Appl. Math. J. Chinese Univ.
2008, 23(4): 490-500

Modified constructions of binary sequences using multiplicative inverse

CHEN Zhi-xiong[1,2] LIN Zhi-xing[1]

Abstract. Two new families of finite binary sequences are constructed using multiplicative inverse. The sequences are shown to have strong pseudorandom properties by using some estimates of certain exponential sums over finite fields. The constructions can be implemented fast since multiplicative inverse over finite fields can be computed in polynomial time.

§1 Introduction

In the last decade, a new constructive approach has been developed to study pseudorandomness of finite binary sequences. To the best of our knowledge, the starting work is [1]. The work was motivated by the facts that pseudorandom binary sequences have many applications such as in stream ciphers and the theory of pseudorandomness can be used to analyze certain sequences. Mauduit and Sárközy[1] first introduced the following measures of pseudorandomness for a finite binary sequence with length N:

$$S_N = \{s_1, s_2, \cdots, s_N\} \in \{+1, -1\}^N.$$

The *well-distribution measure* of S_N is defined as

$$W(S_N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} s_{a+jb} \right|,$$

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbf{N}$ and $1 \le a \le a + (t-1)b \le N$, while the *correlation measure of order* k (or *order* k *correlation measure*) of S_N is defined as

$$C_k(S_N) = \max_{M,D} \left| \sum_{n=1}^{M} s_{n+d_1} s_{n+d_2} \cdots s_{n+d_k} \right|,$$

Received: 2007-06-23
MR Subject Classification: 94A60, 11K45
Keywords: stream cipher, binary sequence, multiplicative inverse, pseudorandomness, exponential sum
Digital Object Identifier(DOI): 10.1007/s11766-008-1855-8
Supported by the Open Funds of Key Lab of Fujian Province University Network Security and Cryptology (07B005); the Funds of the Education Department of Fujian Province (JA07164) and the Natural Science Foundation of Fujian Province of China (2007F3086)

where the maximum is taken over all $D = (d_1, \cdots, d_k)$ with non-negative integers $0 \le d_1 < \cdots < d_k$ and M such that $M + d_k \le N$.

S_N is considered as a "good" pseudorandom sequence, if both $W(S_N)$ and $C_k(S_N)$ (at least for small k) are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$). It was shown in [2] that for a "truly" random sequence $S_N \in \{+1, -1\}^N$ (i.e., choosing $S_N \in \{+1, -1\}^N$ with probability $1/2^N$), both $W(S_N)$ and $C_k(S_N)$ (for some fixed k) are around $N^{1/2}\log^c(N)$ with "near 1" probability. From [1] the Legendre sequence forms a "good" pseudorandom sequence. Many other "good" (but slightly inferior) binary sequences were designed in the literature, see for example [1-6] and references therein.

Very recently, Liu[7,8], Louboutin, Rivat and Sárközy[9] present some constructions of finite binary sequences (see below) related to Lehmer numbers respectively. These sequences are shown to be "good" pseudorandom sequences.

Let p be an odd prime. We denote by $F_p = \{0, 1, \cdots, p-1\}$ the finite field of p elements, by F_p^* the multiplicative group of F_p. Let

$$\overline{\gamma} = \begin{cases} \gamma^{-1}, & \text{if } \gamma \in F_p^*, \\ 0, & \text{if } \gamma = 0. \end{cases}$$

For any $\gamma \in F_p^*$, we always suppose that $\overline{\gamma} \in \{1, \cdots, p-1\}$.

Construction 1.[9] Let $f(x) \in F_p[x]$ be of degree d with $1 \le d < p$. Suppose $f(n), \overline{f(n)} \in \{0, \cdots, p-1\}$ for any $n \in F_p$. Define the sequence $E_{p-1} = \{s_1, s_2, \cdots, s_{p-1}\}$ by

$$s_n := \begin{cases} +1, & \text{if } f(n) \equiv \overline{f(n)} \pmod 2, \\ -1, & \text{if } f(n) \not\equiv \overline{f(n)} \pmod 2. \end{cases}$$

Then the bounds hold

$$W(E_{p-1}) \ll (d+s)p^{1/2}\log^3(p) \quad \text{and} \quad C_2(E_{p-1}) \ll (d+s)p^{1/2}\log^5(p),$$

where s is the number of distinct roots of $f(x)$ in an algebraic closure of F_p.

It is easy to see for $n \in \{1, \cdots, p-1\}$, $s_n = (-1)^{f(n)+\overline{f(n)}}$.

