Construction of Pseudorandom Binary Sequences using Additive Characters

Christian Mauduit
Joël Rivat
András Sárközy

Vienna, Preprint ESI 1184 (2002)  
July 17, 2002

Supported by the Austrian Federal Ministry of Education, Science and Culture
Available via http://www.esi.ac.at
CONSTRUCTION OF PSEUDORANDOM BINARY SEQUENCES USING ADDITIVE CHARACTERS.

CHRISTIAN MAUDUIT, JOËL RIVAT, AND ANDRÁS SÁRKÖZY

Abstract. In earlier papers the authors studied finite pseudorandom binary sequences, and they constructed sequences with strong pseudorandom properties. In these earlier constructions multiplicative characters were used. In this paper a new construction is presented which utilizes properties of additive characters. These new sequences can be computed fast, they are well-distributed relative to arithmetic progressions and their correlations of “small” order are “small”, but the price paid for the fast computation is that the correlations of “large” order can be “large”.

1. Introduction

Throughout this paper we write $e(\alpha) = \exp(2i\pi \alpha)$ and $e_p(a) = e(a/p)$.

In a series of papers we (partly with further coauthors) studied finite pseudorandom binary sequences

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

In particular, in [4] Mauduit and Sárközy first introduced the following measures of pseudorandomness: the well-distribution measure of $E_N$ is defined by

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

where the maximum is taken over all $a, b, \ell \in \mathbb{N}$ such that $1 \leq a \leq a + (\ell - 1)b \leq N$, and the correlation measure of order $k$ of $E_N$ is defined as

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

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ and $M$ such that $0 \leq d_1 < \cdots < d_k \leq N - M$. Then the sequence is considered as a “good” pseudo-random sequence if both these measures $W(E_N)$ and $C_k(E_N)$ (at least for “small” $k$) are “small” in terms of $N$ (in particular, both are $o(N)$ as $N \to \infty$). Indeed, later Cassaigne, Mauduit and Sárközy [2] showed 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, in [4] it was shown that the Legendre symbol forms a “good” pseudo-random sequence. More exactly, let \( p \) be an odd prime, and

\[
N = p - 1, \quad e_n = \left( \frac{n}{p} \right), \quad E_N = \{e_1, \ldots, e_N\}.
\]

Then by Theorem 1 in [4] we have

\[
W(E_N) \ll p^{1/2} \log p \ll N^{1/2} \log N
\]

and

\[
C_k(E_N) \ll k p^{1/2} \log p \ll kN^{1/2} \log N
\]

Later Goubin, Mauduit and Sárközy [3] extended this construction considerably to a large family of “good” pseudorandom binary sequences. This construction and its most important properties are described in the following theorem (proved in [3]):

**Theorem 1.** Assume that \( p \) is a prime number, \( f(X) \in \mathbb{F}_p[X] \) (\( \mathbb{F}_p \) being the field of the modulo \( p \) residue classes) has degree \( k \) \((> 0)\), \( f(X) \) has no multiple zero in \( \mathbb{F}_p \) (the algebraic closure of \( \mathbb{F}_p \)), and the binary sequence \( E_p = \{e_1, \ldots, e_p\} \) is defined by

\[
e_n = \begin{cases} 
\left( \frac{f(n)}{p} \right) & \text{for } (f(n), p) = 1, \\
+1 & \text{for } p \mid f(n).
\end{cases}
\]

Then we have

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

Moreover, assume that also \( \ell \in \mathbb{N} \), and one of the following assumptions holds:

1. \( \ell = 2; \)
2. \( \ell < p, \) and 2 is a primitive root modulo \( p; \)
3. \( 4k \ell < p. \)

Then we also have

\[
C_\ell(E_p) < 10k \ell p^{1/2} \log p.
\]

(They also presented examples showing that if none of these conditions holds, then \( C_\ell(E_p) \) can be large. See also [6].)

In [7] Sárközy constructed further “good” pseudorandom binary sequences. This construction was based on the notion of index (“discrete logarithm”), and the properties of the *multiplicative* characters play an important rôle in it.

