Hardy-Ramanujan Journal 48 (2025) Part A, 184-199 submitted 10/03/2025, accepted 05/01/2026, revised 05/01/2026

On Finite Pseudorandom Binary Sequences: Generalized polynomials

Manfred G. Madritsch and Robert F. Tichy

Abstract. In the present paper we generate binary pseudorandom sequences using generalized polynomials. A generalized polynomial is a function in whose description we not only allow addition and product (as it is the case in usual polynomials) but also the floor function. We estimate the well-distribution measure, looking at the "randomness" along arithmetic progressions.

Keywords. pseudorandom, binary sequence, generalized polynomials, well-distribution, correlation.

2010 Mathematics Subject Classification. Primary 11K45; Secondary 11K06, 11K36, 11J71.

1. Introduction

A finite pseudorandom binary sequence is a finite sequence over the alphabet $\{-1,+1\}$. These sequences and their consideration were introduced amongst others by Mauduit and Sárközy [MaSá97] and play an important role in financial mathematics as well as computer sciences.

In order to quantify the random behaviour of such a sequence, Mauduit and Sárközy introduced three measurements in [MaSá97]: normality, well-distribution along arithmetic progressions and small multiple correlations. The present article focuses on the well-distribution measure – the randomness of the sequence by only looking at arithmetic progressions. A clever way to investigate them is to look at sums of elements (along arithmetic progressions). In particular, if the sum is rather large (in absolute value), then there must be more elements of one kind, meaning that the sequence cannot be very "random". This simple observation is also the reason why we preferred the alphabet $\{-1,+1\}$ over $\{0,1\}$.

Now we want to be more precise. Let $E_N=(e_n)_{n=1}^N\in\{-1,+1\}^N$ be a finite pseudorandom binary sequence. Then for three integers $a\in\mathbb{N}^*$, $b\in\mathbb{Z}$ and $M\in\mathbb{N}^*$ such that $1\leq a+b<aM+b\leq N$, we consider a sum of the form

$$U(E_N,M,a,b)=\sum_{m=1}^{M}e_{am+b}.$$

The well-distribution measure is the maximal absolute value we might obtain by suitable choosing a,b and M, *i.e.*

$$W(E_N)=\max_{a,b,M}\left|U(E_N,M,a,b)\right|=\max_{a,b,M}\left|\sum_{m=1}^{M}e_{am+b}\right|.$$

Clearly we have $W(E_N)\leq N$. The limiting distribution of the well-distribution measure of a true random binary sequences has been established by Aistleitner [Ais13].

A canonical way for constructing a pseudorandom binary sequence, is to take the fractional part of a sequence of real numbers. In particular, we set

$$\chi(x)=\begin{cases}+1 & \text{if } x-\lfloor x\rfloor<\frac{1}{2},\\ -1 & \text{if } x-\lfloor x\rfloor\geq\frac{1}{2}.\end{cases}$$

We thank episciences.org for providing open access hosting of the electronic journal *Hardy-Ramanujan Journal*

Then every finite sequence $(u_n)_{n=1}^N$ of real numbers gives rise to a pseudorandom binary sequence via $e_n = \chi(u_n)$ for $1 \leq n \leq N$. Moreover this choice links the estimation of the well-distribution measure with the discrepancy of the underlying sequence. We define the discrepancy D_N of a sequence $(u_n)_{n=1}^N$ of real numbers by

$$D_N\left((u_n)_{n=1}^N\right) = \sup_{0\leq a<b\leq 1}\left|\frac{\#\{1\leq n\leq N\colon \{u_n\}\in[a,b[}{N} - (b-a)\right|.$$

Then for $a \in \mathbb{N}^*$, $b \in \mathbb{Z}$ and $M \in \mathbb{N}^*$ such that $1 \leq a+b \leq aM+b \leq N$, we have

$$\begin{aligned}|U(E_N,M,a,b)| &= \left|\sum_{m=1}^M e_{am+b}\right| \\ &\leq \left|\sum_{m=1}^M\left(\mathbb{1}_{\{u_{am+b}\}\leq\frac12} - \frac12\right)\right| + \left|\sum_{m=1}^M\left(\mathbb{1}_{\{u_{am+b}\}>\frac12} - \frac12\right)\right| \leq 2MD_M\left((u_{am+b})_{m=1}^M\right).\end{aligned}$$

Therefore uniformly distributed sequences and sequences with low discrepancy are good candidates for pseudorandom sequences with low well-distribution measure. In the present paper we focus on polynomial-like sequences. For different sequences and more general information on uniform distribution and the discrepancy we refer the interested reader to the book of Drmota and Tichy [DrTi97].

Mauduit and Sárközy considered in Part 5 [MaSá00a] and Part 6 [MaSá00b] of their series the case $f(n) = \alpha n^k$ with α real and $k \geq 1$ an integer. Their results depend on the coefficients of the continued fraction expansion of α. If, on the one hand, the coefficients are bounded, then they could show, that there exists an η depending only on α and k such that

$$W(E_N) \ll N^{1-\eta+\varepsilon},$$

where the implied constant also depends on α and k. If, on the other hand, there is no such bound for the coefficients of the continued fraction expansion of α, then they could show that

$$W(E_N) \gg N.$$

These considerations were extended to the Piatetski-Shapiro sequence $u_n = n^c$, where $c > 1$ is not an integer. Mauduit, Rivat and Sárközy [MRS02] could show an estimate $U(E_N, M, a, b)$, provided that a is not too large (with respect to N). These functions are part of the larger class of pseudo-polynomials. A pseudo-polynomial is a function $f(x)$ of the form

$$f(x) = \alpha_d x^{\beta_d} + \cdots + \alpha_1 x^{\beta_1},$$

where $\alpha_1,\ldots,\alpha_d,\beta_1,\ldots,\beta_d$ are reals with $\alpha_d \neq 0$, $\beta_d > \cdots > \beta_1 > 0$ and at least one $\beta_i \notin \mathbb{Z}$.

The sequences of pseudo-polynomials carry many properties of polynomials like forming a Poincaré set P. Let $(X, \mathfrak{B}, \mu, T)$ be a measure preserving dynamical system. Then we call a set $P \subset \mathbb{N}^*$ a Poincaré set (or set of recurrence) if for each set $A \in \mathfrak{B}$ of positive measure $\mu(A) > 0$, there exists $n \in P$ such that $A \cap T^n(A) \neq \emptyset$. Bergelson *et al.* [BKM14] showed that the sets formed by a pseudo-polynomial sequence are Poincaré sets. This was later extended by the authors [MaTi16] to other polynomial like families as well as to questions around approximation in [MaTi19]. For more on the connection of uniform distribution, dynamical systems and approximation we refer to the monograph of Montgomery [Mon94].

