On discrepancy estimates for pseudorandom vectors constructed by the elliptic curve congruential generator

[1,2]Ziran Liu, [1]Chung Pang Mok

[1]Shanghai Institute for Mathematics and Interdisciplinary Sciences (SIMIS)
Shanghai 200433, China
[2]Research Institute of Intelligent Complex Systems, Fudan University,
Shanghai 200433, China

zliu@simis.cn, cpmok@simis.cn

Abstract

This paper studies the problem of discrepancy estimates for pseudorandom vectors constructed by the elliptic curve congruential generator, particularly in the non-translational case. Two families of results are obtained. First, in a full-coset regime characterized by a *relative maximal period condition* (RMPC) on an induced one-dimensional linear congruential generator, one proves bounds of type $q^{1/2}/t$ for the discrepancy D, the serial discrepancy D_s, and, under the corresponding derived RMPC, the non-overlapping discrepancy $\widetilde{D}_s$. Second, in the general sub-period regime, one reduces bounds for D, D_s, and $\widetilde{D}_s$ to estimation of Fourier ℓ^1 masses of admissible index sets attached to one-dimensional linear congruential generators. This isolates the arithmetic bottleneck for further improvement.

Contents

1 Introduction

Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field of cardinality q with identity element $O \in E(\mathbb{F}_q)$; here as usual $E(\mathbb{F}_q)$ is the group of points of $E/\mathbb{F}_q$ with coordinates in $\mathbb{F}_q$. Fix a non-zero integer e and a point $Q \in E(\mathbb{F}_q)$. Consider the affine iteration using the addition law on $E/\mathbb{F}_q$ (here in general for any integer e then $[e]$ is the multiplication by e map on E):

$$P_{n+1} = [e]P_n + Q, \qquad n \geq 0, \tag{1}$$

starting from a point $P_0 \in E(\mathbb{F}_q)$ (the seed); thus we have the points $P_n \in E(\mathbb{F}_q)$ for $n \geq 0$ (recall that by the Hasse bound we have $|\#E(\mathbb{F}_q) - (q+1)| \leq 2q^{1/2}$). This could be regarded as the elliptic curve version of the linear congruential generator, or the elliptic curve congruential generator for short (despite this name, it should be noted though that it is a highly non-linear generator, due to the fact that the addition law of E is given by non-linear rational functions of the coordinates). To ease notations we assume throughout the paper that P_0 lies in a purely periodic orbit, and t denotes the period, i.e. the least positive integer such that $P_t = P_0$.

In [1] an algorithm is given for the construction of pseudorandom vectors in a unit hypercube. The constructions are obtained from the output map when it is being applied to the orbit $\{P_n\}_{n\geq 0}$ (we recall the definitions in section two; see also [2] where Monte Carlo numerical experiments are carried out by using these pseudorandom vectors). In *loc. cit.* we established, in the translation case $e = 1$ (in this paper we call this as case A), explicit upper bounds for the discrepancy D (that gives quantitative measure of uniformity of distribution), the serial s-discrepancy D_s and its non-overlapping version $\widetilde{D}_s$ (that give quantitative measure of statistical independence, here $2 \leq s \leq t$), by reducing these bounds to bounds for additive character sums over (cyclic) subgroups of $E(\mathbb{F}_q)$, and then applying square-root cancellation for such sums. These discrepancies bounds in particular justify the name *pseudorandom* when $t \gg q^{1/2+\epsilon}$ for $\epsilon > 0$ (at least in the translational case $e = 1$). In this paper we focus on the case where $e \neq 1$. This presents much more serious difficulties, though it was observed in *loc. cit.* that if the period is maximal, i.e. $t = \#E(\mathbb{F}_q)$, then the same estimate for the discrepancy D remains valid by reducing the situation to a maximal translation orbit. However the estimation of the serial s-discrepancy D_s, and the non-overlapping s-discrepancy $\widetilde{D}_s$ remain open when $e \neq 1$ (even in the case $t = \#E(\mathbb{F}_q)$).

The main results proved in this paper are of two kinds:

1. In a *full-coset regime* (Case B), the orbit does not necessarily cover $E(\mathbb{F}_q)$, but it covers a full coset of a cyclic subgroup canonically attached to (e, P_0, Q). In this regime one recovers bounds of type $q^{1/2}/t$ as in [1].

2. In the *general sub-period regime* (Case C), the orbit is a proper subset of that coset. In this regime the discrepancy problem is reduced to the estimation of Fourier ℓ^1 mass of an admissible index set associated with a one-dimensional linear congruential generator.

The paper is organized as follows. Section 2 recalls some of the materials from [1] including the definitions of the output map, the notion of discrepancies, relation with Walsh functions, and exponential sums over subgroups of $E(\mathbb{F}_q)$. Section 3 treats the full-coset regime and proves bounds of size $q^{1/2}/t$ under the relative maximal period condition. Section 4 treats the general sub-period regime and reduces all three discrepancy problems to the estimation of Fourier masses. Section 5 analyzes the arithmetic structure of the index sequence and derives the strengthened results in the no mixed local factors regime (see Corollary 26 of Section 5.1 for the definition).

2 Résumé from [1]

2.1 The digital output map

As usual p is the characteristic of the finite field $\mathbb{F}_q$. Write

$$q = p^{ar}$$

with integers $a, r \geq 1$, and fix the tower of field extensions:

$$\mathbb{F}_q/\mathbb{F}_{p^a}/\mathbb{F}_p.$$

(in Monte Carlo applications one fixes a choice of a, r and p, and then put $q = p^{ar}$). Choose an $\mathbb{F}_{p^a}$-basis $\{\lambda_1, \ldots, \lambda_r\}$ of $\mathbb{F}_q$ with the corresponding dual basis $\{\lambda'_1, \ldots, \lambda'_r\}$ with respect to $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^a}}$, and an $\mathbb{F}_p$-basis $\{\kappa_1, \ldots, \kappa_a\}$ of $\mathbb{F}_{p^a}$, with the corresponding dual basis $\{\kappa'_1, \ldots, \kappa'_a\}$ with respect to $\mathrm{Tr}_{\mathbb{F}_{p^a}/\mathbb{F}_p}$. Following section 2.3 of [1], define for any $\eta \in \mathbb{F}_q$ and $1 \leq j \leq r$:

$$\phi_j(\eta) := \sum_{i=1}^{a} \frac{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\eta \lambda'_j \kappa'_i)}{p^i} \in [0, 1).$$

(here we fix $\{0, 1, \cdots, p-1\} \subset \mathbb{Z}$ to be the set of representatives of elements of $\mathbb{F}_p$). We remark that in the notation of [1] we have $\phi_j(\eta) = \Phi(\langle \eta \rangle_j)$ for any $\eta \in \mathbb{F}_q$ and $1 \leq j \leq r$.

Let x, y be the usual affine Weierstrass coordinates for $E/\mathbb{F}_q$ (with respect to a choice of affine Weierstrass equation for $E/\mathbb{F}_q$). Define

$$G : E(\mathbb{F}_q) \setminus \{O\} \to [0, 1)^{2r}$$

by the following: for $P \in E(\mathbb{F}_q) \setminus \{O\}$, put

$$G(P) := \big(\phi_1(x(P)), \ldots, \phi_r(x(P)), \phi_1(y(P)), \ldots, \phi_r(y(P))\big) \in [0, 1)^{2r}. \tag{2}$$

This is the the output map G defined in [1] (with respect to the above choices): for each $P \in E(\mathbb{F}_q) \setminus \{O\}$, the elements $x(P)$ and $y(P)$ of $\mathbb{F}_q$ are expanded relative to the chosen field bases and then converted into points of $[0, 1)$ by base-p expansions. Thus we obtain the point $G(P)$ in the unit hypercube $[0, 1)^{2r}$. The output map G is easily seen to be injective.

In [1] one also assigns an output value to O, namely $G(O) = (1, \ldots, 1)$ (in fact assigning any point in $[0, 1]^{2r} \setminus [0, 1)^{2r}$ as a value for $G(O)$ works equally well). This gives the (injective) output map $G : E(\mathbb{F}_q) \to [0, 1]^{2r}$

2.2 Notation for admissible output collections

For the orbit $\{P_n\}_{n\geq 0}$ of (1), which we assume as in the Introduction that it is purely periodic with t being the period: $P_t = P_0$, the admissible output collection $\mathcal{P} \subset [0,1)^{2r}$ is:

$$\mathcal{P} := \big\{G(P_n)\big\}_{\substack{0\leq n<t \\ P_n\neq O}}.$$

Its cardinality is denoted as N^*.

For integers $2 \leq s \leq t$, the admissible serial s-tuple collection, denoted by $\mathcal{P}^{(s)} \subset [0,1)^{2rs}$, is given by:

$$\big\{(G(P_n),\ldots,G(P_{n+s-1}))\big\}_{\substack{0\leq n<t \\ P_n,\cdots,P_{n+s-1}\neq O}}$$

with the block $(G(P_n),\ldots,G(P_{n+s-1}))$ being regarded as a point of $[0,1)^{2rs}$. The cardinality of $\mathcal{P}^{(s)}$ is denoted as N_s^*.

Finally for $2 \leq s \leq t$ the admissible non-overlapping s-tuple collection, denoted by $\widetilde{\mathcal{P}}^{(s)} \subset [0,1)^{2rs}$, is given by:

$$\big\{(G(P_{ns}),G(P_{ns+1})\ldots,G(P_{ns+s-1}))\big\}_{\substack{0\leq n<t/\gcd(s,t) \\ P_{ns},P_{ns+1}\cdots,P_{ns+s-1}\neq O}}$$

with the block $(G(P_{ns}),G(P_{ns+1})\ldots,G(P_{ns+s-1}))$ again being regarded as a point of $[0,1)^{2rs}$. The cardinality of $\widetilde{\mathcal{P}}^{(s)}$ is denoted as $\widetilde{N}_s^*$.

If the orbit $\{P_n\}_{n\geq 0}$ avoids O, then $N^* = N_s^* = t$, and $\widetilde{N}_s^* = t/\gcd(s,t)$. If the orbit contains O, the admissible counts are obtained by deleting exactly those points or blocks in which O appears; in this case we have $N^* = t-1$, $N_s^* = t-s$, and $\widetilde{N}_s^* = (t-s)/\gcd(s,t)$.

Throughout the paper, any bound on discrepancy (the definition is recalled in section 2.3 below) that involves:

$$\mathcal{P}, \quad \mathcal{P}^{(s)}, \quad \widetilde{\mathcal{P}}^{(s)}$$

is understood under the natural assumption that the corresponding admissible point collection is nonempty.

2.3 Point collections and discrepancy

Firstly consider in general any finite collection of points $\mathcal{P}$ in $[0,1)^d$ (here d is any positive integer). Here below we consider axis-parallel d-dimensional box of the form:

$$B = \prod_{j=1}^{d} [a_j, b_j) \subset [0,1)^d,$$

The *extreme discrepancy* or just discrepancy of $\mathcal{P} \subset [0,1)^d$ is

$$D(\mathcal{P}) := \sup_B \left| \frac{\#(\mathcal{P}\cap B)}{\#\mathcal{P}} - \mathrm{vol}(B) \right|,$$

where the supremum runs over all axis-parallel d-dimensional boxes B in $[0,1)^d$ (it is regarded as undefined if $\mathcal{P}$ is empty). We have $0 \leq D(\mathcal{P}) \leq 1$ and it is a quantitative measure of the uniformity

of distribution of $\mathcal{P}$ with respect to the usual Lebesgue measure on $[0,1)^d$ (the closer is $D(\mathcal{P})$ to zero, the more uniform is the distribution).

Now in general consider a finite sequence of t *distinct* points:

$$\{v_n\}_{0\le n<t}, \quad v_n \in [0,1]^d$$

in the unit hypercube $[0,1]^d$ of dimension d. Denote by $\mathcal{P} \subset [0,1)^d$ the admissible collection given by:

$$\mathcal{P} = \{v_0, \cdots, v_{t-1}\} \cap [0,1)^d$$

The discrepancy of the sequence $\{v_n\}_{0\le n<t}$ is then defined to be the discrepancy of $\mathcal{P} \subset [0,1)^d$.

For $2 \le s \le t$ the admissible *serial s-tuple collection* is

$$\mathcal{P}^{(s)} := \big\{(v_n, \ldots, v_{n+s-1})\big\}_{\substack{0\le n<t \\ v_n,\cdots,v_{n+s-1}\in[0,1)^d}}$$

where the indices are taken modulo t, and the block $(v_n, \ldots, v_{n+s-1})$ being understood as a point of $[0,1)^{ds}$; the corresponding serial s-discrepancy of of the sequence $\{v_n\}_{0\le n<t}$, is defined to be the discrepancy of $\mathcal{P}^{(s)} \subset [0,1)^{ds}$.

