Some New Results on the Cross Correlation of m-Sequences

Tao Zhang, Shuxing Li, Tao Feng, and Gennian Ge

***Abstract*— The determination of the cross correlation between an m-sequence and its decimated sequence has been a long-standing research problem. Considering a ternary m-sequence of period $3^{3r}-1$, we determine the cross correlation distribution for decimations $d=3^r+2$ and $d=3^{2r}+2$, where $\gcd(r,3)=1$. Meanwhile, for a binary m-sequence of period $2^{2lm}-1$, we make an initial investigation for the decimation $d=(2^{2lm}-1)/(2^m+1)+2^s$, where $l\geq 2$ is even and $0\leq s\leq 2m-1$. It is shown that the cross correlation takes at least four values. Furthermore, we confirm the validity of two famous conjectures due to Sarwate *et al.* and Helleseth in this case.**

***Index Terms*— Cross correlation, cross correlation distribution, decimation, m-sequences, Weil sums.**

I. Introduction

DURING the last decades, many applications of sequences with low correlation have been found in cryptography, radar and wireless communication systems [12]. In the CDMA system, a popular method to spread the spectrum is the use of sequences. Using sequences with low (auto and cross) correlation values, the interference of different users during the transmission can be reduced. Therefore, sequences with low correlation have been an important research problem enjoying considerable interests [17].

Let p be a prime. Let $\{a_t\}$ and $\{b_t\}$ be two sequences of period N with elements from a finite field $\mathrm{GF}(p)$. The cross correlation between $\{a_t\}$ and $\{b_t\}$ at shift τ is defined by

$$C_{a,b}(\tau)=\sum_{t=0}^{N-1}\omega^{a_{t+\tau}-b_t},$$

where $0\leq\tau<N$ and ω is a complex p-th root of unity.

There have been many researches concerning the maximal linear sequence (m-sequence). Since an m-sequence owns the ideal two-level auto correlation, many authors focus on the cross correlation between a pair of m-sequences (see [2], [3], [6], [8], [9], [13], [19], [23] and the references therein).

Recall that the trace function from finite field $E=\mathrm{GF}(p^n)$ onto its subfield $F=\mathrm{GF}(p^r)$ is defined by

$$Tr_r^n(x)=x+x^{p^r}+x^{p^{2r}}+\cdots+x^{p^{n-r}}.$$

For $r=1$, we get the absolute trace function mapping onto the prime field $GF(p)$, which is denoted by Tr_n or Tr. A p-ary m-sequence $\{a_t\}$ of period p^n-1 can be represented by

$$a_t=\mathrm{Tr}(\beta\alpha^t),\quad 0\leq t\leq p^n-2,$$

where $\beta\in\mathrm{GF}(p^n)^*$ and α is a primitive element of $\mathrm{GF}(p^n)$.

Suppose $(d,p^n-1)=1$. The d-decimation of $\{a_t\}$, which is denoted by $\{a_{dt}\}$, is also an m-sequence with the same period. Note that if $d\in\{1,p,\ldots,p^{n-1}\}$, $\{a_{dt}\}$ is simply a cyclic shift of $\{a_t\}$. The cross correlation between $\{a_t\}$ and $\{a_{dt}\}$ takes two values and is easy to compute [13, Theorem 3.1]. Below, we always consider the nondegenerate decimation d where $d\notin\{1,p,\ldots,p^{n-1}\}$. The cross correlation between an m-sequence of period p^n-1 and its d-decimation can be described by

$$\begin{aligned}C_d(\tau)&=\sum_{t=0}^{p^n-2}\omega^{a_{t+\tau}-a_{dt}}\\&=-1+\sum_{x\in\mathrm{GF}(p^n)}\chi(\alpha^\tau x-x^d),\end{aligned}$$

where $\chi(x)=w^{\mathrm{Tr}(x)}$ for any $x\in\mathrm{GF}(p^n)$ and $0\leq\tau\leq p^n-2$. Clearly, calculating the cross correlation value is to compute the Weil sum

$$\mathrm{C}_d(z)=\sum_{x\in\mathrm{GF}(p^n)^*}\chi(zx-x^d),$$

where $z\in\mathrm{GF}(p^n)^*$. Hence, computing the cross correlation distribution is to determine the multiset

$$\{\mathrm{C}_d(z)\mid z\in\mathrm{GF}(p^n)\}.$$

Noting that the cross correlation distribution essentially arises in many other contexts with various names, please refer to the appendix of [23] for more details.

For the cross correlation function between an m-sequence and its d-decimation, an overview of known results can be found in [8], [13], and [5]. Besides, further generalizations

Manuscript received September 29, 2013; revised February 18, 2014; accepted March 1, 2014. Date of publication March 11, 2014; date of current version April 17, 2014. T. Feng was supported in part by the Fundamental Research Fund for the Central Universities of China, in part by Zhejiang Provincial Natural Science Foundation under Grant LQ12A01019, in part by the National Natural Science Foundation of China under Grant 11201418, and in part by the Research Fund for Doctoral Programs through the Ministry of Education of China under Grant 20120101120089. G. Ge was supported in part by the National Natural Science Foundation of China under Grant 61171198 and in part by Zhejiang Provincial Natural Science Foundation of China under Grant LZ13A010001.

T. Zhang and S. Li are with the Department of Mathematics, Zhejiang University, Hangzhou 310027, China (e-mail: tzh@zju.edu.cn; sxli@zju.edu.cn).

T. Feng is with the Department of Mathematics, Zhejiang University, Hangzhou 310027, China, and also with the Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China (e-mail: tfeng@zju.edu.cn).

G. Ge is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China, and also with the Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China (e-mail: gnge@zju.edu.cn).

