New pseudorandom sequences constructed using multiplicative inverses

by

HUANING LIU (Xi’an)

1. Introduction. In a series of papers Mauduit, Rivat and Sárközy (partly with other authors) studied finite pseudorandom binary sequences

\[ E_N = \{e_1, \ldots, e_N\} \in \{-1, +1\}^N. \]

In [5] Mauduit and Sárközy first introduced the following measures of pseudorandomness: the well-distribution measure of \( E_N \) is defined by

\[ W(E_N) = \max_{a, b, t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|, \]

where the maximum is taken over all \( a, b, t \in \mathbb{N} \) with \( 1 \leq a \leq a+(t-1)b \leq N \). The correlation measure of order \( k \) of \( E_N \) is

\[ C_k(E_N) = \max_{M, D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k} \right|, \]

where the maximum is taken over all \( D = (d_1, \ldots, d_k) \) and \( M \) with \( 0 \leq d_1 < \cdots < d_k \leq N - M \), and the combined (well-distribution-correlation) PR-measure of order \( k \)

\[ Q_k(E_N) = \max_{a, b, t, D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \right| \]

is defined for all \( a, b, t, D = (d_1, \ldots, d_k) \) with \( 1 \leq a + jb + d_i \leq N \) \((i = 1, \ldots, k)\). In [6] the connection between the measures \( W \) and \( C_2 \) was studied.

A pseudorandom sequence \( E_N \) is considered to be “good” if both \( W(E_N) \) and \( C_k(E_N) \) (at least for small \( k \)) are “small” in terms of \( N \). Later Cas-
saigne, Mauduit and Sárközy [3] proved that this terminology is justified since for almost all \( E_N \in \{-1,+1\}^N \), both \( W(E_N) \) and \( C_k(E_N) \) are less than \( N^{1/2}(\log N)^c \). Moreover, it was shown in [5] that the Legendre symbol forms a “good” pseudorandom sequence. In [1] and [2], Cassaigne and coauthors studied the pseudorandomness of the Liouville function, defined as \( \lambda(n) = (-1)^{\Omega(n)} \) (\( \Omega(n) \) being the number of prime factors of \( n \) counted with multiplicity) and also of \( \gamma(n) = (-1)^{\omega(n)} \) (\( \omega(n) \) being the number of distinct prime factors of \( n \)). Furthermore, let

\[
K(m, n; p) = \sum_{a=1}^{p-1} e\left(\frac{ma + n\bar{a}}{p}\right)
\]

denote the Kloosterman sums, where \( e(y) = e^{2\pi iy} \), \( p \) is a prime, and \( \bar{a} \) is the multiplicative inverse of \( a \) modulo \( p \) such that \( 1 \leq \bar{a} \leq p-1 \). Fou-}

vry (with coauthors) [4] showed that the signs of \( K(1, n; p) \) form a “good” pseudorandom binary sequence.

Assume that \( p \) is a prime number, \( f(x) \in \mathbb{F}_p[x] \) has degree \( k \) (\( 0 < k < p \)) and no multiple zero in \( \overline{\mathbb{F}_p} \), and \( r_p(n) \) is defined to be the least non-negative residue of \( n \) modulo \( p \). Define the binary sequence \( E_p = (e_1, \ldots, e_p) \) by

\[
e_n = \begin{cases} 
+1 & \text{if } (f(n), p) = 1 \text{ and } r_p(f(n)) < p/2, \\
-1 & \text{if either } (f(n), p) = 1 \text{ and } r_p(f(n)) > p/2, \text{ or } p \mid f(n).
\end{cases}
\]

Mauduit and Sárközy [7] proved that this large family of finite binary sequences has strong pseudorandom properties.