We similarly define the admissible *non-overlapping* s-tuple collection as:

$$\widetilde{\mathcal{P}}^{(s)} := \big\{(v_{ns}, v_{ns+1}, \ldots, v_{ns+s-1})\big\}_{\substack{0\le n<t/\gcd(s,t) \\ v_{ns},v_{ns+1},\cdots,v_{ns+s-1}\in[0,1)^d}}$$

again with indices taken modulo t, and the block $(v_{ns}, v_{ns+1} \ldots, v_{ns+s-1})$ being understood as a point of $[0,1)^{ds}$. The corresponding non-overlapping s-discrepancy of of the sequence $\{v_n\}_{0\le n<t}$, is defined to be the discrepancy of $\widetilde{\mathcal{P}}^{(s)} \subset [0,1)^{ds}$.

Given the finite sequence $\{v_n\}_{0\le n<t}$ the discrepancy is a quantitative measure of the uniformity of distribution (with respect to the usual Lebesgue measure of $[0,1)^d$), while the serial s-discrepancy (or its non-overlapping version) is a quantitative measure of statistical independence of s successive terms of the sequence.

2.4 Walsh function and Erdös-Turan-Koksma type inequality

We recall the base-p Walsh function system. Firstly some notations. For any non-negative integer k we write:

$$k = \sum_{i=1}^{\infty} k(i) p^{i-1}, \qquad k(i) \in \{0, 1, \cdots, p-1\}$$

be the unique expansion of k in base p (all but finitely many of the $k(i)$'s are equal to zero). Next every $\xi \in [0,1)$ has a unique base p expansion:

$$\xi = \sum_{i=1}^{\infty} \frac{\xi(i)}{p^i}, \qquad \xi(i) \in \{0, 1, \cdots, p-1\}$$

with the condition that $\xi(i) \ne p-1$ for infinitely many i. Then define:

$$w_k(\xi) = \exp\Big(\frac{2\pi i}{p} \sum_{i=1}^{\infty} k(i)\xi(i)\Big)$$

We refer to k as the Walsh frequency.

In dimension $d \geq 1$, for $\mathbf{k} = (k^{(1)}, \cdots, k^{(d)})$ where $k^{(1)}, \cdots, k^{(d)}$ are non-negative integers, and $\xi = (\xi^{(1)} \cdots, \xi^{(d)})$, where $\xi^{(1)}, \cdots, \xi^{(d)} \in [0,1)$, define:

$$w_{\mathbf{k}}(\xi) = w_{k^{(1)}}(\xi^{(1)}) \cdots w_{k^{(d)}}(\xi^{(d)})$$

We refer to $\mathbf{k}$ as the vector Walsh frequency, or for short, again just as Walsh frequency.

For $\mathcal{P} \subset [0,1)^d$ a (non-empty) finite set, put for Walsh frequency $\mathbf{k}$:

$$S(w_{\mathbf{k}}, \mathcal{P}) = \frac{1}{\#\mathcal{P}} \sum_{\xi \in \mathcal{P}} w_{\mathbf{k}}(\xi)$$

Now fix a positive integer a and we make the assumption that for all $\xi \in \mathcal{P}$, all the coordinates of $p^a \cdot \xi$ are integers. Note that this condition is satisfied with $\mathcal{P}$ being the admissible output collection, or the admissible serial (or non-overlapping) s-tuple collection as in section 2.2 (with the same value of a in section 2.1). Now with respect to this fixed value of a and the dimension d, we let Δ_d to be the set of all $\mathbf{k} = (k^{(1)}, \cdots, k^{(d)})$ such that $0 \leq k^{(1)}, \cdots, k^{(d)} < p^a$. Finally put $\Delta_d^* = \Delta_d \setminus \{(0, \cdots, 0)\}$.

We now state the Erdös-Turn-Koksma type inequality with respect to the Walsh function system as established by Hellekalek [4]:

Lemma 1. *(Corollary 4 of [4]) Let $\mathcal{P} \subset [0,1)^d$ be a finite point collection lying on the grid $\{0, 1/p^a, \ldots, (p^a-1)/p^a\}^d$. Assume that for every nonzero Walsh frequency $\mathbf{k} \in \Delta_d^*$ one has:*

$$|S(w_{\mathbf{k}}, \mathcal{P})| \leq B,$$

for some real number B. Then there is some absolute constant C_0 such that:

$$D(\mathcal{P}) \leq 1 - \left(1 - \frac{1}{p^a}\right)^d + B \left(C_0 \ln(p^a) + 1\right)^d, \tag{3}$$

In [4] a value of C_0 is given as 2.43, or one can take $C_0 = 1.78$ by [3, Lemma 2.1]. Note also that the term:

$$1 - \left(1 - \frac{1}{p^a}\right)^d$$

is as a discretization error term.

2.5 Evaluation of Walsh function on the image of the output map

We now consider the evaluation of the Walsh function on the image of the output map G; thus the dimension d is now equal to $2r$. The value of a is as in section 2.1.

Firstly let

$$\psi_1(z) := \exp\left(\frac{2\pi i}{p} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(z)\right), \qquad z \in \mathbb{F}_q,$$

be the standard non-trivial additive character of $\mathbb{F}_q$. Any other non-trivial additive character of $\mathbb{F}_q$ is then given by ψ_a for some $a \in \mathbb{F}_q^\times$, where $\psi_a(z) = \psi_1(a \cdot z)$ for $z \in \mathbb{F}_q$.

Lemma 2. *For each nonzero Walsh frequency $\mathbf{k} \in \Delta_{2r}^*$ there exists elements $\eta_{\mathbf{k}}, \widetilde{\eta}_{\mathbf{k}} \in \mathbb{F}_q$, not both zero, such that for all $P \in E(\mathbb{F}_q) \setminus \{O\}$, we have:*

$$w_{\mathbf{k}}(G(P)) = \psi_1\big(\eta_{\mathbf{k}} \cdot x(P) + \widetilde{\eta}_{\mathbf{k}} \cdot y(P)\big).$$

Consequently, for any subset $S \subset E(\mathbb{F}_q)$, and the point collection

$$\mathcal{P} = \{G(P)\}_{P \in S,\ P \neq O},$$

one has

$$|\mathcal{P}| \cdot S(w_{\mathbf{k}}, \mathcal{P}) = \sum_{P \in S,\ P \neq O} \psi_1\big(\eta_{\mathbf{k}} \cdot x(P) + \widetilde{\eta}_{\mathbf{k}} \cdot y(P)\big) \tag{4}$$

Proof. This is a standard computation, see [1, (5.2)–(5.3)] or [3, (2.2)–(2.3)]. Explicitly with $\mathbf{k} = (k^{(1)}, \cdots, k^{(2r)})$ we have:

$$\eta_{\mathbf{k}} = \sum_{j=1}^{r} \sum_{i=1}^{a} k^{(j)}(i) \lambda_j' \kappa_i'$$

and

$$\widetilde{\eta}_{\mathbf{k}} = \sum_{j=1}^{r} \sum_{i=1}^{a} k^{(r+j)}(i) \lambda_j' \kappa_i'$$

□

2.6 Twisted subgroup character sums

We need the following square-root cancellation estimate of Kohel-Shparlinski [5]. Firstly $\mathbb{F}_q(E)$ is the function field of E over $\mathbb{F}_q$, and $\overline{\mathbb{F}}_q(E)$ is the function field of E over $\overline{\mathbb{F}}_q$ (the algebraic closure of $\mathbb{F}_q$). We say that an element $f \in \mathbb{F}_q(E)$ is *non-degenerate*, if $f \neq g^p - g$ for any $g \in \overline{\mathbb{F}}_q(E)$ (f is thus necessarily non-constant).

Lemma 3. *(Corollary 1 of [5]) Let $H \subset E(\mathbb{F}_q)$ be a subgroup, and ω be a group character of H. For ψ a nontrivial additive character of $\mathbb{F}_q$ and a non-degenerate $f \in \mathbb{F}_q(E)$, we have:*

$$\left| \sum_{\substack{P \in H \\ f(P) \neq \infty}} \omega(P) \psi(f(P)) \right| \leq 2 \deg(f)\, q^{1/2}. \tag{5}$$

Moreover, if the polar divisor of f is supported on a single prime divisor of E, then

$$\left| \sum_{\substack{P \in H \\ f(P) \neq \infty}} \omega(P) \psi(f(P)) \right| \leq (1 + \deg(f))\, q^{1/2}. \tag{6}$$

2.7 Auxiliary facts on separable multiplication maps and poles

The following two lemmas are standard and are used repeatedly in the proofs. These concern the geometric properties of E, i.e. of E over $\overline{\mathbb{F}}_q$.

Lemma 4. *Let $n \in \mathbb{Z}$. Then $[n] : E \to E$ is an isogeny of degree n^2; it is separable if $\gcd(n, p) = 1$. Moreover:*

(i) for every $A \in E(\overline{\mathbb{F}}_q)$, the translation map $\tau_A(P) := P + A$ is an automorphism of E over $\overline{\mathbb{F}}_q$ (as a genus one curve), so in particular is of degree 1;

(ii) for every nonconstant $f \in \overline{\mathbb{F}}_q(E)$,

$$\deg(f \circ \tau_A) = \deg(f), \qquad \deg(f \circ [n]) = n^2 \deg(f),$$

and hence

$$\deg(f \circ (\tau_A \circ [n])) = n^2 \deg(f);$$

(iii) if $\gcd(n, p) = 1$ and f has a pole of order m at $Q \in E(\overline{\mathbb{F}}_q)$, then $f \circ (\tau_A \circ [n])$ has poles of order m at the set $[n]^{-1}(Q - A)$. In particular, since $[n]$ is separable, this set has cardinality equal to n^2 over $\overline{\mathbb{F}}_q$.

Proof. We work with E over $\overline{\mathbb{F}}_q$. It is immediate that translations are automorphisms of E (as a genus one curve). It is also standard fact that the map $[n]$ is an isogeny of degree n^2 and is separable whenever $\gcd(n, p) = 1$. The degree identities follow from standard facts on morphisms of curves and pullback of rational functions.

For part (iii), if f has a pole of order m at Q, then $f \circ \tau_A$ has a pole of order m at $Q - A$. Pulling back by the separable map $[n]$ preserves the pole order at each point of the fibre and yields exactly n^2 distinct preimages. □

Lemma 5. *Let $f \in \overline{\mathbb{F}}_q(E)$. If f has a pole whose order is not divisible by p, then $f \neq h^p - h$ for any $h \in \overline{\mathbb{F}}_q(E)$.*

Proof. We again work with E over $\overline{\mathbb{F}}_q$. If h has a pole of order m at some point of $E(\overline{\mathbb{F}}_q)$, then $h^p - h$ has a pole of order pm there, since the term h^p dominates h at the pole. Therefore every pole order of a function of the form $h^p - h$ is divisible by p. The claim follows. □

3 The full-coset regime (Case B)

Throughout this section assume $|e| \geq 2$ (indeed when $e = -1$ then the period of the orbit is at most two and so this case could be ignored). As in the Introduction we assume that the orbit $\{P_n\}_{n \geq 0}$ is purely periodic and we let t be the period.

3.1 Orbit reduction to a cyclic coset

Lemma 6 (Orbit reduction to a cyclic coset)**.** *Let $\{P_n\}_{n \geq 0}$ satisfy (1). Define*

$$\beta_n := \frac{e^n - 1}{e - 1} \in \mathbb{Z} \qquad (n \geq 0;\ \beta_0 = 0), \qquad R := P_1 - P_0 = (e - 1)P_0 + Q \in E(\mathbb{F}_q).$$

Then for all $n \geq 0$,

$$P_n = P_0 + [\beta_n]R. \tag{7}$$

In particular, the full orbit $\{P_n\}_{n \geq 0}$ is contained in the coset $P_0 + \langle R \rangle$, where $\langle R \rangle$ is the cyclic subgroup of $E(\mathbb{F}_q)$ generated by R.