Communicated by T. Helleseth, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2014.2311113

TABLE I
CROSS CORRELATION DISTRIBUTION BETWEEN A BINARY m-SEQUENCE OF PERIOD 2^n-1 AND ITS d-DECIMATION WITH $(d, 2^n-1)=1$

Sources	d	♯ cro-co
Gold [11]	$d=2^k+1, \frac{n}{(n,k)}$ is odd	3
Kasami [22]	$d=2^{2k}-2^k+1$, $\frac{n}{(n,k)}$ is odd	3
Welch [2]	$d=2^k+3$, $n=2k+1$	3
Hollmann and Xiang [19]	$d=2^{2k}+2^k-1$, $k=\frac{n-1}{4}$ if $n\equiv 1 \pmod 4$ and $k=\frac{3n-1}{4}$ if $n\equiv 3 \pmod 4$	3
Cusick and Dobbertin [6]	$d=2^k+2^{\frac{k+1}{2}}+1$, $n=2k$, k is odd	3
Cusick and Dobbertin [6]	$d=2^{k+1}+3$, $n=2k$, k is odd	3
Niho [29]	$d=2^{2k+1}-1$, $n=4k$	4
Niho [29]	$d=(2^{2k}+1)(2^k-1)+2$, $n=4k$	4
Dobbertin [7]	$\sum_{i=0}^{2k}2^{im}$, $n=4k$, $0<m<n$, $\gcd(m,n)=1$	4
Helleseth and Rosendahl [18]	$d=(2^{2k}+2^{s+1}-2^{k+1}-1)/(2^s-1)$, $n=2k$, $2s\|k$	4
Dobbertin et al. [8]	$d=(2^k-1)s+1$, $s\equiv 2^r(2^r\pm 1)^{-1} \pmod{2^k+1}$, $v_2(r)<v_2(k)$	4
Helleseth [13]	$d=2^k+3$, $n=2k$	5
Dobbertin [7]	$d=2^{2k}+2^k+1$, $n=4k$, k is odd	5
Johansen and Helleseth [20]	$d=\frac{5}{3}$, n is odd	5
Johansen et al. [21]	$d=\frac{17}{5}$, n is odd	5
Boston and McGuire [1]	$d=11$, n is odd	5
Helleseth [14]	$d=2^{2k}-2^k+1$, $n=4k$, k is even	6
Helleseth [13]	$d=\frac{1}{3}(2^n-1)+2^s$, n is even, $s<n$ and $\frac{1}{3}2^{-s}(2^n-1)\neq 2 \pmod 3$	6
Dobbertin et al. [8]	$d=3\cdot 2^{k-1}-1$, $n=2k$, k is odd	6
Feng et al. [10]	$d=2^{t+1}+3$, $n=2t$, $t\equiv 2 \pmod 4$ and $t\geq 6$	7

have been made to study the cross correlation of an m-sequence and its d-decimated sequence with $\gcd(d, p^n-1)>1$ (see [16], [26]–[28], [31], [32]). When $p=2$ and $(d, 2^n-1)=1$, the known results on the cross correlation distribution of an m-sequence and its decimation are listed in Table I, where $v_2(k)$ is the largest power of 2 dividing k. Meanwhile, Table II summaries the known results on the cross correlation distribution when p is an odd prime.

There are many methods which have been proposed to determine the cross correlation distribution. With the help of some known exponential sums, Helleseth [13], [15] computed the cross correlation distribution for several decimations. Luo and Feng [25] used the technique of quadratic forms to attack this problem. In [8], Dobbertin et al. developed a delicate method involving the use of Dickson polynomials.

In this paper, we consider the cross correlation between a ternary m-sequence of period $3^{3r}-1$ and its d-decimation with $d=3^r+2$ or $d=3^{2r}+2$, where $(r,3)=1$. Following the idea of Dobbertin [7] and Feng et al. [10], we completely determine the cross correlation distribution. Besides, for the binary m-sequence of period $2^{2lm}-1$ and decimation $d=\frac{2^{2lm}-1}{2^m+1}+2^s$, with $l\geq 2$ being even and $0\leq s\leq 2m-1$, we obtain some results on the cross correlation values. When l is odd, the decimation d is of Niho type, which has been extensively studied [3], [8], [9], [18], [19], [29]. Recall that any nondegenerate decimation leads to at least three cross correlation values [13, Theorem 4.1]. We further prove that the cross correlation takes at least four values for this decimation. While it seems pretty hard to determine the cross correlation distribution, we confirm the validity of the following two famous conjectures due to Sarwate et al. [30] and Helleseth [13] respectively. Below, we define $\mathrm{S}_d(z)=\mathrm{C}_d(z)+1$.

Conjecture 1. *[30] Let $n=2t$ and $p=2$, then* $\max_{z\in GF(2^n)}|S_d|\geq 2^{t+1}$.

Conjecture 2. *[13] If $p^n>2$ and $d\equiv 1 \pmod{p-1}$, then $S_d(z)=0$ for some $z\in GF(p^n)^*$.*

This paper is organized as follows. In Section 2, we determine the cross correlation distribution for a ternary m-sequence and its decimated sequence mentioned above. In Section 3, we present some results on the cross correlation between a binary m-sequence and its d-decimation, where the above two conjectures are verified for $d=\frac{2^{2lm}-1}{2^m+1}+2^s$, with $l\geq 2$ being even and $0\leq s\leq 2m-1$. Section 4 concludes the paper.

II. THE CROSS CORRELATION DISTRIBUTION FOR THE TERNARY m-SEQUENCE

In this section, for the ternary m-sequence of period $3^{3r}-1$, we determine the cross correlation distribution with decimation $d=3^r+2$ or $d=3^{2r}+2$, where $(r,3)=1$.

