arXiv:2302.03964v1 [math.NT] 8 Feb 2023

素数幂模下递归矩阵伪随机数生成器的分布

´ ´ ´LASZLO MERAI 和 IGOR E. SHPARLINSKI

Abstract. 给定一个矩阵 $A \in$一般线性群$_d(\mathbb{Z})$。我们研究由以下形式的线性递推关系生成的向量 $\mathbf{u}_n$ 的伪随机性：

$$\mathbf{u}_{n+1} \equiv A\mathbf{u}_n \pmod{p^t}, \qquad n = 0, 1, \ldots,$$

模 p^t，其中 p 为固定素数，$t \geqslant 1$为充分大的整数。我们研究这类序列在极短区间上的分布，这种长度是以往方法无法处理的。我们的技术基于 N. M. Korobov（1972）估计二重 Weyl 和的方法，以及 K. Ford（2002）提出的 Vinogradov 均值定理的完全显式形式。此外，我们还结合了 I. E. Shparlinski（1978）工作中的一些思想，以构造 $\mathbf{u}_n$ 各坐标的多项式表示，并控制其多项式表示中系数的 p-进阶。

1. Introduction

1.1. 递归同余伪随机数。设 p是一个固定的素数（特别地，所有隐含常数都允许依赖于 p）。设 $t \geqslant 1$ 是一个整数，$\mathcal{R}_t = \mathbb{Z}/p^t\mathbb{Z}$ 是模 p^t的剩余类环，我们始终假设它由集合 $\{0, \ldots, p^t - 1\}$表示。

给定一个矩阵 $A \in \mathrm{GL}_d(\mathbb{Z})$，我们考虑序列

$$\mathfrak{U} = (\mathbf{u}_n)_{n=0}^{\infty}, \qquad \mathbf{u}_n \in \mathcal{R}_t^d, \tag{1.1}$$

由 $\mathcal{R}_t$上的 d 维向量组成，并通过以下关系迭代生成

$$\mathbf{u}_{n+1} \equiv A\mathbf{u}_n \qquad n = 0, 1, \ldots, \tag{1.2}$$

对于某个初始向量 $\mathbf{u} = \mathbf{u}_0$,，使得 $\mathbf{u}_0$ 的至少一个分量是 $\mathcal{R}_t$ 中的单位元。更明确地，我们也可以写成

$$\mathbf{u}_n \equiv A^n\mathbf{u}_0 \qquad n = 0, 1, \ldots \tag{1.3}$$

2010年数学主题分类。11K38，11K45，11L07。关键词和短语：矩阵同余伪随机数、素数幂、指数和、Vinogradov 均值定理。

容易看出，向量（1.1）满足线性递推关系

$$\mathbf{u}_{n+d} \equiv a_{d-1}\mathbf{u}_{n+d-1} + \ldots + a_0\mathbf{u}_n \pmod{p^t}, \qquad n = 0, 1, \ldots, \tag{1.4}$$

其中

$$f(X) = X^d - a_{d-1}X^{d-1} - \ldots - a_0 \in \mathbb{Z}[X] \tag{1.5}$$

是特征多项式，它属于 A。特别地，向量的分量（1.1），更一般地，任何形如$\mathbf{v}A^n\mathbf{u}_0$, 的序列都满足（1.4）的标量类比（下文中我们始终假设向量的方向经过安排，使向量乘法可以进行）。

事实上，我们对向量序列（1.1）的研究基于对同余和标量线性递推序列的指数和的考察

$$u = (u_n)_{n=1}^{\infty} \in \mathcal{R}_t^{\infty} \tag{1.6}$$

由下列关系生成

$$u_{n+d} \equiv a_{d-1}u_{n+d-1} + \ldots + a_0u_n \pmod{p^t}, \quad 0 \leqslant u_n < p^t, \tag{1.7}$$

对于 $n = 0$，1，.....，并取某些初始值 u_0、 $\ldots u_{d-1} \in \mathcal{R}_t$。

由（1.2）、（1.6）或（1.7）所生成的序列，是伪随机向量的常见来源，已有不少研究对其进行了探讨，参见 [17, 第 10 节。1] 及其中的参考文献。然而，过去采用的相当初等的方法，无法为此类序列的分布提供任何非平凡的信息。唯一的例外是 [20], 的结果，但它仅适用于完整周期 τ_t ，并且表明，在某些自然条件下，小数部分 $\{u_n/p^t\}$, $n = 1, \ldots, \tau_t$, 偏离均匀分布的程度不超过 $\tau_t^{-1/d+o(1)}$ ，当 $t \to \infty$。形式化的表述另见（1.13）。

在此，我们以 [13]和 [20], 的思路为基础，并通过若干新论证进一步加以拓展。

我们注意到，我们的结果与 [15] 针对所谓反演生成器所获得的结果强度相近。特别是，正如 [15] 中一样，我们将和化为一族次数不断增长的多项式的韦尔和，因此，正如 [15], 中一样，该方向上近期取得的突破（例如参见 [4], ）并不适用于我们的情形。不过，与 [15], 针对矩阵生成器的做法颇为不同，我们并不控制这些多项式每个系数的 p-整除性。相反，我们借鉴 [20] 的一些思路，考察连续 d 个系数组成的组中共同的 p-整除性。

1.2. 我们的结果。按照建立分布均匀性结果的标准方法，我们首先给出指数和的一个上界。

设 $A \in \mathrm{GL}_d(\mathbb{Z})$，且 $\mathbf{u}$、$\mathbf{v} \in \mathbb{Z}^d$ 为非零向量。我们考虑和式

$$S_{p^t}(N;\mathbf{u},\mathbf{v}) = \sum_{n=0}^{N-1} \mathbf{e}\left(\frac{1}{p^t}\mathbf{v}A^n\mathbf{u}\right),$$

其中，按照惯例，我们记 $\mathbf{e}(z) = \exp(2\pi i z)$。

运用 Korobov 的方法 [13]以及采用 Ford 给出的 Vinogradov 均值定理的显式形式[8], ，我们可以估计 $S_{p^t}(N;\ \mathbf{u}、\mathbf{v})$ 对于满足 N在范围（1.8）

$$\tau_t \geqslant N \geqslant \exp\left(c\,(t\log p)^{2/3}\right) \tag{1.8}$$

对于某个绝对常数 $c > 0$，其仅取决于 p 以及特征多项式（1.5） A，前提是它满足某些自然条件。

我们注意到，范围（1.8）涵盖了 N 的取值，其中这些取值小于周期 τ_t的任意次幂。

我们回顾一下我们的假设：1.7是 $(u_n)_{n=1}^{\infty}$所满足的最短线性递推关系，因此 f 在1.5中的多项式确实是该序列的特征多项式（有时也称为最小多项式）。

若多项式 $f \in \mathbb{Z}[X]$ 的根 $\lambda_1, \ldots, \lambda_s$ 及其非平凡比值 λ_i/λ_j, $1 \leqslant i < j \leqslant s$, 中不含单位根，则称该多项式为非退化多项式。

