DISTRIBUTION OF SHORT SUBSEQUENCES OF INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS MODULO 2^t

LÁSZLÓ MÉRAI AND IGOR E. SHPARLINSKI

Abstract. In this paper we study the distribution of very short sequences of inversive congruential pseudorandom numbers modulo 2^t. We derive a new bound on exponential sums with such sequences and use it to estimate their discrepancy. The technique we use is based on the method of N. M. Korobov (1972) of estimating double Weyl sums and a fully explicit form of the Vinogradov mean value theorem due to K. Ford (2002), which has never been used in this area and is very likely to find further applications.

1. Introduction

1.1. **Background on the Möbius tranformation.** Let $t \geqslant 3$ be an integer and write $\mathcal{U}_t = \mathcal{R}_t^*$ for the group of units of the residue ring $\mathcal{R}_t = \mathbb{Z}/2^t\mathbb{Z}$ modulo 2^t. Then $\#\mathcal{U}_t = 2^{t-1}$. It is often be convenient to identify elements of $\mathcal{R}_t$ with the corresponding elements of the least residue system modulo 2^t.

We fix a matrix

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{R}_t)$$

with

$$M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \bmod 2. \tag{1.1}$$

We then consider sequences generated by iterations of the *Möbius tranformation*

$$M: \ x \mapsto \frac{m_{11}x + m_{12}}{m_{21}x + m_{22}} \tag{1.2}$$

which, under the condition (1.1), is always defined over $\mathcal{U}_t$, that is, $M : \mathcal{U}_t \to \mathcal{U}_t$.

2010 *Mathematics Subject Classification.* 11K38, 11K45, 11L07.

Key words and phrases. Inversive congruential pseudorandom numbers, prime powers, exponential sums, Vinogradov mean value theorem.

That is for $u_0 \in \mathcal{R}_t$ we consider the trajectory

$$u_n = M(u_{n-1}) = M^n(u_0), \qquad n = 1, 2, \ldots, \tag{1.3}$$

generated by iterations of the Möbius tranformation (1.2) associated with M.

Assume that the characteristic polynomial of M has two *distinct* eigenvalues ϑ_1 and ϑ_2 from the algebraic closure $\overline{\mathbb{Q}}_2$ of the field of 2-adic fractions $\mathbb{Q}_2$.

It is not difficult to prove by induction on n that there is an explicit representation of the form

$$u_n = \frac{\gamma_{11}\vartheta_1^n + \gamma_{12}\vartheta_2^n}{\gamma_{21}\vartheta_1^n + \gamma_{22}\vartheta_2^n} \tag{1.4}$$

with some coefficients $\gamma_{ij} \in \overline{\mathbb{Q}}_2$, $i, j = 1, 2$.

Here we consider the split case when the eigenvalues $\vartheta_1, \vartheta_2 \in \mathbb{Z}_2$ are 2-adic integers, in which case, interpolating, we also have $\gamma_{ij} \in \mathbb{Z}_2$, $i, j = 1, 2$.

It is easy to see that in this case we can assume that

$$\gamma_{21} \equiv 1 \bmod 2 \qquad \text{and} \qquad \gamma_{22} \equiv 0 \bmod 2.$$

Then, defining $g \in \mathcal{U}_t$ by the equation

$$g = \vartheta_1/\vartheta_2$$

we have $g \in \mathcal{R}_t$ (recall that M is invertible in $\mathcal{R}_2$), thus the sequence generated by (1.3), the representation (1.4) has the form

$$u_n = \frac{a}{g^n - b} + c \tag{1.5}$$

with some coefficients $a, b, c \in \mathcal{R}_t$. Furthermore, it is also easy to see that

$$b \equiv 0 \bmod 2.$$

1.2. **Motivation.** The sequences (1.3) are interesting in their own rights but they have also been used as a source of pseudorandom number generation where this sequence is known as the *inversive generator*, for example, see [4] for the period length and [10] for distributional properties.

More precisely, let τ be the multiplicative order of g modulo 2^t. Then (u_n) is a periodic sequence with period length τ, provided that a is odd.

Niederreiter and Winterhof [10], extending the results of [9] from odd prime powers to powers of 2, obtained nontrivial results for segments of these sequences of length N satisfying

$$\tau \geqslant N \geqslant 2^{(1/2+\eta)t} \tag{1.6}$$

for any fixed $\eta > 0$ and sufficiently large t.

