DE GRUYTER
OPEN

uniform distribution theory

DOI: 10.1515/udt-2016–0004
Unif. Distrib. Theory **11** (2016), no.1, 47–58

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 λ-function and the Möbius μ-function for integers, Carlitz [2] introduced the mappings λ and μ 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

$$\mu(F) = \begin{cases} \lambda(F) & \text{if } F \text{ is squarefree,} \\ 0 & \text{otherwise,} \end{cases} \qquad F \in \mathbb{F}_q[X].$$

2010 Mathematics Subject Classification: 11K45, 11T06, 11T24, 11T71.
Keywords: polynomials, finite fields, irreducible factors, pseudorandom sequence, balancedness, well-distribution, correlation measure, linear complexity, polynomial Liouville function, polynomial Möbius function.
The authors are partially supported by the Austrian Science Fund FWF Project F5511-N26 which is part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

Carlitz [2] proved

$$\sum_{\deg F=d} \lambda(F) = (-1)^d q^{\lfloor (d+1)/2 \rfloor} \tag{1}$$

and

$$\sum_{\deg F=d} \mu(F) = \begin{cases} 0 & \text{if } d \geq 2, \\ -q & \text{if } d = 1, \end{cases} \tag{2}$$

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 $D_1, \dots, D_\ell \in \mathbb{F}_q[X]$ of degree smaller than d, q odd, and $(\epsilon_1, \dots, \epsilon_\ell) \in \{0,1\}^\ell \setminus (0, \dots, 0)$, Carmon and Rudnick [3, Theorem 1.1] have recently proved that

$$\sum_{\deg F=d} \mu(F+D_1)^{\epsilon_1} \cdots \mu(F+D_\ell)^{\epsilon_\ell} = O\big(\ell d q^{d-1/2}\big), \quad d \geq 2. \tag{3}$$

(For $d = 1$ the sum trivially equals $(-1)^{\sum_{j=1}^{\ell} \epsilon_j} q$.) 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 λ instead of μ 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 ℓ, 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 ℓ, 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 $\{0, 1, \dots, p-1\}$ 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

$$F_n(X) = X^d + n_{d-1}X^{d-1} + \cdots + n_1 X + n_0$$

if

$$n = n_0 + n_1 p + \cdots + n_{d-1} p^{d-1}, \quad 0 \leq n_0, n_1, \dots, n_{d-1} < p.$$

We study finite binary sequences $S_{p^d} = (s_0, \dots, s_{p^d-1}) \in \{-1,+1\}^{p^d}$ with the property

$$s_n = \lambda(F_n) = \mu(F_n), \quad F_n \text{ squarefree}. \tag{4}$$

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 (4) for all $n = 0,1,\dots,N-1$ such that F_n is squarefree, we have*

$$\sum_{n=0}^{N-1} s_n = O\Big(d\big(Np^{-1/2} + p^{1/2}\log p\big)\Big) \quad \text{if } d \text{ is even}$$

and

$$O\Big(d\big(Np^{-1/2} + p^{3/2}\log p\big)\Big) \quad \text{if } d \text{ is odd.}$$

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

For a given binary sequence

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

Mauduit and Sárközy [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 ℓ* of E_N by

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

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

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

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

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

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

Theorem 3. *We have the following bound on the correlation measure of order ℓ:*

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

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 *Nth 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 Nth 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,

$$\begin{vmatrix} 1 & n_{d-1} & \cdots & n_1 & n_0 & 0 & \cdots & 0 \\ 0 & 1 & n_{d-1} & \cdots & n_1 & n_0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & 1 & n_{d-1} & \cdots & n_1 & n_0 \\ d & (d-1)n_{d-1} & \cdots & n_1 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & d & (d-1)n_{d-1} & \cdots & n_1 & 0 \\ 0 & 0 & 0 & 0 & d & (d-1)n_{d-1} & \cdots & n_1 \end{vmatrix}.$$

Note that

$$D(F_n) = (-1)^{d+1}d^d n_0^{d-1} + (-1)^d (d-1)^{d-1} n_1^d + h(n_0, n_1, n - n_0 - n_1 p),$$

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 $d-1$.