Proof. By induction on n one first obtains

$$P_n = [e^n]P_0 + [\beta_n]Q,$$

using the recursion $\beta_{n+1} = e\beta_n + 1$. Subtracting P_0 gives

$$P_n - P_0 = [e^n - 1]P_0 + [\beta_n]Q = [\beta_n]\big((e-1)P_0 + Q\big) = [\beta_n]R,$$

which is (7). □

Lemma 7. *With R as above put $m = \mathrm{ord}(R)$, the order of R in $E(\mathbb{F}_q)$. Then:*

$$\gcd(e, m) = 1.$$

Proof. Let $d := \gcd(e, m)$. If $d > 1$, then the defining recursion $\beta_{n+1} = e\beta_n + 1$ gives, modulo d,

$$\beta_{n+1} \equiv e\beta_n + 1 \equiv 1 \pmod{d} \qquad (n \geq 0),$$

because $d \mid e$. Hence

$$\beta_n \equiv 1 \pmod{d} \qquad \text{for all } n \geq 1,$$

while $\beta_0 \equiv 0 \pmod{d}$. On the other hand as t is the period of the orbit we have $P_t = P_0$, so Lemma 6 gives

$$[\beta_t]R = O.$$

Since $\mathrm{ord}(R) = m$, it follows that $m \mid \beta_t$, hence $d \mid \beta_t$. This contradicts $\beta_t \equiv 1 \pmod{d}$. Therefore $d = 1$. □

Thus let

$$m := \mathrm{ord}(R), \qquad H := \langle R \rangle \subset E(\mathbb{F}_q).$$

Reducing (7) modulo H, one sees that the period t of the orbit $\{P_n\}_{n\geq 0}$ is equal to the period of the sequence $\{\beta_n \bmod m\}_{n\geq 0}$. Moreover,

$$\beta_{n+1} \equiv e\beta_n + 1 \pmod{m}, \qquad \beta_0 \equiv 0 \pmod{m}. \tag{8}$$

Thus the triple (e, P_0, Q) that defines the elliptic curve congruential generator (1) then induces a linear congruential generator (LCG) on $\mathbb{Z}/m\mathbb{Z}$.

3.2 The relative maximal period condition

Definition 8 (RMPC)**.** The triple (e, P_0, Q) is said to satisfy the *relative maximal period condition* if the LCG (8) has full period $m = \mathrm{ord}(R)$, that is,

$$\{\beta_0, \ldots, \beta_{t-1} \bmod m\} = \mathbb{Z}/m\mathbb{Z}.$$

Equivalently, $t = m$, i.e. the orbit point set is the full coset $P_0 + \langle R \rangle$.

Lemma 9 (Hull–Dobell criterion for RMPC)**.** *The LCG (8) has full period m if and only if:*

(i) for every prime $\ell \mid m$, one has $\ell \mid (e-1)$;

(ii) if $4 \mid m$, then $4 \mid (e-1)$.

Proof. This is the classical Hull–Dobell criterion for the LCG $x_{n+1} \equiv ex_n + 1 \pmod{m}$ to have maximal period. □

As a simple example: take $Q = O$; let $M = \mathrm{ord}(P_0)$ and in the following ℓ denotes a prime dividing M; put $e = 1 + \prod_{\ell \mid M} \ell$ if 8 does not divide M, and $e = 1 + 2\prod_{\ell \mid M} \ell$ if 8 divides M. Then $e - 1$ divides M, and $R = P_1 - P_0 = [e-1]P_0$, hence $m = \mathrm{ord}(R) = M/(e-1)$. The Hull-Dobell criterion for RMPC is then seen to be satisfied.

3.3 Discrepancy bound under RMPC

Theorem 10 (Discrepancy bound in the full-coset regime)**.** *Assume RMPC and so* $t = m = \mathrm{ord}(R)$*. Define the admissible point collection as in section 2.1:*

$$\mathcal{P} := \{G(P_n)\}_{\substack{0\le n<t \\ P_n\neq O}} \subset [0,1)^{2r}, \qquad N^* := |\mathcal{P}|.$$

(recall that $N^* = t$ *if the orbit* $\{P_n\}_{n\ge 0}$ *avoids* O*, and is equal to* $t-1$ *otherwise).*

Assume $p \ge 5$*. Then*

$$D(\mathcal{P}) \le 1 - \Big(1 - \frac{1}{p^a}\Big)^{2r} + \frac{4q^{1/2}}{N^*}\big(C_0 \ln(p^a) + 1\big)^{2r}. \tag{9}$$

Proof. Under RMPC, Lemma 6 gives:

$$\{P_0, \dots, P_{t-1}\} = \{P_0 + [u]R : u \in \mathbb{Z}/t\mathbb{Z}\}.$$

Consider any nonzero Walsh frequency $\mathbf{k} \in \Delta_{2r}^*$. By Lemma 2,

$$N^* S(w_{\mathbf{k}}, \mathcal{P}) = \sum_{\substack{u=0 \\ P_0+[u]R\neq O}}^{t-1} \psi_1\big(\eta_{\mathbf{k}} \cdot x(P_0 + [u]R) + \widetilde{\eta}_{\mathbf{k}} \cdot y(P_0 + [u]R)\big).$$

with $\eta_{\mathbf{k}}, \widetilde{\eta}_{\mathbf{k}} \in \mathbb{F}_q$, not noth equal to zero.

Define

$$f_{\mathbf{k},P_0} := \eta_{\mathbf{k}} \cdot x \circ \tau_{P_0} + \widetilde{\eta}_{\mathbf{k}} \cdot y \circ \tau_{P_0} \in \mathbb{F}_q(E).$$

The polar divisor of $f_{\mathbf{k},P_0}$ is supported at the single point $-P_0$, with the order of pole being equal to either 2 or 3 (it is equal to 2 exactly when $\widetilde{\eta}_{\mathbf{k}}$ is zero); hence $\deg(f_{k,P_0}) \le 3$. Since $p \ge 5$, it follows in particular that the order of pole is not divisible by p; therefore Lemma 5 shows that $f_{\mathbf{k},P_0}$ is non-degenerate. We then have with $H = \langle R \rangle$:

$$\begin{aligned} N^* S(w_{\mathbf{k}}, \mathcal{P}) &= \sum_{\substack{u=0 \\ P_0+[u]R\neq O}}^{t-1} \psi_1(f_{\mathbf{k},P_0})([u]R) \\ &= \sum_{\substack{P\in H \\ f_{\mathbf{k},P_0}(P)\neq\infty}} \psi_1(f_{\mathbf{k},P_0})(P) \end{aligned}$$

Now applying Lemma 3 in the single-pole form (6) yields

$$\left| \sum_{\substack{P\in H \\ f_{\mathbf{k},P_0}(P)\neq\infty}} \psi_1(f_{\mathbf{k},P_0}(P)) \right| \le (1 + \deg(f_{\mathbf{k},P_0}))q^{1/2} \le 4q^{1/2}.$$

Hence $|S(w_{\mathbf{k}}, \mathcal{P})| \le 4q^{1/2}/N^*$ for every nonzero Walsh frequency $\mathbf{k} \in \Delta_{2r}^*$. Applying Lemma 1 with $d = 2r$ proves (9). □

3.4 Serial discrepancy bound under RMPC

Theorem 11 (Serial discrepancy in the full-coset regime)**.** *Assume RMPC,* $\gcd(e,p)=1$*, and* $p\geq 5$*. Fix* $2\leq s\leq t$*. Let* $\mathcal{P}^{(s)}\subset[0,1)^{2rs}$ *be the admissible serial* s*-tuple collection attached to the orbit* $\{P_n\}_{n\geq 0}$*, and let* $N_s^*:=|\mathcal{P}^{(s)}|$*.*

Then

$$D(\mathcal{P}^{(s)})\leq 1-\Big(1-\frac{1}{p^a}\Big)^{2rs}+\frac{6q^{1/2}\big(\sum_{\iota=0}^{s-1}e^{2\iota}\big)+s}{N_s^*}\big(C_0\ln(p^a)+1\big)^{2rs}. \tag{10}$$

Proof. Again under RMPC we have $t=m=\mathrm{ord}(R)$. Using the identity

$$\beta_{n+\iota}=\beta_\iota+e^\iota\beta_n$$

in $\mathbb{Z}$, one obtains

$$P_{n+\iota}=P_\iota+[e^\iota u]R,\qquad P_\iota=P_0+[\beta_\iota]R,\qquad u:=\beta_n \bmod t.$$

Define:

$$U_s:=\{u\in\mathbb{Z}/t\mathbb{Z}:P_\iota+[e^\iota u]R\neq O \text{ for all } 0\leq\iota\leq s-1\}$$

then the admissible serial s-tuple point collection $\mathcal{P}^{(s)}$ is the image of U_s under the injective map:

$$u\in\mathbb{Z}/t\mathbb{Z}\longmapsto\big(G(P_0+[u]R),G(P_1+[eu]R),\dots,G(P_{s-1}+[e^{s-1}u]R)\big)\in[0,1]^{2rs}.$$

In particular $|U_s|=|\mathcal{P}^{(s)}|=N_s^*$, that we recall is equal to t (resp. $t-s$) if the orbit $\{P_n\}_{n\geq 0}$ avoids O (resp. otherwise).

Now given a nonzero Walsh frequency $\mathbf{k}\in\Delta_{2rs}^*$, we then obtain as in Lemma 2 (see for example [1, (5.6)–(5.7)]), coefficients $(\eta_{\mathbf{k},\iota},\widetilde{\eta}_{\mathbf{k},\iota})\in\mathbb{F}_q^2$ for $0\leq\iota\leq s-1$, not all zero, such that

$$N_s^*S(w_{\mathbf{k}},\mathcal{P}^{(s)})=\sum_{u\in U_s}\psi_1\big(g_{\mathbf{k}}([u]R)\big),$$

explicitly,

$$\eta_{\mathbf{k},\iota}=\sum_{j=1}^{r}\sum_{i=1}^{a}k^{(2r\iota+j)}(i)\lambda_j'\kappa_i',$$

$$\widetilde{\eta}_{\mathbf{k},\iota}=\sum_{j=1}^{r}\sum_{i=1}^{a}k^{(2r\iota+r+j)}(i)\lambda_j'\kappa_i',$$

and

$$g_{\mathbf{k}}:=\sum_{\iota=0}^{s-1}\Big(\eta_{\mathbf{k},\iota}\cdot x\circ\tau_{P_\iota}\circ[e^\iota]+\widetilde{\eta}_{\mathbf{k},\iota}\cdot y\circ\tau_{P_\iota}\circ[e^\iota]\Big)\in\mathbb{F}_q(E).$$

For each $0\leq\iota\leq s-1$ the element:

$$\eta_{\mathbf{k},\iota}\cdot x+\widetilde{\eta}_{\mathbf{k},\iota}\cdot y\in\mathbb{F}_q(E).$$

is either identically equal to zero (namely when $\eta_{\mathbf{k},\iota}$ and $\widetilde{\eta}_{\mathbf{k},\iota}$ are both zero), or is non-constant with degree equal to 2 or 3, with a single pole supported at O (of order equal to 2 or 3). Hence the ι-th summand (in the sum that defines $g_{\mathbf{k}}$):

$$\eta_{\mathbf{k},\iota} \cdot x \circ \tau_{P_\iota} \circ [e^\iota] + \widetilde{\eta}_{\mathbf{k},\iota} \cdot y \circ \tau_{P_\iota} \circ [e^\iota] \in \mathbb{F}_q(E)$$

is either identically equal to zero, or is non-constant with degree equal to $2e^{2\iota}$ or $3e^{2\iota}$. In particular we obtain:

$$\deg(g_{\mathbf{k}}) \leq 3 \sum_{\iota=0}^{s-1} e^{2\iota}. \tag{11}$$

We next show that $g_{\mathbf{k}}$ is non-degenerate for each $\mathbf{k} \in \Delta^*_{2rs}$.

Let $0 \leq \iota_0 \leq s-1$ be maximal with $(\eta_{k,\iota_0}, \widetilde{\eta}_{k,\iota_0}) \neq (0,0)$. By Lemma 4 (here we use the condition that $\gcd(e,p) = 1$), the ι_0-th summand:

$$\eta_{\mathbf{k},\iota_0} \cdot x \circ \tau_{P_{\iota_0}} \circ [e^{\iota_0}] + \widetilde{\eta}_{\mathbf{k},\iota_0} \cdot y \circ \tau_{P_{\iota_0}} \circ [e^{\iota_0}] \in \mathbb{F}_q(E)$$

has pole set $[e^{\iota_0}]^{-1}(-P_{\iota_0})$ over $\overline{\mathbb{F}}_q$, with cardinality $e^{2\iota_0}$, and the order of these poles is either all equal to 2, or all equal to 3.

Now for each $\iota < \iota_0$, the cardinality of the pole set of the ι-th summand has is at most $e^{2\iota}$. Hence the union of all pole sets for $\iota < \iota_0$ has cardinality at most

$$\sum_{\iota=0}^{\iota_0-1} e^{2\iota} < e^{2\iota_0} \qquad (|e| \geq 2).$$

Therefore there exists a point P^* which is a pole of the ι_0-th summand and not a pole of any smaller ι-th summand. At P^* the ι_0-th summand has pole order 2 or 3. Thus $g_{\mathbf{k}}$ itself has a pole of order 2 or 3 at P^*. Since $p \geq 5$, this pole order is not divisible by p, and Lemma 5 implies that $g_{\mathbf{k}}$ is non-degenerate.