Here using very different techniques we significantly reduce the range (1.6) and obtain results which are nontrivial for much shorter segments, namely, for

$$\tau \geqslant N \geqslant 2^{ct^{2/3}} \tag{1.7}$$

for some absolute constant $c > 0$.

We also consider this as an opportunity to introduce new techniques into the area of pseudorandom number generation which we believe may have more applications and lead to new advances.

1.3. **Our results.**

Here we establish upper bounds for the exponential sums

$$S_h(L,N) = \sum_{n=L}^{L+N-1} \mathbf{e}\left(hu_n/2^t\right), \qquad 1 \leqslant N \leqslant \tau,$$

where, as usual, we denote $\mathbf{e}(z) = \exp(2\pi i z)$ and, as before, τ is the multiplicative order of g modulo 2^t.

Using the method of Korobov [8] together with the use of the Vinogradov mean value theorem in the explicit form given by Ford [6], we can estimate $S_h(L,N)$ for the values N in the range (1.7).

Throughout the paper we always use the parameter

$$\rho = \frac{\log N}{t} \tag{1.8}$$

which controls the size of N relative to the modulus 2^t on a logarithmic scale.

Theorem 1.1. *Let* $\gcd(g,2) = \gcd(a,2) = 1$ *and write*

$$g^2 = 1 + w_\beta 2^\beta, \quad \gcd(w_\beta, 2) = 1.$$

Then for $2^{8\beta} < N \leqslant \tau$ *we have*

$$|S_h(L,N)| \leqslant cN^{1-\eta\rho^2}$$

where ρ *is given by* (1.8), *for some absolute constants* $c, \eta > 0$ *uniformly over all integers* h *with* $\gcd(h,2) = 1$.

From a sequence (u_n) defined by (1.5) we derive the *inversive congruential pseudorandom numbers with modulus* 2^t:

$$u_L/2^t, u_{L+1}/2^t, \ldots, u_{L+N-1}/2^t \in [0,1).$$

The *discrepancy* $D(L,N)$ of these numbers is defined by

$$D(L,N) = \sup_{J \subset [0,1)} \left| \frac{A(J,N)}{N} - |J| \right|,$$

where the supremum is taken over all subintervals J of $[0,1)$, $A(N,J)$ is the number of point $u_n/2^t$ in J for $L \leqslant n < L+N$, and $|J|$ is the length of J. The *Erdős–Turán inequality* (see [5, Theorem 1.21]) allows us to give an upper bound on the discrepancy $D(L,N)$ in terms of $S_h(L,N)$.

Theorem 1.2. *Let (u_n) be as in Theorem 1.1 and assume that $2^{32\beta} < N \leqslant \tau$. Then we have*

$$D(L,N) \leqslant c_0 N^{-\eta_0 \rho^2}$$

where ρ is given by (1.8), for some constants $c_0, \eta_0 > 0$.

Writing

$$N^{-\rho^2} = \exp\left(-\frac{(\log N)^3}{t^2}\right)$$

we see that Theorems 1.1 and 1.2 are nontrivial in the range (1.7).

2. Preparation

2.1. **Notation.** We recall that the notations $U \ll V$, and $V \gg U$ are equivalent to the statement that the inequality $|U| \leqslant cV$ holds with some absolute constant $c > 0$.

We use the notation v_2 to the 2-adic valuation, that is, for non-zero integers $a \in \mathbb{Z}$ we let $\mathrm{v}_2(a) = k$ if 2^k is the highest power of 2 which divides a, and $\mathrm{v}_2(a/b) = \mathrm{v}_2(a) - \mathrm{v}_2(b)$ for $a, b \neq 0$.

2.2. **Multiplicative order of integers.** The following assertion describes the order of elements modulo powers of 2.

Lemma 2.1. *Let $g \neq \pm 1$ be an odd integer and write*

$$g^2 = 1 + w_\beta 2^\beta, \quad \gcd(w_\beta, 2) = 1.$$

Then for $s \geqslant \beta$ the multiplicative order τ_s of g modulo 2^s is $\tau_s = 2^{s-\beta+1}$ and

$$g^{\tau_s} = 1 + w_s 2^s, \quad \gcd(w_s, 2) = 1. \tag{2.1}$$

Proof. First we note that $\beta \geqslant 2$. We prove (2.1) by induction of s.