Mauduit and Sárközy [5] extended the problem from binary sequences to sequences of \( k \) symbols. They extended the definition of pseudorandomness to this case, and then they showed that if \( p \) is a prime, \( N = p - 1, \) \( g \) is a primitive root modulo \( p \) and the *multiplicative* character \( \chi_1 \) modulo \( p \) is defined by

\[
\chi_1(g) = e\left(\frac{1}{k}\right)
\]
then the sequence
\[ E_N = \{e_1, \ldots, e_N\} \quad \text{with} \quad e_n = \chi_1(n) \]
is a “good” pseudorandom sequence of \( k \) symbols. (Note that (1) is a special case of this construction.)

We have also studied the pseudorandom properties of many other sequences, but in all the other cases the upper bounds obtained for \( W(E_N) \) and \( C_t(E_N) \) were much weaker, than in the constructions described above.

Note that in all these top quality constructions the multiplicative characters play a crucial rôle. It is a natural idea to try to give further “good” constructions by using “additive” characters instead of the multiplicative ones. The simplest construction of this type seems to be the following one: let \( p \) be an odd prime number, \( f(X) \in \mathbb{F}_p[X] \), and define \( E_p = \{e_1, \ldots, e_p\} \) by
\[
(5) \quad e_n = \begin{cases} 
+1 & \text{if } 0 \leq r_p(f(n)) < p/2, \\
-1 & \text{if } p/2 \leq r_p(f(n)) < p.
\end{cases}
\]
where \( r_p(n) \) denotes the unique \( r \in \{0, \ldots, p-1\} \) such that \( n \equiv r \mod p \). This paper is devoted to the study of the sequence (5).

Clearly, the sequence (5) can be computed fast. Moreover, we will show that for this sequence both \( W(E_N) \) and the correlations of “small” order are “small”:

**Theorem 2.** For \( f \in \mathbb{F}_p[X] \) of degree \( d \) and \( E_p = \{e_1, \ldots, e_p\} \) defined by (5), we have
\[
(6) \quad W(E_p) \ll dp^{1/2}(\log p)^2.
\]

**Theorem 3.** For \( f \in \mathbb{F}_p[X] \) of degree \( d \) and \( E_p = \{e_1, \ldots, e_p\} \) defined by (5), we have for \( 2 \leq \ell \leq d-1 \),
\[
(7) \quad C_\ell(E_p) \ll dp^{1/2}(\log p)^{\ell+1}.
\]

On the other hand, we can show that certain correlations of “large” order can be “large”:

**Theorem 4.** For any \( k = 2^t \) there exists a constant \( c = c(k) > 0 \) such that if \( p \) is a prime number large enough, \( f \in \mathbb{F}_p[X] \) is of degree \( k \) and \( E_p = \{e_1, \ldots, e_p\} \) is defined by (5), then
\[
(8) \quad \max_{1 \leq T < T+M \leq p} \left| \sum_{n=T}^{T+M} e_n e_{n+1} \cdots e_{n+k-1} \right| \gg cp.
\]

**Corollary 1.** For any \( k = 2^t \), if \( p \) is a prime number large enough, \( f \in \mathbb{F}_p[X] \) is of degree \( k \) and \( E_p = \{e_1, \ldots, e_p\} \) is defined by (5), then
\[
C_k(E_p) \gg p.
\]
2. Exponential sums

The proofs of Theorem 2 and Theorem 3 will be based on the following exponential sum estimate:

**Lemma 1.** For any polynomial \( f(X) \in \mathbb{F}_p[X] \) of degree \( d \geq 2 \) and any integers \( M \) and \( K \) with \( 1 \leq K < p \) we have

\[
\left| \sum_{n=1}^{M+K} e_p(f(n)) \right| \leq d p^{1/2} \log p.
\]

This follows from a theorem of Weil [9] by using an inequality of Vinogradov as it is described by Tietäväinen in [8] and indeed, probably Tietäväinen was the first who proved this result (see also [1], Lemma 2).