Finally for every $\mathbf{k} \in \Delta^*_{2rs}$ let

$$U_{\mathbf{k}} := \{u \in \mathbb{Z}/t\mathbb{Z} : g_{\mathbf{k}}([u]R) \neq \infty\}.$$

Then $U_s \subseteq U_{\mathbf{k}}$ for every $\mathbf{k} \in \Delta^*_{2rs}$, and in any case:

$$|U_{\mathbf{k}} \setminus U_s| \leq |\mathbb{Z}/t\mathbb{Z} \setminus U_s| \leq s.$$

Since each summand $\psi_1(g_{\mathbf{k}}([u]R))$ has absolute value 1 on $U_{\mathbf{k}}$, one obtains

$$\left| \sum_{u \in U_s} \psi_1(g_{\mathbf{k}}([u]R)) \right| \leq \left| \sum_{u \in U_{\mathbf{k}}} \psi_1(g_{\mathbf{k}}([u]R)) \right| + s.$$

Now with $H = \langle R \rangle$ we have:

$$\sum_{u \in U_{\mathbf{k}}} \psi_1(g_{\mathbf{k}}([u]R)) = \sum_{\substack{P \in H \\ g_{\mathbf{k}}(P) \neq \infty}} \psi_1(g_{\mathbf{k}}(P))$$

so Lemma 3 applied to the sum on the RHS (which is applicable as we have shown that $g_{\mathbf{k}}$ is non-degenerate), together with (11), give:

$$\left|\sum_{u\in U_{\mathbf{k}}} \psi_1(g_{\mathbf{k}}([u]R))\right| \le 2\deg(g_{\mathbf{k}})q^{1/2} \le 6q^{1/2}\sum_{\iota=0}^{s-1} e^{2\iota}.$$

Thus to conclude for every $\mathbf{k} \in \Delta^*_{2rs}$ we obtain:

$$\left|N_s^* S(w_{\mathbf{k}}, \mathcal{P}^{(s)})\right| \le 6q^{1/2}\sum_{\iota=0}^{s-1} e^{2\iota} + s.$$

Applying Lemma 1 with $d = 2rs$ proves (10). □

Remark 12. If the orbit $\{P_n\}_{n\ge 0}$ avoids O, then the boundary correction term $+s$ in (10) is not needed.

3.5 Non-overlapping discrepancy bound under a derived RMPC

Definition 13 (Derived RMPC)**.** Fix $s \ge 2$ and define

$$R_s := P_s - P_0, \quad \gamma_n = \frac{e^{ns}-1}{e^s-1}$$

Let $m_s := \mathrm{ord}(R_s)$. The *derived RMPC of step s* is the requirement that the LCG

$$\gamma_{n+1} \equiv e^s\gamma_n + 1 \pmod{m_s}, \qquad \gamma_0 \equiv 0 \pmod{m_s},$$

has full period m_s.

Just as in Lemma 9, by using the classical Hull-Dobell criterion, we see that the derived RMPC of step s is satisfied, if and only if:

(i) for every prime $\ell \mid m_s$, one has $\ell \mid (e^s - 1)$;

(ii) if $4 \mid m_s$, then $4 \mid (e^s - 1)$.

In particular as $m_s | m$ (because $R_s = P_s - P_0 = [\beta_s]R \in \langle R\rangle$), we see that RMPC implies derived RMPC of step s for any $s \ge 2$.

Theorem 14 (Non-overlapping discrepancy in the full-coset regime)**.** *Assume* $|e| \ge 2$, $\gcd(e, p) = 1$, *and* $p \ge 5$. *Fix* $s \ge 2$ *and assume the derived RMPC of step* s. *Let* $\widetilde{\mathcal{P}}^{(s)}$ *be the admissible non-overlapping* s*-tuple collection, and let* $\widetilde{N}_s^* := |\widetilde{\mathcal{P}}^{(s)}|$. *Then*

$$D(\widetilde{\mathcal{P}}^{(s)}) \le 1 - \left(1 - \frac{1}{p^a}\right)^{2rs} + \frac{6q^{1/2}\left(\sum_{\iota=0}^{s-1} e^{2\iota}\right) + s/\gcd(s,t)}{\widetilde{N}_s^*}\left(C_0\ln(p^a)+1\right)^{2rs}. \tag{12}$$

Proof. Firstly, the period of the sequence $\{P_{ns}\}_{n\geq 0}$ is equal to $L_s := t/\gcd(s,t)$, and by direct computation one has

$$P_{ns} = P_0 + [\gamma_n]R_s,$$

from which is follows firstly that that L_s is equal to the period of the LCG $\{\gamma_n \bmod m_s\}_{n\geq 0}$; secondly, the derived RMPC of step s is equivalent to the condition that the sequence $\{P_{ns}\}_{n\geq 0}$ traverses the full coset $P_0 + \langle R_s\rangle$, i.e. that:

$$L_s = m_s.$$

More generally one again obtain by direct computation that for $0 \leq \iota \leq s-1$ and $n \geq 0$:

$$P_{ns+\iota} = P_\iota + [e^\iota \gamma_n]R_s.$$

Thus under the derived RMPC of step s, define:

$$\widetilde{U}_s := \{u \in \mathbb{Z}/L_s\mathbb{Z} : P_\iota + [e^\iota u]R_s \neq O \text{ for all } 0 \leq \iota \leq s-1\}$$

then the admissible non-overlapping s-tuple collection $\widetilde{\mathcal{P}}^{(s)}$ is the image of $\widetilde{U}_s$ under the injective map:

$$u \in \mathbb{Z}/L_s\mathbb{Z} \longmapsto \big(G(P_0 + [u]R_s), G(P_1 + [eu]R_s), \ldots, G(P_{s-1} + [e^{s-1}u]R_s)\big) \in [0,1]^{2rs}.$$

Thus $|\widetilde{U}_s| = |\widetilde{\mathcal{P}}^{(s)}| = \widetilde{N}_s^*$, that we recall is equal to $L_s = t/\gcd(s,t)$ if the orbit $\{P_n\}_{n\geq 0}$ avoids O, and is equal to $(t-s)/\gcd(s,t)$ otherwise. In particular that

$$|\mathbb{Z}/L_s\mathbb{Z} \setminus \widetilde{U}_s| \leq s/\gcd(s,t).$$

The rest of the proof is then similar to the proof of Theorem 11. Fix $\mathbf{k} \in \Delta_{2rs}^*$. Then we have by similar considerations:

$$\widetilde{N}_s^* S(w_{\mathbf{k}}, \widetilde{\mathcal{P}}^{(s)}) = \sum_{u \in \widetilde{U}_s} \psi_1\big(g_{\mathbf{k}}([u]R_s)\big),$$

where $g_{\mathbf{k}} \in \mathbb{F}_q(E)$ is the same as in *loc. cit.*:

$$g_{\mathbf{k}} := \sum_{\iota=0}^{s-1} \Big(\eta_{\mathbf{k},\iota} \cdot x \circ \tau_{P_\iota} \circ [e^\iota] + \widetilde{\eta}_{\mathbf{k},\iota} \cdot y \circ \tau_{P_\iota} \circ [e^\iota]\Big)$$

and recall that we have established that

$$\deg(g_{\mathbf{k}}) \leq 3\sum_{\iota=0}^{s-1} e^{2\iota}$$

and that $g_{\mathbf{k}}$ is non-degenerate (under the same assumptions that $p \geq 5$ and $\gcd(e,p) = 1$).

Let

$$\widetilde{U}_{\mathbf{k}} := \{u \in \mathbb{Z}/L_s\mathbb{Z} :\ g_{\mathbf{k}}([u]R_s) \neq \infty\}.$$

Then $\widetilde{U}_s \subseteq \widetilde{U}_{\mathbf{k}}$, and so in any case that:

$$|\widetilde{U}_{\mathbf{k}} \setminus \widetilde{U}_s| \leq |\mathbb{Z}/L_s\mathbb{Z} \setminus \widetilde{U}_s| \leq s/\gcd(s,t).$$

Therefore

$$\left|\sum_{u\in\widetilde{U}_s}\psi_1(g_{\mathbf{k}}([u]R_s))\right| \le \left|\sum_{u\in\widetilde{U}_k}\psi_1(g_{\mathbf{k}}([u]R_s))\right| + s/\gcd(s,t).$$

Applying Lemma 3 with H being the cyclic subgroup $\langle R_s\rangle$ yields

$$\left|\sum_{u\in\widetilde{U}_{\mathbf{k}}}\psi_1(g_{\mathbf{k}}([u]R_s))\right| \le 2\deg(g_{\mathbf{k}})q^{1/2} \le 6q^{1/2}\sum_{\iota=0}^{s-1}e^{2\iota}.$$

Therefore

$$\left|\widetilde{N}_s^* S(w_{\mathbf{k}},\widetilde{\mathcal{P}}^{(s)})\right| \le 6q^{1/2}\sum_{\iota=0}^{s-1}e^{2\iota} + s/\gcd(s,t).$$

Finally applying Lemma 1 in dimension $2rs$ proves (12). □

Remark 15. If the orbit $\{P_n\}_{n\ge0}$ avoids O, then the boundary correction term $+s/\gcd(s,t)$ in (12) is not needed.

4 The general sub-period regime (Case C)

We retain the notation

$$R=(e-1)P_0+Q, \qquad m=\mathrm{ord}(R), \qquad H=\langle R\rangle,$$

$$\beta_n := \frac{e^n-1}{e-1}\in\mathbb{Z} \qquad (n\ge0;\ \beta_0=0)$$

and we write

$$B=\{\beta_0,\dots,\beta_{t-1} \bmod m\}\subset\mathbb{Z}/m\mathbb{Z}$$

for the cycle associated with the LCG (8) (recall that the period t of $\{P_n\}_{n\ge0}$ coincides with the period of the LCG (8); in particular $|B|=t$). Unlike Case B (namely RMPC), in this section we do **not** require $t=m$ (nor do we require the derived RMPC); thus apriori we could not directly apply Lemma 3. To deal with this we use Fourier techniques.

4.1 Definition of the Fourier ℓ^1 mass

Definition 16 (Fourier transform and Fourier ℓ^1 mass)**.** Let $M\ge1$ be a positive integer and let $A\subset\mathbb{Z}/M\mathbb{Z}$ be an arbitrary subset. Define the Fourier transform of $\mathbf{1}_A$ (the characteristic function of A as a subset of $\mathbb{Z}/M\mathbb{Z}$) as:

$$\widehat{\mathbf{1}_A}^{(M)}(j) := \sum_{u\in A} e^{-2\pi iju/M}, \qquad 0\le j<M,$$

and the Fourier ℓ^1 mass of A:

$$\mathcal{L}_M(A) := \frac{1}{M}\sum_{j=0}^{M-1}\left|\widehat{\mathbf{1}_A}^{(M)}(j)\right|.$$

We have the elementary but useful:

Lemma 17. *Let $M \geq 1$ and let $A \subset \mathbb{Z}/M\mathbb{Z}$ be an arbitrary subset. Then*

$$\mathcal{L}_M(A) \leq \sqrt{|A|}.$$

Proof. Parseval gives

$$\sum_{j=0}^{M-1} \left|\widehat{\mathbf{1}_A}^{(M)}(j)\right|^2 = M|A|.$$

Applying Cauchy–Schwarz,

$$\sum_{j=0}^{M-1} \left|\widehat{\mathbf{1}_A}^{(M)}(j)\right| \leq \sqrt{M}\sqrt{M|A|} = M\sqrt{|A|}.$$

Dividing by M gives the result. □

Lemma 18. *Let $S \in E(\mathbb{F}_q)$ has order M, and let $H_S = \langle S \rangle$. For any subset $A \subset \mathbb{Z}/M\mathbb{Z}$ and any function $F : H_S \to \mathbb{C}$, we have:*

$$\sum_{u \in A} F([u]S) = \frac{1}{M} \sum_{j=0}^{M-1} \widehat{\mathbf{1}_A}^{(M)}(j) \sum_{P \in H_S} \omega_j(P) F(P), \tag{13}$$

where for $j = 0, 1 \cdots, M-1$, ω_j is the group character of H_S given by $\omega_j([u]S) := e^{2\pi i j u/M}$.