Clearly, we have (2.1) with $s = \beta$. Furthermore, if (2.1) holds for some $s \geqslant \beta$, then by squaring it we get

$$g^{2\tau_s} = 1 + w_s 2^{s+1} + w_s^2 2^{2s+2} = 1 + w_{s+1} 2^{s+1},$$

with $w_{s+1} = 1 + w_s 2^{s-1} \equiv 1 \bmod 2$. Hence (2.1) also holds with $s+1$ in place of s. □

2.3. **Explicit form of the Vinogradov mean value theorem.** Let $N_{k,n}(M)$ be the number of integral solutions of the system of equations

$$x_1^j + \ldots + x_k^j = y_1^j + \ldots + y_k^j, \qquad j = 1, \ldots, n,$$
$$1 \leqslant x_i, y_i \leqslant M, \qquad i = 1, \ldots, k.$$

Our application of Lemma 2.3 below rests on a version of the Vinogradov mean value theorem which gives a precise bound on $N_{k,n}(M)$. We use its fully explicit version given by Ford [6, Theorem 3], which we present here in the following weakened and simplified form.

Lemma 2.2. *For every integer $n \geqslant 129$ there exists an integer $k \in [2n^2, 4n^2]$ such that for any integer $M \geqslant 1$ we have*

$$N_{k,n}(M) \leqslant n^{3n^3} M^{2k-0.499n^2}.$$

We note that the recent striking advances in the Vinogradov mean value theorem due to Bourgain, Demeter and Guth [3] and Wooley [11] are not suitable for our purposes here as they contain implicit constants that depend on k and n, while in our approach k and n grow together with M.

2.4. **Double exponential sums with polynomials.** Our main tool to bound the exponential sum $S_h(L, N)$ is the following result of Korobov [8, Lemma 3].

Lemma 2.3. *Assume that*

$$\left|\alpha_\ell - \frac{a_\ell}{q_\ell}\right| \leqslant \frac{1}{q_\ell^2} \qquad \text{and} \qquad \gcd(a_\ell, q_\ell) = 1,$$

for some real α_ℓ and integers a_ℓ, q_ℓ, $\ell = 1, \ldots, n$. Then for the sum

$$S = \sum_{x,y=1}^{M} \mathbf{e}\left(\alpha_1 xy + \ldots + \alpha_n x^n y^n\right)$$

we have

$$|S|^{2k^2} \leqslant \left(64k^2 \log(3Q)\right)^{n/2} M^{4k^2-2k} N_{k,n}(M) \prod_{\ell=1}^{n} \min\left\{M^\ell, \sqrt{q_\ell} + \frac{M^\ell}{\sqrt{q_\ell}}\right\},$$

where

$$Q = \max\{q_\ell \ : \ 1 \leqslant \ell \leqslant n\}.$$

We also need the following simple result which allows us to reduce single sums to double sums.

Lemma 2.4. *Let $f : \mathbb{R} \to \mathbb{R}$ be an arbitrary function. Then for any integers $M, N \geqslant 1$ and $a \geqslant 0$, we have*

$$\left|\sum_{x=0}^{N-1} \mathbf{e}(f(x))\right| \leqslant \frac{1}{M^2} \sum_{x=0}^{N-1} \left|\sum_{y,z=1}^{M} \mathbf{e}(f(x+ayz))\right| + 2aM^2.$$

Proof. Examining the non-overlapping parts of the sums below, we see that for any positive integers y and z

$$\left|\sum_{x=0}^{N-1} \mathbf{e}(f(x)) - \sum_{x=0}^{N-1} \mathbf{e}(f(x+ayz))\right| \leqslant 2ayz.$$

Hence

$$\left|M^2 \sum_{x=0}^{N-1} \mathbf{e}(f(x)) - \sum_{y,z=1}^{M} \sum_{x=0}^{N-1} \mathbf{e}(f(x+ayz))\right| \leqslant 2a \sum_{y,z=1}^{M} yz \leqslant 2aM^4.$$

Changing the order of summation and using the triangle inequality, the result follows. □

2.5. **Sums of binomial coefficients.** We need results of certain sums of binomial coefficients. The first ones are immediate and we leave the proof for the reader.

