ON THE PSEUDORANDOMNESS
OF THE LIOUVILLE FUNCTION OF POLYNOMIALS
OVER A FINITE FIELD

LÁSZLÓ MÉRAI — ARNE WINTERHOF

Dedicated to the memory of Professor Pierre Liardet

ABSTRACT. We study several pseudorandom properties of the Liouville function and the Möbius function of polynomials over a finite field. More precisely, we obtain bounds on their balancedness as well as their well-distribution measure, correlation measure, and linear complexity profile.

Communicated by Manfred Kühleitner

1. Introduction

In analogy to the Liouville \( \lambda \)-function and the Möbius \( \mu \)-function for integers, Carlitz \cite{Carlitz} introduced the mappings \( \lambda \) and \( \mu \) for polynomials over the finite field \( \mathbb{F}_q \) by

\[
\lambda(F) = (-1)^{\omega(F)}, \quad F \in \mathbb{F}_q[X],
\]

where \( \omega(F) \) denotes the number of irreducible factors of \( F \) (counted in multiplicities), and

\[
\mu(F) = \begin{cases} 
\lambda(F) & \text{if } F \text{ is squarefree,} \\
0 & \text{otherwise,}
\end{cases} \quad F \in \mathbb{F}_q[X].
\]
Carlitz [2] proved
\[ \sum_{\deg F = d} \lambda(F) = (-1)^d q^{(d+1)/2} \] (1)
and
\[ \sum_{\deg F = d} \mu(F) = \begin{cases} 0 & \text{if } d \geq 2, \\ -q & \text{if } d = 1, \end{cases} \] (2)
where the sums are over all monic polynomials \( F \in \mathbb{F}_q[X] \) of degree \( d \).

For \( \ell \geq 2, d \geq 2 \), distinct polynomials \( D_1, \ldots, D_\ell \in \mathbb{F}_q[X] \) of degree smaller than \( d \), \( q \) odd, and \( (\epsilon_1, \ldots, \epsilon_\ell) \in \{0, 1\}^\ell \setminus \emptyset \), Carmon and Rudnick [3, Theorem 1.1] have recently proved that
\[ \sum_{\deg F = d} \mu(F + D_1)^{\epsilon_1} \cdots \mu(F + D_\ell)^{\epsilon_\ell} = O(\ell d q^{d-1/2}), \quad d \geq 2. \] (3)
(For \( d = 1 \) the sum trivially equals \( (-1) \sum_{j=1}^\ell \epsilon_j q^j \).) Since the number of monic squarefree polynomials over \( \mathbb{F}_q \) of degree \( d \geq 2 \) is \( q^d - q^{d-1} \) (see for example [12, Proposition 2.3]) the same result holds for \( \lambda \) instead of \( \mu \) as well.

(1), (2), and (3) are results on the global pseudorandomness of polynomials of degree \( d \) over \( \mathbb{F}_q \). More precisely, (1), (2), and (3) are essentially results on two measures of pseudorandomness, the balancedness and the correlation measure of order \( \ell \), respectively, for all monic polynomials of degree \( d \). In this article we focus on the local pseudorandomness, that is, we deal only with the first \( N < p^d \) monic polynomials of degree \( d \) (in the lexicographic order). The main motivation for doing this is to derive binary sequences and to analyze several measures of pseudorandomness for binary sequences: the balancedness, the well-distribution measure, the correlation measure of order \( \ell \), and the linear complexity profile. In particular, to obtain a lower bound on the linear complexity profile we need a local analog of (3). Although our results can be extended to any finite field of odd characteristic we focus on prime fields to avoid a more complicated notation. More precisely, let \( p > 2 \) be a prime and denote by \( \mathbb{F}_p \) the finite field of \( p \) elements which we identify with the set of integers \( \{0, 1, \ldots, p-1\} \) equipped with the usual arithmetic modulo \( p \). We order the monic polynomials over \( \mathbb{F}_p \) of degree \( d \geq 2 \) in the following way. For \( 0 \leq n < p^d \) put
\[ F_n(X) = X^d + n_{d-1}X^{d-1} + \cdots + n_1X + n_0 \]
if
\[ n = n_0 + n_1p + \cdots + n_{d-1}p^{d-1}, \quad 0 \leq n_0, n_1, \ldots, n_{d-1} < p. \]
We study finite binary sequences \( S_{p^d} = (s_0, \ldots, s_{p^d-1}) \in \{-1, +1\}^{p^d} \) with the property
\[ s_n = \lambda(F_n) = \mu(F_n), \quad F_n \text{ squarefree}. \] (4)
Our results will be independent of the choice of $s_n \in \{-1, +1\}$ for non-squarefree $F_n$.