As was said in [5], the search for new approaches and new constructions should be continued. The purpose of this paper is to give some new examples of pseudorandom sequences. Define

\[
e_n = \begin{cases} 
(-1)^{\pi+n+x} & \text{if } p \nmid n \text{ and } p \nmid n + x, \\
1 & \text{otherwise},
\end{cases}
\]

where \( x \) is an integer with \( 1 \leq x \leq p - 1 \). We shall prove that \( \{e_n\} \) is a “good” pseudorandom sequence:

**Theorem 1.1.** Let \( p \) be an odd prime, and let \( E_{p-1} = \{e_1, \ldots, e_{p-1}\} \) be defined by (1.1). Then

\[
W(E_{p-1}) \ll p^{1/2} \log^3 p, \quad C_2(E_{p-1}) \ll p^{1/2} \log^5 p, \quad Q_2(E_{p-1}) \ll p^{1/2} \log^5 p.
\]

**2. Some lemmas.** We need the following lemmas.

**Lemma 2.1 ([9]).** Let \( p \) be a prime, and \( m \) and \( n \) be integers. Then

\[
K(m, n; p) \ll (m, n, p)^{1/2} p^{1/2},
\]

where \( (m, n, p) \) denotes the greatest common divisor of \( m, n \) and \( p \).
Lemma 2.2 ([8]). For any polynomials \(g(x), h(x) \in \mathbb{F}_p[x]\) such that the rational function \(f(x) = g(x)/h(x)\) is not constant on \(\mathbb{F}_p\), let \(s\) be the number of distinct roots of \(h(x)\). Then
\[
\left| \sum_{n \in \mathbb{F}_p, \ h(n) \neq 0} e\left( \frac{g(n)}{h(n)p} \right) \right| \leq (\max(\deg(g), \deg(h)) + s - 1) \sqrt{p}.
\]

Lemma 2.3. For \(1 \leq a, b, x, r, s \leq p - 1\) and \(1 \leq u \leq p\), we have
\[
\Psi = \sum_{j=0}^{p-1} e\left( \frac{ra + jb + sa + jb + x + uj}{p} \right) \ll \sqrt{p}.
\]

Proof. If \(u = p\), from the properties of a residue system we get
\[
\Psi = \sum_{j=0}^{p-1} e\left( \frac{ra + jb + sa + jb + x}{p} \right) = \sum_{j=0}^{p-1} e\left( \frac{ra +ja + sa + j + x}{p} \right)
\]
\[
= \sum_{j=1}^{p-1} e\left( \frac{rj + sj + x}{p} \right).
\]
Since
\[
\bar{j} + \bar{x} \equiv jx \bar{x} + xj = xj \bar{x} + \bar{j} \equiv \bar{x}(\bar{j} + \bar{x}) \equiv \bar{x} - \bar{x}^2 \bar{j} + \bar{x} \mod p,
\]
by Lemma 2.1 we have
\[
\Psi = \sum_{j=1}^{p-1} e\left( \frac{rj + s(\bar{x} - \bar{x}^2 \bar{j} + \bar{x})}{p} \right)
\]
\[
= e\left( \frac{\bar{x}(s - r)}{p} \right) \sum_{j=1}^{p-1} e\left( \frac{r(\bar{j} + \bar{x}) - s\bar{x}^2 \bar{j} + \bar{x}}{p} \right)
\]
\[
= e\left( \frac{\bar{x}(s - r)}{p} \right) \sum_{\substack{j=1 \to p-1 \mod p \ k}} e\left( \frac{rj - s\bar{x}^2 \bar{j}}{p} \right) \ll \sqrt{p}.
\]
Now we suppose \(1 \leq u \leq p - 1\). Then
\[
\Psi = \sum_{j=0}^{p-1} e\left( \frac{r(a + jb + x) + sa + jb + uj(a + jb)(a + jb + x)}{(a + jb)(a + jb + x)p} \right).
\]
Let \( g(j) = r(a + jb + x) + s(a + jb) + uj(a + jb)(a + jb + x) \), and \( h(j) = (a + jb)(a + jb + x) \). Since \( 1 \leq u, b \leq p-1 \), we have \( 0 < \deg(h) < \deg(g) \). That is to say, the rational function \( g/h \) over \( \mathbb{F}_p \) is not constant. Then Lemma 2.2 yields the assertion.