In order to express the terms of the sequence \( E_p \) with exponential sums we will use the following representation:

**Lemma 2.** For \( n \in \mathbb{Z} \) and \( p \) an odd integer, we have

\[
\frac{1}{p} \sum_{|x| < p/2} v_p(a) e_p(an) = \begin{cases} 
  +1 & \text{if } r_p(n) < \frac{p}{2}, \\
  -1 & \text{otherwise}, 
\end{cases}
\]

where \( v_p(a) \) is a function of period \( p \) such that

\[
v_p(0) = 1; \quad v_p(a) = 1 + i \left( \frac{(-1)^a - \cos(\pi a/p)}{\sin(\pi a/p)} \right) \quad (1 \leq |a| < p/2).
\]

Furthermore, \( v_p(a) \) satisfies

\[
v_p(a) = \begin{cases} 
  O(1) & \text{if } a \text{ is even}, \\
  -\frac{2\pi a}{\pi a} + O(1) & \text{if } a \text{ is odd}.
\end{cases}
\]

**Proof.** Since for \( r \in \mathbb{Z}, \)

\[
\frac{1}{p} \sum_{|x| < p/2} e_p(a(n - r)) = \begin{cases} 
  1 & \text{if } n \equiv r \mod p, \\
  0 & \text{otherwise}, 
\end{cases}
\]

we have

\[
\frac{1}{p} \sum_{|x| < p/2} \left( 1 - \sum_{1 \leq r < p/2} (e_p(ar) - e_p(-ar)) \right) e_p(an) = \begin{cases} 
  +1 & \text{if } r_p(n) < \frac{p}{2}, \\
  -1 & \text{otherwise}, 
\end{cases}
\]

The value of \( v_p(a) \) is obtained by computing the geometric sums over \( r \) above, and (10) follows from (9) by an easy computation. \( \square \)

3. The proof of Theorem 2

We have to prove that for any \( 0 < m < p, 0 \leq r < m, 1 \leq M < p \), we have the estimate

\[
\left| \sum_{r+km \leq M} e_{r+km} \right| \ll d p^{1/2} (\log p)^2.
\]
By lemma 2, we have
\[\sum_{r + km \leq M} e_{r+km} = \frac{1}{p} \sum_{|e| < p/2} v_p(a) \sum_{r + km \leq M} e_p(a f(r + km)).\]

> From the estimate of Lemma 1 and the fact that \(f(r + Xm)\) is a polynomial of the same degree of \(f\) (notice that \(m\) is invertible modulo \(p\)), we get
\[\left| \sum_{r + km \leq M} e_{r+km} \right| \leq \frac{1}{p} \left( \sum_{|e| < p/2} |v_p(a)| \right) dp^{1/2} (\log p) + |v_p(0)|,\]

and the result follows from (9) and (10) using the estimate
\[|v_p(a)| \ll \frac{p}{a} \quad (1 \leq |a| < p/2).

4. The proof of Theorem 3

For \(M < p\) and \(0 \leq d_1 < \cdots < d_\ell \leq p - M\), we have
\[
\sum_{n \leq M} e_{n+d_1} \cdots e_{n+d_\ell} = \frac{1}{p^\ell} \sum_{|a_1| < p/2} \cdots \sum_{|a_\ell| < p/2} v_p(a_1) \cdots v_p(a_\ell) \sum_{n \leq M} e_p(a_1 f(n + d_1) + \cdots + a_\ell f(n + d_\ell)).
\]

If it is true that the polynomial \(a_1 f(X + d_1) + \cdots + a_\ell f(X + d_\ell)\) is of degree \(\geq 2\), for any \((a_1, \ldots, a_\ell) \neq (0, \ldots, 0)\) in the sum above, then by Lemma 1, we get
\[
\left| \sum_{n \leq M} e_{n+d_1} \cdots e_{n+d_\ell} \right| \leq \frac{1}{p^\ell} \left( \sum_{|e| < p/2} |v_p(a)| \right)^\ell dp^{1/2} \log p + M.
\]

Thus by Lemma 2,
\[
\left| \sum_{n \leq M} e_{n+d_1} \cdots e_{n+d_\ell} \right| \ll dp^{1/2} (\log p)^{\ell+1}.
\]

It remains to study the degree of the polynomial \(a_1 f(X + d_1) + \cdots + a_\ell f(X + d_\ell)\).