First we prove the following local analog of (1) and (2) on the balancedness of the sequence $S_{p^d}$.

**Theorem 1.** For $d \geq 2$, $1 \leq N < p^d$, and $s_n$ satisfying (3) for all $n = 0, 1, \ldots, N-1$ such that $F_n$ is squarefree, we have

$$
\sum_{n=0}^{N-1} s_n = O\left(d(Np^{-1/2} + p^{1/2} \log p)\right)
$$

if $d$ is even

and

$$
O\left(d(Np^{-1/2} + p^{3/2} \log p)\right)
$$

if $d$ is odd.

Next, we study several pseudorandom properties of $S_{p^d}$. For a survey on pseudorandom sequences and their desirable properties we refer to \cite{17}.

For a given binary sequence

$$
E_N = (e_0, \ldots, e_{N-1}) \in \{-1, +1\}^N.
$$

Mauduit and Sárközy \cite{9} defined the well-distribution measure of $E_N$ 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 $a, b, t \in \mathbb{N}$ such that

$$
0 \leq a \leq a + (t-1)b < N,
$$

and the correlation measure of order $\ell$ of $E_N$ by

$$
C_\ell(E_N) = \max_{M, D} \left| \sum_{n=0}^{M-1} e_{n+d_1}e_{n+d_2}\cdots e_{n+d_\ell} \right|
$$

where the maximum is taken over all $D = (d_1, \ldots, d_\ell)$ and $M$ such that

$$
0 \leq d_1 < d_2 < \cdots < d_\ell \leq N - M.
$$

We will prove the following bounds on the well-distribution measure and the correlation measure of order $\ell$ for $S_{p^d}$.

**Theorem 2.** We have the following bound on the well-distribution measure:

$$
W(S_{p^d}) = O(dp^{d-1/2} \log p), \quad d \geq 2.
$$

**Theorem 3.** We have the following bound on the correlation measure of order $\ell$:

$$
C_\ell(S_{p^d}) = O(\ell^2 dp^{d-1/2} \log p), \quad d \geq 2.
$$
LÁSZLÓ MÉRAI — ARNE WINTERHOF

Theorem 3 allows us to derive a lower bound on the linear complexity of the binary sequence $S'_{p^d} = (s'_1, s'_2, \ldots, s'_{p^d})$ defined by the relation $s_n = (-1)^{s'_n}$.

For an integer $N \geq 1$ the $N$th linear complexity $L(r, N)$ of a sequence $r = (r_0, \ldots, r_{T-1})$ of length $T$ over the finite field $\mathbb{F}_2$ is the smallest positive integer $L$ such that there are constants $c_1, \ldots, c_L \in \mathbb{F}_2$ satisfying the linear recurrence relation

$$r_{n+L} = c_{L-1}r_{n+L-1} + \cdots + c_0 r_n, \quad \text{for } 0 \leq n < N - L.$$

If $r$ starts with $N - 1$ zeros, then we define

$$L(r, N) = 0 \quad \text{if } r_{N-1} = 0, \quad \text{and } \quad L(r, N) = N \quad \text{if } r_{N-1} = 1.$$

The sequence $(L(r, N))_{1 \leq N \leq T}$ is the linear complexity profile of $r$.

