Large families of pseudorandom binary sequences constructed by using the Legendre symbol

by

HUANING LIU and JING GAO (Xi’an)


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

First they introduced the following pseudorandom measures.

**Definition 1.1.** 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 \( 1 \leq a \leq a+(t-1)b \leq N \).

**Definition 1.2.** The correlation measure of order \( l \) of \( E_N \) is defined by

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

where the maximum is taken over all \( D = (d_1, \ldots, d_l) \) and \( M \) with \( 0 \leq d_1 < \cdots < d_l \leq N - M \).

The sequence is considered to be a “good” pseudorandom sequence if both \( W(E_N) \) and \( C_l(E_N) \) (at least for small \( l \)) are “small” in terms of \( N \). Later J. Cassaigne, C. Mauduit and A. Sárközy [1] proved that this terminology is justified since for almost all \( E_N \in \{-1, +1\}^N \), both \( W(E_N) \) and \( C_l(E_N) \) are less than \( N^{1/2}(\log N)^c \).

Many pseudorandom binary sequences have been studied. For example, C. Mauduit and A. Sárközy [3] proved that the Legendre symbol yields a “good” pseudorandom sequence.

2010 Mathematics Subject Classification: 11K45, 11L40.

Key words and phrases: pseudorandom binary sequence, Legendre symbol, character sum.
Proposition 1.1. Let \( N = p - 1 \), \( e_n = \chi_2(n) \), and \( E_N = (e_1, \ldots, e_N) \), where \( \chi_2 \) is the quadratic character modulo \( p \). Then

\[
W(E_N) < N^{1/2} \log N, \quad C_l(E_N) < l N^{1/2} \log N.
\]

L. Goubin, C. Mauduit and A. Sárközy [2] extended the above construction:

Proposition 1.2. Suppose \( p \) is a prime, \( f(x) \in \mathbb{F}_p[x] \) has degree \( k \) (\( > 0 \)) and no multiple zero in \( \mathbb{F}_p \), and the binary sequence \( E_p = (e_1, \ldots, e_p) \) is defined by

\[
(1.1) \quad e_n = \begin{cases} 
\chi_2(f(n)) & \text{for } (f(n), p) = 1, \\
+1 & \text{for } p \mid f(n).
\end{cases}
\]

Then

\[
W(E_p) < 10kp^{1/2} \log p.
\]

If moreover \( l \in \mathbb{N} \) satisfies one of the following assumptions:

(i) \( l = 2 \); (ii) \( l < p \) and 2 is a primitive root modulo \( p \); (iii) \((4k)^l < p\),

then also

\[
C_l(E_p) < 10klp^{1/2} \log p.
\]

Later many large families of “good” pseudorandom sequences have been given, but still construction (1.1) is the best one. In this paper we give further large families of pseudorandom binary sequences constructed from the Legendre symbol, and study the pseudorandom properties by using an estimate for character sums. The main results are the following.

Theorem 1.1. Let \( p > 2 \) be a prime, and let \( f(x) \in \mathbb{F}_p[x] \) be any polynomial. Define the binary sequence \( E_{p-1} = (e_1, \ldots, e_{p-1}) \) by

\[
(1.2) \quad e_n = \begin{cases} 
\chi_2(f(n) + \overline{n}) & \text{for } (f(n) + \overline{n}, p) = 1, \\
+1 & \text{for } p \mid f(n) + \overline{n},
\end{cases}
\]

where \( \overline{n} \) is the multiplicative inverse of \( n \) modulo \( p \) with \( n\overline{n} \equiv 1 \pmod{p} \) and \( 1 \leq \overline{n} \leq p - 1 \). Then

\[
W(E_{p-1}) < 9(\deg(f) + 2)p^{1/2} \log p + \deg(f).
\]

If moreover the congruence \( f(x) + f(-x) \equiv 0 \pmod{p} \) has no solution, then

\[
C_2(E_{p-1}) < 18(\deg(f) + 2)p^{1/2} \log p + 2 \deg(f).
\]

On the other hand, if the congruence \( xf(x) + 1 \equiv 0 \pmod{p} \) has no solution, then for any \( l \in \mathbb{N} \),

\[
C_l(E_{p-1}) < 9l(\deg(f) + 2)p^{1/2} \log p + l \deg(f).
\]

Remark 1.1. Our construction is not new. It is a variant of (1.1), since

\[
\chi_2(f(n) + \overline{n}) = \chi_2(n^2 f(n) + n) \quad \text{for } (n, p) = 1.
\]
However, we can also control this construction for a new different set of polynomials $f$ under new conditions independent of those in Proposition 1.2.