P r o o f o f T h e o r e m 1. Put $N-1 = N_0 + N_1 p + N_2 p^2$ with $0 \le N_0, N_1 < p$. Then we have

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

where

$$S_1 = \sum_{n_2=0}^{N_2-1}\left|\sum_{n_0,n_1=0}^{p-1} s_{n_0+n_1p+n_2p^2}\right|,$$

$$S_2 = \left|\sum_{n_1=0}^{N_1-1}\sum_{n_0=0}^{p-1} s_{n_0+n_1p+N_2p^2}\right|,$$

$$S_3 = \left|\sum_{n_0=0}^{N_0} s_{n_0+N_1p+N_2p^2}\right|.$$

In the first case (d even), write

$$s_{n_0+n_1p+n_2p^2} = \left(\frac{D(F_{n_0+n_1p+n_2p^2})}{p}\right) \quad \text{if } D(F_{n_0+n_1p+n_2p^2}) \ne 0.$$

Note that there are at most $d-1$ different n_0 with $0 \le n_0 < p$ 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)

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

(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,

$$\begin{aligned}
S_1 &\leq \sum_{n_2=0}^{N_2-1}\sum_{n_1=0}^{p-1}\left(\left|\sum_{n_0=0}^{p-1}\left(\frac{D(F_{n_0+n_1p+n_2p^2})}{p}\right)\right| + d - 1\right)\\
&\leq N_2p\big((d-2)p^{1/2} + d - 1\big),\\
S_2 &\leq \sum_{n_1=0}^{N_1-1}\left(\left|\sum_{n_0=0}^{p-1}\left(\frac{D(F_{n_0+n_1p+N_2p^2})}{p}\right)\right| + d - 1\right)\\
&\leq N_1\big((d-2)p^{1/2} + d - 1\big),\\
S_3 &\leq \left|\sum_{n_0=0}^{N_0}\left(\frac{D(F_{n_0+N_1p+N_2p^2})}{p}\right)\right| + d - 1\\
&\leq (d-1)p^{1/2}\log p + d - 1,
\end{aligned}$$

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

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

and the result follows, since $N_2p < N/p$. □

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

$$\sum_{j=0}^{t-1} s_{a+bj} = \sum_{j=0}^{T-1} s_{a+bj} + O(p). \tag{5}$$

For $0 \leq a \leq a+bj \leq p^d - 1$ let

$$a = a_0 + a_1 p + a_2 p^2, \quad 0 \leq a_0,\ a_1 < p,\ 0 \leq a_2 < p^{d-2}$$

and

$$j = j_0 + j_1 p + j_2 p^2, \quad 0 \leq j_0,\ j_1 < p,\ 0 \leq j_2 < p^{d-2}.$$

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

$$a + bj = z_0 + z_1 p + z_2 p^2, \quad 0 \leq z_0, z_1 < p,\ 0 \leq z_2 < p^{d-2},$$

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

$$s_{a+bj} = \left(\frac{D(F_{z_0+z_1p+z_2p^2})}{p}\right) \quad \text{if } D\big(F_{z_0+z_1p+z_2p^2}\big) \neq 0.$$