Brandstätter and Winterhof [1] proved a lower bound on the $N$th linear complexity $L(E'_N, N)$ of a sequence $E'_N = (e'_0, \ldots, e'_{N-1})$ over $\mathbb{F}_2$ terms of the correlation measure $C_\ell(E_N)$ of the finite sequence $E_N = (e_0, \ldots, e_{N-1}) \in \{-1, +1\}^N$ defined by $e_n = (-1)^{e'_n}$.

**Lemma 1.** Let $E'_N = (e'_0, \ldots, e'_{N-1})$ be a finite sequence over $\mathbb{F}_2$ of length $N$. Writing $e_n = (-1)^{e'_n}$ for $0 \leq n \leq N - 1$, we have

$$L(E'_N, N) \geq N - \max_{2 \leq \ell \leq L(e'_N, N)+1} C_\ell(E_N).$$

By Theorem 3 and Lemma 1 we immediately get the following lower bound.

**Corollary 2.** For fixed $d \geq 2$ and any $1 \leq N < p^d$ we have

$$L(S'_N, N) \gg \frac{N^{1/2}}{d^{1/2}p^{d/2-1/4}(\log p)^{1/2}}$$

for the sequence $S'_N = (s'_0, \ldots, s'_{N-1})$, where $s'_n$ ($0 \leq n < N$) is defined by $s_n = (-1)^{s'_n}$.

2. Proofs

As in [3] we start with Pellet’s formula, see [11],

$$\lambda(F) = \mu(F) = \left( \frac{D(F)}{p} \right) \quad \text{if } D(F) \neq 0,$$

where $\left( \frac{\cdot}{p} \right)$ denotes the Legendre symbol and $D(F)$ the discriminant of $F$. (See also Stickelberger [15] and Skolem [14] as well as [6, 16] for a short proof.)
Moreover, \((-1)^{d(d-1)/2} D(F_n)\) equals the following determinant of a \((2d - 1) \times (2d - 1)\) matrix,

\[
\begin{vmatrix}
1 & n_{d-1} & \cdots & n_1 & n_0 & 0 & \cdots & 0 \\
0 & 1 & n_{d-1} & \cdots & n_1 & n_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 1 & n_{d-1} & \cdots & n_1 & n_0 \\
d & (d-1)n_{d-1} & \cdots & n_1 & 0 & \cdots & 0 & \vdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & d & (d-1)n_{d-1} & \cdots & n_1 \\
0 & 0 & 0 & 0 & 0 & d & (d-1)n_{d-1} & \cdots & n_1 \\
\end{vmatrix}
\]

Note that

\[
D(F_n) = (-1)^{d+1} d^n n_0^{d-1} + (-1)^d (d-1)^{d-1} n_1^d + h(n_0, n_1, n - n_0 - n_1p),
\]

where \(h(X_0, X_1, X_2)\) is a polynomial over \(\mathbb{F}_p\) of relative degrees in \(X_0\) at most \(d - 2\) and in \(X_1\) at most \(d - 1\).

**Proof of Theorem** Put \(N - 1 = N_0 + N_1p + N_2p^2\) with \(0 \leq N_0, N_1 < p\). Then we have

\[
\left| \sum_{n=0}^{N-1} s_n \right| \leq S_1 + S_2 + S_3,
\]

where

\[
S_1 = \sum_{n_2=0}^{N_2-1} \sum_{n_0, n_1=0}^{p-1} s_{n_0 + n_1p + n_2p^2},
\]

\[
S_2 = \sum_{n_1=0}^{N_1-1} \sum_{n_0=0}^{p-1} s_{n_0 + n_1p + N_2p^2},
\]

\[
S_3 = \sum_{n_0=0}^{N_0} s_{n_0 + N_1p + N_2p^2}.
\]