Lemma 2.5. *Let n be a positive integer. Then*

(1) for any integer $k \leqslant n$ we have

$$\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1};$$

(2) for any polynomial $P(X) \in \mathbb{Z}[X]$ of degree $\deg P < n$ we have

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} P(j) = 0.$$

Lemma 2.6. *For any n, k with $k \leqslant n$ we have*

$$\sum_{\substack{\ell_1+\ldots+\ell_k=n\\ \ell_1,\ldots,\ell_k\geqslant 1}} \frac{n!}{\ell_1!\ldots\ell_k!} = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^n.$$

Proof. As

$$\sum_{\ell_1+\ldots+\ell_k=n} \frac{n!}{\ell_1!\ldots\ell_k!} = k^n$$

the result follows directly from the inclusion–exclusion principle. □

3. Proofs of the main results

3.1. **Proof of Theorem 1.1.** As

$$u_{n+L} = \frac{a}{g^{n+L} - b} + c = \frac{ag^{-L}}{g^n - bg^{-L}} + c,$$

we can assume, that $L = 0$ and we put

$$S_h(0, N) = S_h(N).$$

We can also assume, that $a = 1$ and $c = 0$. Finally we assume, that

$$N \geqslant 2^{6t^{1/2}}$$

since otherwise the result is trivial, see (1.7).

Define

$$r = \frac{t \log 2}{\log N} = \rho^{-1} \log 2,$$

where ρ is given by (1.8). First assume, that

$$r \geqslant 129$$

and put

$$s = \left\lfloor \frac{t}{4r} \right\rfloor \quad \text{and} \quad \kappa = \left\lceil \frac{t}{s} \right\rceil - 1.$$

Then

$$s > \beta, \quad 2^s \leqslant N^{1/4}, \quad r \leqslant \kappa < s,$$

if N is large enough. Indeed,

$$s \geqslant \frac{t}{4r} - 1 = \frac{\log N}{4 \log 2} - 1 \geqslant 2\beta - 1 > \beta \quad \text{and} \quad 2^s \leqslant 2^{\frac{t}{4r}} = N^{1/4}.$$

Moreover,

$$\kappa \geqslant \frac{t}{s} - 1 \geqslant 4r - 1 \geqslant r$$

and

$$\kappa \leqslant \frac{t}{s} \leqslant \frac{(\log N)^2}{36(\log 2)^2 s} = \frac{t^2}{36r^2 s} \leqslant s.$$

Let τ_s be the order of g modulo 2^s. As $s > \beta$,

$$g^{\tau_s} = 1 + w \cdot 2^s \quad \text{with } \gcd(w, 2) = 1$$

by Lemma 2.1. Clearly, for all even x, we have

$$\frac{1}{1 - x} \equiv 1 + x + \ldots + x^{t-1} \bmod 2^t,$$

thus

$$\begin{aligned} u_{n\cdot\tau_s} &\equiv \frac{-1}{b-g^{n\cdot\tau_s}} \equiv \frac{-1}{1-(1-b+g^{n\tau_s})} \equiv -\sum_{\ell=0}^{t-1}(1-b+g^{n\cdot\tau_s})^\ell \\ &\equiv -\sum_{\ell=0}^{t-1}(1-b+(1+w\cdot 2^s)^n)^\ell \\ &\equiv -\sum_{\ell=0}^{t-1}\left(2-b+\sum_{i=1}^{n}\binom{n}{i}(w\cdot 2^s)^i\right)^\ell \bmod 2^t. \end{aligned}$$

Define

$$F_\kappa(n) = \sum_{\ell=0}^{\kappa}(w\cdot 2^s)^\ell \sum_{j=0}^{t-1}\sum_{\nu=1}^{j}\binom{j}{\nu}(2-b)^{j-\nu}\sum_{\substack{i_1+\ldots+i_\nu=\ell\\ i_1,\ldots,i_\nu\geqslant 1}}\binom{n}{i_1}\ldots\binom{n}{i_\nu}.$$

Then

$$u_{n\cdot\tau_s} \equiv -F_\kappa(n) \bmod 2^t.$$

The expression $\kappa!F_\kappa(n)$ is a polynomial of $2^s n$ of degree at most κ. Thus we can define the integers $a_0,\ldots,a_\kappa$ by

$$\kappa!F_\kappa(n) = \sum_{\ell=0}^{\kappa} a_\ell 2^{\ell s} n^\ell.$$

Then the coefficients satisfy

$$a_\ell \equiv \frac{\kappa!}{\ell!}w^\ell \sum_{j=1}^{t-1}\sum_{\nu=1}^{j}\binom{j}{\nu}(2-b)^{j-\nu}\sum_{\substack{i_1+\ldots+i_\nu=\ell\\ i_1,\ldots,i_\nu\geqslant 1}}\frac{\ell!}{i_1!\ldots i_\nu!} \bmod 2^s.$$