**Lemma 3.** Let \(p\) a prime number, \(1 \leq k < p\), \(f \in \mathbb{F}_p[X]\), of degree \(d \geq k\), and let \(x_1, \ldots, x_k\) be \(k\) different elements of \(\mathbb{F}_p\). Then for all \((a_1, \ldots, a_k) \in \mathbb{F}_p^k \setminus (0, \ldots, 0)\), the polynomial
\[g(X) := a_1 f(X + x_1) + \cdots + a_k f(X + x_k)\]

is of degree \(\geq d - k + 1\).
Proof. Suppose that the degree of \( g \) is at most \( d - k \). Then by Taylor expansion, we have

\[
g(X) = (a_1 + \cdots + a_k) f(X) + (a_1 x_1 + \cdots + a_k x_k) f'(X) + (a_1 x_1^2 + \cdots + a_k x_k^2)(2!)^{-1} f^{(2)}(X) + \cdots + (a_1 x_1^{k-1} + \cdots + a_k x_k^{k-1})(k-1)!^{-1} f^{(k-1)}(X) + R(X)
\]

where \( R(X) \) is a polynomial of degree at most \( d - k \). Thus we must have

\[
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
x_1 & x_2 & \cdots & x_k \\
\vdots & \vdots & \ddots & \vdots \\
x_1^{k-2} & x_2^{k-2} & \cdots & x_k^{k-2}
\end{pmatrix}
\begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
a_k
\end{pmatrix} =
\begin{pmatrix}
0 \\
0 \\
\vdots \\
0
\end{pmatrix}
\]

The determinant of this Vandermonde matrix is non-zero, hence \( (a_1, \ldots, a_k) = (0, \ldots, 0) \).

With the hypothesis \( 2 \leq \ell \leq d - 1 \) in Theorem 3, Lemma 3 implies that the degree of \( a_1 f(X + d_1) + \cdots + a_\ell f(X + d_\ell) \) is at least 2, which completes the proof of Theorem 3.

5. Vandermonde systems

In order to get a lower bound for the correlation we need to investigate more closely the Vandermonde systems which appear in the proof of Theorem 3.

Lemma 4. Let \( x_1, \ldots, x_k \) be \( k \) different elements of \( \mathbb{Z} \). Then the solutions of the linear system

\[
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
x_1 & x_2 & \cdots & x_k \\
\vdots & \vdots & \ddots & \vdots \\
x_1^{k-2} & x_2^{k-2} & \cdots & x_k^{k-2}
\end{pmatrix}
\begin{pmatrix}
y_1 \\
y_2 \\
\vdots \\
y_k
\end{pmatrix} =
\begin{pmatrix}
0 \\
0 \\
\vdots \\
0
\end{pmatrix}
\]

in \( \mathbb{Q}^k \) are of the form \( (\lambda u_1, \ldots, \lambda u_k) \) with \( \lambda \in \mathbb{Q} \), for some \( (u_1, \ldots, u_k) \in \mathbb{Z}^k \) (unique apart from sign) such that \( u_1 \cdots u_k \neq 0 \) and \( \gcd(u_1, \ldots, u_k) = 1 \).

Proof. The rank of this system is \( k - 1 \) (the first \( k - 1 \) columns form a non-vanishing Vandermonde determinant), thus the solutions form a vector space of dimension 1 over \( \mathbb{Q} \). Hence there exists a non-trivial solution \( (y_1, \ldots, y_k) \in \mathbb{Q}^k \), and all the solutions can be obtained by multiplying by \( \lambda \in \mathbb{Q} \). If we choose to multiply \( (y_1, \ldots, y_k) \) by the least common multiple of the denominators of the \( y_j \)'s we obtain a non-trivial solution \( (\tilde{u}_1, \ldots, \tilde{u}_k) \in \mathbb{Z}^k \).

We can then divide this solution by \( \gcd(\tilde{u}_1, \ldots, \tilde{u}_k) \) and finally obtain a non-trivial solution \( (u_1, \ldots, u_k) \in \mathbb{Z}^k \) such that \( \gcd(u_1, \ldots, u_k) = 1 \). Then all the solutions in \( \mathbb{Q}^k \) are of the form \( (\lambda u_1, \ldots, \lambda u_k) \) with \( \lambda \in \mathbb{Q} \).
It remains to show that $u_1 \cdots u_k \neq 0$.