Inspired by these results, Bergelson, Kolesnik and Son [BKS19] considered the even larger class of Hardy fields. These fields consist of functions that behave asymptotically like a power function, however, they are not polynomials. Therefore even if they behave like an integer power their derivative does not vanish identically, which is normally a mayor problem in the consideration. In their paper [BKS19] they showed, amongst other things, that the set $\{f(n) \colon n \in \mathbb{N}^*\}$, where f is from a Hardy field is a Poincaré set. Using this more general class of functions Rivat together with the two authors [MRT24] extended the above results for the well-distribution measure. Thereby they got rid of the dependency on the size of a providing a general bound.

Another class of polynomial-like function became of recent interest in dynamical systems. This is the set of generalized polynomials GP, where we also allow the floor function in their description. To be more specific let GP_0 be the usual ring of polynomials $\mathbb{R}[x]$ with real coefficients. Then $\mathrm{GP} = \bigcup_{n=1}^{\infty} \mathrm{GP}_n$, where, for $n \geq 1$, we recursively define

$$\mathrm{GP}_n = \mathrm{GP}_{n-1} \cup \{v + w \colon v, w \in \mathrm{GP}_{n-1}\} \cup \{v \cdot w \colon v, w \in \mathrm{GP}_{n-1}\} \cup \{\lfloor v \rfloor : v \in \mathrm{GP}_{n-1}\}.$$

Bergelson, Håland and Son [BHS21] recently characterized that $u_n = f(n)$ with $f \in \mathrm{GP}$ is uniformly distributed provided g fulfils some canonical conditions, which are very similar to the notion of finite type below. However, they do not give a general discrepancy estimate. Hofer and Ramaré [HoRa16] and Mukhopadhyay, Ramaré and Viswanadham [MRV18] considered the discrepancy of the sequence $u_n = f(n)$ where $f(n) = \beta \lfloor \alpha p(n) \rfloor$ with p a monic polynomial and α and β reals, such that $(\alpha, \alpha\beta)$ is of finite type t.

Definition 1.1. *Let $\gamma_1, \ldots, \gamma_s$ be reals and $t > 0$. Then we say that $(\gamma_1, \ldots, \gamma_s)$ is of finite type t if there exists a constant $c(\varepsilon, \gamma_1, \ldots, \gamma_s) = c > 0$ such that for all integers $n_1, \ldots, n_s$ with $(n_1, \ldots, n_s) \neq (0, \ldots, 0)$ we have*

$$\prod_{j=1}^{s} \left(\max\left(1, |n_j|\right)\right)^{t+\varepsilon} \left\| \sum_{j=1}^{s} n_j \gamma_j \right\| \geq c,$$

where $\|\cdot\|$ denotes the distance to the nearest integer.

The aim of the present paper is to extend our above considerations of the well-distribution measure for sequences based on function from Hardy fields to these general polynomials.

Theorem 1.1. *Let $\alpha_1, \alpha_2, \beta$ be reals and let*

$$f(x) = \beta \left\lfloor \alpha_1 \left\lfloor \alpha_2 p(x) \right\rfloor \right\rfloor,$$

where $p \in \mathbb{R}[x]$ is a monic polynomial of degree $d \geq 2$. Furthermore we denote by $E_N = (e_n)_{n=1}^{N}$ with $e_n = \chi(f(n))$ the corresponding pseudorandom binary sequence. Suppose that

$$(\alpha_2, \alpha_1\alpha_2, \alpha_1\alpha_2\beta)$$

is of finite type t. Then there exists $\eta = \eta(f, t) > 0$ depending only on f and t such that

$$W(E_N) \ll N^{1-\eta+\varepsilon},$$

where the implied constant depends on f, t and ε.

Note that we may calculate η explicitly for a given function f and finite type t. However, since this exponent is far from the expected one, we omit the details to the reader.

2. Utilities

2.A. Discrepancy estimates

As we already mentioned above the well-distribution measure is in strong relation with the discrepancy of a sequence modulo 1. A standard way of estimating is the Erdős-Turán inequality.

Lemma 2.1. (Erdős-Turán) *For any integers $N > 0$, $H > 0$, and any sequence $(u_n)_{n=1}^N$ of N real numbers we have*

$$D_N\left((u_n)_{n=1}^N\right) \leq \frac{2}{H+1} + 2\sum_{h=1}^{H}\frac{1}{h}\left|\frac{1}{N}\sum_{n=1}^{N}e(hu_n)\right|.$$

Proof. For a proof see Lemma 2.5 of Kuipers and Niederreiter [KuNi74] (for smaller coefficients see also Rivat and Tenenbaum [RiTe05]).

For sequences of the form $u_n = n\theta$ with real θ we the following estimate will be more useful.

Lemma 2.2. *Let $\theta \in \mathbb{R}\setminus\mathbb{Q}$ be an irrational number. Then for any positive integers $L \geq 1$ and $J \geq 1$ the discrepancy of the sequence $(\ell\theta)_{\ell=1}^L$ satisfies*

$$D_L\left((\ell\theta)_{\ell=1}^L\right) \leq C\left(\frac{1}{J} + \frac{1}{L}\sum_{j=1}^{J}\frac{1}{j\left\|j\theta\right\|}\right),$$

where C is an absolute constant.

Proof. This is [KuNi74, Lemma 3.2].

2.B. Floor function

In the description of general polynomials, the floor function is allowed. However, we will rewrite the floor function using the fractional part since this is a 1-periodic function. For reals $x, \tau \in \mathbb{R}$ we write

$$F(x,\tau) = e\left(\tau\{x\}\right). \tag{2.1}$$

Since the fractional part is discontinuous at the integers, we use convolution for smoothing and introduce the following r-fold convolution

$$G_r(x,\tau,\delta) = \frac{1}{(2\delta)^r}\left(\mathbb{1}_{[-\delta,\delta]} \star \cdots \star \mathbb{1}_{[-\delta,\delta]} \star F(x,\tau)\right), \tag{2.2}$$

where $r \geq 1$ is an integer and $\delta > 0$. The following lemma deals with the error we have in considering G instead of F.

Lemma 2.3. *For any sequence $\{u_n\}_{n\geq 0}$ of real numbers, and any positive integer N we have*

$$\sum_{0\leq n<N}\left|F(u_n,\tau) - G_r(u_n,\tau,\delta)\right| \ll Nr\delta + Nr^2\delta\left|\tau\right| + ND_N(u_n).$$

Proof. This is Lemma 10 of Hofer and Ramaré [HoRa16].

Now, as usual, we denote by $\widehat{G_r}$ the (discrete) Fourier transform of G_r (with respect to x):

$$G_r(x,\tau,\delta) = \sum_{k\in\mathbb{Z}}\widehat{G_r}(k,\tau,\delta)e\left(-kx\right).$$

The properties of this transformation are twofold. On the one hand we use the following lemma to truncate the infinite sum.

Lemma 2.4. *Let K be a positive integer such that $|\tau + k| \geq \frac{k}{2}$ for $k \in \mathbb{Z}$ with $|k| > K$. Then*

$$\sum_{|k|>K} \widehat{G_r}(k, \tau, \delta) \ll (\delta K)^{-r}.$$

Proof. This is Lemma 3 of Mukhopadhyay *et al.* [MRV18].