**Lemma 2.4.** For \( 1 \leq r_1, s_1, r_2, s_2, x \leq p-1 \), \( 1 \leq d_1 < d_2 \leq p-1 \) and \( 1 \leq u \leq p \), we have

\[
\Omega = \sum_{n=1}^{p} e\left( \frac{r_1 n + d_1 + s_1 n + d_1 + x + r_2 n + d_2 + s_2 n + d_2 + x + un}{p} \right) \ll \sqrt{p}.
\]

**Proof.** Let

\[
g(n) = r_1(n + d_1 + x)(n + d_2)(n + d_2 + x) + s_1(n + d_1)(n + d_2)(n + d_2 + x)
+ r_2(n + d_1)(n + d_1 + x)(n + d_2)
+ s_2(n + d_1)(n + d_1 + x)(n + d_2)
+ un(n + d_1)(n + d_1 + x)(n + d_2)(n + d_2 + x),
\]

\[
h(n) = (n + d_1)(n + d_1 + x)(n + d_2)(n + d_2 + x).
\]

We have

\[
\Omega = \sum_{n=1}^{p} e\left( \frac{g(n)}{h(n)p} \right).
\]

If \( 1 \leq u \leq p-1 \), then \( 0 < \deg(h) < \deg(g) \) and it remains to apply Lemma 2.2.

If \( u = p \), we need to prove \( g(n) \not\equiv 0 \mod p \). Suppose that \( g(n) \equiv 0 \mod p \). Then comparing the coefficients of \( n^3, n^2, n \) and \( n^0 \) we have

\[
\begin{align*}
    r_1 + s_1 + r_2 + s_2 &\equiv 0 \mod p, \\
    r_1(d_1 + 2d_2 + 2x) + s_1(d_1 + 2d_2 + x) + r_2(2d_1 + d_2 + 2x) \\
    + s_2(2d_1 + d_2 + x) &\equiv 0 \mod p, \\
    r_1(2d_1d_2 + d_2^2 + d_1x + 3d_2x + x^2) + s_1(2d_1d_2 + d_2^2 + d_1x + d_2x) \\
    + r_2(2d_1d_2 + d_2^2 + d_1x + d_2x + x^2) \\
    + s_2(2d_1d_2 + d_2^2 + d_1x + d_2x) &\equiv 0 \mod p, \\
    r_1(d_1^2d_2 + d_1d_2x + d_2^2x + d_2x^2) + s_1(d_1^2d_2 + d_1d_2x) \\
    + r_2(d_1^2d_2 + d_2^2x + d_1d_2x + d_1x^2) + s_2(d_1^2d_2 + d_1d_2x) &\equiv 0 \mod p.
\end{align*}
\]
This gives
\[\begin{align*}
r_1(d_2 - d_1 + x) + s_1(d_2 - d_1) + r_2x &\equiv 0 \pmod{p}, \\
r_1(d_2^2 - d_1^2 + 2d_2x + x^2) + s_1(d_2^2 - d_1^2) + r_2x(2d_1 + x) &\equiv 0 \pmod{p}, \\
r_1(d_1d_2^2 - d_1^2d_2 + d_2x + d_2^2x^2) + s_1(d_1d_2^2 - d_1^2d_2) + r_2x(d_1^2 + d_1x) &\equiv 0 \pmod{p},
\end{align*}\]
hence
\[\begin{align*}
r_1(d_2^3 + d_2^2 - 2d_1d_2 - d_1x + d_2x) + s_1(d_1^2 + d_2^2 - 2d_1d_2 + d_1x - d_2x) &\equiv 0 \pmod{p}, \\
r_1(d_1^3 - 2d_1^2d_2 + d_1d_2^2 - d_1^2d_2 + d_2^2x + d_2^2x^2) + s_1d_1(d_1^2 + d_2^2 - 2d_1d_2 + d_1x - d_2x) &\equiv 0 \pmod{p}.
\end{align*}\]
Therefore
\[r_1x(d_2 - d_1)(d_2 - d_1 + x) \equiv 0 \pmod{p},\]
and consequently \(d_2 \equiv d_1 - x \pmod{p}\). Inserting this in (2.1), we have
\[\begin{align*}
r_1 + s_1 + r_2 + s_2 &\equiv 0 \pmod{p}, \\
3d_1r_1 + (3d_1 - x)s_1 + (3d_1 + x)r_2 + 3d_1s_2 &\equiv 0 \pmod{p}, \\
d_1^2r_1 + (d_1 - x)^2s_1 + (d_1 + x)^2r_2 + d_1^2s_2 &\equiv 0 \pmod{p}, \\
d_1^2(d_1 - x)r_1 + d_1(d_1 - x)^2s_1 + d_1(d_1^2 + x^2)r_2 + d_1^2(d_1 - x)s_2 &\equiv 0 \pmod{p}.
\end{align*}\]
This implies \(s_1 \equiv r_2 \equiv 0 \pmod{p}\), which is impossible. So \(g(n) \not\equiv 0 \pmod{p}\), and an appeal to Lemma 2.2 completes the proof.