Suppose that there exists $i \in \{1, \ldots, k\}$ such that $u_i = 0$. By permutation of the indexes, we may assume that $i = k$. Then

$$
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
x_1 & x_2 & \cdots & x_k \\
\vdots & \vdots & \ddots & \vdots \\
x_k^{-2} & x_k^{-2} & \cdots & x_k^{-2}
\end{pmatrix}
\begin{pmatrix}
u_1 \\
\vdots \\
u_{k-1} \\
0
\end{pmatrix} =
\begin{pmatrix}
0 \\
0 \\
\vdots \\
0
\end{pmatrix}
$$

which implies that

$$
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
x_1 & x_2 & \cdots & x_{k-1} \\
\vdots & \vdots & \ddots & \vdots \\
x_k^{-2} & x_k^{-2} & \cdots & x_{k-1}^{-2}
\end{pmatrix}
\begin{pmatrix}
u_1 \\
\vdots \\
u_{k-1}
\end{pmatrix} =
\begin{pmatrix}
0 \\
0 \\
\vdots \\
0
\end{pmatrix}
$$

But the determinant of this matrix is not zero, hence $(u_1, \ldots, u_{k-1}) = (0, \ldots, 0)$ and

$$(u_1, \ldots, u_k) \neq (0, \ldots, 0)$$

which contradicts the definition of $u_1, \ldots, u_k$. \qed

6. The proof of Theorem 4

Our aim is to try to construct a “large” sum with $0 \leq d_1 < d_2 < \cdots < d_k$. We first assume only that $k \geq 3$. Later in the proof we will discuss why we need to restrict ourselves to less general $k$ and $d_j$’s.

By Lemma 4 there exists $(u_1, \ldots, u_k) \in \mathbb{Z}^k$ (unique apart from sign) such that $u_1 \cdots u_k \neq 0$, $\gcd(u_1, \ldots, u_k) = 1$ and

$$
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
d_1 & d_2 & \cdots & d_k \\
\vdots & \vdots & \ddots & \vdots \\
d_k^{-2} & d_k^{-2} & \cdots & d_k^{-2}
\end{pmatrix}
\begin{pmatrix}
u_1 \\
u_2 \\
\vdots \\
u_k
\end{pmatrix} =
\begin{pmatrix}
0 \\
0 \\
\vdots \\
0
\end{pmatrix}
$$

We observe that $(u_1, \ldots, u_k)$ depends only on $(d_1, \ldots, d_k)$. Let now $p$ be a prime number large enough. For all $i \in \{1, \ldots, k\}$ we have $u_j \not\equiv 0 \mod p$. Then by the same argument as in the proof of Lemma 3, if $f \in \mathbb{F}_p[X]$ is of degree $k$, we obtain that the degree of the polynomial

$$a_1 f(X + d_1) + \cdots + a_k f(X + d_k)$$

is at most 1 if and only if $(a_1, \ldots, a_k) = a \cdot (u_1, \ldots, u_k)$ (in $\mathbb{F}_p^k$) with $|a| < p/2$.

For $1 \leq T < p$, $1 \leq M < p/2$ and $0 \leq d_1 < \cdots < d_k \leq p - M - T$, we consider

$$S := \sum_{n=T+1}^{T+M} e_{n+d_1} \cdots e_{n+d_k}$$

$$= \frac{1}{p^k} \sum_{|a_1| < p/2} \cdots \sum_{|a_k| < p/2} v_p(a_1) \cdots v_p(a_k) \sum_{n=T+1}^{T+M} e_p(a_1 f(n+d_1) + \cdots + a_k f(n+d_k)).$$
We may split the summations over $(a_1, \ldots, a_k)$ above into $S = S_1 + S_2$ where $S_1$ involves
only those $a_j$'s such that $(a_1, \ldots, a_k) = a \cdot (u_1, \ldots, u_k) \mod p$:
\[
S_1 = \frac{1}{p^k} \sum_{|a| < p/2} v_p(a u_1) \cdots v_p(a u_k) \sum_{n=0}^{T+M} e_p(a u f(n + d_1) + \cdots + a u_k f(n + d_k)),
\]
and $S_2$ involves the remaining terms.