Construction 2.[8] Suppose $\overline{\gamma} \in \{0, \cdots, p-1\}, \forall \gamma \in F_p$. Define the sequence $E'_{p-1} = \{s'_1, s'_2, \cdots, s'_{p-1}\}$ by

$$s'_n := \begin{cases} (-1)^{n+\overline{n}}, & \text{if } n \text{ is a quadratic residue mod } p, \\ (-1)^{n+\overline{n}+1}, & \text{if } n \text{ is a quadratic nonresidue mod } p. \end{cases}$$

Then the bounds hold $W(E'_{p-1}) \ll p^{1/2}\log^2(p)$ and $C_2(E'_{p-1}) \ll p^{1/2}\log^3(p)$.

Construction 3.[7] Suppose $\overline{\gamma} \in \{0, \cdots, p-1\}$ for any $\gamma \in F_p$. Let $c \in \{1, \cdots, p-1\}$ be a fixed number. Define the sequence $E''_{p-1} = \{s''_1, s''_2, \cdots, s''_{p-1}\}$ by

$$s''_n := \begin{cases} (-1)^{\overline{n}+\overline{n+c}}, & \text{if } p \nmid n(n+c), \\ 1, & \text{otherwise.} \end{cases}$$

Then the bounds hold $W(E''_{p-1}) \ll p^{1/2}\log^3(p)$ and $C_2(E''_{p-1}) \ll p^{1/2}\log^5(p)$.

We note that in the above three constructions, the numbers

$$f(n) + \overline{f(n)}, n + \overline{n}, \overline{n} + \overline{n + c} \in \{0, \cdots, 2p-2\}$$

for all $n \in \{1, \cdots, p-1\}$. In particular, it seems difficult to consider the correlation measure of higher order (> 2).

Motivated by these constructions, we present two new constructions. One is a variation of Construction 3, the other is constructed using power functions. We estimate their well-distribution measure and correlation measure of order $k(\geq 2)$, which indicate that the resulting sequences may form "good" pseudorandom sequences.

Throughout this paper, the implied constants in the symbol " $\ll$ " are absolute.

§2 New constructions

In our constructions, we will use 0 and 1 to represent the terms of a binary sequence.

Definition 1. Suppose $\overline{\gamma} \in \{0, \cdots, p-1\}$ for any $\gamma \in F_p$. Let $c \in \{1, \cdots, p-1\}$ be a fixed number. Define the sequence $\mathcal{X}_{p-1} = \{x_1, x_2, \cdots, x_{p-1}\}$ by

$$x_n := \begin{cases} 1, & \text{if } [\overline{n} + \overline{n+c}]_p \text{ is odd}, \\ 0, & \text{if } [\overline{n} + \overline{n+c}]_p \text{ is even}, \end{cases}$$

where $[u]_p$ denotes the unique $r \in \{0, 1, \cdots, p-1\}$ such that $u \equiv r \pmod p$.

Definition 2. Suppose $\overline{\gamma} \in \{0, \cdots, p-1\}$ for any $\gamma \in F_p$ and $c \in \{1, \cdots, p-1\}$ is a fixed number. Let $\eta \in F_p^*$ be a fixed primitive element. Define the sequence $\mathcal{Y}_{p-1} = \{y_1, y_2, \cdots, y_{p-1}\}$ by

$$y_n := \begin{cases} 0, & \text{if } \overline{\eta^n} \equiv \overline{\eta^n + c} \pmod 2, \\ 1, & \text{if } \overline{\eta^n} \not\equiv \overline{\eta^n + c} \pmod 2. \end{cases}$$

2.1. Well-distribution and correlation of $\mathcal{X}_{p-1}$

Theorem 1. Let $\mathcal{X}_{p-1} = \{x_1, x_2, \cdots, x_{p-1}\}$ be defined as in Definition 1. Then we have

$$W(\mathcal{X}_{p-1}) \ll p^{1/2} \log^2(p)$$

and

$$C_k(\mathcal{X}_{p-1}) \ll 2^k k p^{1/2} \log^{k+1}(p)$$

for $k < p$. In particular, $C_2(\mathcal{X}_{p-1}) \ll p^{1/2} \log^3(p)$.

In order to prove Theorem 1, we need some basic results. Let $e_m(z) = \exp(2\pi i z/m)$.

Lemma 1.[10,11] Let $m > 1$ be a positive integer. Then

$$\sum_{c=0}^{m-1} \left| \sum_{z=H+1}^{H+N} e_m(cz) \right| \leq m(1 + \log(m))$$

holds for any integers H and $1 \leq N \leq m$.

Lemma 2. Let p be an odd prime number and $\lambda \in \mathbf{Z}$ with $0 \le |\lambda| \le \frac{p-1}{2}$. We define

$$U(\lambda) := \sum_{r=0}^{(p-1)/2} e_p(-2\lambda r) - \sum_{r=1}^{(p-1)/2} e_p(2\lambda r). \tag{1}$$

Then the following bound holds: $\sum_{|\lambda|\le (p-1)/2} |U(\lambda)| \le 2p(1+\log(p))$.