On the other hand the second lemma considers the case of higher moments of the Fourier coefficients.

Lemma 2.5. *Let $\tau \in \mathbb{R}$ and $0 < \delta < \min\left(\frac{1}{2|\tau|}, 1\right)$. Then for $p > 1$ we have*

$$\sum_{k\in\mathbb{Z}} \left|\widehat{G_r}(k, \tau, \delta)\right|^p \ll_p 1.$$

Proof. This is Lemma 4 of Mukhopadhyay *et al.* [MRV18].

2.C. Exponential sum estimates

Above we stated the Erdős-Turán inequality (Lemma 2.1) turning the estimation of the discrepancy into one of exponential sums. The aim here is Lemma 3.2 below. However, we need some tools for its proof. The first deals with the classical idea of Weyl differencing.

Lemma 2.6. *Suppose that $\lambda_1, \lambda_2, \ldots, \lambda_N$ is a sequence of complex numbers, each with $|\lambda_i| \leq 1$, and define $\Delta\lambda_m = \lambda_m$, $\Delta_r\lambda_m = \lambda_{m+r}\overline{\lambda_m}$ and*

$$\Delta_{r_1,\ldots,r_k,s}\lambda_m = (\Delta_{r_1,\ldots,r_k}\lambda_{m+s})\,\overline{(\Delta_{r_1,\ldots,r_k}\lambda_m)}.$$

Then for any given $k \geq 1$, and real number $Q \in [1, N]$,

$$\left|\frac{1}{8N}\sum_{m=1}^{N}\lambda_m\right|^{2^k} \leq \frac{1}{8Q} + \frac{1}{8Q^{2-2^{-k+1}}}\sum_{r_1=1}^{Q}\sum_{r_2=1}^{Q^{\frac{1}{2}}}\cdots\sum_{r_k=1}^{Q^{2^{-k+1}}}\left|\frac{1}{N}\sum_{m=1}^{N-r_1-\cdots-r_k}\Delta_{r_1,\ldots,r_k}\lambda_m\right|.$$

Proof. This is a variant of a lemma of Weyl-van der Corput (see [GrKo91, Lemma 2.7]) as given in [GrRa96, Lemma 8.3].

Weyl differencing turns the sum into a linear one. The second tool connects this linear exponential sum with approximation properties of the coefficient.

Lemma 2.7. *For every real number α and all integers $N_1 < N_2$,*

$$\sum_{n=N_1+1}^{N_2} e(\alpha n) \ll \min\left(N_2 - N_1, \|\alpha\|^{-1}\right).$$

Proof. This is Lemma 4.7 of Nathanson [Nat96].

Finally we need a link between the sum of the minima and the discrepancy of $n\alpha$-sequences.

Lemma 2.8. *Let $\xi \in \mathbb{R}$ and let $L \in \mathbb{N}^*$ be a positive integer. Then*

$$\sum_{\ell=1}^{L}\min\left(N, \|\ell\xi\|^{-1}\right) \ll L\log N\left(1 + ND_L\left((\ell\xi)_{\ell=1}^{L}\right)\right).$$

Proof. We divide the interval $[0,1]$ into N parts and denote by E_n the number of elements $\|\ell\xi\|$ that fall in the n-th, *i.e.* for $0 \leq n < N$ we set

$$E_n := \#\left\{\ell \leq L \colon \frac{n}{N} < \|\ell\xi\| \leq \frac{n+1}{N}\right\}.$$

Clearly we have

$$\sum_{\ell=1}^{L} \min\left(N, \frac{1}{\|\ell\xi\|}\right) = NE_0 + \sum_{\ell\notin E_0} \frac{1}{\|\ell\xi\|} \leq NE_0 + \sum_{n=1}^{N-1} \frac{N}{n} E_n.$$

By the definition of discrepancy we obtain that

$$E_n = \frac{2L}{N} + \mathcal{O}\left(LD_L\left((\ell\xi)_{\ell=1}^{L}\right)\right).$$

Plugging this into the sum of the minima yields the desired bound.

3. A discrepancy estimate

We start our considerations with a first discrepancy estimate.

Proposition 3.1. *Let $p \in \mathbb{R}[X]$ be a monic polynomial of degree $d \geq 2$ and let $a \in \mathbb{N}^*$ and $b \in \mathbb{Z}$ be integers. Furthermore suppose that α is of finite type t and that*

$$a \leq N^{\frac{2-2^{2-d}}{dt}}.$$

Then for $\varepsilon > 0$

$$D_N\left((\alpha p(an+b))_{n=1}^{N}\right) \ll a^{\frac{dt}{2^{d-1}(t+1)+t}+\varepsilon} N^{-\frac{2-2^{2-d}}{2^{d-1}(2t+1)+t}+\varepsilon},$$

where the implied constant depends on ε, d and t.

Although this seems very classic, because no floor function is involved in this variant, we want to provide a proof here for the sake of completeness. This also allows us to present and prove our general tool for the occurring exponential sums.

Lemma 3.2. *Let p be a monic polynomial of degree $d \geq 2$ and $a \in \mathbb{N}^*$ and $b \in \mathbb{Z}$ be two integers. Furthermore suppose that $(\gamma_1, \ldots, \gamma_s) \in \mathbb{R}^s$ is of finite type t with $t > 0$. Then for N sufficiently large we have*

$$\left|\sum_{n=1}^{N} e\left(\left(k_1\gamma_1 + \cdots + k_s\gamma_s\right) p(an+b)\right)\right|^{2^{d-1}} \ll \left(a^{sd}\left|k_1 \cdots k_s\right|\right)^{\frac{t}{st+1}+\varepsilon} N^{2^{d-1}-\frac{2-2^{2-d}}{st+1}+\varepsilon}.$$

Proof. We start by an application of Lemma 2.6 with $Q = N$ to get

$$\left|\sum_{n=1}^{N} e\left(\left(k_1\gamma_1 + \cdots + k_s\gamma_s\right) p(an+b)\right)\right|^{2^{d-1}}$$
$$\ll N^{2^{d-1}-1} + N^{2^{d-1}+2^{2-d}-3} \sum_{r_1=1}^{N} \cdots \sum_{r_{d-1}=1}^{N^{2^{2-d}}} \left|\sum_{n=1}^{N} e\left(d!\left(k_1\gamma_1 + \cdots + k_s\gamma_s\right) a^d r_1 \cdots r_{d-1} n\right)\right|.$$

Applying Lemma 2.7 to the innermost sum yields

$$\left|\sum_{n=1}^{N} e\left(\left(k_1\gamma_1+\cdots+k_s\gamma_s\right)p(an+b)\right)\right|^{2^{d-1}} \ll N^{2^{d-1}-1} + N^{2^{d-1}+2^{2-d}-3}\sum_{r_1=1}^{N}\cdots\sum_{r_{d-1}=1}^{N^{2^{2-d}}}\min\left(N, \left\|d!\left(k_1\gamma_1+\cdots+k_s\gamma_s\right)a^d r_1\cdots r_{d-1}\right\|^{-1}\right).$$