Since in $S_2$ the degree of the polynomials involved is $\geq 2$, by the same argument as in
the proof of Theorem 3 we obtain
\[
S_2 \ll k p^{1/2} (\log p)^{k+1},
\]
hence without any assumption over $d_1, \ldots, d_k$ we obtain
\[
S = S_1 + O(k p^{1/2} (\log p)^{k+1}).
\]

It remains to show that $S_1$ is indeed “large”. For this purpose we shall need a better
control over the sum $S_1$, at the cost of assuming that at least one of the $u_j$'s is equal to 1.

Let $1 \leq A < p$ be a parameter to be fixed later. In $S_1$, let us consider the contribution
$S_3$ of those $a$'s which satisfy $A \leq |a| < p/2$. If at least one of the $u_j$'s (say $u_{j_0}$) is equal to
1, in which case $|v_p(a u_{j_0})| = |v_p(a)| \ll p/A$, we majorize the summation over $n$ trivially by
$M$, to get
\[
S_3 \ll \frac{M}{p^k A} \sum_{A \leq |a| < p/2, j \neq j_0} \prod_{j \neq j_0} |v_p(a u_j)|.
\]
We may now relax the condition $A \leq |a|$ and by Hölder inequality we obtain
\[
S_3 \ll \frac{M}{Ap^{k-1}} \prod_{j \neq j_0} \left( \sum_{|a| < p/2} |v_p(a u_j)|^{k-1} \right)^{1/(k-1)}
\]
which, since $u_j$ is invertible modulo $p$, leads to
\[
S_3 \ll \frac{M}{Ap^{k-1}} \sum_{|b| < p/2} |v_p(b)|^{k-1} \ll \frac{M}{Ap^{k-1}} \sum_{1 \leq |b| < p/2} \left| \frac{p}{b} \right|^{k-1} \ll \frac{M}{A}
\]
for $k \geq 3$.

Furthermore, for the $a$'s which are even and satisfy $|a| < A$, we observe that $|a u_j| < p/2$
(since $p$ is large enough) and $a u_j$ is even, for all $i$, thus their contribution to $S_1$ is at most
\[
\ll \frac{1}{p^k} \sum_{|a| < A} M \ll \frac{AM}{p^k} \ll p^{2-k}.
\]

Hence we have proved that if at least one of the $u_j$'s is equal to 1, then
\[
S = S_4 + O \left( \frac{M}{A} \right) + O(k p^{1/2} (\log p)^{k+1}) + O(p^{2-k})
\]
where $S_4$ denotes for the contribution to $S$ of the $a$’s which are odd and satisfy $|a| < A$:

$$S_4 := \frac{1}{p^M} \sum_{a \equiv 1 \mod 2} v_p(a u_1) \cdots v_p(a u_k) \sum_{n=T+1}^{T+M} e_p(a u_1 f(n + d_1) + \cdots + a u_k f(n + d_k)).$$

We remark here that if at least one of the $u_j$’s is even, then $S_4$ will be “small”:

$$S_4 \ll \frac{1}{p^M} \sum_{1 \leq s < A} \left( \frac{p}{a} \right)^{k-1} M \ll \frac{M}{p}.$$

In order to obtain a “large” sum $S_4$, we need to have the $v_p(a u_j)$ as large as possible, which can be obtained only if $a u_j$ is odd, i.e., if $u_j$ is odd. Hence we will assume that all the $u_j$’s are odd and one of them is equal to 1. Under these conditions we recall that also $|a u_j| < p/2$ so we may use

$$v_p(a u_j) = -\frac{2i p}{\pi a u_j} + O(1).$$

This enables us to write

$$S_4 = \frac{(-2i/\pi)^k}{u_1 \cdots u_k} \sum_{a \equiv 1 \mod 2} a^{-k} \sum_{n=T+1}^{T+M} e_p(a u_1 f(n + d_1) + \cdots + a u_k f(n + d_k)) + O \left( \frac{kAM}{p} \right).$$

Furthermore we may write

$$u_1 f(n + d_1) + \cdots + u_k f(n + d_k) = \lambda n + \mu,$$

where $\lambda$ and $\mu$ depend only on the coefficients of $f$ and on $d_1, \ldots, d_k$, so that $|\lambda|$ and $|\mu|$ are bounded by some $L > 0$ independent of $p$.