Proof. Since $|U(\lambda)| \le \left|\sum_{r=0}^{(p-1)/2} e_p(-2\lambda r)\right| + \left|\sum_{r=1}^{(p-1)/2} e_p(2\lambda r)\right|$, the desired result follows from Lemma 1.

Lemma 3.[7,12] For any polynomials $g(x), h(x) \in F_p[x]$ such that the rational function $F(x) = g(x)/h(x)$ is not constant on F_p, let χ be a nontrivial multiplicative character of F_p and s the number of distinct roots of the polynomial $h(x)$ in an algebraic closure of F_p. For $p \nmid \lambda$, we have

(i) $\left|\sum_{\substack{\xi\in F_p\\ h(\xi)\neq 0}} e_p(\lambda F(\xi))\right| \le (\max(\deg(g), \deg(h)) + s^* - 2)\sqrt{p} + \delta$, where $s^* = s$ and $\delta = 1$ if $\deg(g) \le \deg(h)$, and $s^* = s+1$ and $\delta = 0$ otherwise.

(ii) $\left|\sum_{\substack{\xi\in F_p^*\\ h(\xi)\neq 0}} e_p(\lambda F(\xi))\,\chi(\xi)\right| \le (\max(\deg(g), \deg(h)) + s^* - 1)\sqrt{p}$, where $s^* = s$ if $\deg(g) \le \deg(h)$, and $s^* = s+1$ otherwise.

Remark 1. Let $F(x)$ be defined as in Lemma 3. According to Lemma 3 and Lemma 1, one can estimate incomplete sums

$$\sum_{\substack{n=A+1\\ h(n)\neq 0}}^{B} e_p(F(n)) \quad\text{and}\quad \sum_{\substack{n=A+1\\ h(\eta^n)\neq 0}}^{B} e_p(F(\eta^n)),$$

where $0 \le A < B \le p-1$ and $\eta \in F_p^*$ is a primitive element. In fact,

$$\begin{aligned}\sum_{\substack{n=A+1\\ h(n)\neq 0}}^{B} e_p(F(n)) &= \sum_{n=A+1}^{B} \sum_{\substack{m=0\\ h(m)\neq 0}}^{p-1} e_p(F(m)) \cdot \tfrac{1}{p}\sum_{\mu=0}^{p-1} e_p(\mu(n-m))\\ &= \tfrac{1}{p}\sum_{\mu=0}^{p-1}\sum_{n=A+1}^{B} e_p(\mu n) \sum_{\substack{m=0\\ h(m)\neq 0}}^{p-1} e_p(F(m)-\mu m),\end{aligned}$$

and

$$\begin{aligned}\sum_{\substack{n=A+1\\ h(\eta^n)\neq 0}}^{B} e_p(F(\eta^n)) &= \sum_{n=A+1}^{B} \sum_{\substack{m=1\\ h(\eta^m)\neq 0}}^{p-1} e_p(F(\eta^m)) \cdot \tfrac{1}{p-1}\sum_{\mu=1}^{p-1} e_{p-1}(\mu(m-n))\\ &= \tfrac{1}{p-1}\sum_{\mu=1}^{p-1}\sum_{n=A+1}^{B} e_{p-1}(-\mu n) \sum_{\substack{\xi=1\\ h(\xi)\neq 0}}^{p-1} e_p(F(\xi))\,\chi_\mu(\xi),\end{aligned}$$

where $\chi_\mu(\eta^m) = e_{p-1}(\mu m)$ is a multiplicative character of F_p.

Proof of Theorem 1. Let $f(n)=\overline{n}+\overline{n+c}$. For any $1\le n\le p-1$ with $p\nmid(n+c)$ we have

$$\frac{1}{p}\sum_{r=0}^{(p-1)/2}\sum_{|\lambda|\le(p-1)/2}e_p(\lambda(f(n)-2r))=\begin{cases}1, & \text{if } [f(n)]_p \text{ is even},\\ 0, & \text{if } [f(n)]_p \text{ is odd},\end{cases}\tag{2}$$

and

$$\frac{1}{p}\sum_{r=1}^{(p-1)/2}\sum_{|\lambda|\le(p-1)/2}e_p(\lambda(f(n)+2r))=\begin{cases}0, & \text{if } [f(n)]_p \text{ is even},\\ 1, & \text{if } [f(n)]_p \text{ is odd}.\end{cases}\tag{3}$$

Subtracting (3) from (2) yields

$$\frac{1}{p}\sum_{|\lambda|\le(p-1)/2}e_p(\lambda f(n))U(\lambda)=\begin{cases}1, & \text{if } [f(n)]_p \text{ is even},\\ -1, & \text{if } [f(n)]_p \text{ is odd},\end{cases}$$

where $U(\lambda)$ is defined as in Lemma 2.