In the first case \((d \text{ even})\), write

\[
s_{n_0 + n_1p + n_2p^2} = \left( \frac{D(F_{n_0 + n_1p + n_2p^2})}{p} \right) \text{ if } D(F_{n_0 + n_1p + n_2p^2}) \neq 0.
\]

Note that there are at most \(d - 1\) different \(n_0\) with \(0 \leq n_0 < p\) for any fixed \(n_1\) and \(n_2\) with \(D(F_{n_0 + n_1p + n_2p^2}) = 0\).
Since now $D(F_{n_0+n_1p+n_2p^2})$ has odd degree in $n_0$, for any pair $(n_1,n_2)$ the monic polynomial $f(X) = -d^{-d}D(F_{X+n_1p+n_2p^2})$ is not a square and we can apply the Weil bound (for complete character sums)

$$\left| \sum_{n \in \mathbb{F}_p} \left( a f(n) \right) \right| \leq (\deg(f) - 1)p^{1/2}, \quad a \neq 0,$$

(see for example [13, Theorem 2G] or [8, Theorem 5.41]) directly to estimate $S_1$ and $S_2$ and the standard method for reducing incomplete character sums to complete ones, see for example [7, Chapter 12] or [18, Theorem 2], to estimate $S_3$,

$$S_1 \leq \sum_{n_2=0}^{N_2-1} \sum_{n_1=0}^{p-1} \left( \sum_{n_0=0}^{p-1} \left( D(F_{n_0+n_1p+n_2p^2}) \right) \right) + d - 1 \leq N_2p((d-2)p^{1/2} + d - 1),$$

$$S_2 \leq \sum_{n_1=0}^{N_1-1} \left( \sum_{n_0=0}^{p-1} \left( D(F_{n_0+n_1p+N_2p^2}) \right) \right) + d - 1 \leq N_1((d-2)p^{1/2} + d - 1),$$

$$S_3 \leq \sum_{n_0=0}^{N_0} \left( D(F_{n_0+N_1p+N_2p^2}) \right) + d - 1 \leq (d - 1)p^{1/2} \log p + d - 1,$$

and hence the result since $N_1 + N_2p < N/p$. In the second case ($d$ odd) the sums over $n_0$ can be trivial but not the sums over $n_1$. Hence, we get

$$S_1 + S_2 + S_3 \leq N_2p((d-1)p^{1/2} + d) + (dp^{1/2} \log p + d)p + N_0$$

and the result follows, since $N_2p < N/p$. \hfill \square

**Proof of Theorem 2** We can assume without loss of generality, that $d < p^{1/2}$, since otherwise the theorem is trivial. Fix $a,b,t$ with $0 \leq a \leq a + (t - 1)b \leq p^d - 1$. If $t < p^{d-1} + 1$, then we use the trivial bound