在全文中，我们始终使用参数

$$\rho = \frac{\log N}{t\log p} \tag{1.9}$$

它在对数尺度上控制 N 相对于模数 p^t 的大小。

我们还称向量对 $(\mathbf{u}, \mathbf{v}) \in \mathcal{R}_t^d \times \mathcal{R}_t^d$ 是适当的，如果序列 $u_n = \mathbf{v}A^n\mathbf{u}$ 不满足任何模 p 的长度小于 d 的线性递推关系。

最后，如果 $\mathbf{u} = (u_0, \ldots, u_{d-1}) \in \mathbb{Z}^d$ p 满足

$$\gcd(u_0, \ldots, u_{d-1}, p) = 1.$$

定理 1.1。 假设特征多项式 f 在 (1.6)模 p 且 最大公约数$(a_0, p) = 1$。那么，对每一对适当向量， $(\mathbf{u}、\mathbf{v}) \in \mathcal{R}_t^d \times \mathcal{R}_t^d$，有

$1 \leqslant N \leqslant \tau_t$ 我们有

$$|S_{p^t}(N; \mathbf{u}, \mathbf{v})| \leqslant cN^{1-\eta\rho^2/(d^4(\log d)^2)},$$

其中 ρ 由下式给出 (1.9)，其中某个常数 c 仅取决于 f 和p，而 $\eta > 0$是某个绝对常数。

现在注意，若 f 模 p 不可约，则任意 p-本原向量 $\mathbf{u},\mathbf{v} \in \mathcal{R}_t^d$ 构成一个适当对。

对于由 $\mathfrak{U} = (\mathbf{u}_n)_{n=0}^{\infty}$ 通过（1.2）定义的序列，或更明确地说，如（1.3）所示，我们用 $D_{\mathfrak{U}}(N)$ 表示差异度，其对应的向量为

$$p^{-t}\mathbf{u}_n \in [0,1)^d, \qquad n = 1, \ldots, N, \tag{1.10}$$

其定义为

$$D_{\mathfrak{U}}(N) = \sup_{J \subset [0,1)} \left| \frac{A_{\mathfrak{U}}(\mathcal{B}, N)}{N} - \operatorname{vol} \mathcal{B} \right|, \tag{1.11}$$

其中，上确界取遍所有形如以下形式的盒子 $\mathcal{B}$

$$\mathcal{B} = [\alpha_1, \beta_1] \times \ldots \times [\alpha_d, \beta_d] \subseteq [0,1)^d,$$

且 $A_{\mathfrak{U}}(N, \mathcal{B})$ 是落入 1.10) 中的点 $\mathcal{B}$，且

$$\operatorname{vol} \mathcal{B} = (\beta_1 - \alpha_1) \cdots (\beta_d - \alpha_d)$$

是 $\mathcal{B}$的体积。著名的 *Koksma–Sz ̈*usz 不等式 [12, 21](另见 [6, 定理 1.21]) 使我们能够根据定理 $D_{\mathfrak{U}}(N)$ 1.1 中估计的指数和，给出差异度 1.1的上界。

定理 1.2。 假设特征多项式 f 在 (1.6) 模 p不可约且非退化。若 $\mathbf{u}$ 是 p- 本原的，则对于$1 \leqslant N \leqslant \tau_t$ 有

$$D_{\mathfrak{U}}(N) \leqslant c_0 N^{-\eta_0\rho^2/(d^4(\log d)^2)} (\log N)^d$$

其中某个常数 c_0 仅取决于 f 和 p，而 $\eta_0 > 0$是某个绝对常数。

写作

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

我们看到，定理1.1 和1.2 在区间（1.8）中是非平凡的。

1.3. 相关结果。我们首先回顾一下，在 $d = 1$ 相近强度的结果，如定理1.1 和1.2 由 Korobov 给出 [13]。

另一方面，对于任意的 d，但仅在对整个周期求和的情况下，即对于 $N = \tau_t$，有如下界

$$|S_{p^t}(\tau_t; \mathbf{u}, \mathbf{v})| \leqslant \tau_t^{1-1/d+o(1)}, \qquad t \to \infty, \tag{1.12}$$

已在[20], 中推导出。在定理1.2的条件下，可由此得到差异度的如下界:

$$D_{\mathfrak{U}}(\tau_t) \leqslant \tau_t^{-1/d+o(1)}, \qquad t \to \infty, \tag{1.13}$$

另见 [7,公式 (7.8)]。

此外，对于差异度定义式 ($A_{\mathfrak{U}}(N$中的计数函数， $\mathcal{B})$ 当1.11时，对于 $N = \tau_t$和立方体 $\mathcal{B} = [\alpha, \ \alpha + \delta]^d$有

$$A_{\mathfrak{U}}(\tau_t, \mathcal{B}) = O(\tau_t \delta)$$

(隐含常数仅依赖于 f 和 p)，对于较小的1.13，它优于式 ($\delta = o(\tau_t^{-1/d})$, ; 见 [7, 定理 7。6]此外，对于维数问题，或者等价地，对于 $\mathcal{B} = [\alpha, \ \alpha + \delta] \times [0, \ 1]^{d-1}$，有如下下界

$$A_{\mathfrak{U}}(\tau_t, \mathcal{B}) \geqslant \frac{1}{d} \tau_t \delta + O(1),$$

见 [7, 定理 7。5], 这再次优于（1.13），对于 $\delta = o(\tau_t^{-1/d})$。

此外，沿着[16], 的思路，也可以研究具有素数指标 ℓ的向量 $\mathbf{u}_\ell$ 的分布，另见[11]。

研究序列（1.2）模大素数的分布无疑是一个非常有趣的问题，它也与量子混沌的一个离散模型有关，见 [19]。然而，在这一情形下，除了一些非常初等的界之外，较强的结果目前只对 $A \in \mathrm{SL}_d(\mathbb{Z})$ [18]已知，尤其是对 $d = 2$，见 [2, 14, 18]。

1.4. 记号。我们回顾一下，记号 $U \ll V$和 $V \gg U$ 等价于断言不等式 $|U| \leqslant cV$ 以某个绝对常数 $c > 0$成立。

我们用记号 ν_p 表示 p-进赋值；也就是说，对于非零整数 $a \in \mathbb{Z}$，若 p的最高次幂整除 a，则令 $\nu_p(a) = k$ 为 p^k；并且对于 a、 $b \neq 0$, 令 $\nu_p(a/b) = \mathrm{v}_p(a) - \mathrm{v}_p(b)$。当 $\mathfrak{p}$ 是数域的一个素理想时，我们也用 $\nu_\mathfrak{p}$ 表示类似定义的 $\mathfrak{p}$-进赋值。