It is easy to see that for any $1\le n\le p-1$ with $p\nmid(n+c)$,

$$(-1)^{x_n}=\frac{1}{p}\sum_{|\lambda|\le(p-1)/2}e_p(\lambda f(n))U(\lambda).\tag{4}$$

For $a,b,t\in\mathbf{N}$ with $1\le a\le a+(t-1)b\le p-1$, we have

$$\begin{aligned}
\left|\sum_{j=0}^{t-1}(-1)^{x_{a+jb}}\right| &\le \left|\sum_{\substack{j=0\\ p\nmid a+jb+c}}^{t-1}(-1)^{x_{a+jb}}\right|+1=\frac{1}{p}\left|\sum_{\substack{j=0\\ p\nmid a+jb+c}}^{t-1}\sum_{|\lambda|\le(p-1)/2}U(\lambda)e_p(\lambda f(a+jb))\right|+1\\
&= \frac{1}{p}\left|\sum_{|\lambda|\le(p-1)/2}U(\lambda)\sum_{\substack{j=0\\ p\nmid a+jb+c}}^{t-1}e_p(\lambda f(a+jb))\right|+1\\
&\le \frac{1}{p}\sum_{|\lambda|\le(p-1)/2}|U(\lambda)|\cdot\left|\sum_{\substack{j=0\\ p\nmid a+jb+c}}^{t-1}e_p(\lambda f(a+jb))\right|+1\\
&\le \frac{1}{p}\left(\sum_{|\lambda|=1}^{(p-1)/2}|U(\lambda)|\cdot\left|\sum_{\substack{j=0\\ p\nmid a+jb+c}}^{t-1}e_p(\lambda f(a+jb))\right|+t\right)+1\\
&\le \frac{1}{p}\sum_{|\lambda|=1}^{(p-1)/2}|U(\lambda)|\cdot\left|\sum_{\substack{j=0\\ p\nmid a+jb+c}}^{t-1}e_p(\lambda f(a+jb))\right|+2.
\end{aligned}$$

Now by Lemmas 2 and 3, we obtain the bound of $W(\mathcal{X}_{p-1})$.

For $D=(d_1,\cdots,d_k)$ and M with $0\le d_1<\cdots<d_k\le p-1-M$, there are at most k elements $n(1\le n\le M<p-1)$ such that $p|(n+d_j+c)$ for at least one number $j:1\le j\le k$.

Then we have

$$\begin{aligned}\left|\sum_{n=1}^{M}(-1)^{x_{n+d_1}+\cdots+x_{n+d_k}}\right| &\le \left|\sum_{\substack{n=1\\ p\nmid(n+d_j+x)\\ 1\le j\le k}}^{M}\prod_{i=1}^{k}\left(\frac{1}{p}\sum_{|\lambda_i|\le(p-1)/2}U(\lambda_i)e_p(\lambda_i f(n+d_i))\right)\right|+k\\ &= \frac{1}{p^k}\left|\sum_{|\lambda_1|\le(p-1)/2}\cdots\sum_{|\lambda_k|\le(p-1)/2}U(\lambda_1)\cdots U(\lambda_k)\sum_{\substack{n=1\\ p\nmid(n+d_j+x)\\ 1\le j\le k}}^{M}e_p(\sum_{i=1}^{k}\lambda_i f(n+d_i))\right|+k\\ &\le \frac{1}{p^k}\left(\left(\sum_{0<|\lambda_i|\le(p-1)/2}|U(\lambda_i)|\right)^k\cdot\left|\sum_{\substack{n=1\\ p\nmid(n+d_j+c)\\ 1\le j\le k}}^{M}e_p\left(\sum_{i=1}^{k}\lambda_i f(n+d_i)\right)\right|+M\right)+k.\end{aligned}$$

If $\sum_{i=1}^{k}\lambda_i f(y+d_i)$ is a nonconstant rational function in $F_p(y)$ when $\lambda_1,\cdots,\lambda_k$ are not all zero,

then by Lemma 3, $\left|\sum_{\substack{n=1\\ p\nmid(n+d_j+c)\\ 1\le j\le k}}^{M}e_p\left(\sum_{i=1}^{k}\lambda_i f(n+d_i)\right)\right|\le 4k\sqrt{p}(1+\log(p))$. So

$$\left|\sum_{n=1}^{M}(-1)^{x_{n+d_1}+\cdots+x_{n+d_k}}\right|\le 4k2^k\sqrt{p}(1+\log(p))^{k+1}+k+1=O(k2^k\sqrt{p}\log^{k+1}(p)).$$