$$\left| \sum_{j=0}^{t-1} s_{a+bj} \right| \leq t.$$
Now we assume \( t \geq p^{d-1} + 1 \) and thus \( b < p \). Put
\[
T = p \left\lfloor \frac{t}{p} \right\rfloor.
\]
Then we have \( t - T = O(p) \) and
\[
\sum_{j=0}^{T-1} s_{a+bj} = \sum_{j=0}^{T-1} s_{a+bj} + O(p).
\] (5)
For \( 0 \leq a \leq a + bj \leq p^d - 1 \) let
\[
a = a_0 + a_1 p + a_2 p^2, \quad 0 \leq a_0, a_1 < p, \quad 0 \leq a_2 < p^{d-2}
\]
and
\[
j = j_0 + j_1 p + j_2 p^2, \quad 0 \leq j_0, j_1 < p, \quad 0 \leq j_2 < p^{d-2}.
\]
Put
\[
w_0 = \left\lfloor \frac{a_0 + bj_0}{p} \right\rfloor \quad \text{and} \quad w_1 = \left\lfloor \frac{a_1 + bj_1 + w_0}{p} \right\rfloor.
\]
Then we have
\[
a + bj = z_0 + z_1 p + z_2 p^2, \quad 0 \leq z_0, z_1 < p, \quad 0 \leq z_2 < p^{d-2},
\]
with
\[
z_0 = a_0 + bj_0 - w_0 p, \quad z_1 = a_1 + bj_1 + w_0 - w_1 p, \quad z_2 = a_2 + bj_2 + w_1,
\]
and
\[
s_{a+bj} = \left( \frac{D(F_{z_0+z_1 p+z_2 p^2})}{p} \right) \quad \text{if} \quad D(F_{z_0+z_1 p+z_2 p^2}) \neq 0.
\]
Note that we have at most \((b + 1)\) possible choices for \( w_0 \) and for \( w_1 \) since \( 0 \leq w_0, w_1 \leq b \).
We define
\[
S_{w_0,w_1} = \left\{ a + jb : 0 \leq j < T, \left\lfloor \frac{a_0 + bj_0}{p} \right\rfloor = w_0, \left\lfloor \frac{a_1 + bj_1 + w_0}{p} \right\rfloor = w_1 \right\}
\]
and note that these sets define a partition of \( \{a + jb : 0 \leq j < T\} \). For each \((w_0, w_1)\) the set \( S_{w_0,w_1} \) is of the form
\[
S_{w_0,w_1} = \left\{ a_0 - w_0 p + bj_0 + (w_0 + a_1 - w_1 p + bj_1)p + (w_1 + a_2 + bj_2)p^2 : k_i \leq j_i < K_i, \quad i = 0, 1, 2 \right\},
\]
where \( k_i = k_i(w_0, w_1) \) and \( K_i = K_i(w_0, w_1) \) for \( i = 0, 1, 2 \) defined as
\[
k_0 = \max \left\{ 0, \left\lfloor \frac{w_0 p - a_0}{b} \right\rfloor \right\}, \quad K_0 = \min \left\{ p, \left\lfloor \frac{(w_0 + 1) p - a_0}{b} \right\rfloor \right\},
\]
\[ k_1 = \max \left\{ 0, \frac{w_1 p - a_0 - w_0}{b} \right\}, \quad K_1 = \min \left\{ p, \frac{(w_1 + 1)p - a_0 - w_0}{b} \right\}, \]
\[ k_2 = 0, \quad K_2 = \frac{T - 1}{p^2} - \left\lfloor \frac{w_1}{p} \right\rfloor. \]

We remark, that both \( K_0 - k_0 \) and \( K_1 - k_1 \) are \( O(p/b) \). If \( d \) is even, the absolute value of (5) is at most
\[
\sum_{w_0, w_1} K_1(w_0, w_1) \sum_{j_1 = k_1(w_0, w_1)} K_2(w_0, w_1) \sum_{j_2 = k_2(w_0, w_1)} \left| K_0(w_0, w_1) \left( \frac{D(F_{a_0 - w_0 p + b j_0 + (w_0 + a_1 - w_1 p + b j_1)p + (w_1 + a_2 + b j_2)p^2})}{p} \right) \right| \tag{6}
\]

As before, \( D(F_X + (w_0 + a_1 - w_1 p + b j_1)p + (w_1 + a_2 + b j_2)p^2) \in \mathbb{F}_p[X] \) has odd degree, thus we can apply the Weil-bound after using the standard technique to reduce incomplete sums to complete ones and get, that (6) is
\[ O \left( \frac{b^2 p T}{b^2 p^2} d p^{1/2} \log p \right) = O \left( b T d p^{-1/2} \log p \right). \]

Since \( b T = O \left( p^d \right) \) we get the result for even \( d \). For odd \( d \), the proof is similar. □

The proof of Theorem 3 is based on the following form of [3, Proposition 2.1].