From Theorem 1.1 we immediately get the following corollaries.

**Corollary 1.1.** Let $p > 2$ be a prime and $f_1(x) = h_1^2(x) + h_2(x) - c \in \mathbb{F}_p[x]$, where $h_1(x) = a_1x + a_3x^3 + a_5x^5 + \cdots \in \mathbb{F}_p[x]$, $h_2(x) = b_1x + b_3x^3 + b_5x^5 + \cdots \in \mathbb{F}_p[x]$, and $c$ is any quadratic nonresidue modulo $p$. Define $E_{p-1}' = (e_1', \ldots, e_{p-1}')$ by

$$e'_n = \begin{cases} 
\chi_2(f_1(n) + \overline{n}) & \text{for } (f_1(n) + \overline{n}, p) = 1, \\
+1 & \text{for } p | f_1(n) + \overline{n}.
\end{cases}$$

Then

$$W(E_{p-1}') < 9(\deg(f_1) + 2)p^{1/2}\log p + \deg(f_1),$$

$$C_2(E_{p-1}') < 18(\deg(f_1) + 2)p^{1/2}\log p + 2\deg(f_1).$$

**Corollary 1.2.** Let $p > 2$ be a prime with $p \equiv 3 \pmod{4}$, and $f_2(x) = xg^2(x)$, where $g(x) \in \mathbb{F}_p[x]$ is any polynomial. Define $E_{p-1}'' = (e_1'', \ldots, e_{p-1}'')$ by

$$e''_n = \begin{cases} 
\chi_2(f_2(n) + \overline{n}) & \text{for } (f_2(n) + \overline{n}, p) = 1, \\
+1 & \text{for } p | f_2(n) + \overline{n}.
\end{cases}$$

Then for any $l \in \mathbb{N}$,

$$W(E_{p-1}'') < 9(\deg(f_2) + 2)p^{1/2}\log p + \deg(f_2),$$

$$C_1(E_{p-1}'') < 9l(\deg(f_2) + 2)p^{1/2}\log p + l\deg(f_2).$$

### 2. Proof of Theorem 1.1

**Lemma 2.1 ([3, Theorem 2]).** Suppose that $p$ is a prime number, $\chi$ is a nonprincipal character modulo $p$ of order $d$, $f(x) \in \mathbb{F}_p[x]$ has degree $k$ and factorization $f(x) = b(x - x_1)^{d_1} \cdots (x - x_s)^{d_s}$ (where $x_i \neq x_j$ for $i \neq j$) in $\overline{\mathbb{F}}_p$ with $(d, d_1, \ldots, d_s) = 1$. Let $X, Y$ be real numbers with $0 < Y \leq p$. Then

$$\left| \sum_{X < n \leq X + Y} \chi(f(n)) \right| < 9kp^{1/2}\log p.$$

Now we prove Theorem 1.1. For $a, b, t$ with $1 \leq a \leq a + (t - 1)b \leq p - 1$, by (1.2) we have

$$\left| \sum_{j=0}^{t-1} e_{a+jb} \right| \leq \left| \sum_{j=0}^{t-1} \chi_2(f(a + jb) + \overline{a + jb}) \right| + \deg(f)$$

$$= \left| \sum_{j=0}^{t-1} \chi_2((a + jb)^2 f(a + jb) + (a + jb)) \right| + \deg(f) = \left| \sum_{j=0}^{t-1} \chi_2(F(j)) \right| + \deg(f).$$
It is easy to show that \( F(j) \) has a simple zero \( j = -a/b \). Then from Lemma 2.1 we get
\[
\left| \sum_{j=0}^{t-1} e_{a+jb} \right| < 9(\deg(f) + 2)p^{1/2} \log p + \deg(f).
\]

Therefore
\[
W(E_{p-1}) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right| < 9(\deg(f) + 2)p^{1/2} \log p + \deg(f).
\]

