom sequences with low correlation have important applications in digital communications, radar ranging and cryptography [2], [3], [20]. For instance, a sequence set with sequences at least 2 can be used in the direct sequence spread spectrum (DSSS) system, in which each transmitter uses a unique sequence as its signature [4]. In this case, not only the low autocorrelation is preferred, but also the low cross-correlation is expected to extract the signal of the desired user from the rest of users. However, the maximum correlation magnitude of sequence sets is bounded from the well known Welch bound [5].

Let S be a family of M polyphase sequences of period N, denoted by

$$S = \{\mathbf{s}_i = \{s_i(t)\}_{t=0}^{N-1} : 0 \le i \le M-1\},$$

where each $s_i(t)$ is a q-th root of unity for all $0 \le t \le N-1$. For sequences $\mathbf{s}_i, \mathbf{s}_j \in S$, the periodic cross-correlation of $\mathbf{s}_i$ and $\mathbf{s}_j$ is given by

$$R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) = \sum_{t=0}^{N-1} s_i(t)s_j^*(t+\tau), 0 \le \tau \le N-1,$$

where s^* denotes the complex conjugate of s. The periodic autocorrelation function of $\mathbf{s}_i$ at the shift phase τ is denoted by $R_{\mathbf{s}_i}(\tau)$ if $\mathbf{s}_i = \mathbf{s}_j$. Then, the maximum magnitude $\theta_{\max}$ of the sequence family S is given by

$$\theta_{\max} = \max\{\theta_a, \theta_c\},$$

where

$$\theta_c = \max\{|R_{\mathbf{s}_i,\mathbf{s}_j}(\tau)| : 0 \le i \ne j \le M-1, 0 \le \tau < N\},$$
$$\theta_a = \max\{|R_{\mathbf{s}_i}(\tau)|, |R_{\mathbf{s}_j}(\tau)| : 0 \le i \le M-1, 0 < \tau < N\}.$$

From [5], we knew that the Welch bound of any sequences set S is $\theta_{\max} \gtrsim f(M)\sqrt{N}$, where $f(M) = \sqrt{\frac{(M-1)N}{MN-1}}$, and the Welch bound $\theta_{\max} \gtrsim \sqrt{N}$ if the family size M grows. Given the period of the sequences in a sequence family, the size of this sequence family seems to be limited. Therefore, this leads to a tradeoff between the maximum correlation and family size in a sequence family. Up to now, some results on the construction of sequence families with low correlation and suitable family size has been widely concerned [6]–[19], we also list the known families of sequences in the Table 1. Although the maximum correlation values of some sequence families in Table 1 asymptotically satisfies the Welch bound, their family sizes are not large enough.

One powerful tool to construct new sequence families are characters over finite fields or rings. In [6], a family of sequences is constructed based on the additive and multiplicative characters over prime field. The estimation of hybrid character sums is used to obtain the bounds of the maximum correlation. Ke et al. [7] generalized the sequence family introduced in [6] to a general finite field. Recently, Zhou et al. [8] obtained a class of asymptotically optimal polyphase sequence family by using the additive and multiplicative characters over finite field. Gu et al. [9] extended the sequence family in [8] to the Galois ring. Inspired by above ideas, we will generalize the sequence families over Galois rings in [9] to get a new family of polyphase sequence with a larger family size, while keeping low correlation.

The rest of this paper is organized as follows. Section 2 introduces the notation and related results. In Sect. 3, we present a new family of sequences by using the additive and multiplicative characters over Galois rings. The upper bound on the correlation of this sequence family is obtained by the estimation of characters sum. Section 4 concludes this letter.

Manuscript received December 9, 2021.
Manuscript revised March 7, 2022.
Manuscript publicized April 20, 2022.

[†]The authors are with School of Mathematics and Statistics, Fujian Normal University, Fuzhou, 350117, P. R. China.
[††]The author is with Department of Mathematics, Zhengzhou University, Zhengzhou, Henan, 450001, P. R. China.