**Lemma 3.** For given \( 0 \leq d_1 < d_2 < \cdots < d_\ell < p^d \) let \( G \subset \{1, 2, \ldots, p^{d-1}\} \) the set of integers \( a \) such that \( D(F_{X + a p + d_1} \in \mathbb{F}_p[X] \) is squarefree and coprime to \( D(F_{X + a p + d_i}) \in \mathbb{F}_p[X] \) for \( i = 2, 3, \ldots, \ell \). Then, for the complement of \( G \) we have
\[ |G^c| = |\{1, 2, \ldots, p^{d-1}\} \setminus G| \leq 3 \ell d^2 p^{d-2}. \]

**Proof of Theorem 3** We can assume without loss of generality, that \( d < p^{1/2} \), since otherwise the theorem is trivial.

Let \( M \in \mathbb{N} \) and let \( 0 \leq d_1 < d_2 < \cdots < d_\ell < p^d - M \) be integers. If \( M \leq p^{d-1} \) we use the trivial bound
\[ \sum_{n=0}^{M-1} s_{n+d_1} s_{n+d_2} \cdots s_{n+d_\ell} \leq M. \]

Now, we assume \( M \geq p^{d-1} + 1 \). Let
\[ T = p \left\lfloor \frac{M}{p^d} \right\rfloor. \]
PSEUDORANDOMNESS OF THE LIOUVILLE FUNCTION OF POLYNOMIALS

Then we have $M - T = O(p)$ and
\[
\left| \sum_{n=0}^{M-1} s_{n+d_1} s_{n+d_2} \ldots s_{n+d_\ell} \right| = \left| \sum_{n=0}^{T-1} s_{n+d_1} s_{n+d_2} \ldots s_{n+d_\ell} \right| + O(p).
\]

As it has already been written
\[
n = n_0 + n_1 p, \quad 0 \leq n_0 < p, \quad 0 \leq n_1 < p^{d-1}
\]
and
\[
d_i = d_{i,0} + d_{i,1} p, \quad 0 \leq d_{i,0} < p, \quad 0 \leq d_{i,1} < p^{d-1}, \quad i = 1, 2, \ldots, \ell.
\]
If
\[
w_i = \left\lfloor \frac{n_0 + d_{i,0}}{p} \right\rfloor \in \{0, 1\}, \quad i = 1, 2, \ldots, \ell,
\]
then
\[
n + d_i = z_{i,0} + z_{i,1} p, \quad 0 \leq z_{i,0} < p, \quad 0 \leq z_{i,1} < p^{d-1}, \quad i = 1, 2, \ldots, \ell,
\]
with
\[
z_{i,0} = n_0 + d_{i,0} - w_i p, \quad z_{i,1} = n_1 + d_{i,1} + w_i, \quad i = 1, 2, \ldots, \ell,
\]
and
\[
s_{n+d_i} = \left( \frac{D(F_{z_{i,0}+z_{i,1}p})}{p} \right) \quad \text{if} \quad D(F_{z_{i,0}+z_{i,1}p}) \neq 0, \quad i = 1, 2, \ldots, \ell.
\]

For $(w_1, w_2, \ldots, w_\ell) \in \{0, 1\}^\ell$ write
\[
S_{w_i, d_i} = \left\{ n : 0 \leq n < T, \left\lfloor \frac{n_0 + d_{i,0}}{p} \right\rfloor = w_i \right\}
\]
\[
= \{ j_0 + j_1 p : k_{i,0} \leq j_0 < K_{i,0}, \quad k_{i,1} \leq j_1 < K_{i,1} \},
\]
where
\[
k_{i,0} = k_{i,0}(w_i) = \max \{0, pw_i - d_{i,0} \}, \quad K_{i,0} = K_{i,0}(w_i) = \min \{p, p(w_i + 1) - d_{i,0} \}
\]
and
\[
k_{i,1} = k_{i,1}(w_i) = 0, \quad K_{i,1} = K_{i,1}(w_i) = T/p.
\]
LÁSZLÓ MÉRAI — ARNE WINTERHOF