We want to get rid of the multiple sum. Therefore we denote by $T(m)$ the number of representations of m as product of $r_1\cdots r_{d-1}$, *i.e.*

$$T(m) = \left|\left\{(r_1,\ldots,r_{d-1}) \in [1,N]\times\cdots\times[1,N^{2^{2-d}}] : m = r_1\cdots r_{d-1}\right\}\right|.$$

Thus

$$\left|\sum_{n=1}^{N} e\left(\left(k_1\gamma_1+\cdots+k_s\gamma_s\right)p(an+b)\right)\right|^{2^{d-1}} \ll N^{2^{d-1}-1} + N^{2^{d-1}+2^{2-d}-3}\sum_{m=1}^{N^{2-2^{2-d}}} T(m)\min\left(N, \left\|d!\left(k_1\gamma_1+\cdots+k_s\gamma_s\right)a^d m\right\|^{-1}\right).$$

Using estimates for the divisor function (*cf.* the proof of [Nat96, Lemma 4.14]) we get that $T(m) \ll m^{\varepsilon} \ll N^{\varepsilon}$ and therefore

$$\left|\sum_{n=1}^{N} e\left(\left(k_1\gamma_1+\cdots+k_s\gamma_s\right)p(an+b)\right)\right|^{2^{d-1}} \ll N^{2^{d-1}-1} + N^{2^{d-1}+2^{2-d}-3+\varepsilon}\sum_{m=1}^{N^{2-2^{2-d}}} \min\left(N, \left\|d!(k_1\gamma_1+\cdots+k_s\gamma_s)a^d m\right\|^{-1}\right).$$

Now by Lemma 2.8 we get for the sum of minima that

$$\sum_{m=1}^{L}\min\left(N, \left\|d!(k_1\gamma_1+\cdots+k_s\gamma_s)a^d m\right\|^{-1}\right) \ll L(\log N)\left(1 + ND_L\left(\left(d!(k_1\gamma_1+\cdots+k_s\gamma_s)a^d m\right)_{m=1}^{L}\right)\right), \quad (3.3)$$

where we have set $L = N^{2-2^{2-d}}$ for short.

Since $(\gamma_1,\ldots,\gamma_s)$ is of finite type t, it exists $c = c(\varepsilon,\gamma_1,\ldots,\gamma_s) > 0$ such that

$$\left\|d!(k_1\gamma_1+\cdots+k_s\gamma_s)a^d m\right\| \geq \frac{c(\varepsilon,\gamma_1,\ldots,\gamma_s)}{(d!a^d m)^{st+\varepsilon}\left|k_1\cdots k_s\right|^{t+\varepsilon}}.$$

Thus by Lemma 2.2 we get for $J \geq 1$ that

$$D_L\left(\left(d!(k_1\gamma_1+\cdots+k_s\gamma_s)a^d m\right)_{m=1}^{L}\right) \ll \frac{1}{J} + \frac{1}{L}\sum_{j=1}^{J} j^{-1}(a^d j)^{st+\varepsilon}\left|k_1\cdots k_s\right|^{t+\varepsilon} \ll \frac{1}{J} + \frac{1}{L}(a^d J)^{st+\varepsilon}\left|k_1\cdots k_s\right|^{t+\varepsilon}.$$

Choosing
$$J = a^{-d\frac{st}{st+1}} \left|k_1 \cdots k_s\right|^{-\frac{t}{st+1}} L^{\frac{1}{st+1}}$$
we get
$$\sum_{m=1}^{L} \min\left(N, \left\|d!ma^d(h\alpha_2 - k)\alpha\right\|^{-1}\right) \ll a^{d\frac{st}{st+1}+\varepsilon} \left|k_1 \cdots k_s\right|^{\frac{t}{st+1}+\varepsilon} N^{3-2^{2-d}-\frac{2-2^{2-d}}{st+1}+\varepsilon},$$
which together with 3.3 proves the lemma.

With this tool in hand we are able to prove the first estimation.

Proof of Proposition 3.1. The proof follows three steps. First, we use the Erdős-Turán inequality which transforms the discrepancy estimate in an exponential sum estimate. Then we use Lemma 3.2, our key lemma for the exponential sums. Finally we choose the parameter H in the Erdős-Turán inequality accordingly. This last step provides us with the bound on a.

Starting with an application of the Erdős-Turán inequality (Lemma 2.1) we obtain
$$D_N\left((\alpha p(an+b))_{n=1}^N\right) \ll \frac{1}{H} + \sum_{h=1}^{H} \frac{1}{h} \left|\frac{1}{N}\sum_{n=1}^{N} e\left(h\alpha p(an+b)\right)\right|, \tag{3.4}$$
where $H \geq 1$ is a parameter we will choose later.

An application of Lemma 3.2 yields
$$\left|\sum_{n=1}^{N} e(h\alpha p(an+b))\right|^{2^{d-1}} \ll N^{2^{d-1}-\frac{2-2^{2-d}}{t+1}+\varepsilon} \left(a^d h\right)^{\frac{t}{t+1}+\varepsilon}.$$

Finally plugging everything into (3.4) and setting
$$H = \left\lceil N^{\frac{2-2^{2-d}}{2^{d-1}(2t+1)}} a^{\frac{dt}{2^{d-1}(2t+1)+t}} \right\rceil \geq 1$$
proves the proposition.

4. The first iteration

Now we add the floor function to our generating function and establish the following proposition.

Proposition 4.1. *Let α and β be reals and let $p \in \mathbb{R}[x]$ be a monic polynomial of degree $d \geq 2$. Suppose that $(\alpha, \alpha\beta)$ is of finite type t with $t > 0$. Then*
$$D_N\left((\beta\left\lfloor \alpha p(an+b)\right\rfloor)_{n=1}^N\right) \ll a^{\frac{2dt}{2^{d-1}(2t+1)+4t+1}} N^{-\frac{2-2^{2-d}}{2^{d-1}(2t+1)+7t+2}}.$$

Proof. By Lemma 2.1 we get that
$$D_N\left((\beta\left\lfloor \alpha p(an+b)\right\rfloor)_{n=1}^N\right) \ll \frac{1}{H} + \sum_{h=1}^{H} \frac{1}{h} \left|\frac{1}{N}\sum_{n=1}^{N} e\left(h\beta\left\lfloor \alpha p(an+b)\right\rfloor\right)\right|, \tag{4.5}$$
where $H \geq 1$ is a positive integer we choose later.