*This research was supported by the National Natural Science Foundation of China (No.61772292, No.61772476), the Provincial Natural Science Foundation of Fujian (No.2019J01273), and Fujian Normal University Innovative Research Team (No.IRTL1207).

a) E-mail: ylyfjnu@163.com
b) E-mail: keph@fjnu.edu.cn (Corresponding author)
c) E-mail: zuling_chang@zzu.edu.cn

DOI: 10.1587/transfun.2021EAL2111

2. Preliminaries

Let p be a prime, k be a positive integer and $q = p^k$. Let $e \geq 1$ be a fixed integer. A monic polynomial $f(x) \in \mathbb{Z}_{p^e}[x]$ is said to be a basic irreducible polynomial of degree k if $f(x) \mod p \in \mathbb{Z}_p[x]$ is a monic irreducible polynomial of degree k. The Galois ring $\mathrm{GR}(p^e, k)$ of characteristic p^k is defined by

$$\mathrm{R}_{e,k} = \mathrm{GR}(p^e, k) = \mathbb{Z}_{p^e}[x]/\langle f(x)\rangle,$$

where $f(x)$ is a basic irreducible polynomial of degree k over $\mathbb{Z}_{p^e}$. Let $\beta_k \in \mathrm{R}_{e,k}$ such that the order of β_k is $q-1$ and define $\mathrm{T}^*_{e,k} = \langle\beta_k\rangle$. $\mathrm{R}_{e,k}$ is a local ring with unique maximal ideal $p\mathrm{R}_{e,k}$. The unit set $\mathrm{R}^*_{e,k} = \mathrm{R}_{e,k} \setminus p\mathrm{R}_{e,k}$ in $\mathrm{R}_{e,k}$ is a multiplicative group with the following structure

$$\mathrm{R}^*_{e,k} = \mathrm{T}^*_{e,k} \times (1 + p\mathrm{R}_{e,k}).$$

It can be shown that every element $z \in \mathrm{R}_{e,k}$ has a unique p-adic representation

$$z = z_0 + z_1 p + z_2 p^2 + \cdots + z_{e-1}p^{e-1}, z_i \in \mathrm{T}_{e,k},$$

where $\mathrm{T}_{e,k} = \mathrm{T}^*_{e,k} \cup \{0\}$.

Let $\tau_k(z)$ be the Frobenius map of $\mathrm{R}_{e,k}$ over $\mathbb{Z}_{p^e}$ given by

$$\tau_k(z) = z_0^p + z_1^p p + z_2^p p^2 + \cdots + z_{e-1}^p p^{e-1}.$$

Then τ_k is a generator of the Galois group of $\mathrm{R}_{e,k}/\mathbb{Z}_{p^e}$. The group is a cyclic group of order k.

The trace mapping $\mathrm{Tr} : \mathrm{R}_{e,k} \to \mathbb{Z}_{p^e}$ is defined by

$$\mathrm{Tr}(z) = z + \tau_k(z) + \cdots + \tau_k^{k-1}(z), z \in \mathrm{R}_{e,k}.$$

2.1 Additive and Multiplicative Characters over Galois Rings

An additive character of $\mathrm{R}_{e,k}$ is a homomorphism mapping from additive group $(\mathrm{R}_{e,k}, +)$ to $(\mathbb{C}^*, \cdot)$ defined by

$$\psi(v) = e^{\frac{2\pi i \mathrm{Tr}(v)}{p^e}}, v \in \mathrm{R}_{e,k}.$$

It is easily seen that ψ is an additive character of $\mathrm{R}_{e,k}$, called the canonical additive character. For $u \in \mathrm{R}_{e,k}$, define $\psi_u(v) = \psi(uv)$. ψ_u is also an additive character. In the case $u = 0$, we call $\psi_0(v)$ trivial additive character. Otherwise, we call it nontrivial. In fact, $\{\psi_u\}_{u\in\mathrm{R}_{e,k}}$ consists of all the additive characters of $\mathrm{R}_{e,k}$.