If $\lambda \equiv 0 \mod p$ (for instance if $\lambda = 0$), then

$$\sum_{n=T+1}^{T+M} e_p(a(\lambda n + \mu)) \gg M.$$ 

If $\lambda \not\equiv 0 \mod p$, we are still able to choose of $T$ and $M$ for which the previous sum is large. We consider $0 \leq T_1 < p$ such that $\lambda T_1 + \mu \equiv 0 \mod p$. In order to ensure that $[T, T + M] \subset [1, N]$, we choose $T = T_1$ if $T_1 < p/2$ and $T = T_1 - M$ otherwise. Then we observe that

$$e_p(a(\lambda n + \mu)) = e_p(a(\lambda T_1 + \mu)) e_p(a\lambda(n - T_1)) = e_p(a\lambda(n - T_1)).$$

In order to keep the argument of this complex number small, we choose $M = \lfloor p/(4AL) \rfloor$, for which whenever $T < n \leq T + M$ and $|a| \leq A$,

$$\left| \frac{a\lambda(n - T_1)}{p} - \frac{AML}{p} \right| \leq \frac{1}{4},$$

and therefore

$$\Re \sum_{n=T+1}^{T+M} e_p(a(\lambda n + \mu)) = \Re \sum_{n=T+1}^{T+M} e_p(a\lambda(n - T_1)) \gg M \gg \frac{p}{AL}.$$
Under these assumptions, we get the lower bound:
\[
\Re(i^k u_1 \cdots u_k S_4) + O \left( |u_1 \cdots u_k| \frac{M}{p} \right) \gg \left( \frac{2}{\pi} \right)^k \sum_{a \equiv 1 \mod 2} a^{-k} \frac{p}{AL} \gg \frac{p}{AL}.
\]
But \( M/p = O(1/AL) \), thus
\[
S_4 \gg \frac{p}{AL |u_1 \cdots u_k|}.
\]
Since \( u_1, \ldots, u_k \) depend only on the \( d_j \)'s, they are bounded independently of \( p \) by some \( U > 0 \). We conclude that
\[
S \gg \frac{p}{ALU^k} + O \left( \frac{p}{A^2} \right) + O(kp^{1/2}(\log p)^{k+1}) + O(p^{2-k}).
\]
If, as we may, we choose \( A \) to be large enough, independently of \( p \), then the first term dominates the error term, and we get
\[
S \geq c(k, d_1, \ldots, d_k) \ p,
\]
for some \( c(k, d_1, \ldots, d_k) > 0 \), provided that the corresponding \( u_j \)'s are all odd, and one of them is equal to 1.

In order to complete the proof of Theorem 4, we now choose \( k = 2^t \) and \( d_i = i - 1 \) for \( i = 1, \ldots, k \). We recall that \( f \in \mathbb{F}_p[X] \) is of degree \( k \). Then we have seen that there is a unique \( (u_1, \ldots, u_k) \in \mathbb{Z}^k \) with \( u_k > 0, u_1 \cdots u_k \neq 0, \gcd(u_1, \ldots, u_k) = 1 \), such that
\[
u_1 f(X + d_1) + \cdots + u_k f(X + d_k)
\]
is of degree 1. Actually the values of the \( u_i \)'s follow from the following result.

**Lemma 5.** Consider the forward difference operator \( \Delta \) defined by
\[
\Delta f(x) = f(x + 1) - f(x),
\]
and write \( \Delta_1 = \Delta, \Delta_m = \Delta_{m-1}(\Delta) \) for \( m = 2, 3, \ldots \). Then

1. We have
\[
\Delta_m f(x) = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} f(x + j);
\]
2. \( \Delta_m \) is linear:
\[
\Delta_m(\alpha f(x) + \beta g(x)) = \alpha \Delta_m f(x) + \beta \Delta_m g(x);
\]
3. If \( f \) is a polynomial of degree \( d \) then \( \Delta_m f \) is a polynomial of degree \( d - m \) for \( 1 \leq m \leq d \), and \( \Delta_m f = 0 \) for \( m > d \).