3. Proof of Theorem 1.1. For \(a, b, t\) with \(1 \leq a \leq a + (t - 1)b \leq p - 1\), by (1.1) we have
\[
\sum_{j=0}^{t-1} e_{a+jb} = \sum_{j=0}^{t-1} (-1)^{a+jb+a+jb+x} + O(1)
\]

\[
= \frac{1}{p^3} \sum_{j=0}^{p-1} \sum_{l=0}^{t-1} \sum_{u=1}^{p} e\left(\frac{u(j-l)}{p}\right) \sum_{e=1}^{p-1} \sum_{r=1}^{p-1} e\left(\frac{r(a+jb-c)}{p}\right)
\]

\[
\times \sum_{d=1}^{p-1} \sum_{s=1}^{p-1} e\left(\frac{s(a+jb+x-d)}{p}\right)(-1)^e + O(1)
\]

\[
= \frac{1}{p^3} \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \sum_{u=1}^{t-1} \sum_{l=0}^{p-1} e\left(-\frac{ul}{p}\right) \sum_{c=1}^{p-1} (-1)^e \left(-\frac{rc}{p}\right) \sum_{d=1}^{p-1} (-1)^d e\left(-\frac{sd}{p}\right)
\]

\[
\times \sum_{j=0}^{p-1} e\left(\frac{ra+jb+sa+jb+x+uj}{p}\right) + O(1).
\]
Since
\[
\sum_{l=0}^{p-1} e\left(-\frac{ul}{p}\right) < \frac{1}{|\sin(\pi u/p)|} \quad \text{for } p \nmid u,
\]
(3.1)
\[
\sum_{c=1}^{t-1} (-1)^c e\left(-\frac{rc}{p}\right) < \frac{1}{|\sin(\pi/2 - \pi r/p)|},
\]
from Lemma 2.3 we have
\[
\sum_{j=0}^{t-1} e_{a+jb} \ll \frac{tp^{1/2}}{p^3} \sum_{r=1}^{p-1} \frac{1}{|\sin(\pi/2 - \pi r/p)|} \sum_{s=1}^{p-1} \frac{1}{|\sin(\pi/2 - \pi s/p)|}
\]
\[
+ \frac{p^{1/2}}{p^3} \sum_{r=1}^{p-1} \frac{1}{|\sin(\pi/2 - \pi r/p)|} \sum_{s=1}^{p-1} \frac{1}{|\sin(\pi/2 - \pi s/p)|} \sum_{u=1}^{p-1} \frac{1}{|\sin(\pi u/p)|}
\]
\[
\ll p^{1/2} \log^3 p.
\]
Therefore
\[
W(E_{p-1}) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right| \ll p^{1/2} \log^3 p.
\]