Let g be a fixed primitive element of $\mathrm{T}^*_{e,k}$. For $0 \leq l \leq q-2$, the canonical multiplicative character χ can be defined by

$$\chi(g^l) = e^{\frac{2\pi i l}{q-1}}.$$

For $0 \leq j \leq q-2$, define $\chi_j(g^l) = \chi(g^{lj})$. χ_j is also an multiplicative character of $\mathrm{T}^*_{e,k}$. Given two characters χ_j and $\chi_{j'}$, one can form the product $\chi_j\chi_{j'}$ by setting $\chi_j\chi_{j'}(g) = \chi_j(g)\chi_{j'}(g)$ for all $g \in \mathrm{T}^*_{e,k}$. χ_j's are all the multiplicative characters of $\mathrm{T}^*_{e,k}$ and form a cyclic group with $q-1$ elements. The order of each character χ_j is a divisor of $q-1$.

2.2 Estimates of Characters Sum over Galois Rings

Let $f(x)$ be a polynomial over $\mathrm{R}_{e,k}$ with $f(0) \neq 0$ and $f(x)$ not identically 0. A unique p-adic representation of $f(x)$ is given by

$$f(x) = f_0(x) + f_1(x)p + \cdots + f_{e-1}(x)p^{e-1},$$

where $f_i(x)$ is a polynomial of degree d_i with coefficients in $\mathrm{T}_{e,k}$ for $i = 0, 1, \ldots, e-1$. Define the weighted e-degree of $f(x)$ by $W_e(f(x)) = \max\{d_0 p^{e-1}, d_1 p^{e-2}, \ldots, d_{e-1}\}$.

Definition 1: Let $f(x)$ be a polynomial as above and $f_i(x) = \sum_{j=0}^{d_i} f_{i,j}x^j$, where $f_{i,j} \in \mathrm{T}_{e,k}$. For $0 \leq i \leq e-1, 0 \leq j \leq d_i$, the polynomial $f(x)$ is called nondegenerate if $f_{i,j} \equiv 0,\ j \equiv 0 \pmod p$.

The following two well-known lemmas on the character sums will be used to estimate correlation function of sequence families.

Lemma 1: ([20]) Let $f(x) \in \mathrm{R}_{e,k}[x]$ be nondegenerate with weighted e-degree $W_e(f(x))$ and $\psi_{e,k}$ a nontrivial additive character of $\mathrm{R}_{e,k}$. Then

$$|\sum_{\xi\in\mathrm{T}_{e,k}} \psi_{e,k}(f(\xi))| \leq (W_e(f(x)) - 1)\sqrt{q}.$$

Lemma 2: ([20]) Let $f(x) \in \mathrm{R}_{e,k}[x]$ be nondegenerate with weighted e-degree $W_e(f(x))$, $\psi_{e,k}$ a nontrivial additive character of $\mathrm{R}_{e,k}$ and χ a nontrivial multiplicative character of $\mathrm{T}^*_{e,k}$. Then

$$|\sum_{\xi\in\mathrm{T}^*_{e,k}} \psi_{e,k}(f(\xi))\chi(\xi)| \leq W_e(f(x))\sqrt{q}.$$

3. Construction of a New Sequence Family from Galois Rings

In this section, we will construct a new family of polyphase sequences from the additive and multiplicative characters over Galois Rings. Let $\mathrm{R}_{e,k} = \mathrm{GR}(p^e, k)$ and $\xi \in \mathrm{R}_{e,k}$ with order $q-1$.

Construction 1: Given integer r, $0 < r \leq p-1$, denote

$$D_r = \{(a; b_r, b_{r-1}, \ldots, b_1) | 1 \leq a \leq M-1, b_i \in \mathrm{R}^*_{e,k}, 1 \leq i \leq r\},$$

where M is a positive integer satisfying $M|q-1$. Let $d = (a; b_r, b_{r-1}, \ldots, b_1) \in D_r$, for $0 \leq t \leq q-2$, the sequence s_d is then given by

$$s_d(t) = \psi(\sum_{i=1}^{r} b_i(\xi^t)^i)\chi^a(\xi^t),$$

where ψ is a nontrivial additive character of $\mathrm{R}_{e,k}$ and χ is a

Table 1 Comparison of parameters and maximum correlations of several sequence families.