As above we concentrate on the exponential sum. Using our definitions of F and G_r with integer $r \geq 1$ and real $\delta > 0$ in (2.1) and (2.2), respectively, we obtain

$$\begin{aligned}\sum_{n=1}^{N} e\left(h\beta\left\lfloor \alpha p(an+b)\right\rfloor\right) &= \sum_{n=1}^{N} e\left(h\beta\alpha p(an+b)\right) F\left(\alpha p(an+b), -h\beta\right) \\ &= \sum_{n=1}^{N} e\left(h\beta\alpha p(an+b)\right) G_r\left(\alpha p(an+b), -h\beta, \delta\right) + \mathcal{O}\left(R\right),\end{aligned} \tag{4.6}$$

where

$$R = \sum_{n=1}^{N} \left|F(\alpha p(an+b), -h\beta) - G_r(\alpha p(an+b), -h\beta, \delta)\right|.$$

Using Lemma 2.3 together with the estimate of the distribution in Proposition 3.1 we get for the error term R that

$$\begin{aligned}R &\ll Nr\delta + Nr^2\delta\left|h\beta\right| + ND_N\left(\left(\alpha p(an+b)\right)_{n=1}^{N}\right) \\ &\ll Nr\delta + Nr^2\delta\left|h\beta\right| + a^{\frac{dt}{2t+1}+\varepsilon} N^{1-\frac{2-2^{2-d}}{2^{d-1}(2t+1)}+\varepsilon}.\end{aligned}$$

We return to the exponential sum. Fourier transforming G_r we get

$$\begin{aligned}&\sum_{n=1}^{N} e\left(h\beta\alpha p(an+b)\right) G_r\left(\alpha p(an+b), -h\beta, \delta\right) \\ &= \sum_{k\in\mathbb{Z}} \widehat{G_r}(k, -h\beta, \delta) \sum_{n=1}^{N} e\left((h\beta - k)\alpha p(an+b)\right) \\ &= \sum_{|k|\leq K} \widehat{G_r}(k, -h\beta, \delta) \sum_{n=1}^{N} e\left((h\beta - k)\alpha p(an+b)\right) + \mathcal{O}\left(N(\delta K)^{-r}\right),\end{aligned} \tag{4.7}$$

where we used Lemma 2.4 in the last step.

Again we concentrate on the weighted exponential sum. The idea is to apply Lemma 3.2. Using Holder's inequality we separate the Fourier coefficient and the exponential sum. Thus

$$\begin{aligned}&\sum_{|k|\leq K} \widehat{G_r}(k, -h\beta, \delta) \sum_{n=1}^{N} e\left((h\beta - k)\alpha p(an+b)\right) \\ &\ll \left(\sum_{|k|\leq K} \left|\widehat{G_r}(k, -h\beta, \delta)\right|^{\frac{2^{d-1}}{2^{d-1}-1}}\right)^{\frac{2^{d-1}-1}{2^{d-1}}} \left(\sum_{|k|\leq K} \left|\sum_{n=1}^{N} e\left((h\beta - k)\alpha p(an+b)\right)\right|^{2^{d-1}}\right)^{\frac{1}{2^{d-1}}} \\ &\ll \left(\sum_{|k|\leq K} \left|\sum_{n=1}^{N} e\left((h\beta - k)\alpha p(an+b)\right)\right|^{2^{d-1}}\right)^{\frac{1}{2^{d-1}}},\end{aligned}$$

where, this time, we used Lemma 2.5 in the last step.

Since the vector $(\alpha, \alpha\beta)$ is of finite type t, an application of Lemma 3.2 yields

$$\left|\sum_{n=1}^{N} e((h\beta - k)\alpha p(an+b))\right|^{2^{d-1}} \ll a^{d\frac{2t}{2t+1}+\varepsilon} \left|hk\right|^{\frac{t}{2t+1}+\varepsilon} N^{2^{d-1}-\frac{2-2^{2-d}}{2t+1}+\varepsilon}.$$

Summing over k we get

$$\sum_{|k|\leq K} \widehat{G_r}(k,-h\beta,\delta)\sum_{n=1}^{N} e\left((h\beta-k)\alpha p(an+b)\right) \ll a^{\frac{d}{2^{d-1}}\frac{2t}{2t+1}+\varepsilon}\left|h\right|^{\frac{t}{2^{d-1}(2t+1)}+\varepsilon}K^{\frac{3t+1}{2^{d-1}(2t+1)}+\varepsilon}N^{1-\frac{2-2^{2-d}}{2^{d-1}(2t+1)}+\varepsilon}.$$

Let $\rho>0$ and $\theta>0$ be real parameters, which we will choose in an instant. Then we set

$$\delta^{-1}=hN^{\theta} \quad \text{and} \quad K=h^{\rho}N^{\theta},$$

Plugging every estimate we have so far in (4.7) and then in (4.6) and (4.5) yields

$$D_N\left(\left(\beta\left\lfloor\alpha p(an+b)\right\rfloor\right)_{n=1}^{N}\right) \ll a^{\frac{d}{2^{d-1}}\frac{2t}{2t+1}+\varepsilon}H^{\frac{t}{2^{d-1}(2t+1)}+\rho\frac{3t+1}{2^{d-1}(2t+1)}+\varepsilon}N^{-\frac{2-2^{2-d}}{2^{d-1}(2t+1)}+\theta\frac{3t+1}{2^{d-1}(2t+1)}+\varepsilon} + H^{r(1-\rho)}+H^{-1}+N^{-\theta}+N^{-\theta}\log H+a^{d\frac{t}{2t+1}+\varepsilon}N^{-\frac{2-2^{2-d}}{2^{d-1}(2t+1)}+\varepsilon}.$$

Now we choose $\rho=1+\varepsilon_1$, with $\varepsilon_1=\varepsilon_1(\varepsilon,t)>0$ sufficiently small, and r an integer such that $r>\frac{1}{\varepsilon_1}$. Then clearly $H^{r(1-\rho)}\ll H^{-1}$. Finally we set $H=a^{-\sigma}N^{\theta}$ with

$$\sigma=\frac{2dt}{2^{d-1}(2t+1)+4t+1} \quad \text{and} \quad \theta=\frac{2-2^{2-d}}{2^{d-1}(2t+1)+7t+2}$$

yielding the desired estimate.

5. The second iteration

Now we iterate the process one step further and provide the following.