For \(0 \leq d_1 < d_2 \leq p - 1 - M\), from (1.1), (3.1) and Lemma 2.4 we have
\[
\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} = \sum_{n=1}^{M} (-1)^{n+d_1+n+d_1+x+n+d_2+n+d_2+x} + O(1)
\]
\[
= \frac{1}{p^3} \sum_{n=1}^{p} \sum_{l=1}^{p} \sum_{c_1=1}^{p-1} \sum_{r_1=1}^{p-1} e\left(\frac{u(n-l)}{p}\right) e\left(\frac{r_1(\overline{n+d_1}-c_1)}{p}\right)
\]
\[
\times \sum_{d_1=1}^{p-1} \sum_{s_1=1}^{p} e\left(\frac{s_1(\overline{n+d_1+x}-d_1)}{p}\right) \sum_{c_2=1}^{p-1} \sum_{r_2=1}^{p-1} e\left(\frac{r_2(\overline{n+d_2}-c_2)}{p}\right)
\]
\[
\times \sum_{d_2=1}^{p-1} \sum_{s_2=1}^{p} e\left(\frac{s_2(\overline{n+d_2+x}-d_2)}{p}\right) (-1)^{c_1+d_1+c_2+d_2} + O(1)
\]
\[
= \frac{1}{p^5} \sum_{r_1=1}^{p-1} \sum_{s_1=1}^{p} \sum_{r_2=1}^{p-1} \sum_{s_2=1}^{p} \sum_{u=1}^{p-1} \sum_{l=1}^{p-1} e\left(-\frac{ul}{p}\right)
\]
\[
\times \sum_{c_1=1}^{p-1} (-1)^{c_1} e\left(-\frac{r_1 c_1}{p}\right) \sum_{d_1=1}^{p-1} (-1)^{d_1} e\left(-\frac{s_1 d_1}{p}\right)
\]
\[ \times \sum_{c_2=1}^{p-1} (-1)^{c_2} e \left( - \frac{r_2 c_2}{p} \right) \sum_{d_2=1}^{p-1} (-1)^{d_2} e \left( - \frac{s_2 d_2}{p} \right) \]
\[ \times \sum_{n=1}^{p} \sum_{p|n+d_1, n+d_1+x} \sum_{p|n+d_2, n+d_2+x} \]
\[ + O(1) \]
\[ \ll \frac{M p^{1/2} \sum_{r_1=1}^{p-1}}{p^5} \left| \sin \left( \frac{\pi}{2 - \pi r_1} \right) \right| \sum_{s_1=1}^{p-1} \left| \sin \left( \frac{\pi}{2 - \pi s_1} \right) \right| \]
\[ \times \sum_{r_2=1}^{p-1} \left| \sin \left( \frac{\pi}{2 - \pi r_2} \right) \right| \sum_{s_2=1}^{p-1} \left| \sin \left( \frac{\pi}{2 - \pi s_2} \right) \right| \]
\[ + \frac{p^{1/2}}{p^5} \sum_{r_1=1}^{p-1} \left| \sin \left( \frac{\pi}{2 - \pi r_1} \right) \right| \sum_{s_1=1}^{p-1} \left| \sin \left( \frac{\pi}{2 - \pi s_1} \right) \right| \]
\[ \times \sum_{r_2=1}^{p-1} \left| \sin \left( \frac{\pi}{2 - \pi r_2} \right) \right| \sum_{s_2=1}^{p-1} \left| \sin \left( \frac{\pi}{2 - \pi s_2} \right) \right| \sum_{u=1}^{p-1} \left| \sin \left( \frac{\pi u}{p} \right) \right| \]
\[ \ll p^{1/2} \log^5 p. \]

Therefore
\[ C_2(E_{p-1}) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \right| \ll p^{1/2} \log^5 p. \]