It remains to prove if $\lambda_1,\cdots,\lambda_k$ are not all zero, $\sum_{i=1}^{k}\lambda_i f(y+d_i)$ is a nonconstant rational function. Suppose that there are $s(1\le s\le k<p)$ elements $\lambda_{i1},\cdots,\lambda_{is}$ are not zero (while other coefficients are zero), i.e.,

$$F(y)\triangleq\sum_{i=1}^{k}\lambda_i f(y+d_i)=\lambda_{i1}f(y+d_{i1})+\lambda_{i2}f(y+d_{i2})+\cdots+\lambda_{is}f(y+d_{is}).$$

Let

$$H(y)=(y+d_{i1})(y+d_{i1}+c)(y+d_{i2})(y+d_{i2}+c)\cdots(y+d_{is})(y+d_{is}+c)\in F_p[y].$$

If $\beta\in F_p$ is a zero of $H(y)$ and $(y-\beta)^2\nmid H(y)$, then β is a pole of $F(y)$, therefore $F(y)$ is nonconstant. While if

$$H(y)=(y+d_{i1})^2(y+d_{i2})^2\cdots(y+d_{is})^2,$$

then since $d_{i1}<d_{i2}<\cdots<d_{is}$, we have

$$\begin{cases} d_{i1}\equiv d_{j1}+c \pmod p,\\ d_{i2}\equiv d_{j2}+c \pmod p,\\ \cdots\\ d_{is}\equiv d_{js}+c \pmod p,\end{cases}$$

where $d_{j1}, d_{j2}, \cdots, d_{js}$ is a permutation of $d_{i1}, d_{i2}, \cdots, d_{is}$. So $sc \equiv 0 \pmod p$, which yields $c = 0$. it is a contradiction since $c \in \{1, \cdots, p-1\}$. Therefore, there exists a zero β of $H(y)$ such that $(y-\beta)^2 \nmid H(y)$, which makes $F(y)$ to be nonconstant. The proof is completed.

2.2. Well-distribution and correlation of $\mathcal{Y}_{p-1}$

Theorem 2. Let $\mathcal{Y}_{p-1} = \{y_1, y_2, \cdots, y_{p-1}\}$ be defined as in Definition 2. Then we have

$$W(\mathcal{Y}_{p-1}) \ll p^{1/2}\log^3(p) \quad \text{and} \quad C_2(\mathcal{Y}_{p-1}) \ll p^{1/2}\log^5(p).$$

Lemma 4. $\sum\limits_{|\lambda| \le (p-1)/2} \left| \sum\limits_{u=1}^{p-1} (-1)^u e_p(-\lambda u) \right| \le 2p(1+\log(p))$.

Proof. In fact,

$$\sum_{u=1}^{p-1}(-1)^u e_p(-\lambda u) = \sum_{r=1}^{(p-1)/2} e_p(-2\lambda r) - \sum_{r=1}^{(p-1)/2} e_p(-\lambda(2r-1)).$$

Then the proof is similar to that of Lemma 2.

Proof of Theorem 2. Our approach follows the path of [7,8]. It is easy to see for $n \in \{1, \cdots, p-1\}$ with $p \nmid (\eta^n + c)$,

$$(-1)^{y_n} = (-1)^{\overline{\eta^n} + \overline{\eta^n + c}}. \tag{5}$$

For $a, b, t \in \mathbf{N}$ with $1 \le a \le a + (t-1)b \le p-1$, we have

$$\begin{aligned}
&\left| \sum_{j=0}^{t-1} (-1)^{y_{a+jb}} \right| \le \left| \sum_{\substack{j=0 \\ p \nmid \eta^{a+jb}+c}}^{t-1} (-1)^{\overline{\eta^{a+jb}} + \overline{\eta^{a+jb}+c}} \right| + 1 \\
&= \frac{1}{p^2} \left| \sum_{\substack{j=0 \\ p \nmid \eta^{a+jb}+c}}^{t-1} \sum_{u=1}^{p-1} \sum_{|\lambda| \le (p-1)/2} e_p(\lambda(\overline{\eta^{a+jb}} - u)) \right. \\
&\qquad \left. \times \sum_{v=1}^{p-1} \sum_{|\mu| \le (p-1)/2} e_p(\mu(\overline{\eta^{a+jb}+c} - v))(-1)^{u+v} \right| + 1 \\
&= \frac{1}{p^2} \left| \sum_{|\lambda| \le (p-1)/2} \sum_{u=1}^{p-1} (-1)^u e_p(-\lambda u) \right. \\
&\qquad \left. \times \sum_{|\mu| \le (p-1)/2} \sum_{v=1}^{p-1} (-1)^v e_p(-\mu v) \sum_{\substack{j=0 \\ p \nmid \eta^{a+jb}+c}}^{t-1} e_p(\lambda \overline{\eta^{a+jb}} + \mu \overline{\eta^{a+jb}+c}) \right| + 1.
\end{aligned}$$