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

$$S_{w_0,w_1} = \Big\{ a_0 - w_0 p + bj_0 + \big(w_0 + a_1 - w_1 p + bj_1\big)p + \big(w_1 + a_2 + bj_2\big)p^2 : \\ k_i \leq j_i < K_i,\ i = 0,1,2 \Big\},$$

where $k_i = k_i(w_0, w_1)$ and $K_i = K_i(w_0, w_1)$ $(i = 0,1,2)$ defined as

$$k_0 = \max\left\{0, \left\lceil \frac{w_0 p - a_0}{b} \right\rceil \right\}, \quad K_0 = \min\left\{p, \left\lceil \frac{(w_0+1)p - a_0}{b} \right\rceil \right\},$$

$$k_1 = \max\left\{0, \left\lfloor \frac{w_1 p - a_0 - w_0}{b} \right\rfloor\right\}, \quad K_1 = \min\left\{p, \left\lfloor \frac{(w_1+1)p - a_0 - w_0}{b} \right\rfloor\right\},$$

$$k_2 = 0, \quad K_2 = \frac{T-1}{p^2} - \left\lceil \frac{w_1}{p} \right\rceil.$$

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

$$\sum_{w_0,w_1} \sum_{j_1=k_1(w_0,w_1)}^{K_1(w_0,w_1)} \sum_{j_2=k_2(w_0,w_1)}^{K_2(w_0,w_1)} \left| \sum_{j_0=k_0(w_0,w_1)}^{K_0(w_0,w_1)} \left(\frac{D(F_{a_0-w_0p+bj_0+(w_0+a_1-w_1p+bj_1)p+(w_1+a_2+bj_2)p^2})}{p} \right) \right| \tag{6}$$

As before,

$$D(F_{X+(w_0+a_1-w_1p+bj_1)p+(w_1+a_2+bj_2)p^2}) \in \mathbb{F}_p[X]$$

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

$$O\left(b^2 \frac{p}{b} \frac{T}{p^2} d p^{1/2} \log p\right) = O\left(bTdp^{-1/2} \log p\right).$$

Since $bT = O\left(p^d\right)$ 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 $0 \le d_1 < d_2 < \cdots < d_\ell < p^d$ let $G \subset \{1, 2, \ldots, p^{d-1}\}$ the set of integers a such that $D(F_{X+ap+d_1}) \in \mathbb{F}_p[X]$ is squarefree and coprime to $D(F_{X+ap+d_i}) \in \mathbb{F}_p[X]$ for $i = 2, 3, \ldots, \ell$. Then, for the complement of G we have*

$$|G^c| = \left|\{1, 2, \ldots, p^{d-1}\} \setminus G\right| \le 3\ell d^2 p^{d-2}.$$

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 $0 \le d_1 < d_2 < \cdots < d_\ell < p^d - M$ be integers. If $M \le p^{d-1}$ we use the trivial bound

$$\left| \sum_{n=0}^{M-1} s_{n+d_1} s_{n+d_2} \ldots s_{n+d_\ell} \right| \le M.$$

Now, we assume $M \ge p^{d-1} + 1$. Let

$$T = p \left\lfloor \frac{M}{p} \right\rfloor.$$

Then we have $M-T=O(p)$ and

$$\left|\sum_{n=0}^{M-1} s_{n+d_1}s_{n+d_2}\dots s_{n+d_\ell}\right| = \left|\sum_{n=0}^{T-1} s_{n+d_1}s_{n+d_2}\dots s_{n+d_\ell}\right| + O(p).$$

As it has already been written

$$n = n_0 + n_1 p, \quad 0 \le n_0 < p, \quad 0 \le n_1 < p^{d-1}$$

and

$$d_i = d_{i,0} + d_{i,1}p, \quad 0 \le d_{i,0} < p, \quad 0 \le d_{i,1} < p^{d-1}, \quad i = 1,2,\dots,\ell.$$

If

$$w_i = \left\lfloor \frac{n_0 + d_{i,0}}{p} \right\rfloor \in \{0,1\}, \quad i = 1,2,\dots,\ell,$$

then

$$n + d_i = z_{i,0} + z_{i,1}p, \quad 0 \le z_{i,0} < p, \quad 0 \le z_{i,1} < p^{d-1}, \quad i = 1,2,\dots,\ell,$$

with

$$\begin{aligned} z_{i,0} &= n_0 + d_{i,0} - w_i p, \\ z_{i,1} &= n_1 + d_{i,1} + w_i, \end{aligned} \qquad i = 1,2,\dots,\ell,$$

and

$$s_{n+d_i} = \left(\frac{D(F_{z_{i,0}+z_{i,1}p})}{p}\right) \quad \text{if } D(F_{z_{i,0}+z_{i,1}p}) \ne 0, \quad i = 1,2,\dots,\ell.$$