We first introduce some notations. Given a prime power $q=p^s$, we have the corresponding finite field GF(q). Let ω be the p-th root of unity. The quadratic character of GF(q) is denoted by η. The canonical additive character of GF(q) is

TABLE II
CROSS CORRELATION DISTRIBUTION BETWEEN A NON-BINARY m-SEQUENCE OF PERIOD p^n-1 AND ITS d-DECIMATION

Sources	p	n	d	$\gcd(d,p^n-1)$	♯ cro-co
Helleseth [13]	odd prime	any	$d=p^{2k}-p^k+1, \frac{n}{(n,k)}$ is odd	1	3
Helleseth [13]	odd prime	any	$d=\frac{1}{2}(p^{2k}+1)$, $\frac{n}{(n,k)}$ is odd	1	3
Dobbertin et al. [9]	3	odd	$d=2\cdot 3^{\frac{n-1}{2}}+1$	1	3
Helleseth [13]	$p^{\frac{n}{2}}\not\equiv 2 \pmod 3$	even	$d=2p^{\frac{n}{2}}-1$	1	4
Helleseth [13]	$p^n\equiv 1 \pmod 4$	any	$d=\frac{1}{2}(p^n-1)+p^i$, $0\le i<n$	1	5
Helleseth [13]	$p\equiv 2 \pmod 3$	even	$d=\frac{1}{3}(p^n-1)+p^i$, $0\le i<n$, $\frac{1}{2}p^{-i}(p^n-1)\not\equiv 2 \pmod 3$	1	6
Helleseth [15]	$p^m\neq 2 \pmod 3$	$0 \pmod 4$	$d=p^{2m}-p^m+1$, $n=4m$	1	6
Luo and Feng [25]	odd prime	any	$d=\frac{p^k+1}{2}$, odd k/e, $e=\gcd(n,k)$	variable	variable
Seo et al. [31]	odd prime	$0 \pmod 4$	$d=(\frac{p^m+1}{2})^2$, $n=2m$	$\frac{p^m+1}{2}$	4
Choi et al. [4]	$3 \pmod 4$	odd	$d=\frac{p^n+1}{p^k+1}+\frac{p^n-1}{2}$, $k\mid n$	2	9

denoted by χ, where $\chi(x)=\omega^{Tr(x)}, \forall x\in \mathrm{GF}(q)$. The Gauss sum $G(\eta,\chi)$ related to η and χ is defined by

$$G(\eta,\chi)=\sum_{x\in \mathrm{GF}(q)^*}\eta(x)\chi(x).$$

The following two lemmas can be found in [24], which will be used later.

Lemma II.1. *[24, Theorem 5.15] Suppose $q=p^s$, where p is an odd prime and s is a positive integer. Then*

$$G(\eta,\chi)=\begin{cases}(-1)^{s-1}q^{\frac{1}{2}}; \text{ if } p\equiv 1 \pmod 4,\\ (-1)^{s-1}i^s q^{\frac{1}{2}}; \text{ if } p\equiv 3 \pmod 4.\end{cases}$$

Lemma II.2. *[24, Theorem 5.33] Let q be an odd prime power and $f(x)=a_2x^2+a_1x+a_0\in GF(q)[x]$ with $a_2\neq 0$. Then*

$$\sum_{c\in GF(q)}\chi(f(c))=\chi(a_0-a_1^2(4a_2)^{-1})\eta(a_2)G(\eta,\chi).$$

The following well known identities can be found in [13].

Lemma II.3. *We have*

$$\sum_{z\in GF(p^n)}S_d(z)=p^n,$$
$$\sum_{z\in GF(p^n)}S_d(z)^2=p^{2n},$$
$$\sum_{z\in GF(p^n)}S_d(z)^3=p^{2n}b_3,$$

where b_3 is the number of common solutions of

$$x+y+1=0,$$
$$x^d+y^d+1=0,$$

such that $x,y\in GF(p^n)$.

As a preparation, we have the following lemma.

Lemma II.4. *Given an integer r with $\gcd(r,3)=1$. Suppose $n=3r$, $d=3^r+2$ or $d=3^{2r}+2$. Then for $x,y\in GF(3^n)$, the number of common solutions of*

$$x+y+1=0,$$

and

$$x^d+y^d+1=0,$$

is 3^r.

Proof: We deal with the case where $d=3^r+2$. When $d=3^{2r}+2$, the proof is similar. Note the above equations are equivalent to

$$(x+1)^d-x^d-1=0.$$

Consequently,

$$(x+1)^{3^r}(x+1)^2-x^{3^r+2}-1=0,$$

which leads to

$$(x-1)(x^{3^r}-x)=0.$$

Hence, we deduce that $x\in GF(3^r)$, which means there are 3^r common solutions. ∎

Now we state our main result.

Theorem II.5. *Given an integer $r\ge 2$ with $\gcd(r,3)=1$. Set $n=3r$, $d=3^r+2$ or $d=3^{2r}+2$. For the ternary m-sequence of period 3^n-1, the cross correlation with its d-decimation is listed as follows. When r is even, the cross correlation distribution is*

$$\begin{array}{rlll} -1 & occurs & \frac{3^{3r}+3^{2r}}{2}-3^r & times\\ 3^{2r}-1 & occurs & 3^r & times\\ 3^{\frac{3r}{2}}-1 & occurs & \frac{3^{3r-1}-3^{2r-1}}{2} & times\\ -3^{\frac{3r}{2}}-1 & occurs & \frac{3^{3r-1}-3^{2r-1}}{2} & times\\ 2\cdot 3^{\frac{3r}{2}}-1 & occurs & \frac{3^{3r-1}-3^{2r-1}}{4} & times\\ -2\cdot 3^{\frac{3r}{2}}-1 & occurs & \frac{3^{3r-1}-3^{2r-1}}{4} & times\end{array}$$

When r is odd, the cross correlation distribution is

-1	*occurs*	$2\cdot 3^{3r-1}+3^{2r-1}-3^r$	*times*
$3^{2r}-1$	*occurs*	3^r	*times*
$3^{\frac{3r+1}{2}}-1$	*occurs*	$\frac{3^{3r-1}-3^{2r-1}}{2}$	*times*
$-3^{\frac{3r+1}{2}}-1$	*occurs*	$\frac{3^{3r-1}-3^{2r-1}}{2}$	*times*

Proof: In the following, we only prove the case $d=3^r+2$. The case $d=3^{2r}+2$ can be handled similarly. We fix $d=3^r+2$, $E=GF(3^n)$, $F=GF(3^r)$ and $n=3r$. It is routine to verify $\gcd(d,3^n-1)=1$.

Let a be a primitive element of $GF(27)$ with

$$a^3+2a+1=0.$$

Since $\gcd(r,3)=1$, we have $E=F(a)$. For any $x\in E$, it can be expressed as

$$x=x_0+x_1a+x_2a^2,$$

where $x_0,x_1,x_2\in F$.