Suppose the multiplicative order of $\eta^b \in F_p^*$ is T. For $\lambda \ne 0$ and $\mu \ne 0$, by Lemma 3 we have

$$\begin{aligned}
&\left| \sum_{\substack{j=0 \\ p \nmid \eta^{a+jb}+c}}^{T-1} e_p(\lambda \overline{\eta^{a+jb}} + \mu \overline{\eta^{a+jb}+c}) \right| = \left| \sum_{\substack{j=0 \\ p \nmid \eta^{a+jb}+c}}^{T-1} e_p(\lambda \overline{\eta^a (\eta^b)^j} + \mu \overline{\eta^a (\eta^b)^j + c}) \right| \\
= \; & \frac{T}{p-1} \left| \sum_{\xi \in F_p^*}{}^{*} e_p \left(\frac{\lambda(\eta^a \xi^{(p-1)/T} + c) + \mu \eta^a \xi^{(p-1)/T}}{\eta^a \xi^{(p-1)/T}(\eta^a \xi^{(p-1)/T} + c)} \right) \right| \le 4p^{1/2} + 1,
\end{aligned}$$

where $\sum^*$ indicates that the poles of the corresponding rational function are excluded from the summation. So by Remark 1 we have

$$\left|\sum_{\substack{j=0\\ p\nmid\eta^{a+jb}+c}}^{t-1} e_p(\lambda\overline{\eta^{a+jb}}+\mu\overline{\eta^{a+jb}+c})\right| \le (4\sqrt{p}+1)(1+\log(p)).$$

Now by Lemma 4 we have

$$\left|\sum_{j=0}^{t-1}(-1)^{y_{a+jb}}\right| \le 4(4\sqrt{p}+1)(1+\log(p))^3.$$

For integers d_1, d_2 and M with $0 \le d_1 < d_2 \le p-1-M$, we have

$$\begin{aligned}
&\left|\sum_{n=1}^{M}(-1)^{y_{n+d_1}+y_{n+d_2}}\right| \le \left|\sum_{\substack{n=1\\ p\nmid(\eta^{n+d_1}+c)(\eta^{n+d_2}+c)}}^{M}(-1)^{\overline{\eta^{n+d_1}}+\overline{\eta^{n+d_1}+c}+\overline{\eta^{n+d_2}}+\overline{\eta^{n+d_2}+c}}\right|+2\\
&= \frac{1}{p^4}\left|\sum_{\substack{n=1\\ p\nmid(\eta^{n+d_1}+c)(\eta^{n+d_2}+c)}}^{M}\sum_{u_1=1}^{p-1}\sum_{|\lambda_1|\le(p-1)/2}e_p(\lambda_1(\overline{\eta^{n+d_1}}-u_1))\right.\\
&\quad\times\sum_{u_2=1}^{p-1}\sum_{|\lambda_2|\le(p-1)/2}e_p(\lambda_2(\overline{\eta^{n+d_1}+c}-u_2))\sum_{u_3=1}^{p-1}\sum_{|\lambda_3|\le(p-1)/2}e_p(\lambda_3(\overline{\eta^{n+d_2}}-u_3))\\
&\quad\left.\times\sum_{u_4=1}^{p-1}\sum_{|\lambda_4|\le(p-1)/2}e_p(\lambda_4(\overline{\eta^{n+d_2}+c}-u_4))\cdot(-1)^{u_1+u_2+u_3+u_4}\right|+2\\
&= \frac{1}{p^4}\left|\sum_{|\lambda_1|\le(p-1)/2}\sum_{u_1=1}^{p-1}(-1)^{u_1}e_p(-\lambda_1u_1)\cdot\sum_{|\lambda_2|\le(p-1)/2}\sum_{u_2=1}^{p-1}(-1)^{u_2}e_p(-\lambda_2u_2)\right.\\
&\quad\times\sum_{|\lambda_3|\le(p-1)/2}\sum_{u_3=1}^{p-1}(-1)^{u_3}e_p(-\lambda_3u_3)\cdot\sum_{|\lambda_4|\le(p-1)/2}\sum_{u_4=1}^{p-1}(-1)^{u_4}e_p(-\lambda_4u_4)\\
&\quad\left.\times\sum_{\substack{n=1\\ p\nmid(\eta^{n+d_1}+c)(\eta^{n+d_2}+c)}}^{M}e_p\left(\lambda_1\overline{\eta^{n+d_1}}+\lambda_2\overline{\eta^{n+d_1}+c}+\lambda_3\overline{\eta^{n+d_2}}+\lambda_4\overline{\eta^{n+d_2}+c}\right)\right|+2.
\end{aligned}$$