Family of sequence	Period	family size	alphabet	$\theta_{\max}$	θ_a
Kasami [10]	p^k-1	$1+p^{\frac{k}{2}}$	p	$1+p^{\frac{k}{2}}$	$1+p^{\frac{k}{2}}$
Frank et al. [11]	p^2	$p-1$	p	p	0
Sidelnikov [12]	p^k-1	p^k	p	$1+p^{\frac{k}{2}}$	$1+p^{\frac{k}{2}}$
Kumar and Moreno [13]	p^k-1	$p^{\frac{k}{2}}$	p	$1+p^{\frac{k}{2}}$	$1+p^{\frac{k}{2}}$
Liu and Komo [14]	p^k-1	$p^{\frac{k}{2}}$	p	$1+p^{\frac{k}{2}}$	$1+p^{\frac{k}{2}}$
Moriuchi and Imamura [15]	p^k-1	$p^{\frac{k}{2}}$	p	$1+p^{\frac{k}{2}}$	$1+p^{\frac{k}{2}}$
Boztas et al.; Udaya et al. [16], [17]	p^k-1	$1+p^k$	4	$1+p^{\frac{k}{2}}$	$1+p^{\frac{k}{2}}$
Udaya et al.; Tang et al.; [17], [18]	$p(p^k-1)$	p^k	4	$p+p^{\frac{k+1}{2}}$	$p+p^{\frac{k+1}{2}}$
Schmidt [6]	p	$(p-2)p^r$	$p(p-1)$	$2+(r+1)p^{\frac{1}{2}}$	$2+rp^{\frac{1}{2}}$
Ke [7]	p^k-1	$(M-1)p^{kr}$	Mp	$(r+1)p^{\frac{k}{2}}+3$	$(r+1)p^{\frac{k}{2}}+3$
Chung et al. [19]	p^2-p	p	p	p	p
Zhou et al. [8]	p^k-1	p^k-1	$p(p^k-1)$	$p^{\frac{k}{2}}$	1
Gu et al. [9]	p^k-1	$p^{ek}-1$	$p^e(p^k-1)$	$p^{e-1}p^{\frac{k}{2}}$	$p^{e-1}p^{\frac{k}{2}}$
This paper	p^k-1	$(M-1)(p^k-1)^r p^{kr(e-1)}$	Mp^e	$rp^{e-1}p^{\frac{k}{2}}$	$(rp^{e-1}-1)p^{\frac{k}{2}}$

nontrivial multiplicative character of $\mathrm{T}^*_{e,k}$ with order M. For $0<r\le p-1$, the sequence family S is denoted by

$$S=\{s_d|d\in D_r\}. \tag{1}$$

It is easy to see that the period of this sequence family is p^k-1 and has family size $(M-1)(p^k-1)^r p^{kr(e-1)}$. In the following, we provide an upper bound on the correlation of this sequence family in Construction 1.

Therorem 1: Let S be the sequence family defined in (1). Then the upper bound on the correlation of S is given by

$$\theta_{\max}(S)\le rp^{e-1}\sqrt{p^k}.$$

Proof 1: For any two sequences s_d and $s_{d'}$ in S, we denote $d=(a;b_r,b_{r-1},\ldots,b_1), d'=(a';b_{r'},b_{r-1'},\ldots,b_{1'})$ then we have

$$s_d(t)=\psi(\sum_{i=1}^{r}b_i(\xi^t)^i)\chi^a(\xi^t),\quad s_{d'}(t)=\psi(\sum_{i=1}^{r}b_{i'}(\xi^t)^i)\chi^{a'}(\xi^t).$$

Let $b(x)=\sum_{i=1}^{r}b_ix^i$ and $b'(x)=\sum_{i=1}^{r}b_{i'}x^i$. For all $0\le\tau\le q-2$, we have

$$\begin{aligned}\mathrm{R}_{s_d,s_{d'}}(\tau)&=\sum_{t=0}^{q-2}\psi(b(\xi^t))\chi^a(\xi^t)\psi^*(b'(\xi^{t+\tau}))\chi^{a'*}(\xi^{t+\tau})\\&=\sum_{x\in\mathrm{T}^*_{e,k}}\psi(b(x)-b'(\theta x))\chi(x^a(\theta x)^{M-a'})\\&=\chi(\theta^{M-a'})\sum_{x\in\mathrm{T}^*_{e,k}}\psi(g(x))\chi_{a-a'}(x),\end{aligned}$$

where $\theta=\xi^\tau$, $g(x)=b(x)-b'(\theta x)$. Thus we discuss the following two cases.