We have $\mathrm{v}_2(a_\ell) = \mathrm{v}_2(\kappa!/\ell!)$. Indeed, as w is odd and b is even, by Lemmas 2.6 and 2.5 we get

$$\begin{aligned} &\sum_{j=1}^{t-1}\sum_{\nu=1}^{j}\binom{j}{\nu}(2-b)^{j-\nu}\sum_{\substack{i_1+\ldots+i_\nu=\ell\\ i_1,\ldots,i_\nu\geqslant 1}}\frac{\ell!}{i_1!\ldots i_\nu!} \\ &\quad\equiv \sum_{j=1}^{\ell}\sum_{\substack{i_1+\ldots+i_j=\ell\\ i_1,\ldots,i_j\geqslant 1}}\frac{\ell!}{i_1!\ldots i_j!} \equiv \sum_{j=1}^{\ell}\sum_{i=0}^{j}(-1)^{j-i}\binom{j}{i}i^\ell \\ &\quad\equiv \sum_{i=0}^{\ell}(-1)^i i^\ell \sum_{j=i}^{\ell}\binom{j}{i} \equiv \sum_{i=0}^{\ell}(-1)^i i^\ell\binom{\ell+1}{i+1} \\ &\quad\equiv -\sum_{i=1}^{\ell+1}(-1)^i\binom{\ell+1}{i}(i-1)^\ell \equiv \binom{\ell+1}{0}(-1)^\ell \equiv 1 \bmod 2 \end{aligned}$$

(we note that the last several congruences are actually equations).

Write $\omega_\ell = \mathrm{v}_2(a_\ell)$. Then

$$\omega_\ell \leqslant \mathrm{v}_2(\kappa!) \leqslant \left\lfloor \frac{\kappa}{2} \right\rfloor + \left\lfloor \frac{\kappa}{4} \right\rfloor + \ldots < \kappa \quad \text{for } \ell < \kappa$$

and $\omega_\kappa = 0$.

To conclude the proof observe, that by Lemma 2.4 we have

$$\begin{aligned} |S_h(N)| &\leqslant \frac{1}{2^{2s}} \sum_{n=0}^{N-1} \left| \sum_{x,y=1}^{2^s} \mathbf{e}\left(\frac{h}{2^t} u_{n+\tau_s xy} \right) \right| + 2\tau_s 2^{2s} \\ &\leqslant \frac{1}{2^{2s}} \sum_{n=0}^{N-1} \left| \sum_{x,y=1}^{2^s} \mathbf{e}\left(\frac{h}{2^t} \cdot \frac{g^{-n}}{g^{\tau_s xy} - bg^{-n}} \right) \right| + 2^{3s} \\ &\leqslant \frac{1}{2^{2s}} \sum_{n=0}^{N-1} \left| \sum_{x,y=1}^{2^s} \mathbf{e}\left(\frac{hg^{-n}(a_1 2^s xy + \ldots + a_\kappa 2^{\kappa s}(xy)^\kappa)}{\kappa! 2^t} \right) \right| + N^{3/4}, \end{aligned}$$

where the coefficients $a_\ell = a_\ell(bg^{-n})$ for $\ell = 1, \ldots, \kappa$, are determined as above with bg^{-n} instead of b.

Write

$$\frac{hg^{-n} a_\ell 2^{\ell s}}{\kappa! 2^t} = \frac{r_\ell}{q_\ell}, \quad \gcd(r_\ell, q_\ell) = 1, \quad \ell = 1, \ldots, \kappa,$$

with

$$2^{t-\ell s-\omega_\ell} \leqslant q_\ell \leqslant \kappa! 2^{t-\ell s-\omega_\ell} \quad \ell = 1, \ldots, \kappa. \tag{3.1}$$

Then

$$|S_h(N)| \leqslant \frac{1}{2^{2s}} \sum_{n=0}^{N-1} \left| \sum_{x,y=1}^{2^s} \mathbf{e}\left(f_n(x,y)\right) \right| + N^{3/4}, \tag{3.2}$$

where

$$f_n(x,y) = \frac{r_1}{q_1} xy + \ldots + \frac{r_\kappa}{q_\kappa} (xy)^\kappa.$$

Put

$$\sigma_n = \sum_{x,y=1}^{2^s} \mathbf{e}\left(f_n(x,y)\right).$$

For κ, there exists a $k \in [2\kappa^2, 4\kappa^2]$ such that for $N_{k,\kappa}$ we have the bound of Lemma 2.2 (with κ instead of n).