As \((w_1, w_2, \ldots, w_\ell)\) runs in \(\{0, 1\}^\ell\), the intersections \(S_{w_1,d_1} \cap \ldots \cap S_{w_\ell,d_\ell}\) are a partition of integers \(0 \leq n < T\). However, it can be shown in the same way as in [10], that there are at most \(\ell + 1\) non-empty intersections. More precisely, let us reorder the integers \(d_1 < d_2 < \ldots < d_\ell\) and the carries \((w_1, w_2, \ldots, w_\ell)\) by the first components of

\[
d_i : \{d_1, d_2, \ldots, d_\ell\} = \{d'_1, d'_2, \ldots, d'_\ell\},
\]
\[
\{w_1, w_2, \ldots, w_\ell\} = \{w'_1, w'_2, \ldots, w'_\ell\},
\]
\[
d'_{1,0} \leq d'_{2,0} \leq \cdots \leq d'_{\ell,0}.
\]

Then writing \(d'_{0,0} = 0\) and \(d'_{0,\ell+1} = p\) we have

\[
\left| \sum_{n=0}^{T-1} s_{n+d_1} s_{n+d_2} \cdots s_{n+d_\ell} \right| \leq \sum_{(w_1, w_2, \ldots, w_\ell) \in \{0, 1\}^\ell} \sum_{n \in S_{w_1,d_1} \cap \ldots \cap S_{w_\ell,d_\ell}} s_{n+d_1} s_{n+d_2} \cdots s_{n+d_\ell}
\]
\[
\leq \sum_{i=1}^{\ell+1} \sum_{j_1=0}^{T/p-1} \sum_{j_0=p-d'_{i,0}-1}^{p-d'_{i,0}} s_{j_0+j_1+p+d_1} s_{j_0+j_1+p+d_2} \cdots s_{j_0+j_1+p+d_\ell}
\]
\[
\leq \sum_{i=1}^{\ell+1} \sum_{j_1=0}^{T/p-1} \left( \sum_{j_0=p-d'_{i,0}-1}^{p-d'_{i,0}-1} \frac{D(F_{j_0+j_1+p+d_1}) D(F_{j_0+j_1+p+d_2}) \cdots D(F_{j_0+j_1+p+d_\ell})}{p} \right) + \ell (d - 1)
\]

(7)

For a fixed \(i\), if \(j_1 \in G\), then the innermost sum is non-trivial. On the other hand we estimate the inner sum of (7) trivially by \(p\) if \(j_1 \notin G\). Then we get that (7) is less than

\[
(\ell + 1) \left( 3 \ell d^2 p^{d-1} + \frac{T}{p} (\ell (d - 1) p^{1/2} \log p + \ell (d - 1)) \right) = O(\ell^2 dp^{d-\frac{1}{2}} \log p)
\]

and the result follows. □
PSEUDORANDOMNESS OF THE LIOUVILLE FUNCTION OF POLYNOMIALS

Final Remarks

• Cassaigne, Ferenzi, Mauduit, Rivat and Sárközy \cite{4, 5} studied the pseudorandomness of the Liouville function for integers.

• Our results as well as the results of \cite{3} are based on Pellet’s result which is not true for characteristic 2. Finding analog results for characteristic 2 would be very interesting.

• In this paper as well as in \cite{3} \( d \) is fixed and \( p \) has to be large with respect to \( d \) to get nontrivial bounds. It would be interesting to study the same problems if \( p \) is fixed and \( d \) goes to infinity.

Acknowledgements. We wish to thank Christian Mauduit for pointing to this problem during a pleasant visit of the second author to Marseille. He also wishes to thank for the hospitality and financial support.

Finally, the authors want to thank the referee for a careful reading and very useful comments.

REFERENCES