Next we consider the correlation measure of \( E_{p-1} \). First we suppose that the congruence \( f(x) + f(-x) \equiv 0 \pmod{p} \) has no solution. For \( 0 \leq d_1 < d_2 \leq p - 1 - M \), by (1.2) we have
\[
\left| \sum_{n=1}^M e_{n+d_1} e_{n+d_2} \right| \\
\leq \left| \sum_{n=1}^M \chi_2(f(n + d_1) + \overline{n + d_1})\chi_2(f(n + d_2) + \overline{n + d_2}) \right| + 2\deg(f) \\
= \left| \sum_{n=1}^M \chi_2((n + d_1)^2 f(n + d_1) + (n + d_1))\chi_2((n + d_2)^2 f(n + d_2) + (n + d_2)) \right| \\
+ 2\deg(f) \\
= \left| \sum_{n=1}^M \chi_2(G(n)) \right| + 2\deg(f).
\]

If \( G(n) \) has no simple zero, then we get
\[
(d_2 - d_1)f(d_2 - d_1) + 1 \equiv 0 \pmod{p}, \quad (d_1 - d_2)f(d_1 - d_2) + 1 \equiv 0 \pmod{p}.
\]

Therefore
\[
f(d_2 - d_1) + f(d_1 - d_2) \equiv 0 \pmod{p},
\]

which is impossible. So \( G(n) \) has at least one simple zero. Then from Lemma 2.1 we have
\[
\left| \sum_{n=1}^M e_{n+d_1} e_{n+d_2} \right| < 18(\deg(f) + 2)p^{1/2} \log p + 2\deg(f).
\]

Therefore
\[
C_2(E_{p-1}) = \max_{M,D} \left| \sum_{n=1}^M e_{n+d_1} e_{n+d_2} \right| < 18(\deg(f) + 2)p^{1/2} \log p + 2\deg(f).
\]

Now we assume that the congruence \( xf(x) + 1 \equiv 0 \pmod{p} \) has no solution. For \( 0 \leq d_1 < \cdots < d_l \leq p - 1 - M \), by (1.2) we have
Since the congruence 
\[ xf_1(x) + 1 \equiv 0 \pmod{p} \] has no solution, \( d_1, \ldots, d_l \) are simple zeros of \( H(n) \). So from Lemma 2.1 we get

\[
\sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_l} < 9l(\deg(f) + 2)p^{1/2} \log p + l \deg(f).
\]

Therefore

\[
C_{l}(E_{p-1}) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_l} \right| < 9l(\deg(f) + 2)p^{1/2} \log p + l \deg(f).
\]

This proves Theorem 1.1.

### 3. Proofs of Corollaries 1.1 and 1.2

First we prove Corollary 1.1. Noting that

\[
f_1(x) = (a_1 x + a_3 x^3 + a_5 x^5 + \cdots)^2 + (b_1 x + b_3 x^3 + b_5 x^5 + \cdots) - c,
\]

we have

\[
f_1(x) + f_1(-x) = 2(a_1 x + a_3 x^3 + a_5 x^5 + \cdots)^2 - 2c.
\]

Since \( c \) is a quadratic nonresidue modulo \( p \), we know that the congruence 
\[ f_1(x) + f_1(-x) \equiv 0 \pmod{p} \] has no solution. Then from Theorem 1.1 we get

\[
W(E'_{p-1}) < 9(\deg(f_1) + 2)p^{1/2} \log p + \deg(f_1),
\]

\[
C_{2}(E'_{p-1}) < 18(\deg(f_1) + 2)p^{1/2} \log p + 2 \deg(f_1).
\]

This proves Corollary 1.1.

On the other hand, we have

\[
xf_2(x) = (xg(x))^2.
\]

Since \(-1\) is a quadratic nonresidue modulo \( p \) for \( p \equiv 3 \pmod{4} \), the congruence 
\[ xf_2(x) + 1 \equiv 0 \pmod{p} \] has no solution. So from Theorem 1.1 we
have
\[ W(E_{p-1}^\prime) < 9(\deg(f_2) + 2)p^{1/2} \log p + \deg(f_2), \]
\[ C_l(E_{p-1}^\prime) < 9l(\deg(f_2) + 2)p^{1/2} \log p + l \deg(f_2). \]
This completes the proof of Corollary 1.2.

Acknowledgments. This research was supported by the National Natural Science Foundation of China under Grant No. 10901128, the Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20090201120061, the Natural Science Foundation of the Education Department of Shaanxi Province of China under Grant No. 09JK762, and the Fundamental Research Funds for Central Universities.

References