Proof. This is the orthogonality relation on $\mathbb{Z}/M\mathbb{Z}$:

$$\mathbf{1}_A(u) = \frac{1}{M} \sum_{j=0}^{M-1} \widehat{\mathbf{1}_A}^{(M)}(j) e^{2\pi i j u/M}.$$

Substituting this expression into:

$$\sum_{u \in A} F([u]S) = \sum_{u \in \mathbb{Z}/M\mathbb{Z}} \mathbf{1}_A(u) F([u]S)$$

yields (13). □

Proposition 19 (Orbit-sum bound via Fourier ℓ^1 mass)**.** *Let $S \in E(\mathbb{F}_q)$ has order M, let $A \subset \mathbb{Z}/M\mathbb{Z}$ be an arbitrary subset, and let $f \in \mathbb{F}_q(E)$ be a rational function that is non-degenerate. Then*

$$\left| \sum_{\substack{u \in A \\ f([u]S) \neq \infty}} \psi_1(f([u]S)) \right| \leq 2 \deg(f)\, q^{1/2}\, \mathcal{L}_M(A). \tag{14}$$

If the polar divisor of f is supported on a single prime divisor of E, one may replace $2\deg(f)$ by $1 + \deg(f)$.

Proof. Define

$$F(P) := \begin{cases} \psi_1(f(P)), & f(P) \neq \infty, \\ 0, & f(P) = \infty. \end{cases}$$

Applying Lemma 18 with this F, the inner sum becomes exactly the finite-value twisted subgroup sum appearing in Lemma 3 (with the subgroup of $E(\mathbb{F}_q)$ being taken to be H_S and the group character being ω_j, $j = 0, 1, \cdots, M-1$). Taking absolute values and summing with weights $\left|\widehat{\mathbf{1}_A}^{(M)}(j)\right| / M$ yields (14). □

4.2 Admissible index sets

Recall the identity ($n \geq 0$):

$$P_n = P_0 + [\beta_n]R$$

and more generally ($n, \iota \geq 0$):

$$P_{n+\iota} = P_\iota + [e^\iota \beta_n]R$$

For one-point discrepancy, define

$$B_{\text{adm}} := \{u \in B : \ P_0 + [u]R \neq O\}.$$

Then $\mathcal{P}$ is the image of B_{adm} under the injective map:

$$u \in B \longmapsto G(P_0 + [u]R) \in [0,1]^{2r}.$$

and so

$$|B_{\text{adm}}| = |\mathcal{P}| = N^*, \qquad |B \setminus B_{\text{adm}}| \leq 1$$

For serial discrepancy of length s, define

$$B_{s,\text{adm}} := \{u \in B : \ P_\iota + [e^\iota u]R \neq O \text{ for all } 0 \leq \iota \leq s-1\}.$$

Then $\mathcal{P}^{(s)}$ is the image of $B_{s,\text{adm}}$ under the injective map:

$$u \in B \longmapsto \big(G(P_0 + [u]R), G(P_1 + [eu]R), \ldots, G(P_{s-1} + [e^{s-1}u]R)\big) \in [0,1]^{2rs}.$$

and so

$$|B_{s,\text{adm}}| = |\mathcal{P}^{(s)}| = N_s^*, \qquad |B \setminus B_{s,\text{adm}}| \leq s$$

For the non-overlapping variant, fix $s \geq 2$ and keep the notation

$$R_s := P_s - P_0, \qquad m_s := \text{ord}(R_s)$$

$$\gamma_n := \frac{e^{ns}-1}{e^s - 1} \in \mathbb{Z} \qquad (n \geq 0; \gamma_0 = 0)$$

$$L_s := t/\gcd(s,t).$$

and recall that L_s is the period of the sequence $\{P_{ns}\}_{n \geq 0}$.

Also recall that:

$$P_{ns} = P_0 + [\gamma_n]R_s, \qquad \gamma_{n+1} \equiv e^s \gamma_n + 1 \pmod{m_s}, \qquad \gamma_0 \equiv 0 \pmod{m_s}.$$

from which one deduces (as seen before) that L_s is equal to the period of the LCG $\{\gamma_n \bmod m_s\}_{n \geq 0}$.

Set

$$\widetilde{B}_s := \{\gamma_0, \ldots, \gamma_{L_s - 1} \bmod m_s\} \subset \mathbb{Z}/m_s\mathbb{Z}.$$

and define:

$$\widetilde{B}_{s,\text{adm}} := \{u \in \widetilde{B}_s : \ P_\iota + [e^\iota u]R_s \neq O \text{ for all } 0 \leq \iota \leq s-1\}.$$

Again recall the more general identity $(n, \iota \geq 0)$:

$$P_{ns+\iota} = P_\iota + [e^\iota \gamma_n] R_s$$

and thus $\widetilde{\mathcal{P}}^{(s)}$ is the image of $\widetilde{B}_{s,\mathrm{adm}}$ under the injective map:

$$u \in \widetilde{B}_s \longmapsto \big(G(P_0 + [u]R_s), G(P_1 + [eu]R_s), \ldots, G(P_{s-1} + [e^{s-1}u]R_s)\big) \in [0,1]^{2rs}.$$

and so

$$|\widetilde{B}_{s,\mathrm{adm}}| = |\widetilde{\mathcal{P}}^{(s)}| = \widetilde{N}_s^*, \qquad |\widetilde{B}_s \setminus \widetilde{B}_{s,\mathrm{adm}}| \leq s/\gcd(s,t)$$

Lemma 20. *Let $M \geq 1$ and let $A \subseteq B \subseteq \mathbb{Z}/M\mathbb{Z}$. Then*

$$\mathcal{L}_M(A) \leq \mathcal{L}_M(B) + |B \setminus A|^{1/2}.$$

In particular,

$$\mathcal{L}_m(B_{\mathrm{adm}}) \leq \mathcal{L}_m(B) + 1,$$
$$\mathcal{L}_m(B_{s,\mathrm{adm}}) \leq \mathcal{L}_m(B) + s^{1/2},$$
$$\mathcal{L}_{m_s}(\widetilde{B}_{s,\mathrm{adm}}) \leq \mathcal{L}_{m_s}(\widetilde{B}_s) + \big(s/\gcd(s,t)\big)^{1/2},$$

Proof. Write $B = A \sqcup C$ with $C = B \setminus A$. Then

$$\widehat{\mathbf{1}_A}^{(M)}(j) = \widehat{\mathbf{1}_B}^{(M)}(j) - \widehat{\mathbf{1}_C}^{(M)}(j),$$

so

$$\left|\widehat{\mathbf{1}_A}^{(M)}(j)\right| \leq \left|\widehat{\mathbf{1}_B}^{(M)}(j)\right| + \left|\widehat{\mathbf{1}_C}^{(M)}(j)\right|.$$

Summing over j and dividing by M gives

$$\mathcal{L}_M(A) \leq \mathcal{L}_M(B) + \mathcal{L}_M(C).$$

Apply Lemma 17 to obtain $\mathcal{L}_M(C) \leq |C|^{1/2}$ and we are done. □

Remark 21. If the orbit $\{P_n\}_{n\geq 0}$ avoids O, then $B = B_{\mathrm{adm}} = B_{s,\mathrm{adm}}$, and $\widetilde{B}_s = \widetilde{B}_{s,\mathrm{adm}}$, and so the boundary correction terms:

$$+1, \qquad +s^{1/2}, \qquad +(s/\gcd(s,t))^{1/2}$$

in Lemma 20 are not needed.

4.3 Discrepancy bound in the general sub-period regime

Theorem 22 (Discrepancy bound via admissible Fourier mass)**.** *Let*

$$\mathcal{P} := \{G(P_n)\}_{\substack{0\leq n<t,\\ P_n \neq O}}, \qquad N^* := |\mathcal{P}|.$$

Assume $p \geq 5$. Then

$$D(\mathcal{P}) \leq 1 - \Big(1 - \frac{1}{p^a}\Big)^{2r} + \frac{4q^{1/2}}{N^*}\,\mathcal{L}_m(B_{\mathrm{adm}})\,\big(C_0 \ln(p^a) + 1\big)^{2r}. \tag{15}$$

Consequently,

$$D(\mathcal{P}) \leq 1 - \Big(1 - \frac{1}{p^a}\Big)^{2r} + \frac{4q^{1/2}}{N^*}\,\big(\mathcal{L}_m(B) + 1\big)\,\big(C_0 \ln(p^a) + 1\big)^{2r}. \tag{16}$$

Proof. We know that $\mathcal{P}$ is the image of B_{adm} under

$$u \in B \longmapsto G(P_0 + [u]R) \in [0,1]^{2r}$$

So given Walsh frequency $\mathbf{k} \in \Delta_{2r}^*$, by Lemma 2, we have

$$N^* S(w_{\mathbf{k}}, \mathcal{P}) = \sum_{u \in B_{\mathrm{adm}}} \psi_1\big(\eta_{\mathbf{k}} x(P_0 + [u]R) + \widetilde{\eta}_{\mathbf{k}} y(P_0 + [u]R)\big).$$

Hence

$$N^* S(w_{\mathbf{k}}, \mathcal{P}) = \sum_{u \in B_{\mathrm{adm}}} \psi_1\big(f_{\mathbf{k},P_0}([u]R)\big).$$

where $f_{\mathbf{k},P_0}$ is as in Theorem 10, where we have shown that it is non-degenerate and $\deg(f_{\mathbf{k},P_0}) \le 3$. Applying Proposition 19 with $f = f_{\mathbf{k},P_0}$, $S = R$, $M = m$, and $A = B_{\mathrm{adm}}$ gives

$$|N^* S(w_{\mathbf{k}}, \mathcal{P})| \le (1 + \deg(f_{\mathbf{k},P_0}))q^{1/2}\,\mathcal{L}_m(B_{\mathrm{adm}}) \le 4q^{1/2}\mathcal{L}_m(B_{\mathrm{adm}}).$$

Applying Lemma 1 with $d = 2r$ yields (15). The rougher estimate (16) follows from Lemma 20. □

4.4 Serial discrepancy in the general sub-period regime

Theorem 23 (Serial discrepancy bound via admissible Fourier mass)**.** *Assume* $|e| \ge 2$, $\gcd(e,p) = 1$, *and* $p \ge 5$. *Fix* $2 \le s < t$ *and let* $\mathcal{P}^{(s)}$ *be the admissible serial* s*-tuple collection, of cardinality* N_s^*. *Then*

$$D(\mathcal{P}^{(s)}) \le 1 - \Big(1 - \frac{1}{p^a}\Big)^{2rs} + \frac{6q^{1/2}}{N_s^*}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\mathcal{L}_m(B_{s,\mathrm{adm}})\,\big(C_0 \ln(p^a) + 1\big)^{2rs}. \tag{17}$$

Consequently,

$$D(\mathcal{P}^{(s)}) \le 1 - \Big(1 - \frac{1}{p^a}\Big)^{2rs} + \frac{6q^{1/2}}{N_s^*}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\big(\mathcal{L}_m(B) + s^{1/2}\big)\,\big(C_0 \ln(p^a) + 1\big)^{2rs}. \tag{18}$$

Proof. We know that $\mathcal{P}^{(s)}$ is the image of $B_{s,\mathrm{adm}}$ under the injective map:

$$u \in B \longmapsto \big(G(P_0 + [u]R), G(P_1 + [eu]R), \ldots, G(P_{s-1} + [e^{s-1}u]R)\big) \in [0,1]^{2rs}$$

So given Walsh frequency $\mathbf{k} \in \Delta_{2rs}^*$, we have as in the proof of Theorem 11:

$$N_s^* S(w_{\mathbf{k}}, \mathcal{P}^{(s)}) = \sum_{u \in B_{s,\mathrm{adm}}} \psi_1\big(g_{\mathbf{k}}([u]R)\big)$$

where $g_{\mathbf{k}}$ is the same function in the proof of Theorem 11, where we have shown that it is non-degenerate and

$$\deg(g_{\mathbf{k}}) \le 3\sum_{\iota=0}^{s-1} e^{2\iota}$$

Applying Proposition 19 with $f = g_{\mathbf{k}}$, $S = R$, $M = m$, and $A = B_{s,\mathrm{adm}}$ yields

$$\Big|N_s^* S(w_{\mathbf{k}}, \mathcal{P}^{(s)})\Big| \le 2\deg(g_{\mathbf{k}})q^{1/2}\,\mathcal{L}_m(B_{s,\mathrm{adm}}) \le 6q^{1/2}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\mathcal{L}_m(B_{s,\mathrm{adm}}).$$

Applying Lemma 1 in dimension $2rs$ yields (17). The rough bound (18) follows from Lemma 20. □