Case 1: when $d=d'$, we only need to consider the nontrivial correlation of R_{s_d}, that is $\theta=\xi^\tau\ne1$. Since $d=d'$, then $\chi_{a-a'}(x)=\chi_0(x)=1$ and $g(x)=\sum_{i=1}^{r}(b_i-b_i\theta^i)x^i$. By assumption $b_i\in\mathrm{R}^*_{e,k},\theta\ne1$, we have $b_i-b_i\theta^i\ne0$. For all $0<r\le p-1$, the weighted e-degree of $g(x)$ has $W_e(g(x))\le rp^{e-1}$. Applying Lemma 1, we have

$$|\mathrm{R}_{s_d}(\tau)|\le(rp^{e-1}-1)\sqrt{q}.$$

Case 2: when $d\ne d'$, then $a-a'\ne0$ and $g(x)=\sum_{i=1}^{r}(b_i-b_{i'}\theta^i)x^i$. By assumption $b_i,b_{i'}\in\mathrm{R}^*_{e,k}$ and $(b_r,b_{r-1},\cdots,b_1)\ne(b_{r'},b_{r-1'},\cdots,b_{1'})$, we have $b_i-b_{i'}\theta^i$ is not all zero. For all $0<r\le p-1$, the weighted e-degree of $g(x)$ has $W_e(g(x))\le rp^{e-1}$. Applying Lemma 2, we have

$$|\mathrm{R}_{s_d,s_{d'}}(\tau)|\le rp^{e-1}\sqrt{q}.$$

The theorem follows. □

The following example illustrates the low correlation of sequence families in Construction 1.

Example 1: Let $p=2,e=2,k=3,w_j=e^{\frac{2\pi iTr(\xi^{t+1})}{j}}$. From Construction 1, let $M=7,r=1,b_1=\xi$. Therefore, we have $D_1=\{(a;b_1)|1\le a\le6,b_1=\xi\}$. Let $d=(a;b_1)$, for $0\le t\le6$, the sequence s_d is then given by $s_d(t)=\psi(b_1\xi^t)\chi^a(\xi^t)$. For $0\le t\le6$, we have

$$\begin{aligned}&(\chi^a(\xi^0),\chi^a(\xi^1),\chi^a(\xi^2),\chi^a(\xi^3),\chi^a(\xi^4),\chi^a(\xi^5),\chi^a(\xi^6))\\&=\begin{cases}(1,w_7,w_7^2,w_7^3,w_7^4,w_7^5,w_7^6), & for\ a=1;\\(1,w_7^2,w_7^4,w_7^6,w_7,w_7^3,w_7^5), & for\ a=2;\\(1,w_7^3,w_7^6,w_7^2,w_7^5,w_7,w_7^4), & for\ a=3;\\(1,w_7^4,w_7,w_7^5,w_7^2,w_7^6,w_7^3), & for\ a=4;\\(1,w_7^5,w_7^3,w_7,w_7^6,w_7^4,w_7^2), & for\ a=5;\\(1,w_7^6,w_7^5,w_7^4,w_7^3,w_7^2,w_7), & for\ a=6;\end{cases}\end{aligned}$$

and $(w_4^{Tr(\xi)},w_4^{Tr(\xi^2)},w_4^{Tr(\xi^3)},w_4^{Tr(\xi^4)},w_4^{Tr(\xi^5)},w_4^{Tr(\xi^6)},w_4^{Tr(\xi^7)})=(w_4^2,w_4^2,w_4,w_4^2,w_4,w_4,w_4^3)$. By using the Magma program, we get $\theta_{\max}(S_d)\approx3.0669<4\sqrt{2}$ and $\theta_a(S_d)\approx2.2361<2\sqrt{2}$.

We list the parameters of some known sequence families in Table 1. From Table 1, the parameters and maximum correlations of these sequence families and our construction

are compared. The results show that the sequence family constructed in this letter not only has low correlation but also has a larger family size compared with other sequence families with the same period.