对于整数理想 $\mathfrak{q}$，我们用 $\mathrm{ord}_\mathfrak{q}\gamma$ 表示代数整数 γ （与 $\mathfrak{q}$ 互素）模 $\mathfrak{q}$ 的阶。也就是说，$\mathrm{ord}_\mathfrak{q}\gamma$ 是满足 $\gamma^t \equiv 1 \pmod{\mathfrak{q}}$ 的最小整数 t。类似地，我们还使用

$\mathrm{ord}_{\mathfrak{q}} A$ 表示矩阵 A 模 $\mathfrak{q}$ 的阶（假设 $\det A$ 与 $\mathfrak{q}$ 互素）。

我们用 $\#\mathcal{S}$ 表示有限集 $\mathcal{S}$ 的基数。

我们用记号 $\lfloor x \rfloor$ 和 $\lceil x \rceil$ 分别表示不大于 x 的最大整数和不小于 $x \in \mathbb{R}$ 的最小整数。于是，我们用 $\{x\} = x - \lfloor x \rfloor \in [0、 1)$ 表示 x 的小数部分。

对于环 $\mathcal{R}$ ，我们用 $\mathcal{R}^{d\times d}$ 表示由 $\mathcal{R}$ 上的矩阵构成的环。

2. Background on linear recurrence sequences

2.1. 代数整数模素数幂理想的阶。假设 $\det A \not\equiv 0$ （模 p），且 A 可对角化，其特征值为 γ_1，……，$\gamma_d \in \overline{\mathbb{Q}}$。设 $\mathbb{K} = \mathbb{Q}(\gamma_1$，……，$\gamma_d)$ 为 A 的特征多项式 f 的分裂域，并设 $\mathcal{O}_{\mathbb{K}}$ 为其整数环。特别地， γ_1，……，$\gamma_d \in \mathcal{O}_{\mathbb{K}}$。于是，对于 $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^d$，我们有

$$u_n = \mathbf{v}A^n\mathbf{u} = \frac{1}{\det A}\left(\alpha_1\gamma_1^n + \ldots, +\alpha_d\gamma_d^n\right), \quad n \geqslant 0, \tag{2.1}$$

对于某些 α_1，……，$\alpha_d \in \mathcal{O}_{\mathbb{K}}$，参见 [7, 第 1.1 节7]。

我们始终假设， f 模 p 没有重根（因此其判别式不能被 p整除）。因此， p是非分歧的，并且我们可以将 p 分解为若干不同素理想的乘积。

现在固定一个整除 p 的素理想 $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{K}}$ ，并用 $\mathbb{Z}_{\mathfrak{p}}$ 表示环 $\mathfrak{p}$-进整数，背景介绍参见 [9,第 6 节4] 。

我们注意到，对于任意 $w \in \mathbb{Z}$ 和 $s \in \mathbb{N}$，整除关系 $p^s \mid w$和 $\mathfrak{p}^s \mid w$ 等价。特别是

$$\mathrm{ord}_{\mathfrak{p}^s} A = \mathrm{ord}_{p^s} A = \tau_s.$$

引理 2.1. 设 $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{K}}$ 为一个素理想，且 $M \in$ 为一般线性群 $\mathrm{GL}_d(\mathbb{Z}_{\mathfrak{p}})$。假设存在 $\mathbf{u} \in \mathbb{Z}_{\mathfrak{p}}^d$，使得 $\mathbf{u} \not\equiv (0$，……，$0)$ （模 $\mathfrak{p}$）。若 $M\mathbf{u} \equiv (0$，……，$0)$ （模 $\mathfrak{p}^w$），则 $\det M \equiv 0$ （模 $\mathfrak{p}^w$）。

证明。将 $M^{-1} = (\det M)^{-1} M^*$写作 $M^* \in \mathbb{Z}_{\mathfrak{p}}^{d\times d}$。如果

$$M\mathbf{u} \equiv (0, \ldots, 0) \pmod{\mathfrak{p}^w},$$

then

$$\det M \cdot \mathbf{u} = M^*M\mathbf{u} \equiv (0, \ldots, 0) \pmod{\mathfrak{p}^w}.$$

由于 $\mathbf{u}$ 有一个分量模 $\mathfrak{p}$ 非零，我们得出 $\det M \equiv 0$ （模 $\mathfrak{p}^w$）。□

对于与素理想 $\mathfrak{p}$ 互素的 γ、 $\lambda \in \mathcal{O}_{\mathbb{K}}$，我们定义 $\tau_s(\gamma$、 $\lambda)$ 为满足以下条件的最小正整数 t：

$$\gamma^t \equiv \lambda^t \pmod{\mathfrak{p}^s}.$$

容易看出， $\tau_1(\gamma、\ \lambda)$ 与 p 互素。

若 $\lambda = 1$，记

$$\tau_s(\gamma) = \tau_s(\gamma, \lambda).$$

引理 2.2. 设 p 是一个有理非分歧素数，且 $p\mathcal{O}_{\mathbb{K}} \subseteq \mathfrak{p}$。设 $\gamma、\ \lambda \in \mathcal{O}_{\mathbb{K}}$ 满足：对于任意 $t \neq 0$，都有 $\gamma^t \neq \lambda^t$。记

$$\tau_*(\gamma, \lambda) = \begin{cases} \tau_1(\gamma, \lambda) & if\ p \neq 2, \\ \tau_2(\gamma, \lambda) & if\ p = 2, \end{cases}$$

并设

$$\beta_{\mathfrak{p}}(\gamma, \lambda) = \nu_{\mathfrak{p}}\left(\gamma^{\tau_*(\gamma,\lambda)} - \lambda^{\tau_*(\gamma,\lambda)}\right).$$

则对于 $s \geqslant 2$，有

$$\tau_s(\gamma, \lambda) = \begin{cases} \tau_*(\gamma, \lambda) & if\ s \leqslant \beta_{\mathfrak{p}}(\gamma, \lambda), \\ \tau_*(\gamma, \lambda) p^{s-\beta_{\mathfrak{p}}(\gamma,\lambda)} & if\ s \geqslant \beta_{\mathfrak{p}}(\gamma, \lambda). \end{cases}$$

证明。只需证明对于 $s \geqslant \beta_{\mathfrak{p}}(\gamma、\ \lambda)$，有

$$\nu_{\mathfrak{p}}((\gamma/\lambda)^{\tau_s(\gamma,\lambda)} - 1) = s,$$

因此，不失一般性，我们可以假设 $\lambda = 1$。

If

$$\gamma^{\tau_s(\gamma)} - 1 = \vartheta_s, \quad \nu_{\mathfrak{p}}(\vartheta_s) = s,$$

then

$$\gamma^{p\cdot\tau_s(\gamma)} = (1 + \vartheta_s)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} \vartheta_s^i + \vartheta_s^p.$$

Here

$$\nu_{\mathfrak{p}}\left(\vartheta_s^p\right) = p \cdot s \qquad \text{and} \qquad \nu_{\mathfrak{p}}\left(\binom{p}{i}\vartheta_s^i\right) = i \cdot s + 1 \text{ for } 1 \leqslant i < p.$$

由于 $p = 2$ 时 $s > 1$，我们可知

$$\nu_{\mathfrak{p}}\left(\binom{p}{i}\vartheta_s^i\right) > s + 1 \quad \text{for } 2 \leqslant i \leqslant p$$

因此 $\nu_{\mathfrak{p}}\left(\gamma^{p\cdot\tau_s(\gamma)} - 1\right) = s + 1$。 □

由引理 2.2可知，存在 s_*，β_* 和 τ_* 使得

(2.2) $\tau_s =$ 的阶为$_{\mathfrak{p}^s} A = \tau_* p^{s-\beta_*}$ 其中 $(\tau_*$ 与 $p) = 1$ 的最大公约数 对于 $s \geqslant s_*$.