Proposition 5.1. *Let α_1, α_2 and β be reals and let $p\in\mathbb{R}[x]$ be a monic polynomial of degree $d\geq 2$. Suppose that the vector $(\alpha_2,\alpha_1\alpha_2,\alpha_1\alpha_2\beta)$ is of finite type t with $t>0$. Then*

$$D_N\left(\left(\beta\left\lfloor\alpha_1\left\lfloor\alpha_2 p(an+b)\right\rfloor\right\rfloor\right)_{n=1}^{N}\right) \ll a^{\frac{3dt}{2^d(3t+1)+5t+1}}N^{-\frac{(2-2^{2-d})2^{d-1}(3t+1)}{(2^{d-1}(3t+1)+21t+5)(2^d(3t+1)+4t+1)}}.$$

Proof. Again we start with the Erdős-Turán inequality: For $H\geq 1$ we obtain

$$D_N\left(\left(\beta\left\lfloor\alpha_1\left\lfloor\alpha_2 p(an+b)\right\rfloor\right\rfloor\right)_{n=1}^{N}\right) \ll \frac{1}{H}+\sum_{h=1}^{H}\frac{1}{h}\left|\frac{1}{N}\sum_{n=1}^{n} e\left(h\beta\left\lfloor\alpha_1\left\lfloor\alpha_2 p(an+b)\right\rfloor\right\rfloor\right)\right|. \tag{5.8}$$

Now we focus on the innermost exponential sum and use the approximation of the fractional part as above to get for an integer $r_1\geq 1$ and a real $\delta_1>0$ (which we will fix later) that

$$\begin{aligned}\sum_{n=1}^{n} & e\left(h\beta\left\lfloor\alpha_1\left\lfloor\alpha_2 p(an+b)\right\rfloor\right\rfloor\right)\\ &=\sum_{n=1}^{n} e\left(h\beta\alpha_1\left\lfloor\alpha_2 p(an+b)\right\rfloor\right)F(\alpha_1\left\lfloor\alpha_2 p(an+b)\right\rfloor,-h\beta) \qquad (5.9)\\ &=\sum_{n=1}^{n} e\left(h\beta\alpha_1\left\lfloor\alpha_2 p(an+b)\right\rfloor\right)G_{r_1}(\alpha_1\left\lfloor\alpha_2 p(an+b)\right\rfloor,-h\beta,\delta_1)+\mathcal{O}(R_1),\end{aligned}$$

where

$$R_1 = \sum_{n=1}^{N} \left| F(\alpha_1 \lfloor \alpha_2 p(an+b) \rfloor, -h\beta) - G_{r_1}(\alpha_1 \lfloor \alpha_2 p(an+b) \rfloor, -h\beta, \delta_1) \right|. \tag{5.10}$$

Again we use the Fourier series expansion of G_{r_1} to get

$$\begin{aligned}
&\sum_{n=1}^{n} e\left(h\beta\alpha_1 \lfloor \alpha_2 p(an+b) \rfloor\right) G_{r_1}(\alpha_1 \lfloor \alpha_2 p(an+b) \rfloor, -h\beta, \delta_1) \\
&\quad = \sum_{k_1 \in \mathbb{Z}} \widehat{G_{r_1}}(k_1, -h\beta, \delta_1) \sum_{n=1}^{n} e\left((h\beta - k_1)\, \alpha_1 \lfloor \alpha_2 p(an+b) \rfloor\right) \\
&\quad = \sum_{|k_1| \leq K_1} \widehat{G_{r_1}}(k_1, -h\beta, \delta_1) \sum_{n=1}^{n} e\left((h\beta - k_1)\, \alpha_1 \lfloor \alpha_2 p(an+b) \rfloor\right) + \mathcal{O}\left(N(\delta_1 K_1)^{-r_1}\right),
\end{aligned}$$

where we applied Lemma 2.4 in the last step.

Since we got rid of only one floor function we need to iterate the whole procedure to eliminate the second one. By a similar argument we get

$$\begin{aligned}
&\sum_{n=1}^{n} e\left((h\beta - k_1)\, \alpha_1 \lfloor \alpha_2 p(an+b) \rfloor\right) \\
&\qquad = \sum_{n=1}^{n} e\left((h\beta - k_1)\, \alpha_1 \lfloor \alpha_2 p(an+b) \rfloor\right) G_{r_2}\left(\alpha_2 p(an+b), -(h\beta - k_1)\alpha_1, \delta_2\right) + \mathcal{O}\left(R_2\right),
\end{aligned}$$

where

$$R_2 = \sum_{n=1}^{N} \left| F\left(\alpha_2 p(an+b), -(h\beta - k_1)\alpha_1\right) - G_{r_2}\left(\alpha_2 p(an+b), -(h\beta - k_1)\alpha_1, \delta_2\right) \right|. \tag{5.11}$$

Furthermore using the Fourier series of G_{r_2} and a truncation yields

$$\begin{aligned}
&\sum_{n=1}^{n} e\left((h\beta - k_1)\, \alpha_1 \lfloor \alpha_2 p(an+b) \rfloor\right) G_{r_2}\left(\alpha_2 p(an+b), -(h\beta - k_1)\alpha_1, \delta_2\right) \\
&\quad = \sum_{|k_2| \leq K_2} \widehat{G_{r_2}}\left(k_2, -(h\beta - k_1)\alpha_1, \delta_2\right) \sum_{n=1}^{n} e\left((h\alpha_1\alpha_2\beta - k_1\alpha_1\alpha_2 - k_2\alpha_2)\, p(an+b)\right) \\
&\qquad + \mathcal{O}\left(N\left(\delta_2 K_2\right)^{-r_2}\right).
\end{aligned}$$

Let's pause for a moment and summarise what we have so far. Plugging everything into the original exponential sum in (5.9) we have

$$\left| \frac{1}{N} \sum_{n=1}^{n} e\left(h\beta \lfloor \alpha_1 \lfloor \alpha_2 p(an+b) \rfloor \rfloor\right) \right| \ll S_1 + S_2 + S_3 + S_4 + S_5, \tag{5.12}$$

where

$$S_1 = \sum_{|k_1|\le K_1} \widehat{G_{r_1}}(k_1, -h\beta, \delta_1) \sum_{|k_2|\le K_2} \widehat{G_{r_2}}(k_2, -(h\beta - k_1)\alpha_1, \delta_2) \times \left| \frac{1}{N} \sum_{n=1}^{n} e\left((h\alpha_1\alpha_2\beta - k_1\alpha_1\alpha_2 - k_2\alpha_2)\, p(an+b)\right) \right|$$

$$S_2 = \sum_{|k_1|\le K_1} \widehat{G_{r_1}}(k_1, -h\beta, \delta_1)\,(\delta_2 K_2)^{-r_2}$$

$$S_3 = \sum_{|k_1|\le K_1} \widehat{G_{r_1}}(k_1, -h\beta, \delta_1) \frac{R_2}{N}$$

$$S_4 = (\delta_1 K_1)^{-r_1} \qquad \text{and}$$

$$S_5 = \frac{R_1}{N}.$$

We start with S_1 since it is the only part involving sums over k_1 and k_2. Applying Hölder's inequality we get

$$|S_1| \ll \left(\sum_{|k_1|\le K_1} \sum_{|k_2|\le K_2} \left| \widehat{G_{r_1}}(k_1, -h\beta, \delta_1) \widehat{G_{r_2}}(k_2, -(h\beta - k_1)\alpha_1, \delta_2) \right|^{\frac{2^{d-1}}{2^{d-1}-1}} \right)^{\frac{2^{d-1}-1}{2^{d-1}}} \times \left(\sum_{|k_1|\le K_1} \sum_{|k_2|\le K_2} \left| \frac{1}{N} \sum_{n=1}^{n} e\left((h\alpha_1\alpha_2\beta - k_1\alpha_1\alpha_2 - k_2\alpha_2)\, p(an+b)\right) \right|^{2^{d-1}} \right)^{\frac{1}{2^{d-1}}}.$$