4.5 Non-overlapping discrepancy in the general sub-period regime

Theorem 24 (Non-overlapping discrepancy bound via admissible Fourier mass)**.** *Assume $|e| \geq 2$, $\gcd(e,p) = 1$, and $p \geq 5$. Fix $s \geq 2$ and let $\widetilde{\mathcal{P}}^{(s)}$ be the admissible non-overlapping s-tuple collection, of cardinality $\widetilde{N}_s^*$. Then*

$$D(\widetilde{\mathcal{P}}^{(s)}) \leq 1 - \Big(1 - \frac{1}{p^a}\Big)^{2rs} + \frac{6q^{1/2}}{\widetilde{N}_s^*}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\mathcal{L}_{m_s}(\widetilde{B}_{s,\mathrm{adm}})\,\big(C_0\ln(p^a)+1\big)^{2rs}. \tag{19}$$

Consequently,

$$D(\widetilde{\mathcal{P}}^{(s)}) \leq 1 - \Big(1 - \frac{1}{p^a}\Big)^{2rs} + \frac{6q^{1/2}}{\widetilde{N}_s^*}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\Big(\mathcal{L}_{m_s}(\widetilde{B}_s) + \big(s/\gcd(s,t)\big)^{1/2}\Big)\,\big(C_0\ln(p^a)+1\big)^{2rs} \tag{20}$$

Proof. We know that $\widetilde{\mathcal{P}}^{(s)}$ is the image of $\widetilde{B}_{s,\mathrm{adm}}$ under the injective map:

$$u \in \widetilde{B}_s \longmapsto \big(G(P_0 + [u]R_s), G(P_1 + [eu]R_s), \ldots, G(P_{s-1} + [e^{s-1}u]R_s)\big) \in [0,1]^{2rs}$$

So given Walsh frequency $\mathbf{k} \in \Delta_{2rs}^*$, we have as in the proof of Theorem 14:

$$\widetilde{N}_s^* S(w_{\mathbf{k}}, \widetilde{\mathcal{P}}^{(s)}) = \sum_{u \in \widetilde{B}_{s,\mathrm{adm}}} \psi_1\big(g_{\mathbf{k}}([u]R_s)\big)$$

Applying Proposition 19 with $f = g_{\mathbf{k}}$, $S = R_s$, $M = m_s$, and $A = \widetilde{B}_{s,\mathrm{adm}}$ yields

$$\Big|\widetilde{N}_s^* S(w_{\mathbf{k}}, \widetilde{\mathcal{P}}^{(s)})\Big| \leq 2\deg(g_{\mathbf{k}})q^{1/2}\,\mathcal{L}_{m_s}(\widetilde{B}_{s,\mathrm{adm}}) \leq 6q^{1/2}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\mathcal{L}_{m_s}(\widetilde{B}_{s,\mathrm{adm}}).$$

Applying Lemma 1 in dimension $2rs$ yields (19). The rough bound (20) again follows from Lemma 20. □

5 Arithmetic structure of the index sequence

Theorem 22, Theorem 23, and Theorem 24 reduce the discrepancy problem to admissible Fourier masses of one-dimensional LCG index sets. This section isolates the arithmetic structure of those index sets.

5.1 Local behavior modulo prime powers

Write the prime-power factorization

$$m = \prod_{\ell} \ell^{\nu_\ell}.$$

For a prime $\ell \mid m$, let

$$a_\ell := v_\ell(e-1).$$

where v_ℓ is the normalized valuation at the prime ℓ.

Lemma 25 (Local behavior modulo prime powers)**.** *Let $\ell^\nu \parallel m$ (so $\nu = \nu_\ell$) and set $a := a_\ell$. Then:*

(a) For every $b \le \min\{a, \nu\}$, one has

$$\beta_n \equiv n \pmod{\ell^b}.$$

In particular, if $a \ge \nu$, then $\beta_n \equiv n \pmod{\ell^\nu}$ for all n.

(b) If $a = 0$, then there exists a unique fixed point $\beta_{*,\ell} \bmod \ell^\nu \in (\mathbb{Z}/\ell^\nu\mathbb{Z})^\times$ such that

$$\beta_{*,\ell} \equiv e\beta_{*,\ell} + 1 \pmod{\ell^\nu},$$

and

$$\beta_n - \beta_{*,\ell} \equiv -\beta_{*,\ell} e^n \pmod{\ell^\nu}.$$

Proof. (a) As $e \equiv 1 \pmod{\ell^b}$, so the recursion (8) becomes

$$\beta_{n+1} \equiv \beta_n + 1 \pmod{\ell^b}, \qquad \beta_0 \equiv 0,$$

hence $\beta_n \equiv n \pmod{\ell^b}$.

(b) If $a = 0$, then $1 - e$ is invertible modulo ℓ^ν, so the fixed-point congruence has a unique solution $\beta_{*,\ell} \bmod \ell^\nu \in (\mathbb{Z}/\ell^\nu\mathbb{Z})^\times$. Subtracting the fixed-point relation from the recursion relation gives

$$(\beta_{n+1} - \beta_{*,\ell}) \equiv e(\beta_n - \beta_{*,\ell}) \pmod{\ell^\nu},$$

and iteration yields the stated formula. □

Corollary 26 (No mixed local factors regime)**.** *Assume that for every prime $\ell \mid m$, one has either $v_\ell(e-1) = 0$ or $v_\ell(e-1) \ge \nu_\ell$. Define*

$$m_{\mathrm{tr}} := \prod_{v_\ell(e-1) \ge \nu_\ell} \ell^{\nu_\ell}, \qquad m_{\mathrm{pow}} := \prod_{v_\ell(e-1) = 0} \ell^{\nu_\ell},$$

Then $m = m_{\mathrm{tr}} m_{\mathrm{pow}}$, $\gcd(m_{\mathrm{tr}}, m_{\mathrm{pow}}) = 1$, and there exists $\beta_* \bmod m_{\mathrm{pow}} \in (\mathbb{Z}/m_{\mathrm{pow}}\mathbb{Z})^\times$ such that under the Chinese Remainder Theorem isomorphism

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_{\mathrm{tr}}\mathbb{Z} \times \mathbb{Z}/m_{\mathrm{pow}}\mathbb{Z},$$

one has

$$\beta_n \longmapsto \big(n \bmod m_{\mathrm{tr}},\ \beta_*(1 - e^n) \bmod m_{\mathrm{pow}}\big).$$

Proof. For every prime power ℓ^{ν_ℓ} dividing m_{tr}, part (a) of Lemma 25 gives $\beta_n \equiv n \bmod \ell^{\nu_\ell}$. For every prime power ℓ^{ν_ℓ} dividing m_{pow}, part (b) gives a local fixed point $\beta_{*,\ell} \bmod \ell^{\nu_\ell} \in (\mathbb{Z}/\ell^{\nu_\ell}\mathbb{Z})^\times$ and hence

$$\beta_n \equiv \beta_{*,\ell}(1 - e^n) \pmod{\ell^{\nu_\ell}}.$$

The Chinese Remainder Theorem then yields unique

$$\beta_* \bmod m_{\mathrm{pow}} \in (\mathbb{Z}/m_{\mathrm{pow}}\mathbb{Z})^\times$$

such that $\beta_* \equiv \beta_{*,\ell} \bmod \ell^{\nu_\ell}$ for every prime ℓ dividing m_{pow}, in other words $\beta_* \bmod m_{\mathrm{pow}}$ is the unique solution of the fixed point congruence:

$$\beta_* = e\beta_* + 1 \bmod m_{\mathrm{pow}}$$

and the claimed formula follows. □

Remark 27. The proofs of Lemma 25 and Corollary 26 depend only on the fact that the recursion is of the form:

$$x_{n+1} \equiv ax_n + 1 \pmod{M}.$$

Accordingly, the same arguments apply verbatim to any such recursion after replacing $(e, m, \{\beta_n\})$ by $(a, M, \{x_n\})$. This observation applies in particular to the setting $(e^s, m_s, \{\gamma_n\})$, and we will use similar notations below with $(e^s, m_s, \{\gamma_n\})$ in place of $(e, m, \{\beta_n\})$.

Remark 28. Lemma 25 shows that the unresolved arithmetic is concentrated in the *mixed* local prime powers, namely those with

$$0 < v_\ell(e-1) < \nu_\ell.$$

If no such factors occur, the index sequence $\{\beta_n \bmod m\}$ is explicitly described by Corollary 26 as a Chinese Remainder Theorem combination of a translation component and a power-generator component.

Remark 29 (Conventions for trivial power components). If $m_{\mathrm{pow}} = 1$, then the pure power component is trivial. In that case we set

$$\tau := 1, \qquad \mathcal{G} := \{0\} \subset \mathbb{Z}/1\mathbb{Z}.$$

Similarly, if $m_{s,\mathrm{pow}} = 1$, we set

$$\tau_s := 1, \qquad \mathcal{G}_s := \{0\} \subset \mathbb{Z}/1\mathbb{Z}.$$

With these conventions, all subsequent formulas remain valid without further case distinctions.

Theorem 30. *Assume the hypotheses of Corollary 26. If $m_{\mathrm{pow}} = 1$, set*

$$\tau := 1, \qquad \mathcal{G} := \{0\} \subset \mathbb{Z}/1\mathbb{Z}.$$

If $m_{\mathrm{pow}} > 1$, set τ to be equal to the order of $e \bmod m_{\mathrm{pow}}$ in the multiplicative group $(\mathbb{Z}/m_{\mathrm{pow}}\mathbb{Z})^\times$ (recall by Lemma 7 we have that e is relatively prime to m, hence relatively prime to m_{pow}), and $\mathcal{G} \subset \mathbb{Z}/m_{\mathrm{pow}}\mathbb{Z}$ the subset:

$$\mathcal{G} := \{\beta_*(1 - e^v) \bmod m_{\mathrm{pow}} : 0 \le v < \tau\} \subset \mathbb{Z}/m_{\mathrm{pow}}\mathbb{Z}.$$

(so $|\mathcal{G}| = \tau$). Assume in addition that

$$\gcd(m_{\mathrm{tr}}, \tau) = 1.$$

Then the following hold:

(i) We have $t = m_{\mathrm{tr}}\tau$.

(ii) Under the Chinese Remainder Theorem isomorphism:

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_{\mathrm{tr}}\mathbb{Z} \times \mathbb{Z}/m_{\mathrm{pow}}\mathbb{Z},$$

the cycle B of the LCG $\{\beta_n \bmod m\}_{n\ge 0}$:

$$B = \{\beta_0, \ldots, \beta_{t-1} \bmod m\}$$

is exactly the Cartesian product

$$B = \mathbb{Z}/m_{\mathrm{tr}}\mathbb{Z} \times \mathcal{G}.$$

(iii) The normalized Fourier ℓ^1 mass satisfies

$$\mathcal{L}_m(B) = \mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G}).$$

Consequently,

$$\mathcal{L}_m(B_{\mathrm{adm}}) \le \mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G}) + 1, \qquad \mathcal{L}_m(B_{s,\mathrm{adm}}) \le \mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G}) + s^{1/2}.$$

Proof. If $m_{\mathrm{pow}} = 1$, then $m_{\mathrm{tr}} = m$, $\tau = 1$, and $\mathcal{G} = \{0\}$. Corollary 26 gives $\beta_n \equiv n \pmod m$, so the period is $t = m = m_{\mathrm{tr}}\tau$, the cycle is $B = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m_{\mathrm{tr}}\mathbb{Z} \times \mathcal{G}$, and $\mathcal{L}_m(B) = 1 = \mathcal{L}_1(\mathcal{G})$. The remaining claims are immediate from Lemma 20. Thus assume $m_{\mathrm{pow}} > 1$. By Corollary 26, under the Chinese Remainder Theorem isomorphism one has:

$$\beta_n \bmod m \longmapsto \big(n \bmod m_{\mathrm{tr}},\ \beta_*(1-e^n) \bmod m_{\mathrm{pow}}\big).$$

The first coordinate has period m_{tr}. The second coordinate has period τ: indeed, if

$$\beta_*(1-e^{n+r}) \equiv \beta_*(1-e^n) \pmod{m_{\mathrm{pow}}},$$

then

$$\beta_* e^n(e^r - 1) \equiv 0 \pmod{m_{\mathrm{pow}}}.$$

Therefore as both e and β_* are invertible modulo m_{pow} we have:

$$e^r \equiv 1 \pmod{m_{\mathrm{pow}}},$$

so $\tau \mid r$. Hence the second coordinate has exact period τ. Thus as t is the period of $\{\beta_n \bmod m\}_{n\ge 0}$ it follows that:

$$t = \mathrm{lcm}(m_{\mathrm{tr}}, \tau) = m_{\mathrm{tr}}\tau,$$

because $\gcd(m_{\mathrm{tr}}, \tau) = 1$. This proves (i).