设 $s \geqslant s_*$。令

$$\gamma_i^{\tau_s} = 1 + \vartheta_i, \qquad i = 1, \ldots, d.$$

我们观察到

$$\vartheta_i \in \mathfrak{p}^s, \quad i = 1, \ldots, d, \qquad \text{and} \qquad \vartheta_j \notin \mathfrak{p}^{s+1} \quad \text{for some } j \in \{1, \ldots, d\}.$$

2.2. 线性递推序列的多项式表示。
由此可见 (2.1) 对于任意整数 m、$n \geqslant 0$ 和 $s \geqslant 1$，我们有

$$\begin{aligned} u_{n+\tau_s m} &= \frac{1}{\det A}\sum_{i=1}^{d}\alpha_i\gamma_i^{n+\tau_s m} = \frac{1}{\det A}\sum_{i=1}^{d}\alpha_i\gamma_i^{n}(1+\vartheta_i)^m \\ &= \frac{1}{\det A}\sum_{i=1}^{d}\alpha_i\gamma_i^{n}\sum_{j=0}^{m}\binom{m}{j}\vartheta_i^{js} = \frac{1}{\det A}\sum_{j=0}^{m}h_{n,j}p^{js}\binom{m}{j} \end{aligned} \tag{2.3}$$

with

$$h_{n,j} = p^{-js}\sum_{i=1}^{d}\alpha_i\gamma_i^{n}\vartheta_i^{j} \in \mathbb{Z}. \tag{2.4}$$

事实上，显然 $\mathfrak{p}^{js}$ 整除（2.4）中的内和；由于 p 未分歧， p 也如此。显然 $h_{n,j} \in \mathbb{Q}$，因此现在可以得出，实际上 $h_{n,j} \in \mathbb{Z}$。

引理 2.3. 令 $h_{n,j}$ $(1 \leqslant j \leqslant m)$ 由 (2.4) 定义，其中 $s \geqslant s_*$。记 $\gamma_0 = 1$ 并令

$$w = \frac{d(d+1)}{2}\max_{1\leqslant i<j\leqslant d}\{\beta_{\mathfrak{p}}(\gamma_i,\gamma_j) - \beta_*, 0\} + 1. \tag{2.5}$$

那么对于任意整数 $j \in [0, m-d+1]$，我们有

$$(h_{n,j},\dots,h_{n,j+d-1}) \not\equiv (0,\dots,0) \pmod{p^w}.$$

证明。假设，

$$(h_{n,j},\dots,h_{n,j+d-1}) \equiv (0,\dots,0) \pmod{\mathfrak{p}^w},$$

正如我们所提到的，这等价于模 p^w 的类似同余式。

令 π 为 $\mathbb{Z}_{\mathfrak{p}}$中极大理想 $\mathfrak{p}$ 的一致化元。由于 $\vartheta_i \in \mathfrak{p}^s$，我们可以写成

$$\bar{\vartheta}_i = \pi^{-s}\vartheta_i \in \mathbb{Z}_{\mathfrak{p}}, \quad 1 \leqslant i \leqslant d.$$

Let

$$\Theta = \begin{pmatrix} \bar{\vartheta}_1^{j} & \dots, & \bar{\vartheta}_d^{j} \\ \vdots & \ddots & \vdots \\ \bar{\vartheta}_1^{j+d-1} & \dots, & \bar{\vartheta}_d^{j+d-1} \end{pmatrix}.$$

Then

$$\begin{aligned} \Theta\,(\alpha_1\gamma_1^n,\dots,\alpha_d\gamma_d^n) &= \left((p/\pi)^{js}h_{n,j},\dots,(p/\pi)^{(j+d-1)s}h_{n,j+d-1}\right) \\ &\equiv (0,\dots,0) \pmod{\mathfrak{p}^w}. \end{aligned}$$

由于 $\left(\alpha_1\gamma_1^k,\ \ldots\ldots,\ \alpha_d\gamma_d^k\right) \not\equiv 0 \pmod{\mathfrak{p}}$，由引理 2.1 可知

$$\begin{aligned}\det \Theta &= \bar{\vartheta}_1^j \ldots \bar{\vartheta}_d^j \prod_{0\leqslant i_1<i_2\leqslant d} \left(\bar{\vartheta}_{i_1} - \bar{\vartheta}_{i_2}\right) \\ &= \bar{\vartheta}_1^j \ldots \bar{\vartheta}_d^j \prod_{0\leqslant i_1<i_2\leqslant d} \frac{\gamma_{i_1}^{\tau_s} - \gamma_{i_2}^{\tau_s}}{\pi^s} \equiv 0 \pmod{\mathfrak{p}^w},\end{aligned}$$

其中我们令 $\gamma_0 = 1$、$\vartheta_0 = 0$。

Thus

$$\gamma_{i_1}^{\tau_s} - \gamma_{i_2}^{\tau_s} \equiv 0 \pmod{\mathfrak{p}^{s+\left\lceil \frac{2w}{d(d+1)} \right\rceil}}$$

对于某个 $1 \leqslant i_1 < i_2 \leqslant d$。

然后，利用（2.2），我们写作

$$\tau_{\mathfrak{p}}\left(\gamma_{i_1}, \gamma_{i_2}\right) p^{s+\left\lceil \frac{2w}{d(d+1)} \right\rceil - \beta\left(\gamma_{i_1}, \gamma_{i_2}\right)} \mid \tau_s = \tau_* p^{s-\beta_*}.$$

由于两个 τ 都与 p 互素，我们得到

$$\left\lceil \frac{2w}{d(d+1)} \right\rceil \leqslant \beta\left(\gamma_{i_1}, \gamma_{i_2}\right) - \beta_*,$$

这与 w 的定义矛盾，从而完成证明。 □

注 2.4。 需要特别注意，参数 w 由 (2.5) 在引理 *2.3* 中定义，并不依赖于序列 (u_n) 在 (2.1)中所对应的适当对 $(\mathbf{u}、\mathbf{v})$。