Since $\gcd(r,3)=1$, we consider the case $r\equiv 2 \pmod 3$ at first, in which $a^{3^r}=a^9$. The first step is to compute a direct representation of $Tr_n(x^d)$ as a function of x_0,x_1 and x_2. Note that $Tr_r^n(1)=Tr_r^n(a)=0$ and $Tr_r^n(a^2)=2$. A lengthy routine computation shows

$$Tr_n(x^d)=Tr_r(x_1x_2^2+x_0x_2^2+2x_1^2x_2+2x_1).$$

Next, we compute $\mathrm{C}_d(z)$ for some fixed $z\in E$. Putting

$$z=z_0+z_1a+z_2a^2$$

with $z_0,z_1,z_2\in F$, we find

$$Tr_n(xz)=Tr_r(2x_2z_2+2x_0z_2+2x_1z_1+2x_2z_0).$$

Define the additive character of F as χ_F, where $\chi_F(x)=\omega^{Tr_r(x)},\forall x\in F$. Consequently, we can compute $\mathrm{S}_d(z)$ as equation (1) on the top of next page, where

$$M=\{x_2\in F|x_2^2=-z_2\}.$$

If $z_2=0$, then $M=\{0\}$. We have

$$\mathrm{S}_d(z)=3^r\sum_{x_1\in F}\chi_F(x_1(1+2z_1))=\begin{cases}0 & \text{if } z_1\neq 1,\\ 3^{2r} & \text{if } z_1=1.\end{cases}$$

If $-z_2$ is a nonsquare in F, then $M=\emptyset$ and $\mathrm{S}_d(z)=0$.

If $-z_2$ is a nonzero square in F, let $z_2=-b^2$, then $M=\{\pm b\}$. Hence,

$$\mathrm{S}_d(z)=3^r\sum_{x_1\in F}\chi_F(bx_1^2+(2b^2+2z_1+1)x_1+2b^3+2bz_0)+3^r\sum_{x_1\in F}\chi_F(2bx_1^2+(2b^2+2z_1+1)x_1+b^3+bz_0).$$

With the help of Lemma II.1 and Lemma II.2, we deduce

$$\mathrm{S}_d(z)=(-1)^{r-1}\cdot i^r\cdot 3^{\frac{3r}{2}}(\eta(b)\chi_F(c)+\eta(2b)\chi_F(-c)),$$

where

$$c=2b^3+2bz_0-(2b^2+2z_1+1)^2b^{-1}.$$

Note that

$$\eta(2)=\begin{cases}1 & \text{if } r \text{ is even},\\ -1 & \text{if } r \text{ is odd}.\end{cases}$$

Suppose $A=\eta(b)\chi_F(c)+\eta(2b)\chi_F(-c)$. Since $\chi_F(c)=\overline{\chi_F(-c)}$, we have

$$A=\begin{cases}\pm 1,\pm 2; & \text{if } r \text{ is even},\\ 0,\pm\sqrt{-3}; & \text{if } r \text{ is odd}.\end{cases}$$

When r is even, $\mathrm{S}_d(z)$ takes six values 0, 3^{2r}, $3^{\frac{3r}{2}}$, $-3^{\frac{3r}{2}}$, $2\cdot 3^{\frac{3r}{2}}$ and $-2\cdot 3^{\frac{3r}{2}}$. For $1\le i\le 6$, use N_i to denote the number of occurrences in the corresponding order above. With Lemma II.3, Lemma II.4 and the above discussion, we get

$$\begin{gathered}N_1=\frac{3^{3r}}{2}+\frac{3^{2r}}{2}-3^r,\\ N_2=3^r,\\ N_1+N_2+N_3+N_4+N_5+N_6=3^{3r},\\ 3^{2r}N_2+3^{\frac{3r}{2}}(N_3-N_4)+2\cdot 3^{\frac{3r}{2}}(N_5-N_6)=3^{3r},\\ 3^{4r}N_2+3^{3r}(N_3+N_4)+4\cdot 3^{3r}(N_5+N_6)=3^{6r},\\ 3^{6r}N_2+3^{\frac{9r}{2}}(N_3-N_4)+8\cdot 3^{\frac{9r}{2}}(N_5-N_6)=3^{7r}.\end{gathered}$$

Thus, we complete the proof for the case $r\equiv 2 \pmod 6$.

When r is odd, $\mathrm{S}_d(z)$ takes four values 0, 3^{2r}, $3^{\frac{3r+1}{2}}$ and $-3^{\frac{3r+1}{2}}$. For $1\le i\le 4$, use N_i to denote the number of occurrences in the corresponding order above. With Lemma II.3, Lemma II.4 and the above discussion, we get

$$\begin{gathered}N_2=3^r,\\ N_1+N_2+N_3+N_4=3^{3r},\\ 3^{2r}N_2+3^{\frac{3r+1}{2}}(N_3-N_4)=3^{3r},\\ 3^{4r}N_2+3^{3r+1}(N_3+N_4)=3^{6r}.\end{gathered}$$

Thus, we complete the proof for the case $r\equiv 5 \pmod 6$.

For the remaining case $r\equiv 1 \pmod 3$, a similar discussion leads to

$$Tr_n(x^d)=Tr_r(2x_2+x_0x_2^2+2x_1^2x_2+2x_1x_2^2+x_1).$$

The cross correlation distribution can be obtained in a similar way. ∎

Remark II.1. *When $r=3$, a numerical experiment shows that the cross correlation distribution for the ternary m-sequence of period 3^9-1 with decimation $d=3^3+2=29$ or $d=3^6+2=731$ is*

-1	*occurs*	13338	*times*
728	*occurs*	27	*times*
242	*occurs*	3159	*times*
-244	*occurs*	3159	*times*

This result is consistent with the distribution presented in Theorem II.5. Hence, in the case where $(r,3)=3$, we conjecture that the correlation distribution is the same as that in Theorem II.5.