For $(w_1, w_2, \dots, w_\ell) \in \{0,1\}^\ell$ write

$$\begin{aligned} S_{w_i,d_i} &= \left\{ n : 0 \le n < T, \left\lfloor \frac{n_0 + d_{i,0}}{p} \right\rfloor = w_i \right\} \\ &= \left\{ j_0 + j_1 p : k_{i,0} \le j_0 < K_{i,0},\ k_{i,1} \le j_1 < K_{i,1} \right\}, \end{aligned}$$

where

$$\begin{aligned} k_{i,0} &= k_{i,0}(w_i) = \max\{0, pw_i - d_{i,0}\}, \\ K_{i,0} &= K_{i,0}(w_i) = \min\{p, p(w_i+1) - d_{i,0}\} \end{aligned}$$

and

$$\begin{aligned} k_{i,1} &= k_{i,1}(w_i) = 0, \\ K_{i,1} &= K_{i,1}(w_i) = T/p. \end{aligned}$$

As $(w_1, w_2, \dots, w_\ell)$ runs in $\{0,1\}^\ell$, the intersections $S_{w_1,d_1} \cap \dots \cap S_{w_\ell,d_\ell}$ are a partition of integers $0 \le n < T$. 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 $d_1 < d_2 < \dots < d_\ell$ and the carries $(w_1, w_2, \dots, w_\ell)$ by the first components of

$$\begin{aligned} d_i \;:\; \{\, d_1,\, d_2, \dots, d_\ell\} &= \{\, d_1',\, d_2', \dots,\, d_\ell'\}, \\ \{w_1, w_2, \dots, w_\ell\} &= \{w_1', w_2', \dots, w_\ell'\}, \\ d_{1,0}' \le\, d_{2,0}' &\le \dots \le d_{\ell,0}'. \end{aligned}$$

Then writing $d_{0,0}' = 0$ and $d_{0,\ell+1}' = p$ we have

$$\begin{aligned} &\left|\sum_{n=0}^{T-1} s_{n+d_1} s_{n+d_2} \dots s_{n+d_\ell}\right| \\ &\le \sum_{(w_1,w_2,\dots,w_\ell)\in\{0,1\}^\ell} \left| \sum_{n\in S_{w_1,d_1}\cap\dots\cap S_{w_\ell,d_\ell}} s_{n+d_1} s_{n+d_2} \dots s_{n+d_\ell}\right| \\ &\le \sum_{i=1}^{\ell+1} \sum_{j_1=0}^{T/p-1} \left| \sum_{j_0=p-d_{i,0}'-1}^{p-d_{i-1,0}'} s_{j_0+j_1p+d_1} s_{j_0+j_1p+d_2} \dots s_{j_0+j_1p+d_\ell}\right| \\ &\le \sum_{i=1}^{\ell+1} \sum_{j_1=0}^{T/p-1} \\ &\left(\left| \sum_{j_0=p-d_{i,0}'}^{p-d_{i-1,0}'-1} \left(\frac{D(F_{j_0+j_1p+d_1}) D(F_{j_0+j_1p+d_2}) \cdots D(F_{j_0+j_1p+d_\ell})}{p}\right)\right| + \ell(d-1)\right) \qquad (7) \end{aligned}$$

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

$$(\ell+1)\Big(3\ell d^2 p^{d-1} + \tfrac{T}{p}\big(\ell(d-1)p^{1/2}\log p + \ell(d-1)\big)\Big) = O\big(\ell^2 d p^{d-\frac{1}{2}} \log p\big)$$

and the result follows. $\square$

Final Remarks

- Cassaigne, Ferenzi, Mauduit, Rivat and Sárközy [4, 5] studied the pseudorandomness of the Liouville function for integers.
- Our results as well as the results of [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 [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

[1] BRANDSTÄTTER, N.—WINTERHOF, A.: *Linear complexity profile of binary sequences with small correlation measure*, Period. Math. Hungar. **52** (2006), no. 2, 1–8.