Then by Lemma 2.3 we have

$$\begin{aligned}|\sigma_n|^{2k^2} \leqslant \left(64k^2\log(3Q)\right)^{\kappa/2} 2^{(4k^2-2k)s} N_{k,\kappa}(2^s)\\ \prod_{\ell=1}^{\kappa} \min\left\{2^{\ell s}, \sqrt{q_\ell} + \frac{2^{\ell s}}{\sqrt{q_\ell}}\right\},\end{aligned} \tag{3.3}$$

where by (3.1) we have $Q \leqslant \kappa! 2^t$ and thus

$$\log(3Q) \leqslant \log(3\kappa! 2^t) \leqslant t\kappa\log(6\kappa). \tag{3.4}$$

By the choice of κ we have $s\kappa < t \leqslant s(\kappa+1)$. As $\omega_\ell \leqslant \kappa \leqslant s$, under

$$\frac{\kappa+1}{2} \leqslant \ell < \kappa$$

we have by (3.1)

$$q_\ell \leqslant \kappa! 2^{s(\kappa+1-\ell)} \leqslant \kappa! 2^{\ell s} \quad \text{and} \quad q_\ell > 2^{s(\kappa-1-\ell)}$$

thus

$$\frac{1}{\sqrt{q_\ell}} + \frac{\sqrt{q_\ell}}{2^{\ell s}} \leqslant \frac{1+\kappa!}{\sqrt{q_\ell}} \leqslant \kappa^\kappa 2^{-\frac{s}{2}(\kappa-1-\ell)}.$$

Whence

$$\begin{aligned}\prod_{\ell=1}^{\kappa} \min\left\{2^{\ell s}, \sqrt{q_\ell} + \frac{2^{\ell s}}{\sqrt{q_\ell}}\right\} &= 2^{s\kappa(\kappa+1)/2} \prod_{\ell=1}^{\kappa} \min\left\{1, \frac{1}{\sqrt{q_\ell}} + \frac{\sqrt{q_\ell}}{2^{\ell s}}\right\}\\ &\leqslant 2^{s\kappa(\kappa+1)/2} \prod_{\frac{\kappa}{2}<\ell<\kappa} \kappa^\kappa 2^{-s(\kappa-1-\ell)/2}\\ &\leqslant \kappa^{\kappa^2} 2^{s\kappa(\kappa+1)/2 - s(\kappa-2)(\kappa-4)/16}.\end{aligned} \tag{3.5}$$

By Lemma 2.2 we have

$$N_{k,\kappa}(2^s) \leqslant \kappa^{3\kappa^3} 2^{2ks - 0.499\kappa^2 s}. \tag{3.6}$$

Combining (3.3), (3.4), (3.5) and (3.6), we have

$$|\sigma_n|^{2k^2} \leqslant \left(64tk^3\log(6\kappa)\right)^{\kappa/2} \kappa^{4\kappa^3} 2^{4k^2 s + s\kappa(\kappa+1)/2 - s(\kappa-2)(\kappa-4)/16 - 0.499\kappa^2 s}$$

and therefore

$$|\sigma_n| \ll t^{1/(16\kappa^3)} 2^{2s - s/(32770\kappa^2)}.$$

Since $t\kappa^2 < (\frac{t}{s})^3 s < (6r)^3 s$, then

$$2^{s/\kappa^2} = N^{rs/(t\kappa^2)} > N^{1/(216r^2)}.$$

Moreover

$$t^{1/\kappa^3} \leqslant N^{\log t/(129r^2\log N)} \leqslant N^{\log\log N/(387r^2\log N)},$$

whence

$$|\sigma_n| \ll 2^{2s} N^{-\eta\rho^2},$$

for some $\eta > 0$ if N is large enough. Thus by (3.2) we have

$$|S_h(N)| \leqslant \frac{1}{2^{2s}} \sum_{n=0}^{N-1} |\sigma_n| + N^{3/4} \ll N^{1-\eta\rho^2} + N^{3/4} \ll N^{1-\eta/r^2}$$

which gives the result for $r \geqslant 129$.