III. Some Results on the Cross Correlation of Binary m-Sequences

In this section, we focus on the cross correlation between a binary m-sequence of period $2^{2lm}-1$ and its d-decimated

$$\begin{aligned}\mathrm{S}_d(z) &= \sum_{x_0,x_1,x_2\in F} \chi_F(2x_1x_2^2 + 2x_0x_2^2 + x_1^2x_2 + x_1 + 2x_2z_2 + 2x_0z_2 + 2x_1z_1 + 2x_2z_0)\\ &= \sum_{x_0,x_1,x_2\in F} \chi_F(x_0(2x_2^2 + 2z_2) + 2x_1x_2^2 + x_1^2x_2 + x_1 + 2x_2z_2 + 2x_1z_1 + 2x_2z_0)\\ &= 3^r \sum_{x_1\in F,x_2\in M} \chi_F(2x_1x_2^2 + x_1^2x_2 + x_1 + 2x_2z_2 + 2x_1z_1 + 2x_2z_0)\end{aligned} \tag{1}$$

sequence with $d = \frac{2^{2lm}-1}{2^m+1} + 2^s$, where $0 \le s \le 2m-1$ and $(2^{s-1} - l, 2^m + 1) = 1$. Note that $(2^{s-1} - l, 2^m + 1) = 1$ is equivalent to $(d, 2^{2lm} - 1) = 1$. Some special cases of this form have been studied before. For example, when $m = 1$, the decimation $d = \frac{2^{2l}-1}{3} + 2^s$ has been studied in [13] where the cross correlation distribution was obtained. If $l = 2$ and $s = 0$, the decimation $d = \frac{2^{4m}-1}{2^m+1}+1$ has also been investigated in [14]. In fact, when l is odd, it is straightforward to verify that d is of Niho type. As shown in [3], for the decimation of Niho type, the cross correlation takes at least four values. Consequently, it is natural to ask if the same thing happens when l is even. In this case, it is clear that d may not be of Niho type. We will show that $\mathrm{C}_d(z)$ also takes at least four values. In addition, we confirm that Conjecture 1 and Conjecture 2 are true for this type of decimation d.

Throughout the rest of this section, we always assume that $d = \frac{2^{2lm}-1}{2^m+1} + 2^s$, where $0 \le s \le 2m-1$, $(2^{s-1}-l, 2^m+1)=1$ and l is even. Let α be a primitive element of $\mathrm{GF}(2^{2lm})$. We define

$$\begin{aligned}C_\infty &= \{0\},\\ C_0 &= \{\alpha^{j(2^m+1)} \mid 0 \le j \le \frac{2^{2lm}-1}{2^m+1} - 1\},\\ C_1 &= \mathrm{GF}(2^{2lm}) \setminus (C_0 \cup C_\infty).\end{aligned}$$

The following lemma is a special case of [13, Lemma 3.5].

Lemma III.1.

$$\sum_{x\in\mathrm{GF}(2^{2lm})} \chi(ax^{2^m+1}) = \begin{cases} 2^{2lm} & \text{if } a \in C_\infty,\\ -2^{(l+1)m} & \text{if } a \in C_0,\\ 2^{lm} & \text{if } a \in C_1.\end{cases}$$

Now, we are ready to prove our result.

Theorem III.2. *Suppose $d = \frac{2^{2lm}-1}{2^m+1} + 2^s$, where $0 \le s \le 2m-1$, $(2^{s-1}-l, 2^m+1) = 1$ and l is even. Then*

(i) *$\mathrm{S}_d(z) = 0$ for some $z \in GF(2^{2lm})^*$;*
(ii) *$\mathrm{C}_d(z)$ takes at least four values;*
(iii) *There exists a $z \in GF(2^{2lm})$ such that $\mathrm{S}_d(z) \ge 2^{lm+1}$.*

Proof: By [13, Theorem 3.8], we have

$$\mathrm{C}_d(z) = -1 + \frac{1}{2^m+1}\sum_{j=0}^{2^m}\sum_{x\in\mathrm{GF}(2^{2lm})} \chi(x^{2^m+1}(z\alpha^j + \alpha^{dj2^{-s}})),$$

where 2^{-s} is the inverse of 2^s modulo $2^{2lm}-1$.

For any $z \in \mathrm{GF}(2^{2lm})$, define

$$n_i(z) = |\{j \mid 0 \le j \le 2^m, z\alpha^j + \alpha^{dj2^{-s}} \in C_i\}|,$$

where $i = 0, 1, \infty$. Thus,

$$\mathrm{C}_d(z) = -1 + \frac{1}{2^m+1}(2^{2lm}n_\infty(z) - 2^{(l+1)m}n_0(z) + 2^{lm}n_1(z)). \tag{2}$$

Equivalently, $\mathrm{S}_d(z) = \frac{2^{lm}}{2^m+1}(2^{lm}n_\infty(z) - 2^m n_0(z) + n_1(z))$ and $2^{lm} \mid \mathrm{S}_d(z)$. Then a direct application of [3, Lemma 3] completes the proof of (i).

Set $A = \{\alpha^j \mid 0 \le j \le 2^m\}$. It follows from the definition of $n_i(z)$ that

$$\begin{aligned}n_\infty(z) &= |\{x \in A \mid zx + x^{d2^{-s}} = 0\}|,\\ n_0(z) &= |\{x \in A \mid (zx + x^{d2^{-s}})^{\frac{2^{2lm}-1}{2^m+1}} = 1\}|,\end{aligned}$$

$n_\infty(z) + n_0(z) + n_1(z) = 2^m + 1$.

Moreover, since $(d2^{-s} - 1, 2^{2lm} - 1) = \frac{2^{2lm}-1}{2^m+1}$, there are exactly $2^m + 1$ choices of $z \in \mathrm{GF}(2^{2lm})$ such that $n_\infty(z) = 1$.

In the following, we will turn to the proof of (ii) and (iii). Since $\mathrm{S}_d(z)$ attains 0 and at least one negative value [3, Lemma 1], it suffices to show that $\mathrm{S}_d(z)$ can take two distinct positive values. Below, we split our discussion into two cases with $l > 2$ and $l = 2$.

Case 1: $l > 2$

Note that $n_\infty(z) + n_0(z) + n_1(z) = 2^m + 1$. When $n_\infty(z) = 1$, by (2), we simply have $\mathrm{S}_d(z) \ge \frac{1}{2^m+1}2^{2lm} - 2^{(l+2)m} = \frac{2^{(l+2)m}(2^{(l-2)m}-1)}{2^m+1} > 2^{lm+1}$.