To prove (ii), let $(u, v) \in \mathbb{Z}/m_{\mathrm{tr}}\mathbb{Z} \times \{0, \dots, \tau - 1\}$. By the Chinese Remainder Theorem (using the assumption that m_{tr} and τ are relatively prime) there exists a unique residue class $n \bmod t$ such that

$$n \equiv u \pmod{m_{\mathrm{tr}}}, \qquad n \equiv v \pmod{\tau}.$$

Since $e^n \equiv e^v \pmod{m_{\mathrm{pow}}}$, Corollary 26 gives

$$\beta_n \bmod m \longmapsto \big(u \bmod m_{\mathrm{tr}},\ \beta_*(1-e^v) \bmod m_{\mathrm{pow}}\big).$$

Thus every element of $\mathbb{Z}/m_{\mathrm{tr}}\mathbb{Z} \times \mathcal{G}$ occurs in B. Conversely, we already know that every $\beta_n \bmod m$ has this form under the Chinese Remainder Theorem isomorphism, thus proving

$$B = \mathbb{Z}/m_{\mathrm{tr}}\mathbb{Z} \times \mathcal{G}.$$

For (iii), observe first that the normalized Fourier ℓ^1 mass is invariant under additive-group isomorphisms. Hence one may compute $\mathcal{L}_m(B)$ on the product group

$$\mathbb{Z}/m_{\mathrm{tr}}\mathbb{Z} \times \mathbb{Z}/m_{\mathrm{pow}}\mathbb{Z}$$

using product characters

$$\chi_{a,b}(x,y) := \exp\Big(-2\pi i\frac{ax}{m_{\mathrm{tr}}}\Big)\exp\Big(-2\pi i\frac{by}{m_{\mathrm{pow}}}\Big),$$

with $0 \le a < m_{\mathrm{tr}}$ and $0 \le b < m_{\mathrm{pow}}$. Since $B = \mathbb{Z}/m_{\mathrm{tr}}\mathbb{Z} \times \mathcal{G}$, one has

$$\widehat{\mathbf{1}_B}^{(m)}(a,b) = \sum_{x\in\mathbb{Z}/m_{\mathrm{tr}}\mathbb{Z}} e^{-2\pi i a x/m_{\mathrm{tr}}} \sum_{y\in\mathcal{G}} e^{-2\pi i b y/m_{\mathrm{pow}}}.$$

The first factor vanishes unless $a = 0$, in which case it equals m_{tr}. Therefore

$$\sum_{a=0}^{m_{\mathrm{tr}}-1}\sum_{b=0}^{m_{\mathrm{pow}}-1} \big|\widehat{\mathbf{1}_B}^{(m)}(a,b)\big| = m_{\mathrm{tr}} \sum_{b=0}^{m_{\mathrm{pow}}-1} \big|\widehat{\mathbf{1}_{\mathcal{G}}}^{(m_{\mathrm{pow}})}(b)\big|.$$

Dividing by $m = m_{\mathrm{tr}}m_{\mathrm{pow}}$ yields

$$\mathcal{L}_m(B) = \mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G}).$$

The final inequalities now follow from Lemma 20. □

Corollary 31 (Improved discrepancy bounds in the no-mixed regime)**.** *Under the hypotheses of Theorem 30,*

$$D(\mathcal{P}) \le 1 - \Big(1-\frac{1}{p^a}\Big)^{2r} + \frac{4q^{1/2}}{N^*}\big(\mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G})+1\big)\big(C_0\ln(p^a)+1\big)^{2r}, \tag{21}$$

$$D(\mathcal{P}^{(s)}) \le 1 - \Big(1-\frac{1}{p^a}\Big)^{2rs} + \frac{6q^{1/2}}{N_s^*}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\big(\mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G})+s^{1/2}\big)\big(C_0\ln(p^a)+1\big)^{2rs}. \tag{22}$$

In particular, since $\mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G}) \le |\mathcal{G}|^{1/2} = \tau^{1/2}$ by Lemma 17, we have:

$$D(\mathcal{P}) \le 1 - \Big(1-\frac{1}{p^a}\Big)^{2r} + \frac{4q^{1/2}}{N^*}\big(\tau^{1/2}+1\big)\big(C_0\ln(p^a)+1\big)^{2r}, \tag{23}$$

$$D(\mathcal{P}^{(s)}) \le 1 - \Big(1-\frac{1}{p^a}\Big)^{2rs} + \frac{6q^{1/2}}{N_s^*}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\big(\tau^{1/2}+s^{1/2}\big)\big(C_0\ln(p^a)+1\big)^{2rs}. \tag{24}$$

Proof. Combine Theorem 30 with Theorem 22, Theorem 23. □

Theorem 32. *Fix $s \ge 2$ and as before:*

$$R_s := P_s - P_0 = [\beta_s]R,$$

$$m_s := \mathrm{ord}(R_s), \qquad \widetilde{B}_s := \{\gamma_0,\dots,\gamma_{L_s-1} \bmod m_s\} \subset \mathbb{Z}/m_s\mathbb{Z},$$

where

$$\gamma_{n+1} \equiv e^s\gamma_n + 1 \pmod{m_s}, \qquad \gamma_0 \equiv 0, \qquad L_s := t/\gcd(t,s).$$

Assume that for every prime $\ell \mid m_s$, one has either $v_\ell(e^s-1) = 0$ or $v_\ell(e^s-1) \ge \nu_{\ell,s}$, where

$$m_s = \prod_\ell \ell^{\nu_{\ell,s}}.$$

Define

$$m_{s,\mathrm{tr}} := \prod_{v_\ell(e^s-1)\geq \nu_{\ell,s}} \ell^{\nu_{\ell,s}}, \qquad m_{s,\mathrm{pow}} := \prod_{v_\ell(e^s-1)=0} \ell^{\nu_{\ell,s}},$$

so $m_s = m_{s,\mathrm{tr}} m_{s,\mathrm{pow}}$ *and* $\gcd(m_{s,\mathrm{tr}}, m_{s,\mathrm{pow}}) = 1$.

If $m_{s,\mathrm{pow}} = 1$, *set*

$$\tau_s := 1, \qquad \mathcal{G}_s := \{0\} \subset \mathbb{Z}/1\mathbb{Z}.$$

If $m_{s,\mathrm{pow}} > 1$, *let* $\gamma_{*,s} \bmod m_{s,\mathrm{pow}} \in (\mathbb{Z}/m_{s,\mathrm{pow}}\mathbb{Z})^\times$ *be the unique solution of*

$$\gamma_{*,s} \equiv e^s \gamma_{*,s} + 1 \pmod{m_{s,\mathrm{pow}}},$$

Set τ_s *to be equal to the order of* $e^s \bmod m_{s,\mathrm{pow}}$ *in the multiplicative group* $(\mathbb{Z}/m_{s,\mathrm{pow}}\mathbb{Z})^\times$, *and*

$$\mathcal{G}_s := \{\gamma_{*,s}(1-(e^s)^v) \bmod m_{s,\mathrm{pow}} : 0 \leq v < \tau_s\}.$$

(and so $|\mathcal{G}_s| = \tau_s$*). Assume moreover that*

$$\gcd(m_{s,\mathrm{tr}}, \tau_s) = 1.$$

Then the following hold:

(i) We have $L_s = m_{s,\mathrm{tr}}\tau_s$.

(ii) Under the Chinese Remainder Theorem isomorphism:

$$\mathbb{Z}/m_s\mathbb{Z} \cong \mathbb{Z}/m_{s,\mathrm{tr}}\mathbb{Z} \times \mathbb{Z}/m_{s,\mathrm{pow}}\mathbb{Z},$$

we have

$$\widetilde{B}_s = \mathbb{Z}/m_{s,\mathrm{tr}}\mathbb{Z} \times \mathcal{G}_s.$$

(iii) The normalized Fourier ℓ^1 *mass satisfies*

$$\mathcal{L}_{m_s}(\widetilde{B}_s) = \mathcal{L}_{m_{s,\mathrm{pow}}}(\mathcal{G}_s).$$

Consequently,

$$\mathcal{L}_{m_s}(\widetilde{B}_{s,\mathrm{adm}}) \leq \mathcal{L}_{m_{s,\mathrm{pow}}}(\mathcal{G}_s) + \big(s/\gcd(s,t)\big)^{1/2}.$$

Proof. If $m_{s,\mathrm{pow}} = 1$, then $\tau_s = 1$ and $\mathcal{G}_s = \{0\}$. In this case the no-mixed hypothesis forces $m_s = m_{s,\mathrm{tr}}$, and the same analysis as in the proof of Lemma 25 and Corollary 26, applied to the recursion:

$$\gamma_{n+1} \equiv e^s \gamma_n + 1 \pmod{m_s}$$

shows that

$$\gamma_n \equiv n \pmod{m_s}.$$

Hence as L_s is the period of $\{\gamma_n \bmod m_s\}_{n\geq 0}$, we have

$$L_s = m_s = m_{s,\mathrm{tr}}\tau_s,$$

and

$$\widetilde{B}_s = \mathbb{Z}/m_s\mathbb{Z} = \mathbb{Z}/m_{s,\mathrm{tr}}\mathbb{Z} \times \mathcal{G}_s,$$

and $\mathcal{L}_{m_s}(\widetilde{B}_s) = 1 = \mathcal{L}_1(\mathcal{G}_s)$. The remaining claim follows from Lemma 20. Thus assume $m_{s,\mathrm{pow}} > 1$. Every prime divisor of $m_{s,\mathrm{pow}}$ satisfies $v_\ell(e^s - 1) = 0$, so the element $1 - e^s$ is invertible modulo $m_{s,\mathrm{pow}}$; hence the fixed-point congruence

$$\gamma_{*,s} \equiv e^s \gamma_{*,s} + 1 \pmod{m_{s,\mathrm{pow}}}$$

has a unique solution in $(\mathbb{Z}/m_{s,\mathrm{pow}}\mathbb{Z})^\times$. The same analysis as in the proof of Lemma 25 and Corollary 26 then yields the decomposition

$$\gamma_n \bmod m_s \longmapsto \big(n \bmod m_{s,\mathrm{tr}},\ \gamma_{*,s}(1 - (e^s)^n) \bmod m_{s,\mathrm{pow}}\big)$$

under the Chinese Remainder Theorem isomorphism. Exactly as in the proof of Theorem 30, the first coordinate has period $m_{s,\mathrm{tr}}$, the second has exact period τ_s, and the hypothesis that $m_{s,\mathrm{tr}}$ and τ_s are co-prime implies that:

$$L_s = \mathrm{lcm}(m_{s,\mathrm{tr}}, \tau_s) = m_{s,\mathrm{tr}}\tau_s.$$

This proves (i). Again by using the hypothesis that $m_{s,\mathrm{tr}}$ and τ_s are co-prime, the same Chinese Remainder Theorem argument as in the proof of Theorem 30 gives the proof of (ii), namely that:

$$\widetilde{B}_s = \mathbb{Z}/m_{s,\mathrm{tr}}\mathbb{Z} \times \mathcal{G}_s.$$

For (iii), compute the Fourier transform of $\mathbf{1}_{\widetilde{B}_s}$ on the product group

$$\mathbb{Z}/m_{s,\mathrm{tr}}\mathbb{Z} \times \mathbb{Z}/m_{s,\mathrm{pow}}\mathbb{Z}.$$

As in the proof of Theorem 30, the full translation factor forces vanishing of all nontrivial frequencies in the first coordinate, and one obtains

$$\mathcal{L}_{m_s}(\widetilde{B}_s) = \mathcal{L}_{m_{s,\mathrm{pow}}}(\mathcal{G}_s).$$

Finally, Lemma 20 gives

$$\mathcal{L}_{m_s}(\widetilde{B}_{s,\mathrm{adm}}) \le \mathcal{L}_{m_s}(\widetilde{B}_s) + (s/\gcd(s,t))^{1/2} = \mathcal{L}_{m_{s,\mathrm{pow}}}(\mathcal{G}_s) + (s/\gcd(s,t))^{1/2}.$$