引理 2.5。 对于任意向量适当对 $(\mathbf{u}、\mathbf{v}) \in \mathcal{R}_t^d \times \mathcal{R}_t^d$ 及相应的序列 (u_n)（由 (2.1) 给出），以下结论成立。对于任意整数 m、$n \geqslant 0$ 和 $t \geqslant s \geqslant s_*$ 满足

$$r \leqslant p^s$$

其中

$$r = \lfloor t/s \rfloor,$$

我们有

$$u_{n+\tau_s m} \equiv \frac{1}{r! \det A} \sum_{j=0}^{r} H_{n,j} p^{sj} m^j \pmod{p^t}$$

其中 $H_{n、\,j} \in \mathbb{Z}$、$j = 0$、……、r，使得对于 $j \in [0、\ r-d+1]$

$$\min\left\{\nu_p\left(H_{n,j}\right), \ldots, \nu_p\left(H_{n,j+d-1}\right)\right\} < w + \nu_p(r!),$$

其中 w 由 (2.5)定义。

证明。令 $s \geqslant s_*$ 由 (2.2) 定义。

将二项式系数 $\binom{m}{i}$ 写成关于 m的多项式，

$$\binom{m}{i} = \frac{c_{i,i} m^i + c_{i,i-1} m^{i-1} + \ldots + c_{i,0}}{i!} \quad \text{with } c_{i,i}, \ldots, c_{i,0} \in \mathbb{Z},$$

并注意到 $c_{i,\ i}=1$。由（2.3），可得

$$\begin{aligned} u_{n+\tau_s m} \equiv & \frac{1}{\det A}\sum_{i=0}^{r} h_{n,i}p^{si}\binom{m}{i} \\ \equiv & \frac{1}{r!\det A}\sum_{i=0}^{r}\frac{r!}{i!}h_{n,i}p^{si}\sum_{j=0}^{i}c_{i,j}m^j \\ \equiv & \frac{1}{r!\det A}\sum_{j=0}^{r}\left(\sum_{i=j}^{r}h_{n,i}\frac{r!}{i!}c_{i,j}p^{s(i-j)}\right)p^{sj}m^j \pmod{p^t} \end{aligned}$$

（其中最后两个同余实际上是等式）。

Put

$$H_{n,j}=\sum_{i=j}^{r}h_{n,i}\frac{r!}{i!}c_{i,j}p^{s(i-j)}.$$

令 $j\in[0,r-d+1]$ 固定，并设 $k\in[j,j+d-1]$ 满足

$$\nu_p(h_{n,k})=\min\left\{\nu_p\left(h_{n,j}\right),\dots,\nu_p\left(h_{n,j+d-1}\right)\right\}.$$

根据引理 2.3，我们有 $\nu_p(h_{n,\ k})<w$。对于这样的指标，由于 $c_{k,\ k}=1$，并且 $r\leqslant p^s$，我们有

$$\nu_p\left(\frac{r!}{k!}c_{k,k}\right)=\nu_p\left(\frac{r!}{k!}\right)<\nu_p\left(\frac{r!}{i!}c_{i,k}p^{s(i-k)}\right),$$

对于 $i=k,\dots,r$，因此

$$\nu_p(H_{n,k})=\nu_p(h_{n,k})+\nu_p(r!/k!)<w+\nu_p(r!)$$

由此即可得出结果。 □

3. Background on exponential sums

3.1. Vinogradov 均值定理的显式形式。设$N_{k,r}(M)$ 为方程组的整数解个数

$$\begin{gathered} x_1^j+\ldots+x_k^j=y_1^j+\ldots+y_k^j, \qquad j=1,\dots,r, \\ 1\leqslant x_i,y_i\leqslant M, \qquad i=1,\dots,k. \end{gathered}$$

我们下面应用引理 3.2 时，依据的是维诺格拉多夫均值定理的一个版本，它对 $N_{k,r}(M)$ 给出了精确的界。我们采用 Ford[8, 定理 3], 给出的完全显式版本，并在此以经过弱化和简化、适合我们需要的形式陈述。

引理 3.1. 存在绝对常数 $c_0 > 0$，使得对于满足 $d \geqslant 2$ 和 $k = \lfloor 6r^2 \log d \rfloor$ 的 $r \geqslant c_0 d$，对任意整数 $M \geqslant 1$，都有

$$N_{k,r}(M) \leqslant r^{3r^3} M^{2k - r(r+1)/2 + \delta_r r^2},$$

对于某个

$$\delta_r \leqslant \frac{1}{1000d}.$$

证明。首先，我们确认 c_0 足够大，使得 $r \geqslant 1000$ 并且 [8, 定理 3]适用。接下来，考察 k 和 r （在我们的记号中仅依赖于它们）的系数，该系数出现在 [8,定理 3] 的界中。我们看到它是若干项的乘积，其中最大的一项是$r^{2.055r^3}$。因此，当 c_0足够大时，我们可以将该系数界定为 r^{3r^3}。现在只需估计 δ_r。

由 [8, 定理 3],，所需结果成立，且

$$\begin{aligned}\delta_r &\leqslant \frac{3}{8}\exp(1/2 - 2k/r^2 + 1.7/r)\\ &\leqslant \frac{3}{8}\exp(1/2 - 2(6r^2\log d - 1)/r^2 + 1.7/r)\\ &\leqslant \frac{3}{8}\exp(2/3 - 12\log d)\end{aligned}$$

因为 $r \geqslant 1000$。还需注意到

$$\frac{3}{8}\exp(2/3) \leqslant 1 \qquad \text{and} \qquad \exp(-12\log d) = d^{-12} \leqslant \frac{1}{1000d}$$

对于 $d \geqslant 2$。 □

我们注意到，Bourgain、Demeter 和 Guth [5] 以及 Wooley [22]近期在 Vinogradov 均值定理方面取得的显著进展并不适用于我们这里的目的，因为其中包含的隐含常数依赖于 k 和 n，而在我们的方法中，k 和 n 会随 M一起增长。

3.2. 含多项式的双重指数和。我们用来界定指数和 $S_{p^t}(N; \mathbf{u}, \mathbf{v})$ 的主要工具是以下 Korobov[13, 引理 3]。

引理 3.2。假设

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

对于某个实数 α_ℓ 和整数 a_ℓ、q_ℓ、$\ell = 1$、.....、r。那么对于和

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

我们有

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

其中

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

我们还需要以下简单结果，它可以将单重和化为双重和。

引理 3.3。设 $f: \mathbb{R} \to \mathbb{R}$ 是任意函数。则对于任意整数 M、$N \geqslant 1$ 和 $a \geqslant 0$，我们有

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

证明。考察下列各和中不重叠的部分，我们看到，对于任意正整数 y 和 z

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

因此

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

交换求和次序并使用三角不等式，即可得到结论。□

3.3. 差异度与 Koksma-Sz¨usz 不等式。 研究分布均匀性的基本工具之一，是著名的*Koksma–Sz*¨usz 不等式 [12, 21] (另见 Drmota 和 Tichy [6, 定理 1。21])，该不等式将点序列的差异度与某些指数和联系起来。