Next, we show that $\mathrm{C}_d(z)$ takes at least four values. Otherwise, assume that $\mathrm{S}_d(z)$ takes three values $\{u, v, 0\}$, where $u > 2^{lm+1}$ and $v < 0$. If $n_\infty(z) = 0$, by (2), we have $\mathrm{S}_d(z) \le 2^{lm}$. Thus, $\mathrm{S}_d(z)$ attains distinct values when $n_\infty(z) = 0$ and $n_\infty(z) = 1$. Therefore, given $z \in \mathrm{GF}(2^{2lm})$, $\mathrm{S}_d(z) = u$ if and only if $n_\infty(z) = 1$. We define

$$\begin{aligned}N_u &= |\{z \in \mathrm{GF}(2^{2lm}) \mid \mathrm{S}_d(z) = u\}|,\\ N_v &= |\{z \in \mathrm{GF}(2^{2lm}) \mid \mathrm{S}_d(z) = v\}|,\\ N_0 &= |\{z \in \mathrm{GF}(2^{2lm}) \mid \mathrm{S}_d(z) = 0\}|.\end{aligned}$$

Note that there are exactly $2^m + 1$ choices of z such that $n_\infty(z) = 1$. We get $N_u = 2^m + 1$. On the other hand, by the first two equations of Lemma II.3, we have

$$\begin{aligned}uN_u + vN_v &= 2^{2lm},\\ u^2N_u + v^2N_v &= 2^{4lm}.\end{aligned}$$

A direct computation shows that $N_u = \frac{2^{2lm}(v-2^{2lm})}{uv-v^2}$. Use $v_2(k)$ to denote the largest power of 2 dividing k. Since $v_2(v) < 2lm$, we simply have $v_2(2^{2lm}(v - 2^{2lm})) = v_2(v) + 2lm$ and $v_2(uv - v^2) = v_2(v) + v_2(u - v)$.

Below, we will show that $v_2(u - v) < 2lm$. Suppose $z_1 \in N_u$. Then $n_\infty(z_1) = 1, n_0(z_1) + n_1(z_1) = 2^m$ and

$$\begin{aligned}u = S_d(z_1) &= \frac{2^{lm}}{2^m+1}(2^{lm} - 2^m n_0(z_1) + n_1(z_1))\\ &= \frac{2^{lm}}{2^m+1}(2^{lm} + 2^m(1 - n_0(z_1)) - n_0(z_1)).\end{aligned}$$

Suppose $z_2 \in N_v$. Then $n_\infty(z_2) = 0, n_0(z_2)+n_1(z_2) = 2^m+1$ and

$$\begin{aligned} v = S_d(z_2) &= \frac{2^{lm}}{2^m+1}(-2^m n_0(z_2) + n_1(z_2)) \\ &= \frac{2^{lm}}{2^m+1}(2^m(1-n_0(z_2)) - n_0(z_2) + 1). \end{aligned}$$

Hence,

$$\begin{aligned} u - v = \frac{2^{lm}}{2^m+1}(&2^{lm} + 2^m(n_0(z_2) - n_0(z_1)) \\ &+ n_0(z_2) - n_0(z_1) - 1). \end{aligned}$$

If $n_0(z_2) - n_0(z_1) - 1 = 0$, then $u - v = \frac{2^{lm}}{2^m+1}(2^{lm} + 2^m)$ and $v_2(u-v) = (l+1)m < 2lm$. If $n_0(z_2) - n_0(z_1) - 1 \neq 0$, since $0 \le n_0(z_1) \le 2^m$ and $0 \le n_0(z_2) \le 2^m + 1$, we have $v_2(n_0(z_2) - n_0(z_1)) \le m$ and $v_2(n_0(z_2) - n_0(z_1) - 1) \le m$. It is straightforward to verify that $2^m(n_0(z_2) - n_0(z_1)) + n_0(z_2) - n_0(z_1) - 1 \neq 0$ and $v_2(2^m(n_0(z_2) - n_0(z_1)) + n_0(z_2) - n_0(z_1) - 1) \le 2m$. Thus, $v_2(u-v) \le (l+2)m < 2lm$.

Consequently, we have $v_2(2^{2lm}(v - 2^{2lm})) > v_2(uv - v^2)$, which implies that N_u is even. This leads to a contradiction to $N_u = 2^m + 1$.

Case 2: $l = 2$

In this case, $d = \frac{2^{4m}-1}{2^m+1} + 2^s$. Let $D_0 = \{\alpha^{j\frac{2^{4m}-1}{2^m+1}} \mid 0 \le j \le 2^m\}$. Suppose $a = \alpha^{2^m+1}$ and $b = \alpha^{\frac{2^{4m}-1}{2^m+1}}$. Then $C_0 = \langle a \rangle$ and $D_0 = \langle b \rangle$. Since $(\frac{2^{4m}-1}{2^m+1}, 2^m + 1) = (2, 2^m + 1) = 1$, any $x \in \mathrm{GF}(2^{2m})^*$ can be uniquely expressed as $a^i b^k$, for some $0 \le i \le \frac{2^{4m}-1}{2^m+1} - 1$ and $0 \le k \le 2^m$. Since

$$zx + x^{d2^{-s}} = za^i b^k + (a^i b^k)^{d2^{-s}} = a^i(zb^k + b^{kd2^{-s}}),$$

$zx + x^{d2^{-s}}$ belongs to C_∞ (resp. C_0, C_1) if and only if $zb^k + b^{kd2^{-s}}$ belongs to C_∞ (resp. C_0, C_1). In addition, given two distinct $x_1, x_2 \in A$ with $x_1 = a^{i_1} b^{k_1}$ and $x_2 = a^{i_2} b^{k_2}$, we have $k_1 \neq k_2$. Otherwise, $x_1 x_2^{-1} \in C_0$, which is impossible by the definition of A. Thus, for $i = 0, 1, \infty$,

$$\begin{aligned} n_i(z) &= |\{x \in A \mid zx + x^{d2^{-s}} \in C_i\}| \\ &= |\{0 \le k \le 2^m \mid zb^k + b^{kd2^{-s}} \in C_i\}| \\ &= |\{x \in D_0 \mid zx + x^{d2^{-s}} \in C_i\}|. \end{aligned}$$