**Proof.** All these properties of the operator \( \Delta_m \) are well-known and easy to verify. \( \square \)

We apply this lemma with \( m = k - 1 = 2^t - 1 \) and get
\[
u_{j+1} = (-1)^{2^t-1-j} \binom{2^t-1}{j} \ (0 \leq j \leq 2^t - 1).
\]
We observe that \( u_{2t} = 1 \), so it remains to check that all the \( u_i \)’s are odd. We write

\[
\binom{2^t - 1}{j} = \frac{2^t - 1}{1} \cdot \frac{2^t - 2}{2} \cdots \frac{2^t - j}{j}
\]

and note that for \( 1 \leq q \leq j \leq 2^t - 1 \) and \( 1 \leq u \leq t \),

\[2^n | q \iff 2^n | 2^t - q,
\]
hence the exponent of 2 in the canonical form of \( \frac{2^t - q}{q} \) is zero, and \( \binom{2^t - 1}{j} \) is odd.

This completes the the proof of Theorem 4.

7. Remarks on the proof of Theorem 4

In the course of the proof of Theorem 4, we have been forced to introduce severe restrictions on the admissible values of the \( u_j \)’s, namely that one of them is equal to 1 (in order to handle the contribution the \( a \)’s with \( |a| > A \)), and that all of the \( u_j \)’s are odd (to make \( v_p(a u_j) \) large). We would like to point out here that if this second condition is not fulfilled, i.e. there is at least an even \( u_j \), and another \( u_i \) is equal to 1, then our proof shows that the corresponding sum \( S \) is small.

The restrictions on the \( u_j \)’s produce restrictions on the \( d_j \)’s. Though we did not investigate in details this matter, we have carried out some computations. Among other we have found the following interesting example: if \( k = 4 \), Theorem 4 shows that the correlation of order 4 is large, and indeed there an \( M \) so that

\[\sum_{n=1}^{M} e_n e_{n+1} e_{n+2} e_{n+3} \gg N.\]

On the other hand, choosing \( d_1 = 0, d_2 = 1, d_3 = 2, d_4 = 4 \), we get \( u_1 = -3, u_2 = 8, u_3 = -6, u_4 = 1. \) Since \( u_4 = 1 \), and \( u_2 \) and \( u_3 \) are even, thus all the sums of the form

\[\sum_{n=1}^{M} e_n e_{n+1} e_{n+2} e_{n+4}\]

are “small”. This shows that in general it is not sufficient to restrict ourselves, although this is costumary, to sums where the subscripts of the \( e \)’s are consecutive integers, since the behaviour of these sums can be very much different from sums with certain other special choices of the \( d_i \)’s.

We expect that if the order of the correlation is greater than the degree of the polynomial, then the correlation is “large” (assuming also, perhaps, that the order of the correlation is even). However, this cannot be shown along these lines since then there are many “large” terms contributing to the sum to be estimated, thus a different approach is needed. We hope to return to this in a subsequent paper.
8. Conclusions

The binary sequence defined by (5) can be computed fast, faster than the other constructions mentioned in the Introduction. For this sequence $E_p$ both $W(E_p)$ and the correlation of “small” ($< \text{degree of } f$) order are “small” but, on the other hand, the correlations of “large” ($\geq \text{degree of } f$) order can be “large”. Thus this construction provides a reasonable alternative to the previous constructions if it suffices to control the correlations of “small” order. On the other hand, if we also have to watch out for the correlations of “large” order, then either we have to use polynomials of “large” order (which makes the computations much slower) or we have to return to the earlier constructions.

References


Christian MAUDUIT, Institut de Mathématiques de Luminy CNRS-UPR 9016, 163 avenue de Luminy, Case 907, 13288 Marseille Cedex 9, France.
E-mail address: mauduit@iml.univ-mrs.fr

Joël RIVAT, Institut Elie Cartan de Nancy, Université Henri Poincaré, B.P. 239, 54506 Vandoeuvre-lès-Nancy, France.
E-mail address: rivat@iecn.u-nancy.fr

András SÁRKÖZY, Eötvös Loránd University, Department of Algebra and Number Theory, H-1117 Budapest, Pázmány Péter sétaút 1/c, Hungary.
E-mail address: sarkozy@cs.elte.hu