在第1.2节的记号中，Koksma–Sz¨usz 不等式可表述如下。

引理 3.4. 对任意整数 $V \geqslant 1$，有

$$D_{\mathfrak{U}}(N) \ll \frac{1}{V} + \frac{1}{N} \sum_{0<\|\mathbf{v}\| \leqslant V} \frac{1}{r(\mathbf{v})} \left|S_{p^t}(N; \mathbf{u}, \mathbf{v})\right|,$$

其中

$$\|\mathbf{v}\| = \max_{j=1,\dots,d} |v_j|, \qquad r(\mathbf{v}) = \prod_{j=1}^{d} \max\left(|v_j|, 1\right),$$

且求和遍历所有满足 $0 < \|\mathbf{v}\| \leqslant V$ 的向量 $\mathbf{v} = (v_1, \dots, v_d) \in \mathbb{Z}^d$。

4. Proofs of the main results

4.1. 预备假设。 我们回顾一下，在 $d = 1$中，与定理 1.1 和 1.2 强度相近的结果由 Korobov 给出 [13]。因此我们可以假设 $d \geqslant 2$。

4.2. 定理 1.1 的证明。 我们可以假设

$$N \geqslant p^{8t^{1/2}}$$

否则结果显然成立，见（1.8）。

Put

$$s = \left\lfloor \frac{\log N}{4 \log p} \right\rfloor, \quad r = \left\lfloor \frac{t}{s} \right\rfloor \quad \text{and} \quad k = \left\lfloor 6r^2 \log d \right\rfloor.$$

于是我们有

$$r < s, \qquad \max\{w, s^*\} \leqslant s, \qquad p^s \leqslant N^{1/4} \tag{4.1}$$

如果 N 足够大，其中 s^* 和 w 分别由（2.2）和（2.5）定义。

首先假设 $r \geqslant c_0 d$，其中 c_0 由引理 3.1定义。必要时增大 c_0，我们可以假设

$$r \geqslant 10d. \tag{4.2}$$

记

$$u_n = \mathbf{v} A^n \mathbf{u}.$$

于是，由引理 2.5 和3.3 可得

$$\begin{aligned} \left|S_{p^t}(N; \mathbf{u}, \mathbf{v})\right| &\leqslant \frac{1}{p^{2s}} \sum_{n=0}^{N-1} \left| \sum_{x,y=1}^{p^s} \mathbf{e}\left(\frac{u_{n+\tau_s xy}}{p^t}\right) \right| + 2\tau_s p^{2s} \\ &\leqslant \frac{1}{p^{2s}} \sum_{n=0}^{N-1} \left| \sum_{x,y=1}^{p^s} \mathbf{e}\left(\frac{1}{p^t\, r!\det A} \sum_{j=0}^{r} H_{n,j} p^{sj} (xy)^j\right) \right| + 2p^{3s}. \end{aligned}$$

回顾（4.1），我们得出

$$|S_{p^t}(N;\mathbf{u},\mathbf{v})| \leqslant \frac{1}{p^{2s}} \sum_{n=0}^{N-1} |\sigma_n| + 2N^{3/4}, \tag{4.3}$$

其中

$$\sigma_n = \sum_{x,y=1}^{p^s} \mathbf{e}(f_n(x,y))$$

and

$$f_n(x,y) = \frac{1}{p^t\, r! \det A} \sum_{j=0}^{r} H_{n,j} p^{sj} (xy)^j.$$

固定指标 n，并写作

$$f_n(x,y) = \frac{a_r}{q_r}(xy)^r + \ldots + \frac{a_1}{q_1}xy + \frac{a_0}{q_0},$$

其中整数 a_j 和 q_j 定义为

$$\frac{H_{n,j}p^{sj}}{p^t\, r! \det A} = \frac{a_j}{q_j} \qquad \text{and} \qquad \gcd(a_j, q_j) = 1, \qquad j = 0, \ldots, r.$$

Put

$$\omega_j = \nu_p(H_{n,j}), \qquad j = 0, \ldots, r,$$

then

$$p^{t-sj-\omega_j} \leqslant q_j \leqslant r! p^{t-sj-\omega_j} \det A, \qquad j = 0, \ldots, r. \tag{4.4}$$

根据引理 3.1，采用上述 k的选择，我们有

$$N_{k,r}(p^s) \leqslant r^{3r^3} p^{2sk - sr(r+1)/2 + \delta_r s r^2}$$

其中某个 $\delta_r \leqslant 1/(1000d)$。然后根据引理 3.2，

$$|\sigma_n|^{2k^2} \leqslant \left(64k^2 \log(3Q)\right)^{r/2} r^{3r^3} p^{4sk^2 - sr(r+1)/2 + \delta_r s r^2} \times \prod_{j=1}^{r} \min\left\{p^{sj}, \sqrt{q_j} + \frac{p^{sj}}{\sqrt{q_j}}\right\}, \tag{4.5}$$

其中

$$Q = \max\{q_j : \ 1 \leqslant j \leqslant r\}.$$

由（4.4），可得 $Q \leqslant r!\ p^t$ 行列式 A 因此

$$\log(3Q) \leqslant \log\left(3r! p^t \det A\right) \leqslant tr \log(3rp \det A). \tag{4.6}$$

通过选择 r，我们有 $s(r-1) < t \leqslant sr$。对于 j，有

$$\frac{r+1}{2} \leqslant j < r$$

根据（4.4），我们有

$$q_j \leqslant r!p^{s(r-j)-\omega_j} \det A \leqslant r!p^{sj} \det A \qquad \text{and} \qquad q_j \geqslant p^{s(r-j-1)-\omega_j}.$$

Thus

$$\frac{\sqrt{q_j}}{p^{sj}} + \frac{1}{\sqrt{q_j}} \leqslant \frac{1 + r! \det A}{\sqrt{q_j}} \leqslant r^r p^{-\frac{s}{2}(r-j-1)+\omega_j/2} \det A.$$

Put

$$\lambda = \left\lfloor \frac{r-1}{2d} \right\rfloor.$$

于是由引理2.5，存在 j_1，……，j_λ 使得

$$\omega_{j_i} \leqslant w + \nu_p(r!) \tag{4.7}$$

and

$$\frac{r+1}{2} + (i-1)d \leqslant j_i \leqslant \frac{r+1}{2} + id. \tag{4.8}$$

As

$$\nu_p(r!) \leqslant \left\lfloor \frac{r}{p} \right\rfloor + \left\lfloor \frac{r}{p^2} \right\rfloor + \ldots \leqslant \frac{r}{p-1} \leqslant r,$$

利用（4.7），得到

$$\begin{aligned}
&\prod_{j=1}^{r} \min\left\{p^{sj}, \sqrt{q_j} + \frac{p^{sj}}{\sqrt{q_j}}\right\} \\
&\qquad = p^{sr(r+1)/2} \prod_{j=1}^{r} \min\left\{1, \frac{\sqrt{q_j}}{p^{sj}} + \frac{1}{\sqrt{q_j}}\right\} \\
&\qquad \leqslant p^{sr(r+1)/2} \prod_{(r+1)/2 \leqslant j \leqslant r} \min\left\{1, \frac{\sqrt{q_j}}{p^{sj}} + \frac{1}{\sqrt{q_j}}\right\} \\
&\qquad \leqslant p^{sr(r+1)/2} \prod_{i=1}^{\lambda} \left(r^r p^{-s(r-j_i-1)/2+(w+r)/2} \det A\right).
\end{aligned}$$