Since $(d2^{-s} - 1, 2^{4m} - 1) = \frac{2^{4m}-1}{2^m+1}$, it is easy to see that $n_\infty(z) = 1$ if and only if $z \in D_0$. Moreover, we have

$$n_0(z) = |\{x \in D_0 \mid (zx + x^{d2^{-s}})^{\frac{2^{4m}-1}{2^m+1}} = 1\}|.$$

From now on, we always regard x and z as elements of D_0. Remind that $x \in D_0$ if and only if $x^{2^m+1} = 1$, the equation

$$(zx + x^{d2^{-s}})^{\frac{2^{4m}-1}{2^m+1}} = 1 \tag{3}$$

is equivalent to

$$\begin{cases} zx + x^{d2^{-s}} \neq 0, \\ 1 + \frac{1}{zx^{d2^{-s}+1}} = 0. \end{cases} \tag{4}$$

Set $u = (d2^{-s} + 1, 2^m + 1)$, $1 + \frac{1}{zx^{d2^{-s}+1}} = 0$ has exactly u solutions in D_0.

If $u < 2^m + 1$, since u is a divisor of $2^m + 1$, $u \le \frac{2^m+1}{3}$. It is easy to verify that $zx + x^{d2^{-s}} = 0$ and $1 + \frac{1}{zx^{d2^{-s}+1}} = 0$ share one common solution if and only if $z = 1$. Hence, we have

$$n_\infty(1) = 1, \quad n_0(1) = u - 1, \quad n_1(1) = 2^m - u + 1,$$

which leads to

$$\begin{aligned} S_d(1) &= \frac{1}{2^m+1}(2^{4m} - 2^{3m}(u-1) + 2^{2m}(2^m - u + 1)) \\ &= 2^{3m} + \frac{2^{3m}}{2^m+1} - 2^{2m}u \\ &\ge 2^{3m} + \frac{2^{3m}}{2^m+1} - 2^{2m} \cdot \frac{2^m+1}{3} \\ &\ge 2^{2m+1}. \end{aligned}$$

Similarly, if $z \neq 1$, we have

$$n_\infty(z) = 1, \quad n_0(z) = u, \quad n_1(z) = 2^m - u,$$

which implies

$$\begin{aligned} \mathrm{S}_d(z) &= \frac{1}{2^m+1}(2^{4m} - 2^{3m}u + 2^{2m}(2^m - u)) \\ &= 2^{3m} - 2^{2m}u \\ &> 0. \end{aligned}$$

Hence, when $u < 2^m + 1$, $\mathrm{S}_d(z)$ takes at least two distinct positive values and one of which is greater than or equal to 2^{2m+1}.

If $u = 2^m + 1$, a similar treatment yields

$$n_\infty(1) = 1, \quad n_0(1) = 2^m, \quad n_1(1) = 0,$$

which implies $S_d(1) = 0$. Meanwhile, for $z \neq 1$, we have

$$n_\infty(z) = 1, \quad n_0(z) = 0, \quad n_1(z) = 2^m,$$

which implies $\mathrm{S}_d(z) = 2^{3m} \ge 2^{2m+1}$. It is easy to see that $\mathrm{S}_d(z) = 2^{3m}$ if and only if $z \in D_0 \setminus \{1\}$. Assume $\mathrm{S}_d(z)$ takes three values. Then 2^{3m} must be the only positive value that $\mathrm{S}_d(z)$ attains. Suppose $\mathrm{S}_d(z) \in \{2^{3m}, v, 0\}$ with $v < 0$. Consequently,

$$\sum_{z \in \mathbb{F}_{2^{4m}}} \mathrm{S}_d(z) = 2^{3m} \cdot 2^m + vN_v < 2^{4m},$$

which contradicts the first equation of Lemma II.3. ■

Remark III.1. *When $l = 2$ and $s = 1$, $d = (2^{2m} + 1)(2^m - 1) + 2$ is of Niho type. This decimation has been studied in [29] where $C_d(z)$ takes exactly four values.*

IV. Conclusion

This paper demonstrates some new results on the cross correlation between an m-sequence and its decimated sequence. We make two contributions to this problem. The first one is the determination of the cross correlation distribution for the ternary m-sequence with period $3^{3r} - 1$ and decimation $d = 3^r + 2$ or $d = 3^{2r} + 2$, where $(r, 3) = 1$. In the case with $(r, 3) = 3$, it is conjectured that the cross correlation distribution is the same as $(r, 3) = 1$. The second one is an initial step towards the cross correlation of binary m-sequences with period $2^{2lm} - 1$ and decimation $d = \frac{2^{2lm}-1}{2^m+1} + 2^s$, where $l \ge 2$ is even and $0 \le s \le 2m - 1$. We prove the cross

correlation takes at least four values. Additionally, we verify that two famous conjectures due to Sarwate et al. and Helleseth are true in this case. For the cross correlation distribution, numerical experiments show that the cross correlation may take eight or more values. Hence, determining the cross correlation distribution seems to be a very challenging problem.

ACKNOWLEDGMENT

The authors would like to thank the two anonymous reviewers for their comments which improve the presentation of this paper, and to Prof. T. Helleseth, the associate editor, for his excellent editorial job.

REFERENCES

[1] N. Boston and G. McGuire, "The weight distributions of cyclic codes with two zeros and zeta functions," *J. Symbolic Comput.*, vol. 45, no. 7, pp. 723–733, 2010.

[2] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture," *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 4–8, Jan. 2000.

[3] P. Charpin, "Cyclic codes with few weights and Niho exponents," *J. Combinat. Theory, Ser. A*, vol. 108, no. 2, pp. 247–259, 2004.

[4] S. T. Choi, J. Y. Kim, and J. S. No, "On the cross-correlation of a p-ary m-sequence and its decimated sequences by $d = \frac{p^n+1}{p^k+1} + \frac{p^n-1}{2}$," *arXiv:1205.5959*.