For \( 1 \leq a + jb + d_2 \leq p - 1 \) and \( 0 \leq d_1 < d_2 \), from (1.1) we have
\[
\sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \\
= \sum_{j=0}^{t} (-1)^{a+jb+d_1} e_{a+jb+d_1+x} + O(1) \\
= \frac{1}{p^5} \sum_{j=0}^{p} \sum_{l=0}^{p} e \left( \frac{u(j-l)}{p} \right) \sum_{c_1=1}^{p-1} \sum_{r_1=1}^{p-1} e \left( \frac{r_1(a+jb+d_1-c_1)}{p} \right) \\
\times \sum_{d_1=1}^{t} e \left( \frac{s_1(a+jb+d_1+x-d_1)}{p} \right) \sum_{c_2=1}^{p-1} e \left( \frac{r_2(a+jb+d_2-c_2)}{p} \right) \\
\[
\times \sum_{d_2=1}^{p-1} \sum_{s_2=1}^{p} e\left(\frac{s_2(a+jb+d_2+x-d_2)}{p}\right)(-1)^{c_1+d_1+c_2+d_2+O(1)}
\]

\[
= \frac{1}{p^5} \sum_{r_1=1}^{p-1} \sum_{s_1=1}^{p-1} \sum_{r_2=1}^{p-1} \sum_{s_2=1}^{p-1} \sum_{t=1}^{p} e\left(-\frac{ul}{p}\right) \sum_{c_1=1}^{p-1} (-1)^{c_1} e\left(-\frac{r_1c_1}{p}\right)
\]

\[
\times \sum_{d_1=1}^{p-1} (-1)^{d_1} e\left(-\frac{s_1d_1}{p}\right) \sum_{c_2=1}^{p-1} (-1)^{c_2} e\left(-\frac{r_2c_2}{p}\right) \sum_{d_2=1}^{p-1} (-1)^{d_2} e\left(-\frac{s_2d_2}{p}\right)
\]

\[
\times \sum_{j=0}^{p} e\left(\frac{r_1a+jb+d_1+s_1a+jb+d_1+x}{p}\right) e\left(\frac{r_2a+jb+d_2+s_2a+jb+d_2+x+uj}{p}\right) + O(1).
\]

By Lemma 2.4 we get
\[
\sum_{j=0}^{p} e\left(\frac{r_1a+jb+d_1+s_1a+jb+d_1+x}{p}\right) e\left(\frac{r_2a+jb+d_2+s_2a+jb+d_2+x+uj}{p}\right)
\]

\[
= e\left(-\frac{u\overline{ab}}{p}\right)
\]

\[
\times \sum_{j=0}^{p} e\left(\frac{r_1j+d_1+s_1j+d_1+x+r_2j+d_2+s_2j+d_2+x+u\overline{bj}}{p}\right)
\]

\[
\ll p^{1/2}.
\]

Then from (3.1) we have
\[
\sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2}
\]

\[
\ll \frac{tp^{1/2}}{p^5} \sum_{r_1=1}^{p-1} \frac{1}{|\sin(\pi/2-\pi r_1/p)|} \sum_{s_1=1}^{p-1} \frac{1}{|\sin(\pi/2-\pi s_1/p)|}
\]

\[
\times \sum_{r_2=1}^{p-1} \frac{1}{|\sin(\pi/2-\pi r_2/p)|} \sum_{s_2=1}^{p-1} \frac{1}{|\sin(\pi/2-\pi s_2/p)|}
\]
New pseudorandom sequences

\[ + \frac{p^{1/2}}{p^5} \sum_{r_1=1}^{p-1} \frac{1}{\sin(\pi/2 - \pi r_1/p)} \sum_{s_1=1}^{p-1} \frac{1}{\sin(\pi/2 - \pi s_1/p)} \times \sum_{r_2=1}^{p-1} \frac{1}{\sin(\pi/2 - \pi r_2/p)} \sum_{s_2=1}^{p-1} \frac{1}{\sin(\pi/2 - \pi s_2/p)} \sum_{u=1}^{p-1} \frac{1}{\sin(\pi u/p)} \leq p^{1/2} \log^5 p. \]

Therefore

\[ Q_2(E_{p-1}) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \right| \leq p^{1/2} \log^5 p. \]

This completes the proof of Theorem 1.1.

References


Department of Mathematics
Northwest University
Xi’an, Shaanxi, P.R. China
E-mail: hnlui@nwu.edu.cn

Received on 9.11.2005
and in revised form on 1.8.2006 (5093)