4. Conclusion

In this letter, we have presented a family of sequences of period $p^k - 1$ with low correlation value by using additive and multiplicative characters over Galois rings. Our result can be regarded as a generalization of the constructions in [9]. Compared with other known sequence families, new constructed sequence families have low correlation and sufficiently large family sizes.

References

[1] P.Z. Fan and M. Darnell, Sequence Design for Communications Applications, Research Studies, London, U.K., 1996.
[2] S.W. Golomb and G. Gong, Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar, Cambridge Univ. Press, Cambridge, U.K., 2005.
[3] Z. Gu, Z. Zhou, Y. Yang, A.R. Adhikary, and X. Cai, "Deterministic compressed sensing matrices from sequences with optimal correlation," IEEE Access, vol.7, pp.16704–16710, Feb., 2019.
[4] R. Scholtz, "The origins of spread-spectrum communication," IEEE Trans. Commun., vol.30, no.5, pp.822–854, 1982.
[5] L. Welch, "Lower bounds on the maximum cross correlation of signals (corresp.)," IEEE Trans. Inf. Theory, vol.20, no.3, pp.397–399, May 1974.
[6] K.U. Schmidt, "Sequence families with low correlation derived from multiplicative and additive characters," IEEE Trans. Inf. Theory, vol.57, no.4, pp.2291–2294, May 2011.
[7] P.H. Ke and S.Y. Zhang, "New classes of sequence families with low correlation by using multiplicative and additive characters," Front. Electr. Electron. Eng., vol.7, pp.308–311, Sept. 2012.
[8] Z. Zhou, T. Helleseth, and U. Parampalli, "A family of polyphase sequences with asymptotically optimal correlation," IEEE Trans. Inf. Theory, vol.64, no.4, pp.2896–2900, May 2018.
[9] Z. Gu, Z. Zhou, M. Sihem, and P. Udaya, "A new family of polyphase sequences with low correlation," Cryptogr. Commun., vol.14, pp.135–144, Aug. 2021.
[10] T. Kasami, "Weight distribution formula for some class of cyclic codes," Technical Report, R-285 (AD632574), Coordinated Sci. Lab., Univ. Illinois Urbana-Champaign, Urbana, IL, USA, 1966.
[11] R.L. Frank, S.A. Zadoff, and R. Heimiller, "Phase shift pulse codes with good periodic correlation properties (corresp.)," IRE Trans. Inf. Theory, vol.IT-8, no.6, pp.381–382, Oct. 1962.
[12] V.M. Sidelnikov, "On mutual correlation of sequences," Soviet Math. Dokl., vol.12, pp.197–201, 1971.
[13] P.V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," IEEE Trans. Inf. Theory, vol.37, no.3, pp.603–616, May 1991.
[14] S.-C. Liu and J.J. Komo, "Nonbinary Kasami sequences over GF(p)," IEEE Trans. Inf. Theory, vol.38, no.4, pp.1409–1412, July 1992.
[15] T. Moriuchi and K. Imamura, "Balanced nonbinary sequences with good periodic correlation properties obtained from modified Kumar-Moreno sequences," IEEE Trans. Inf. Theory, vol.41, no.2, pp.572–576, March 1995.
[16] S. Boztas, R. Hammons, and P.Y. Kumar, "4-phase sequences with near-optimum correlation properties," IEEE Trans. Inf. Theory, vol.38, no.3, pp.1101–1113, May 1992.
[17] P. Udaya and M.U. Siddiqi, "Optimal and suboptimal quadriphase sequences derived from maximal length sequences over $\mathbb{Z}_4$," Appl. Algebra Eng., Commun. Comput., vol.9, no.2, pp.161–191, 1998.
[18] X.H. Tang and P. Udaya, "A note on the optimal quadriphase sequences families," IEEE Trans. Inf. Theory, vol.53, no.1, pp.433–436, Jan. 2007.
[19] J.-H. Chung and K. Yang, "A new class of balanced near-perfect nonlinear mappings and its application to sequence design," IEEE Trans. Inf. Theory, vol.59, no.2, pp.1090–1097, Feb. 2013.
[20] S.Q. Fan and W.B. Han, "Character sums over Galois rings and primitive polynomials over finite fields," Finite Fields and Their Applications, vol.10, no.1, pp.36–52, Jan. 2004.