[5] S. T. Choi and J. S. No, "On the cross-correlation distributions between p-ary m-sequences and their decimated sequences," *IEICE Trans. Fundam.*, vol. E95-A, no. 11, pp. 1808–1818, Nov. 2012.

[6] T. W. Cusick and H. Dobbertin, "Some new three-valued crosscorrelation functions for binary m-sequences," *IEEE Trans. Inf. Theory*, vol. 42, no. 4, pp. 1238–1240, Jul. 1996.

[7] H. Dobbertin, "One-to-one highly nonlinear power functions on GF(2^n)," *Appl. Algebra Eng. Commun. Comput.*, vol. 9, no. 2, pp. 139–152, 1998.

[8] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 613–627, Feb. 2006.

[9] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen, "Ternary m-sequences with three-valued cross-correlation function: New decimations of Welch and Niho type," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1473–1481, May 2001.

[10] T. Feng, K. Leung, and Q. Xiang, "Binary cyclic codes with two primitive nonzeros," *Sci. China Math.*, vol. 56, no. 7, pp. 1403–1412, 2013.

[11] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.)," *IEEE Trans. Inf. Theory*, vol. 14, no. 1, pp. 154–156, Jan. 1968.

[12] S. W. Golomb and G. Gong, *Signal design for good correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[13] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, no. 3, pp. 209–232, 1976.

[14] T. Helleseth, "A note on the cross-correlation function between two binary maximal length linear sequences," *Discrete Math.*, vol. 23, no. 3, pp. 301–307, 1978.

[15] T. Helleseth, "Pairs of m-sequences with a six-valued crosscorrelation," in *Mathematical Properties of Sequences and Other Combinatorial Structures*. Boston, MA, USA: Kluwer, 2003, pp. 1–6.

[16] T. Helleseth, L. Hu, A. Kholosha, X. Zeng, N. Li, and W. Jiang, "Period-different m-sequences with at most four-valued cross correlation," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3305–3311, Jul. 2009.

[17] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, Amsterdam, The Netherlands: North Holland, 1998, pp. 1765–1853.

[18] T. Helleseth and P. Rosendahl, "New pairs of m-sequences with 4-level cross-correlation," *Finite Fields Appl.*, vol. 11, no. 4, pp. 674–683, 2005.

[19] H. D. L. Hollmann and Q. Xiang, "A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences," *Finite Fields Appl.*, vol. 7, no. 2, pp. 253–286, 2001.

[20] A. Johansen and T. Helleseth, "A family of m-sequences with five-valued cross correlation," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 880–887, Feb. 2009.

[21] A. Johansen, T. Helleseth, and A. Kholosha, "Further results on m-sequences with five-valued cross correlation," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5792–5802, Dec. 2009.

[22] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes," *Inf. Control*, vol. 18, no. 4, pp. 369–394, 1971.

[23] D. J. Katz, "Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth," *J. Combinat. Theory, Ser. A*, vol. 119, no. 8, pp. 1644–1659, 2012.

[24] R. Lidl and H. Niederreiter, *Finite fields* (Encyclopedia of Mathematics and its Applications). vol. 20, Reading, MA, USA: Addison-Wesley, 1983.

[25] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter–Matthews function," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5345–5353, Dec. 2008.

[26] G. J. Ness and T. Helleseth, "Cross correlation of m-sequences of different lengths," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1637–1648, Apr. 2006.

[27] G. J. Ness and T. Helleseth, "A new three-valued cross correlation between m-sequences of different lengths," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4695–4701, Oct. 2006.

[28] G. J. Ness and T. Helleseth, "A new family of four-valued cross correlation between m-sequences of different lengths," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4308–4313, Nov. 2007.

[29] Y. Niho, "Multivalued cross-correlation functions between two maximal linear recursive sequence," Ph.D. dissertation, Dept. Electron. Eng., Univ. Southern California, Los Angeles, CA, USA, 1970.

[30] D. Sarwate and M. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593–619, May 1980.

[31] 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 $(\frac{p^{2k}+1}{2})^2$," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3140–3149, Jul. 2008.

[32] Y. Xia, X. Zeng, and L. Hu, "Further crosscorrelation properties of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$," *Appl. Algebra Eng. Commun. Comput.*, vol. 21, no. 5, pp. 329–342, 2010.

Tao Zhang is currently a Ph.D. student at Zhejiang University, Hangzhou, Zhejiang, P. R. China. His research interests include combinatorial design theory, coding theory, algebraic combinatorics, and their interactions.

Shuxing Li is currently a Ph.D. student at Zhejiang University, Hangzhou, Zhejiang, P. R. China. His research interests include combinatorial design theory, coding theory, algebraic combinatorics, and their interactions.

Tao Feng received his Ph.D. degree in 2008 from School of Mathematical Sciences, Peking University. He was then a Research Fellow at Nanyang Technological Univeristy for one year and a Postdoc at University of Delaware for two years. He is now a faculty member of Department of Mathematics, Zhejiang University, Hangzhou, Zhejiang, P. R. China. His research interests include algebraic combinatorics, coding theory, and cryptography.

Gennian Ge received the M.S. and Ph.D. degrees in mathematics from Suzhou University, Suzhou, Jiangsu, P. R. China, in 1993 and 1996, respectively. After that, he became a member of Suzhou University. He was a postdoctoral fellow in the Department of Computer Science at Concordia University, Montreal, QC, Canada, from September 2001 to August 2002, and a visiting assistant professor in the Department of Computer Science at the University of Vermont, Burlington, Vermont, USA, from September 2002 to February 2004. He was a full professor in the Department of Mathematics at Zhejiang University, Hangzhou, Zhejiang, P. R. China, from March 2004 to February 2013. Currently, he is a full professor in the School of Mathematical Sciences at Capital Normal University, Beijing, P. R. China. His research interests include the constructions of combinatorial designs and their applications to codes and crypts. Dr. Ge is on the Editorial Board of *Journal of Combinatorial Designs, Science China Mathematics, Applied Mathematics—A Journal of Chinese Universities*. He received the 2006 Hall Medal from the Institute of Combinatorics and its Applications.