If $r < 129$, define

$$N_0 = \lfloor 2^{t/129} \rfloor \qquad \rho_0 = \frac{\log N_0}{t} = \frac{\log 2}{129} + O(1/t).$$

As $N \leqslant \tau < 2^t$, we have

$$\frac{\log N_0}{\log N} > \frac{1}{129}. \tag{3.7}$$

Then

$$|S_h(N)| \leqslant \sum_{0 \leqslant k < N/N_0} \left| \sum_{n=kN_0}^{(k+1)N_0-1} \mathbf{e}(hu_n/2^t) \right|.$$

Applying the previous argument to the inner sums, we get

$$|S_h(N)| \ll \frac{N}{N_0} N_0^{1-\eta\rho_0^2} \ll N^{1-129^{-3}\eta\rho_0^2}$$

by (3.7). Thus replacing η to $\eta/129^3$, we conclude the proof.

3.2. **Proof of Theorem 1.2.** By the Erdős-Turán inequality, see [5] for any integer $H \geqslant 1$ we have

$$D(L, N) \ll \frac{1}{H} + \frac{2}{N} \sum_{h=1}^{H} \frac{1}{h} |S_h(L, N)|. \tag{3.8}$$

Define

$$H = \left\lfloor \frac{\tau_t}{\sqrt{N}} \right\rfloor,$$

where τ_t is as in Lemma 2.1.

For a given $1 \leqslant h \leqslant H$, write $h = 2^d j$ with odd j and $d \leqslant \log_2 H$. Then consider the sequence (u_n) modulo 2^{t-d}. Then clearly

$$S_h(L, N) = S_{d,j}(L, N).$$

where $S_{d,j}(L, N)$ is defined as $S_j(L, N)$, however with respect to the modulus 2^{t-d}.

By the above choice of parameters, we have

$$t - d \geqslant t - \log_2 H \geqslant \frac{1}{2} \log_2 N + \beta > 17\beta \tag{3.9}$$

by Lemma 2.1, thus

$$\tau_{t-d} = 2^{t-d-\beta+1}. \tag{3.10}$$

Using (3.8), we have

$$
\begin{aligned}
D(L,N) &\ll \frac{1}{H} + \frac{1}{N}\sum_{h=1}^{H}\frac{1}{h}|S_h(L,N)| \\
&\ll \frac{1}{H} + \frac{1}{N}\sum_{0\leqslant d\leqslant \log_2 H}\frac{1}{2^d}\sum_{\substack{1\leqslant j\leqslant H/2^d\\ j \text{ odd}}}\frac{1}{j}|S_{d,j}(L,N)|.
\end{aligned} \tag{3.11}
$$

For fixed d and j put

$$
N_d = \left\lceil \frac{N}{\tau_{t-d}} \right\rceil \qquad \text{and} \qquad K_d = N - N_d\tau_{t-d}.
$$

Then

$$
\begin{aligned}
|S_{d,j}(L,N)| \leqslant \sum_{i=0}^{N_d-2} &|S_{d,j}(L+i\tau_{t-d},\tau_{t-d})| \\
&+ |S_{d,j}(L+(N_d-1)\tau_{t-d},K_d)|.
\end{aligned} \tag{3.12}
$$

If $K_d < 2^{8\beta}$, we use the trivial estimate

$$
|S_{d,j}(L+(N_d-1)\tau_{t-d},K_d)| \leqslant K_d < 2^{8\beta}.
$$

As

$$
8\beta < \frac{1}{2}(t-d-\beta)
$$

by (3.9), we get

$$
|S_{d,j}(L+(N_d-1)\tau_{t-d},K_d)| \leqslant \tau_{t-d}^{1-\eta(t-d)^{-2}(\log \tau_{t-d})^2}. \tag{3.13}
$$

If $K_d \geqslant 2^{8\beta}$, then as $K_d \leqslant \tau_{t-d}$ we also have (3.13) by Theorem 1.1. Thus by (3.12) we have

$$
|S_{d,j}(L,N)| \ll N_d \cdot \tau_{t-d}^{1-\eta(t-d)^{-2}(\log \tau_{t-d})^2} \ll N^{1-\eta(t-d)^{-2}(\log \tau_{t-d})^2/\log N}.
$$