接下来，由（4.8），可得

$$r - j_i - 1 \geqslant (r-3)/2 - id, \qquad i = 1, \ldots, \lambda.$$

我们还注意到，由（4.1）

$$(w+r)/2 \leqslant s.$$

因此，

$$\begin{aligned}
\prod_{i=1}^{\lambda} p^{-s(r-j_i-1)/2+(w+r)/2} &\leqslant \prod_{i=1}^{\lambda} p^{-s((r-3)/2-id)/2+s} \\
&= p^{-\lambda s(r-3-d(\lambda+1))/4+\lambda s} \leqslant p^{-\lambda sr/4} \leqslant p^{-sr^2/(16d)},
\end{aligned}$$

由于我们的假设（4.2）蕴含 $\lambda > r/(4d)$。

然后，将此界和式（4.6）代入式（4.5），我们得到$|\sigma_n|^{2k^2}$

$$\begin{aligned}
&\leqslant \left(2400r^5t(\log d)^2\log(3rp\det A)\right)^{r/2} r^{3r^3+r\lambda}(\det A)^{\lambda}p^{4sk^2-\frac{sr^2}{16d}+\delta_r sr^2}\\
&\leqslant \left(2400r^5t(\log d)^2\log(3rp\det A)\right)^{r/2} r^{3r^3+r\lambda}(\det A)^{\lambda}p^{4sk^2-\frac{123}{2000d}sr^2}\\
&= \left(2400r^5(\log d)^2\log(3rp\det A)\right)^{r/2} r^{3r^3+r\lambda}(\det A)^{\lambda}t^{r/2}p^{4sk^2-\frac{123}{2000d}sr^2}
\end{aligned}$$

因此，利用

$$\frac{123}{2\cdot 6^2\cdot 2000} > \frac{1}{1500},$$

我们得出结论

$$|\sigma_n| \ll \left(\left(1024r^5\log(3rp\det A)\right)^{r/2} r^{3r^3+r\lambda}(\det A)^{\lambda}\right)^{1/(2k^2)} t^{r/(4k^2)}p^{2s-\frac{1}{1500d}\frac{s}{r^2(\log d)^2}}. \tag{4.9}$$

由于 $r \leqslant s/t,$，我们有

$$\frac{s}{r^2} \geqslant \frac{s^3}{t^2} \geqslant \frac{(\log N)^3}{512t^2(\log p)^3} = \frac{\log N}{512\log p}\rho^2.$$

因此

$$p^{s/(r\log d)^2} \geqslant N^{\frac{1}{512(\log d)^2}\rho^2}.$$

另一方面，取 c_0 足够大，使得 $r \geqslant 35$，我们可知

$$r \geqslant \frac{35}{36}(r+1) \geqslant \frac{35t}{36s}.$$

如有必要，增大 c，我们可以假设 $90d \leqslant t/\log t$，否则结论显然成立。

因此，

$$\begin{aligned}
\frac{r}{k^2} &\leqslant \frac{1}{36r^3(\log d)^2} \leqslant \frac{s^3}{35t^3(\log d)^2}\\
&\leqslant \frac{1}{35\cdot 4^3\cdot(\log d)^2}\frac{(\log N)^3}{t^3(\log p)^3} \leqslant \frac{\log N}{1575\cdot 2^7 d\log t\log p(\log d)^2}\rho^2
\end{aligned}$$

从而

$$t^{r/(4k^2)} \leqslant N^{\frac{1}{1575\cdot 2^9 d(\log d)^2}\rho^2}$$

and

$$\left(\left(1024r^5\log(3rp\det A)\right)^{r/2} r^{3r^3+r\lambda}(\det A)^{\lambda}\right)^{1/(2k^2)} \ll 1.$$

因此，由（4.9）可得

$$|\sigma_n| \ll p^{2s}N^{-\eta_0\rho^2/(d(\log d)^2)}$$

对于某个绝对常数 $\eta_0 > 0$，只要 t 足够大即可。

于是，由（4.3），

$$S_{p^t}(N;\mathbf{u},\mathbf{v}) \ll N^{1-\eta_0\rho^2/(d(\log d)^2)} + N^{3/4} \leqslant N^{1-\eta\rho^2/d(\log d)^2)}.$$

若 $r \leqslant c_0 d$，定义

$$N_0 = \left\lfloor N^{r/(4c_0 d)} \right\rfloor \qquad \text{and} \qquad \rho_0 = \frac{\log N_0}{t \log p} > \frac{1}{8c_0 d}\rho. \tag{4.10}$$

Then

$$S_{p^t}(N;\mathbf{u},\mathbf{v}) \leqslant \sum_{0\leqslant k<N/N_0} \left|S_{p^t}(N_0; A^{kN_0}\mathbf{u},\mathbf{v})\right| + N_0.$$

由于 $(A^{kN_0}\mathbf{u},\mathbf{v})$ 也是适当的，将先前的论证应用于内部项，我们得到

$$S_{p^t}(N;\mathbf{u},\mathbf{v}) \ll \frac{N}{N_0} N_0^{1-\eta\rho_0^2} + N_0 \ll N^{1-\frac{\eta}{(8c_0 d)^3}\frac{\rho^2}{d(\log d)^2}}$$

由（4.10）。因此，将 η 替换为 $\eta/(8c_0)^3$, ，我们便完成了证明。

4.3. 定理 **1.2** 的证明。 取 $V = \left\lfloor N^{1/4} \right\rfloor$，并利用以下显然的观察：对于任意满足 $\mathbf{v} \in \mathbb{Z}^d$ 的 $0 < \|\mathbf{v}\| \leqslant V$，如引理 3.4 中所述，我们有

$$\gcd(v_1,\dots,v_d,p^t) = p^\nu \leqslant N^{1/4}$$

其中 ν 是某个整数。对于这样的 $\mathbf{v}$，我们有

$$S_{p^t}(N;\mathbf{u},\mathbf{v}) = S_{p^{t-\nu}}\left(N;\mathbf{u},p^{-\nu}\mathbf{v}\right).$$

若 $N \leqslant \tau_{t-\nu}$，则直接将定理 1.1 的界应用于和 $S_{p^{t-\nu}}\left(N;\ \mathbf{u}\ p^{-\nu}\mathbf{v}\right)$ 并注意到

$$\frac{\log N}{(t-\nu)\log p} \geqslant \rho,$$

因此，随着 ν 增大，所得的界甚至会变得更强。

若 $N > \tau_{t-\nu}$，则利用周期性，我们写作

$$S_{p^{t-\nu}}\left(N;\mathbf{u},\mathbf{v}p^{-\nu}\right) = QS_{p^{t-\nu}}\left(\tau_{t-\nu};\mathbf{u},\mathbf{v}p^{-\nu}\right) + S_{p^{t-\nu}}\left(R;\mathbf{u},\mathbf{v}p^{-\nu}\right),$$