Since $\frac{2^{d-1}}{2^{d-1}-1} > 1$ a double application of Lemma 2.5 yields

$$|S_1| \ll \left(\sum_{|k_1|\le K_1} \sum_{|k_2|\le K_2} \left| \frac{1}{N} \sum_{n=1}^{n} e\left((h\alpha_1\alpha_2\beta - k_1\alpha_1\alpha_2 - k_2\alpha_2)\, p(an+b)\right) \right|^{2^{d-1}} \right)^{\frac{1}{2^{d-1}}}.$$

By assumption $(\alpha_1\alpha_2\beta, \alpha_1\alpha_2, \alpha_2)$ is of type t and we may apply Lemma 3.2 to get

$$|S_1| \ll \left(\sum_{|k_1|\le K_1} \sum_{|k_2|\le K_2} a^{\frac{3dt}{3t+1}+\varepsilon} \left| hk_1k_2 \right|^{\frac{t}{3t+1}+\varepsilon} N^{-\frac{2-2^{2-d}}{3t+1}+\varepsilon} \right)^{\frac{1}{2^{d-1}}}.$$

Summing over k_2 yields

$$|S_1| \ll \left(\sum_{|k_1|\le K_1} a^{\frac{3dt}{3t+1}+\varepsilon} \left| hk_1 \right|^{\frac{t}{3t+1}+\varepsilon} N^{-\frac{2-2^{2-d}}{3t+1}+\varepsilon} K_2^{\frac{4t+1}{3t+1}+\varepsilon} \right)^{\frac{1}{2^{d-1}}}. \tag{5.13}$$

We continue with part S_3 and again use Hölder's inequality to get rid of the Fourier coefficients. Following the same arguments and applying Lemma 2.5 and Lemma 2.3 yields

$$|S_3| \ll \left(\sum_{|k_1|\le K_1} \left| \widehat{G_{r_1}}(k_1, -h\beta, \delta_1) \right|^{\frac{2^{d-1}}{2^{d-1}-1}} \right)^{\frac{2^{d-1}-1}{2^{d-1}}} \left(\sum_{|k_1|\le K_1} \left| \frac{R_2}{N} \right|^{2^{d-1}} \right)^{\frac{1}{2^{d-1}}} \ll \left(\sum_{|k_1|\le K_1} \left(r_2\delta_2 + r_2^2\delta_2 \left| h\beta\alpha_1 - k_1\alpha_1 \right| + D_N\left((\alpha_2 p(an+b))_{n=1}^{N} \right) \right)^{2^{d-1}} \right)^{\frac{1}{2^{d-1}}}. \tag{5.14}$$

Now we want to choose r_2, δ_2 and K_2 such that S_1 dominates S_3. Therefore we first set $\rho_2 = 1+\varepsilon_2$ with $\varepsilon_2 = \varepsilon_2(d,t) > 0$ sufficiently small and $r_2 > \frac{1}{\varepsilon_2}$. Furthermore we set

$$\delta_2^{-1} = |hk_1|\, N^{\theta_2} \quad \text{and} \quad K_2 = |hk_1|^{\rho_2}\, N^{\theta_2} \quad \text{with} \quad \theta_2 = \frac{2-2^{2-d}}{2^{d-1}(3t+1)+4t+1}.$$

Then using Proposition 3.1 for the discrepancy we get that

$$S_3 \ll S_1 \ll \left(\sum_{|k_1| \leq K_1} a^{\frac{3dt}{3t+1}+\varepsilon} |hk_1|^{\frac{5t+1}{3t+1}+\varepsilon} N^{-\frac{2^{d-1}(2-2^{2-d})}{2^{d-1}(3t+1)+4t+1}+\varepsilon} \right)^{\frac{1}{2^{d-1}}}.$$

Summing over k_1 yields

$$S_1 \ll a^{\frac{3dt}{2^{d-1}(3t+1)}+\varepsilon} h^{\frac{5t+1}{2^{d-1}(3t+1)}+\varepsilon} N^{-\frac{2-2^{2-d}}{2^{d-1}(3t+1)+4t+1}+\varepsilon} K_1^{\frac{8t+2}{2^{d-1}(3t+1)}+\varepsilon}.$$

Again we set $\rho_1 = 1+\varepsilon_1$ with $\varepsilon_1 = \varepsilon_1(d,t) > 0$ sufficiently small and $r_1 > \frac{1}{\varepsilon_1}$. Let $\theta_1 > 0$ be a parameter we choose in an instant. Setting

$$\delta_1^{-1} = hN^{\theta_1} \quad \text{and} \quad K_1 = h^{\rho_1} N^{\theta_1}$$

we get

$$S_1 \ll a^{\frac{3dt}{2^{d-1}(3t+1)}+\varepsilon} h^{\frac{13t+3}{2^{d-1}(3t+1)}+\varepsilon} N^{-\frac{2-2^{2-d}}{2^{d-1}(3t+1)+4t+1}+\theta_1 \frac{8t+2}{2^{d-1}(3t+1)}+\varepsilon}.$$

Finally we recall the outer sum over h in (5.8) to get

$$\sum_{h=1}^{H} \frac{1}{h} S_1 \ll a^{\frac{3dt}{2^{d-1}(3t+1)}+\varepsilon} H^{\frac{13t+3}{2^{d-1}(3t+1)}+\varepsilon} N^{-\frac{2-2^{2-d}}{2^{d-1}(3t+1)+4t+1}+\theta_1 \frac{8t+2}{2^{d-1}(3t+1)}+\varepsilon}. \tag{5.15}$$

Now we turn our attention to the sum S_2. Again by Hölder's inequality we get

$$\begin{aligned} |S_2| &\ll \left(\sum_{|k_1| \leq K_1} \left| \widehat{G_{r_1}}(k_1, -h\beta, \delta_1) \right|^{\frac{2^{d-1}}{2^{d-1}-1}} \right)^{\frac{2^{d-1}-1}{2^{d-1}}} \left(\sum_{|k_1| \leq K_1} \left| (\delta_2 K_2)^{-r_2} \right|^{2^{d-1}} \right)^{\frac{1}{2^{d-1}}} \\ &\ll \left(\sum_{|k_1| \leq K_1} |hk_1|^{-2^{d-1}+\varepsilon} \right)^{\frac{1}{2^{d-1}}}, \end{aligned}$$

where we have used that

$$(\delta_2 K_2)^{-r_2} = |hk_1|^{-(\rho_2-1)r_2} \leq |hk_1|^{-1+\varepsilon}.$$