Since η is a primitive element of F_p^*, for $\lambda_1, \cdots, \lambda_4$ are not all zero, by Lemma 3 we have

$$\begin{aligned}
&\sum_{\substack{n=1\\ p\nmid(\eta^{n+d_1}+c)(\eta^{n+d_2}+c)}}^{p-1}e_p\left(\lambda_1\overline{\eta^{n+d_1}}+\lambda_2\overline{\eta^{n+d_1}+c}+\lambda_3\overline{\eta^{n+d_2}}+\lambda_4\overline{\eta^{n+d_2}+c}\right)\\
&= \sum_{\xi\in F_p^*}{}^{*}e_p\left(\lambda_1\overline{\eta^{d_1}\xi}+\lambda_2\overline{\eta^{d_1}\xi+c}+\lambda_3\overline{\eta^{d_2}\xi}+\lambda_4\overline{\eta^{d_2}\xi+c}\right) \le 5\sqrt{p}+1,
\end{aligned}$$

where $\sum^*$ indicates that the poles of the corresponding rational function are excluded from the summation. Now by Remark 1 we have

$$\begin{aligned}
&\left|\sum_{\substack{n=1\\ p\nmid(\eta^{n+d_1}+c)(\eta^{n+d_2}+c)}}^{M}e_p\left(\lambda_1\overline{\eta^{n+d_1}}+\lambda_2\overline{\eta^{n+d_1}+c}+\lambda_3\overline{\eta^{n+d_2}}+\lambda_4\overline{\eta^{n+d_2}+c}\right)\right|\\
&\le (5\sqrt{p}+1)(1+\log(p)).
\end{aligned}$$

So by Lemma 4 we derive

$$\left|\sum_{n=1}^{M}(-1)^{y_{n+d_1}+y_{n+d_2}}\right| \leq 8(5\sqrt{p}+1)(1+\log(p))^5+2,$$

which completes the proof.

2.3. Linear complexity profile

We recall that the *linear complexity profile* of a binary sequence

$$S=\{s_0,s_1,\cdots\}\in\{0,1\}^\infty$$

is the function $L(S,N)$ defined for every positive integer N, as the least order l of a linear recurrence relation

$$s_n=c_1s_{n-1}+\cdots+c_ls_{n-l},\ \ c_i=0,1$$

for all n with $l\leq n\leq N-1$, which S satisfies. We use the convention that $L(S,N)=0$ if the first N elements of S are all zero and $L(S,N)=N$ if the first $N-1$ elements of S are zero and $s_{N-1}=1$. The value

$$L(S)=\sup_{N\geq 1}L(S,N)$$

is called the *linear complexity* of S, see for example [13]. For the linear complexity of any periodic sequence of period t one easily verifies that $L(S)=L(S,2t)\leq t$. It is desirable to have sequences with large linear complexity for cryptographic applications.

Proposition 1.[14] Let S be a $T-$periodic binary sequence. For $2\leq N\leq T-1$ we have

$$L(S,N)\geq N-\max_{1\leq k\leq L(S,N)+1}C_k(S).$$

Corollary 1. Let $\mathcal{X}_{p-1}=\{x_1,x_2,\cdots,x_{p-1}\}$ be defined as in Definition 1. For $2\leq N\leq p-1$ we have

$$L(\mathcal{X}_{p-1},N)=\Omega\left(\frac{\log(N/p^{3/4})}{\operatorname{loglog}(p)}\right).$$

Proof. The proof is similar to that of [14,Corollary 1], we give below for completeness. From Proposition 1 (see the proof of [14,Theorem 1]), we see that

$$N-L(\mathcal{X}_{p-1},N)\leq\max_{1\leq k\leq L(\mathcal{X}_{p-1},N)+1}C_k(\mathcal{X}_{p-1}),$$

which yields

$$N\ll L2^L\sqrt{p}\log^{L+2}(p)$$

by Theorem 1. Suppose $L\leq\log(p^{1/4})$, otherwise the result is trivial. Then we have