[2] CARLITZ, L.: *The arithmetic of polynomials in a Galois field*, Amer. J. Math. **54** (1932), no. 1, 39-50.

[3] CARMON, D.—RUDNICK, Z.: *The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field*, Q. J. Math. **65** (2014), no. 1, 53–61.

[4] CASSAIGNE J.—FERENCZI, S.—MAUDUIT, C.—RIVAT, J.—SÁRKÖZY, A.: *On finite pseudorandom binary sequences. III. The Liouville function. I*, Acta Arith. **87** (1999), no. 4, 367–390.

[5] CASSAIGNE J.—FERENCZI, S.—MAUDUIT, C.—RIVAT, J.—SÁRKÖZY, A.: *On finite pseudorandom binary sequences. IV. The Liouville function. II*, Acta Arith. **95** (2000), no. 4, 343–359.

[6] CONRAD, K.: *Irreducible values of polynomials: a non-analogy*, Number fields and function fields-two parallel worlds, Progr. Math. Vol. 239, Birkhäuser Boston, Boston, MA, 2005. pp. 71–85.

[7] IWANIEC, H.—KOWALSKI, E.: *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ., Vol. 53, Amer. Math. Soc., Providence, RI, 2004.

[8] LIDL, R.—NIEDERREITER, H.: *Finite fields* (Second ed.), Encyclopedia of Mathematics and its Applications. Vol. 20, Cambridge University Press, Cambridge, 1997.

[9] MAUDUIT, C.—SÁRKÖZY, A.: *On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), no. 4, 365–377.

[10] MÉRAI, L.—YAYLA, O.: *Improving results on the pseudorandomness of sequences generated via the additive order*, Discrete Math. **338** (2015), no. 11, 2020–2025.

[11] PELLET, A. E.: *Sur la décomposition dune fonction entiére en facteurs irréductibles suivant un module premier*, Comptes Rendus de l'Académie des Sciences Paris **86** (1878), 1071–1072.

[12] ROSEN, M.: *Number Theory in Function Fields*, Graduate Texts in Mathematics, Vol. 210. Springer-Verlag, New York, 2002.

[13] SCHMIDT, W. M.: *Equations over finite fields: An Elementary Approach* (Second ed.), Kendrick Press, Heber City, UT, 2004.

[14] SKOLEM, T.: *On a certain connection between the discriminant of a polynomial and the umber of its irreducible factors* mod$p$, Norsk. Mat. Tidsskr. **34** (1952), 81–85.

[15] STICKELBERGER, L.: *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper* Verh. 1. Internat. Math.-Kongress. Zürich, 1897, Teubner, Leipzig, 1898, 182–193.

[16] SWAN, R. G.: *Factorization of polynomials over finite fields* Pacific J. Math. **12** (1962), 1099–1106.

[17] TOPUZOĞLU, A.— WINTERHOF, A.: *Pseudorandom sequences* Topics in Geometry, Coding Theory and Cryptography, Algebr. Appl., Vol. 6, Springer, Dordrecht, 2007, pp. 135–166.

[18] WINTERHOF, A.: *Some estimates for character sums and applications*, Des. Codes Cryptogr. **22** (2001), no. 2, 123–131.

Received April 27, 2015
Accepted August 31, 2015

László Mérai
Arne Winterhof
Johann Radon Institute for Comput.
and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69
4040 Linz,
AUSTRIA
E-mail: merai@cs.elte.hu
arne.winterhof@oeaw.ac.at