Summing over k_1 yields

$$\begin{aligned} |S_2| &\ll \left(|h|^{-2^d+1+\varepsilon} N^{2^{d-1}-\theta_1(2^{d-1}-1)+\varepsilon} \right)^{\frac{1}{2^{d-1}}} \\ &\ll h^{-\frac{2^d-1}{2^{d-1}}+\varepsilon} N^{-\theta_1 \frac{2^{d-1}-1}{2^{d-1}}+\varepsilon} \end{aligned}$$

and finally summing over h in (5.8) we get

$$\sum_{h=1}^{H} \frac{1}{h} S_2 \ll H^{-\frac{2^d-1}{2^{d-1}}+\varepsilon} N^{-\theta_1 \frac{2^{d-1}-1}{2^{d-1}}+\varepsilon} \tag{5.16}$$

By similar calculations we obtain

$$\sum_{h=1}^{H} \frac{1}{h} S_4 \ll H^{-1} \quad \text{and} \quad \sum_{h=1}^{H} \frac{1}{h} S_5 \ll N^{-\theta_1}. \tag{5.17}$$

Now we set $H = a^{-\sigma} N^{\theta_1}$ and choose

$$\sigma = \frac{3dt}{2^d(3t+1)+5t+1} \quad \text{and} \quad \theta_1 = \frac{(2-2^{2-d})2^{d-1}(3t+1)}{(2^{d-1}(3t+1)+21t+5)(2^d(3t+1)+4t+1)}.$$

Replacing the four parts (5.15), (5.16) and (5.17) in the Erdős-Turán inequality (5.8) proves the proposition.

6. Proof of Theorem 1.1

As indicated in the introduction we link the estimate of along the arithmetic progressions with the discrepancy estimate we obtained in the section above. To this end we fix an arbitrary arithmetic progression, *i.e.* let $a \in \mathbb{N}^*$, $b \in \mathbb{Z}$ and $1 \le x \le N$. Then

$$\begin{aligned}\left|\sum_{am+b\le x} e_{am+b}\right| &\le \left|\sum_{am+b\le x}\left(\mathbb{1}_{\{f(am+b)\}<\frac{1}{2}} - \frac{1}{2}\right)\right| + \left|\sum_{am+b\le x}\left(\mathbb{1}_{\{f(am+b)\}\ge\frac{1}{2}} - \frac{1}{2}\right)\right| \\ &\le 2MD_M\left(\left(\beta\lfloor\alpha_1\lfloor\alpha_2 p(am+b)\rfloor\rfloor\right)_{m=1}^M\right),\end{aligned}$$

where $M = \left\lfloor \frac{x-b}{a} \right\rfloor$.

Now we distinguish two cases according to the size of a, namely if

$$a \le x^{\frac{1}{(2^d(3t+1)+21t+5)^2}}$$

or not. In the first case we may apply Proposition 5.1 and get that there exists $\eta_1 = \eta_1(d,t)$ such that

$$\left|\sum_{am+b\le x} e_{am+b}\right| \ll x^{1-\eta_1}.$$

In the second case we have

$$a > x^{\frac{1}{(2^d(3t+1)+21t+5)^2}}$$

and a trivially estimate yields

$$\left|\sum_{am+b\le x} e_{am+b}\right| \ll x^{1-\frac{1}{(2^d(3t+1)+21t+5)^2}}.$$

Thus the theorem is proven by these two cases.

Acknowledgement. The first author is supported by project ANR-18-CE40-0018 funded by the French National Research Agency. Furthermore both authors received support from the bilateral project of the Agence nationale de la recherche (ANR-23-CE40-0024) and the Austrian science fund (FWF, I 6750).

References

[Ais13] C. Aistleitner. On the limit distribution of the well-distribution measure of random binary sequences. *J. Théor. Nombres Bordeaux*, 25(2):245–259, 2013.

[BHS21] V. Bergelson, I. J. Hå land Knutson, and Y. Son. An extension of Weyl's equidistribution theorem to generalized polynomials and applications. *Int. Math. Res. Not. IMRN*, (19):14965–15018, 2021.

[BKM14] V. Bergelson, G. Kolesnik, M. Madritsch, Y. Son, and R. Tichy. Uniform distribution of prime powers and sets of recurrence and van der Corput sets in $\mathbb{Z}^k$. *Israel J. Math.*, 201(2):729–760, 2014.

[BKS19] V. Bergelson, G. Kolesnik, and Y. Son. Uniform distribution of subpolynomial functions along primes and applications. *J. Anal. Math.*, 137(1):135–187, 2019.

[DrTi97] M. Drmota and R. F. Tichy. *Sequences, discrepancies and applications*, volume 1651 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.

[GrKo91] S. W. Graham and G. Kolesnik. *van der Corput's method of exponential sums*, volume 126 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1991.

[GrRa96] A. Granville and O. Ramaré. Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients. *Mathematika*, 43(1):73–107, 1996.

[HoRa16] R. Hofer and O. Ramaré. Discrepancy estimates for some linear generalized monomials. *Acta Arith.*, 173(2):183–196, 2016.

[KuNi74] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Wiley-Interscience [John Wiley & Sons], New York, 1974. Pure and Applied Mathematics.

[MRT24] M. G. Madritsch, J. Rivat, and R. F. Tichy. On finite pseudorandom binary sequences: functions from a Hardy field. *Acta Math. Hungar.*, 174(1):121–137, 2024.

[MaTi16] M. G. Madritsch and R. F. Tichy. Dynamical systems and uniform distribution of sequences. In *From arithmetic to zeta-functions*, pages 263–276. Springer, [Cham], 2016.

[MaTi19] M. G. Madritsch and R. F. Tichy. Multidimensional van der Corput sets and small fractional parts of polynomials. *Mathematika*, 65(2):400–435, 2019.

[MRS02] C. Mauduit, J. Rivat, and A. Sárközy. On the pseudo-random properties of n^c. *Illinois J. Math.*, 46(1):185–197, 2002.

[MaSá97] C. Mauduit and A. Sárközy. On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. *Acta Arith.*, 82(4):365–377, 1997.

[MaSá00a] C. Mauduit and A. Sárközy. On finite pseudorandom binary sequences. V. On $(n\alpha)$ and $(n^2\alpha)$ sequences. *Monatsh. Math.*, 129(3):197–216, 2000.

[MaSá00b] C. Mauduit and A. Sárközy. On finite pseudorandom binary sequences. VI. On $(n^k\alpha)$ sequences. *Monatsh. Math.*, 130(4):281–298, 2000.

[Mon94] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994.

[MRV18] A. Mukhopadhyay, O. Ramaré, and G. K. Viswanadham. Discrepancy estimates for generalized polynomials. *Monatsh. Math.*, 187(2):343–356, 2018.

[Nat96] M. B. Nathanson. *Additive number theory*, volume 164 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. The classical bases.

[RiTe05] J. Rivat and G. Tenenbaum. Constantes d'Erdős-Turán. *Ramanujan J.*, 9(1-2):111–121, 2005.

Manfred G. Madritsch
Université de Lorraine, CNRS
IECL, F-54000 Nancy, France

e-mail: manfred.madritsch@univ-lorraine.fr

and

Robert F. Tichy
Graz University of Technology
Institute of Analysis and Number
Theory, 8010 Graz, Austria

e-mail: tichy@tugraz.at