其中

$$Q = \left\lfloor N/\tau_{t-\nu} \right\rfloor \qquad \text{and} \qquad R = N - Q\tau_{t-\nu}.$$

再次将定理 1.1 应用于每个和，并注意到根据引理 2.2

$$\tau_{t-\nu} \gg p^{t-\nu} \geqslant p^t N^{-1/4} \gg N^{3/4}.$$

利用引理 3.4，经过简单计算即可得到所需结果。

5. Comments

这里我们主要关注序列（1.2）的短片段，这也是问题中更具挑战性的方面，从实际角度来看也更为重要。不过，长度为 N 且与 τ_t 相当的较长片段也值得关注。很有可能也可以利用 [20] 中的论证，得到以下关于扭和的界

$$\sum_{n=0}^{\tau_t-1} \mathbf{e}\left(\frac{1}{p^t}\mathbf{v}A^n\mathbf{u}\right)\mathbf{e}\left(bn/\tau_t\right) \ll \tau_t^{1-1/(d+1)+o(1)},$$

这与 (1.12) 类似，只是在指数上略有损失。进一步结合补全技巧（见 [10, 第 12 节。2], 此界可得

$$S_{p^t}(N;\mathbf{u},\mathbf{v}) \ll \tau_t^{1-1/(d+1)+o(1)}$$

以及类似的差异度界。

我们注意到，除了固定素数的幂之外，另一类值得考虑的自然模数是大素数 p 对应的素数模数 p 。如果 A 的特征多项式模 p 完全分裂，那么 Bourgain [1, 命题 3] 的结果允许我们考虑全周期长度为 p^δ 内的区间，其中 $\delta > 0$ 为任意固定值。很可能结合[3] 的思想，可以将其缩短为长度为 $\exp\left(c\log p/\log\log p\right)$ 的区间，其中 $c > 0$ 为某个绝对常数。然而，与本文允许的长度相比，这些长度相对于模数和周期仍然大得多。

Acknowledgement

在本研究准备期间，L. M. 得到奥地利科学基金 FWF 项目 F 5506 的部分资助。该项目属于特别研究计划“拟蒙特卡罗方法：理论与应用”，此外还获得匈牙利国家研究、发展与创新办公室（NRDI）拨款 FK 142960 的资助；I. S. 则获得澳大利亚研究理事会拨款 DP170100786 和 DP200100355 的资助。

References

[1] J. Bourgain, 《莫德尔指数和估计再探》《美国数学会杂志》，18 （2005），477–499。18[2] J. Bourgain, 《关于 CAT 映射量子遍历性的一点说明》，泛函分析的几何方面，数学讲义，第 1910 卷，Springer，柏林，2007，89–98。5

[3] J. Bourgain, 《在源具有最优熵条件下素域中的多线性指数和》, 《几何与泛函分析》, 18（2009）, 1477–1502。18[4] J. Bourgain, 《关于 Vinogradov 平均值》, 《斯捷克洛夫数学研究所论文集》, 296（2017）, 30–40。2[5] J. Bourgain、C. Demeter 和 L. Guth, 《次数高于三的 Vinogradov 平均值定理主要猜想的证明》, 《数学年刊》, 184（2016）, 633–682。11[6]M. Drmota 和 R. F. Tichy, 《序列、差异与应用》, Springer-Verlag, 柏林, 1997。4, 12[7] G. Everest、A. van der Poorten、I. E. Shparlinski 和 T. Ward, 《递推序列》, 《数学调查与专著》, 104, 美国数学会, 普罗维登斯, 罗得岛州, 2003。5, 6[8] K. Ford, 《Vinogradov 积分与黎曼 ζ 函数的界》, 《伦敦数学学会会刊》, 85（2002）, 565–633。3, 10, 11[9] F. O. Gouvˆea, P-进数, Springer, 2020。6[10] H. Iwaniec 和 E. Kowalski, 《解析数论》, 美国数学会, 普罗维登斯, 罗得岛州, 2004。18[11] B. Kerr、L. M´erai 和 I. E. Shparlinski, 《关于梅森数的数字》, 《伊比利亚美洲数学杂志》, 即将出版。5[12] J. F. Koksma, 《关于丢番图不等式的一些定理》, 数学中心论文第 5 号, 阿姆斯特丹, 1950。4, 12[13]N. M. Korobov, 《周期分数中的数字分布》, 《数学文集》, 89（1972）, 654–670（俄文）, 译载于《苏联数学文集》, 18（1974）, 659–676。2, 3, 5, 11, 13[14] P. Kurlberg 和 Z. Rudnick, 《关于环面的线性映射的量子遍历性》, 《数学物理通讯》, 222（2001）, 201–227。5[15] L. M´erai 和 I. E. Shparlinski, 《模 2^t 的逆同余伪随机数短子序列的分布》, 《计算数学》, 89（2020）, 911–922。2[16] L. M´erai 和 I. E. Shparlinski, 《关于素数时刻 M¨obius 变换生成的动力系统》, 《数学科学研究》, 8（2021）, 文章编号 10。5[17] H. Niederreiter, 《随机数生成与拟蒙特卡罗方法》, SIAM 出版社, 1992。2[18] A. Ostafe、I. E. Shparlinski 和 J. F. Voloch, 《矩阵幂的方程与特征和、小子群上的 Kloosterman 和与量子遍历性》, 《国际数学研究论文》, 即将出版。5[19] Z. Rudnick, 《量子映射的算术理论》, 《北约高级研究院关于数论中均匀分布的论文集》, 蒙特利尔, 2005, 《北约科学丛书》, 第 237 卷, Springer, 2007, 331–342。5[20] I. E. Shparlinski, 《带递推序列的指数和的界及其应用》, 《沃罗涅日国立师范学院论文集》, 197（1978）, 74–85（俄文）。2, 5, 18[21] P. Sz¨usz, 《关于均匀分布理论中的一个问题》, 《匈牙利第一届大会会议录》, 布达佩斯, 1952, 461–472（匈牙利文）。4, 12[22] T. D. Wooley, 《嵌套高效同余与 Vinogradov 平均值定理的相关结果》, 《伦敦数学学会会刊》, 118（2019）, 942–1016。11

L.M.: Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenberger Strasse 69, A-4040 Linz, Austria and Department of Computer Algebra, Eötvös Loránd University, H-1117 Budapest, Pazmány Péter sétány 1/C, Hun-gary

电子邮箱：laszlo.merai@oeaw.ac.at

I.E.S.: School of Mathematics and Statistics,
University of NewSouth Wales. Sydney, NSW 2052, Australia
电子邮箱：igor.shparlinski@unsw.edu.au