$$N\ll p^{3/4}\log^{L+3}(p),$$

hence we obtain

$$L\gg\frac{\log(N/p^{3/4})}{\operatorname{loglog}(p)}.$$

Table 1 Comparison of our sequences with some other sequences

Sequences	Length	Well-distributied	Correlation of order k
Legendre sequence	$N = p-1$	$O(p^{1/2}\log(p))$	$O(kp^{1/2}\log(p)); k \geq 2$
index sequence	$N = p-1$	$O(p^{1/2}\log^2(p))$	$O(k4^k p^{1/2}\log^{k+1}(p)); k \geq 2$
E_{p-1}	$N = p-1$	$O(p^{1/2}\log^3(p))$	$O(p^{1/2}\log^5(p)); k = 2$
E'_{p-1}	$N = p-1$	$O(p^{1/2}\log^2(p))$	$O(p^{1/2}\log^3(p)); k = 2$
E''_{p-1}	$N = p-1$	$O(p^{1/2}\log^3(p))$	$O(p^{1/2}\log^5(p)); k = 2$
$\mathcal{X}_{p-1}$	$N = p-1$	$O(p^{1/2}\log^2(p))$	$O(k2^k p^{1/2}\log^{k+1}(p)); k \geq 2$
$\mathcal{Y}_{p-1}$	$N = p-1$	$O(p^{1/2}\log^3(p))$	$O(p^{1/2}\log^5(p)); k = 2$

Remark 2. The implied constant in the symbol "O" may sometimes depend on the degree $\deg(f)$ of a function f adopted in the corresponding constructions and is absolute otherwise.

§3 Conclusions

We have constructed two families of finite binary sequences using multiplicative inverse, which were used in [7,8,9] to construct different sequences described in Constructions 1,2 and 3, respectively. The sequence $\mathcal{X}_{p-1}$ is a variation of Construction 3, while the sequence $\mathcal{Y}_{p-1}$ is constructed using power functions. Two important pseudorandom measures, the well-distribution measure and the correlation measure of order k, are estimated by using some estimates of certain exponential sums.

In Table 1, we compare our sequences with some other sequences, such as the Legendre sequence[1], the index sequence[4] and $E_{p-1}, E'_{p-1}, E''_{p-1}$ described in §1. We conclude that our sequences also have strong pseudo-random properties. So these constructions may provide a very attractive alternative to traditional methods in applications.

From a point of implementation view, the sequences can be computed fast, since the multiplicative inverse can be computed fast (in polynomial time).

Finally we remark that in [15,16] the recursive inversive generators, explicit inversive generators and explicit nonlinear generators are used to build families of binary sequences with strong pseudorandom properties in a different way.

References

1 Mauduit C, Sárközy A. On finite pseudorandom binary sequences I: measures of pseudorandomness, the Legendre symbol, Acta Arithmetica, 1997, 82: 365-377.

2 Cassaigne J, Mauduit C, Sárközy A. On finite pseudorandom binary sequences, VII: the measures of pseudorandomness, Acta Arithmetica, 2002, 103: 97-118.

3 Goubin L, Mauduit C, Sárközy A. Construction of large families of pseudorandom binary sequences, J Number Theory, 2004, 106(1): 56-69.

4 Gyarmati K. On a family of pseudorandom binary sequences, Periodica Mathematica Hungarica, 2004, 49(2): 45-63.

5 Mauduit C, Rivat J, Sárközy A. Construction of pseudorandom binary sequences using additive characters, Monatsh Math, 2004, 141(3): 197-208.

6 Mauduit C, Sárközy A. Construction of pseudorandom binary sequences by using multiplicative inverse, Acta Math Hung, 2005, 108(3): 239-252.

7 Liu H N. New pseudorandom sequences constructed using multiplicative inversive, Acta Arithmetica, 2006, 125(1): 264-275.

8 Liu H N. New pseudorandom sequences constructed by quadratic residues and Lehmer numbers, Proc Amer Math Soc, 2007, 135: 1309-1318.

9 Louboutin S R, Rivat J, Sárközy A. On a problem of D. H. Lehmer, Proc Amer Math Soc, 2007, 135: 969-975.

10 Lidl R, Niederreiter H. Finite Fields, Encyclopedia of Mathematics and its Applications, Vol. 20, second ed., Cambridge: Cambridge University Press, 1997.

11 Shparlinski I E. Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness, Progress in Computer Science and Applied Logic, Vol.22, Basel: Birkhauser Verlag, 2003.

12 Niederreiter H, Winterhof A. On the distribution of some new explicit nonlinear congruential pseudorandom numbers, In: Lecture Notes in Computer Science, Vol 3486, Berlin, Heidelberg: Springer-Verlag, 2005, 266-274.

13 Cusick T W, Ding C, Renvall A. Stream Ciphers and Number Theory, Amsterdam: Elsevier, 1998.

14 Brandstätter N, Winterhof A. Linear complexity profile of binary sequences with small correlation measure, Periodica Mathematica Hungarica, 2006, 52 (2): 1-8.

15 Chen Z X. Finite binary sequences constructed by explicit inversive methods, Finite Fields and Their Applications, 2008, 14 (3): 579-592.

16 Niederreiter H, Rivat J. On the correlation of pseudorandom numbers generated by inversive methods, Monatsh Math, 2008, 153(3): 251-264.

1 Key Laboratory of Applied Mathematics, Putian University, Putian 351100, China

2 Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China