□

Corollary 33 (Improved non-overlapping discrepancy bounds in the derived no-mixed regime)**.** *Under the hypotheses of Theorem 32,*

$$D(\widetilde{\mathcal{P}}^{(s)}) \le 1 - \Big(1 - \frac{1}{p^a}\Big)^{2rs} + \frac{6q^{1/2}}{\widetilde{N}_s^*}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\big(\mathcal{L}_{m_{s,\mathrm{pow}}}(\mathcal{G}_s) + \big(s/\gcd(s,t)\big)^{1/2}\big)\big(C_0 \ln(p^a) + 1\big)^{2rs} \tag{25}$$

and in particular since $\mathcal{L}_{m_{s,\mathrm{pow}}}(\mathcal{G}_s) \le |\mathcal{G}_s|^{1/2} = \tau_s^{1/2}$ *by Lemma 17, we have:*

$$D(\widetilde{\mathcal{P}}^{(s)}) \le 1 - \Big(1 - \frac{1}{p^a}\Big)^{2rs} + \frac{6q^{1/2}}{\widetilde{N}_s^*}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\big(\tau_s^{1/2} + \big(s/\gcd(s,t)\big)^{1/2}\big)\big(C_0 \ln(p^a) + 1\big)^{2rs} \tag{26}$$

Proof. Combine Theorem 24, Theorem 32. □

Theorem 34 (Pure power representation of the Fourier masses in the no-mixed regime)**.** *Under the hypotheses of Theorem 30, one has*

$$\mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G}) = \frac{1}{m_{\mathrm{pow}}} \sum_{b=0}^{m_{\mathrm{pow}}-1} \left| \sum_{v=0}^{\tau-1} \exp\Big(\frac{2\pi i\, be^v}{m_{\mathrm{pow}}}\Big) \right|. \tag{27}$$

Under the hypotheses of Theorem 32, one has

$$\mathcal{L}_{m_{s,\mathrm{pow}}}(\mathcal{G}_s) = \frac{1}{m_{s,\mathrm{pow}}} \sum_{b=0}^{m_{s,\mathrm{pow}}-1} \left| \sum_{v=0}^{\tau_s-1} \exp\Big(\frac{2\pi i\, b(e^s)^v}{m_{s,\mathrm{pow}}}\Big) \right|. \tag{28}$$

Proof. We prove (27); the proof of (28) is identical after replacing

$$(e, m_{\mathrm{pow}}, \beta_*, \tau, \mathcal{G}) \quad \text{by} \quad (e^s, m_{s,\mathrm{pow}}, \gamma_{*,s}, \tau_s, \mathcal{G}_s).$$

If $m_{\mathrm{pow}} = 1$, then $\tau = 1$ and $\mathcal{G} = \{0\}$, so both sides of (27) are equal to 1. Thus assume $m_{\mathrm{pow}} > 1$. By Theorem 30,

$$\mathcal{G} = \{\beta_*(1 - e^v) \bmod m_{\mathrm{pow}} : 0 \le v < \tau\}.$$

Therefore, for each b modulo m_{pow},

$$\sum_{g\in\mathcal{G}} \exp\Big(-\frac{2\pi i b g}{m_{\mathrm{pow}}}\Big) = \exp\Big(-\frac{2\pi i b\beta_*}{m_{\mathrm{pow}}}\Big) \sum_{v=0}^{\tau-1} \exp\Big(\frac{2\pi i\, b\beta_* e^v}{m_{\mathrm{pow}}}\Big).$$

Taking absolute values removes the phase factor $\exp(-2\pi i b\beta_*/m_{\mathrm{pow}})$. Recall that $\beta_* \bmod m_{\mathrm{pow}}$ is invertible and so multiplication by $\beta_* \bmod m_{\mathrm{pow}}$ permutes the residue classes modulo m_{pow}, so averaging over b gives:

$$\mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G}) = \frac{1}{m_{\mathrm{pow}}} \sum_{b=0}^{m_{\mathrm{pow}}-1} \left| \sum_{v=0}^{\tau-1} \exp\Big(\frac{2\pi i\, be^v}{m_{\mathrm{pow}}}\Big) \right|.$$

□

Remark 35. Theorem 34 shows that, in the no-mixed regimes, the remaining analytic input needed to further improve the estimates of the Fourier masses of $\mathcal{G}$ and $\mathcal{G}_s$, is good estimates for exponential sums along the multiplicative orbit

$$1, e, e^2, \ldots, e^{\tau-1} \pmod{m_{\mathrm{pow}}},$$

(or more precisely, what is really needed is estimates of average of these sums with respect to the parameter b as in the statement of Theorem 34); similarly for the orbit generated by e^s modulo $m_{s,\mathrm{pow}}$.

As an illustration we show:

Proposition 36. *Assume the hypotheses of Theorem 30, and suppose in addition that $m_{\mathrm{pow}} = \ell^\nu$, where ℓ is an odd prime, and that $\tau = \ell^{\nu-1}(\ell-1)$. Then we have:*

$$\mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G}) = (2\ell - 3)/\ell \le 2.$$

Consequently,

$$D(\mathcal{P}) \leq 1 - \Big(1 - \frac{1}{p^a}\Big)^{2r} + \frac{12q^{1/2}}{N^*}\big(C_0 \ln(p^a) + 1\big)^{2r}, \tag{29}$$

$$D(\mathcal{P}^{(s)}) \leq 1 - \Big(1 - \frac{1}{p^a}\Big)^{2rs} + \frac{6q^{1/2}}{N_s^*}\Big(\sum_{\iota=0}^{s-1} e^{2\iota}\Big)\Big(2 + s^{1/2}\Big)\big(C_0 \ln(p^a) + 1\big)^{2rs}. \tag{30}$$

Proof. Since $m_{\text{pow}} = \ell^\nu$ (ℓ is an odd prime) and $\tau = \ell^{\nu-1}(\ell - 1)$, so e is a primitive root modℓ^ν. Hence:

$$\sum_{v=0}^{\tau-1} \exp\Big(\frac{2\pi i\, be^v}{m_{\text{pow}}}\Big) = \sum_{x \in (\mathbb{Z}/\ell^\nu\mathbb{Z})^\times} \exp\Big(\frac{2\pi i\, bx}{\ell^\nu}\Big)$$

For $1 \leq b \leq \tau - 1 = \ell^{\nu-1}(\ell-1) - 1$, write $b = c\ell^f$, where $f = v_\ell(b) \leq \nu - 1$ and $\gcd(c, \ell) = 1$. We then have:

$$\begin{aligned}
&\sum_{x \in (\mathbb{Z}/\ell^\nu\mathbb{Z})^\times} \exp\Big(\frac{2\pi i\, bx}{\ell^\nu}\Big) \\
= &\sum_{x \in (\mathbb{Z}/\ell^\nu\mathbb{Z})^\times} \exp\Big(\frac{2\pi i\, cx}{\ell^{\nu-f}}\Big) \\
= &\sum_{x \in (\mathbb{Z}/\ell^\nu\mathbb{Z})^\times} \exp\Big(\frac{2\pi i\, x}{\ell^{\nu-f}}\Big) \\
= &\ \ell^f \sum_{x \in (\mathbb{Z}/\ell^{\nu-f}\mathbb{Z})^\times} \exp\Big(\frac{2\pi i\, x}{\ell^{\nu-f}}\Big)
\end{aligned}$$

(as each $x \in (\mathbb{Z}/\ell^{\nu-f}\mathbb{Z})^\times$ has exaxctly ℓ^f pre-images in $x \in (\mathbb{Z}/\ell^\nu\mathbb{Z})^\times$).

Now using the identity (the ℓ^n-th cyclotomic polynomial, $n \geq 1$):

$$\begin{aligned}
\frac{X^{\ell^n} - 1}{X^{\ell^{n-1}} - 1} &= X^{\ell^{n-1}(\ell-1)} + X^{\ell^{n-1}(\ell-2)} \cdots + X^{\ell^{n-1}} + 1 \\
&= \prod_{x \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times} \Big(X - \exp\Big(\frac{2\pi i\, x}{\ell^n}\Big)\Big)
\end{aligned}$$

we have that the value of:

$$\sum_{x \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times} \exp\Big(\frac{2\pi i\, x}{\ell^n}\Big)$$

is equal to 0 if $n > 1$, and is equal to -1 if $n = 1$.

Hence for $1 \leq b \leq \tau - 1$, the value of the sum

$$\sum_{x \in (\mathbb{Z}/\ell^\nu\mathbb{Z})^\times} \exp\Big(\frac{2\pi i\, bx}{\ell^\nu}\Big)$$

is equal to 0 if $v_\ell(b) < \nu - 1$, and is equal to $-\ell^{\nu-1}$ if $v_\ell(b) = \nu - 1$.

Now in the pure power representation of the Fourier mass $\mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G}) = \mathcal{L}_{\ell^\nu}(\mathcal{G})$ in the no-mixed regime as given in Theorem 34, for the outer sum over $0 \le b \le \tau - 1$, the term $b = 0$ contributes $\tau = \ell^{\nu-1}(\ell-1)$. While for terms corresponding to $b \neq 0$, it contributes the value 0 if $v_\ell(b) < \nu - 1$; while it contributes the value $\ell^{\nu-1}$ if $v_\ell(b) = \nu - 1$, and there are $\ell - 2$ such terms, namely $b = \ell^{\nu-1}, 2\ell^{\nu-1}, \cdots, (\ell-2)\ell^{\nu-1}$. Hence:

$$\begin{aligned} \mathcal{L}_{\ell^\nu}(\mathcal{G}) &= \frac{\ell^{\nu-1}(\ell-1) + \ell^{\nu-1}(\ell-2)}{\ell^\nu} \\ &= \frac{2\ell - 3}{\ell} \end{aligned}$$

In particular $\mathcal{L}_{\ell^\nu}(\mathcal{G}) \le 2$, and on applying Corollary 31 finishes the proof.

□

5.2 Conclusion

The results in Section 4 show that any bounds of the form

$$\frac{q^{1/2}\mathcal{L}_m(B_{\mathrm{adm}})}{N^*} \ll \frac{1}{q^\epsilon}, \qquad \frac{q^{1/2}\mathcal{L}_m(B_{s,\mathrm{adm}})}{N_s^*} \ll \frac{1}{q^\epsilon}, \qquad \frac{q^{1/2}\mathcal{L}_{m_s}(\widetilde{B}_{s,\mathrm{adm}})}{\widetilde{N}_s^*} \ll \frac{1}{q^\epsilon} \tag{31}$$

(here $\epsilon > 0$) would produce the corresponding discrepancy bounds for $\mathcal{P}$, $\mathcal{P}^{(s)}$, and $\widetilde{\mathcal{P}}^{(s)}$ respectively, and hence gives quantitative justification of the uniform distribution (respectively statistical independence) property of $\mathcal{P}$.

This suggests three concrete directions for further improvement. In the no-mixed regime, however, Section 5.1 already reduces the problem completely to the pure power components $\mathcal{G}$ and $\mathcal{G}_s$; in fact as we have seen in Corollary 31 and Corollary 33 in the no-mixed regime case, by using the elementary square root bounds $\mathcal{L}_m(\mathcal{G}) \le |\mathcal{G}|^{1/2}$ and $\mathcal{L}_{m_{\mathrm{pow}}}(\mathcal{G}_s) \le |\mathcal{G}_s|^{1/2}$, one can already give quite explicit sufficient conditions that would ensure that bounds of type (31) holds.

- interval estimates in the pure translation local regime;
- exponential-sum estimates for multiplicative orbits in the pure power local regime; in the no-mixed regime, Theorem 30, Theorem 32, and Theorem 34 reduce the relevant Fourier masses to explicit averages of such sums for the pure power components $\mathcal{G}$ and $\mathcal{G}_s$;
- bilinear-sum methods over elliptic curves, following Shparlinski [6] and Ahmadi–Shparlinski [7], to treat the mixed regime directly.

References

[1] C. P. Mok, Pseudorandom vector generation using elliptic curves and applications to Wiener processes, *Finite Fields Appl.* **85** (2023), 102129.

[2] C. P. Mok, H. Zheng, Monte Carlo Integration Using Elliptic Curves, *Chin. Ann. Math. Ser. B.* **46**(2) (2025), 241–260.

[3] X. Wang, On the distribution of pseudorandom vectors generated by elliptic curves, *Finite Fields Appl.* **93** (2024), 102318.

[4] P. Hellekalek, General discrepancy estimates: the Walsh function system, *Acta Arith.* LXVII (3) (1994), 209–218.

[5] D. Kohel, I. Shparlinski, On exponential sums and group generators for elliptic curves over finite fields, Proc. the 4th Algorithmic Number Theory Symp., in: Lecture Notes in Comput. Sci., vol. 1838, Springer-Verlag, Berlin, 2000, pp. 395–404.

[6] I. E. Shparlinski, Bilinear character sums over elliptic curves, *Finite Fields Appl.* **14** (2008), 132–141.

[7] O. Ahmadi and I. E. Shparlinski, Bilinear character sums and sum-product problems on elliptic curves, *Proc. Edinburgh Math. Soc.* **53** (2010), 1–12.