By (3.9) and (3.10) we have

$$
\frac{(\log \tau_{t-d})^3}{\log N(t-d)^2} = \frac{(t-d-\beta)^3}{\log N(t-d)^2} \geqslant \frac{(t-d-\beta)^3}{\log N t^2} \geqslant \frac{1}{8}\left(\frac{\log N}{t}\right)^2 = \rho^2/8,
$$

whence

$$
|S_{d,j}(L,N)| \ll N^{1-\eta\rho^2/8}.
$$

Then by (3.11),

$$
\begin{aligned}
D(L,N) &\ll \frac{1}{H} + \sum_{0\leqslant d\leqslant \log_2 H}\frac{1}{2^d}\sum_{\substack{1\leqslant j\leqslant H/2^d\\ j \text{ odd}}}\frac{1}{j}N^{-\eta\rho^2/8} \\
&\ll 2^{-(t-\beta)/2} + N^{-\eta\rho^2/8}\log H \ll \frac{1}{t} + N^{-\eta\rho^2/8}\log H \ll N^{-\eta\rho^2/16}
\end{aligned}
$$

if N is large enough.

4. Comments

We note that an extension of our results to the case of sequences (1.5) modulo prime powers p^t with a prime $p \geqslant 3$ is immediate and can be achieved at the cost of merely typographical changes.

We also note that all implied constants are effective and can be evaluated (however at the cost of some additional technical clutter).

It is certainly natural to study the multidimensional distribution of the sequence generated by (1.3), that is, the s-dimensional vectors

$$(u_n, \ldots, u_{n+s-1}), \qquad n = 1, \ldots, N.$$

Our method is capable of addressing this problem, however investigating the 2-divisibility of the corresponding polynomial coefficients which is an important part of our argument in Section 3.1 is more difficult and may require new arguments.

We also use this as an opportunity to pose a question about studying short segments of the inversive generator modulo a large prime p. While results of Bourgain [1,2] give a non-trivial bound on exponential sums for very short segments of sequence $ag^n \bmod p$, $n = 1, \ldots, N$, see also [7, Corollary 4.2], their analogues for even the simplest rational expressions like $1/(g^n - b) \bmod p$ are not known. Obtaining such results beyond the standard range $N \geqslant p^{1/2+\varepsilon}$ (with any fixed $\varepsilon > 0$) is apparently a difficult question requiring new ideas.

Acknowledgement

During the preparation of this wok L. M. was partially supported by the Austrian Science Fund FWF Projects P30405 and I. S. by the Australian Research Council Grants DP170100786 and DP180100201.

References

[1] J. Bourgain, 'Multilinear exponential sums in prime fields under optimal entropy condition on the sources', *Geom. and Funct. Anal.*, **18** (2009), 1477–1502. 13

[2] J. Bourgain, 'On exponential sums in finite fields', *Bolyai Soc. Math. Stud.*, **21**, János Bolyai Math. Soc., Budapest, 2010, 219–242. 13

[3] J. Bourgain, C. Demeter and L. Guth, 'Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three', *Ann. Math.*, **184** (2016), 633–682. 5

[4] W.-S. Chou, 'The period lengths of inversive congruential recursions', *Acta Arith.*, **73** (1995), 325–341. 2

[5] M. Drmota and R. F. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997. 4, 11

[6] K. Ford, 'Vinogradov's integral and bounds for the Riemann zeta function', *Proc. London Math. Soc.*, **85** (2002), 565–633. 3, 5

[7] M. Z. Garaev, 'Sums and products of sets and estimates of rational trigonometric sums in fields of prime order', *Uspekhi Mat. Nauk*, 65 (2010), no.4, 5–66 (in Russian), translated in *Russian Math. Surveys*, **65** (2010), 599–658. 13

[8] N. M. Korobov, 'The distribution of digits in periodic fractions', *Matem. Sbornik*, **89** (1972), 654–670 (in Russian), translated in *Math. USSR-Sb.*, **18** (1974), 659–676. 3, 5

[9] H. Niederreiter and I. E. Shparlinski, 'Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus', *Acta Arith.*, **92** (2000), 89–98. 2

[10] H. Niederreiter and A. Winterhof, 'Exponential sums and the distribution of inversive congruential pseudorandom numbers with power of two modulus', *Int. J. Number Theory*, **1** (2005), 431–438. 2

[11] T. D. Wooley, 'The cubic case of the main conjecture in Vinogradov's mean value theorem, *Adv. in Math.*, **294** (2016), 532–561. 5

L.M.: Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenberger Strasse 69, A-4040 Linz, Austria

E-mail address: laszlo.merai@oeaw.ac.at

I.E.S.: School of Mathematics and Statistics, University of New South Wales. Sydney, NSW 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au