DE GRUYTER
OPEN

uniform distribution theory

DOI: 10.1515/udt-2016–0014
Unif. Distrib. Theory **11** (2016), no.2, 45–89

ON THE GAUSSIAN LIMITING DISTRIBUTION OF LATTICE POINTS IN A PARALLELEPIPED

Mordechay B. Levin

Dedicated to the memory of Professor Pierre Liardet

ABSTRACT. Let $\Gamma \subset \mathbb{R}^s$ be a lattice obtained from a module in a totally real algebraic number field. Let $\mathcal{R}(\boldsymbol{\theta}, \mathbf{N})$ be the error term in the lattice point problem for the parallelepiped $[-\theta_1 N_1, \theta_1 N_1] \times \cdots \times [-\theta_s N_s, \theta_s N_s]$. In this paper, we prove that $\mathcal{R}(\boldsymbol{\theta}, \mathbf{N})/\sigma(\mathcal{R}, \mathbf{N})$ has a Gaussian limiting distribution as $N \to \infty$, where $\boldsymbol{\theta} = (\theta_1, \dots, \theta_s)$ is a uniformly distributed random variable in $[0,1]^s$, $N = N_1 \cdots N_s$ and $\sigma(\mathcal{R}, \mathbf{N}) \asymp (\log N)^{(s-1)/2}$. We obtain also a similar result for the low discrepancy sequence corresponding to Γ. The main tool is the S-unit theorem.

Communicated by Werner Georg Nowak

1. Introduction

1.1. Preliminaries

In 1992, J. Beck (see [Be1]-[Be3])[1] discovered a very surprising phenomenon of randomness of the sequence $\{n\sqrt{2}\}_{n\geq 1}$ and the lattice

$$\left\{(n, n\sqrt{2}+m) | (n,m) \in \mathbb{Z}^2\right\}:$$
$$\operatorname{vol}\left\{(x,y,z) \in [0,1)^3 : \ \frac{\sum_{n=0}^{[xN]} \left(\mathbb{1}_{[0,y)}(\{n\sqrt{2}+z\}) - y\right)}{c_1\sqrt{\log N}} < t\right\} \to \Phi(t)$$

as $N \to \infty$, where $\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-u^2/2} du$, $\mathbb{1}_{\mathcal{O}}(x)$ is the indicator function of $\mathcal{O}$, $c_1 > 0$ and $\{v\}$ is the fractional part of v.

2010 Mathematics Subject Classification: Primary 11P21, 11K38, 11R80; Secondary 60F05.
Keywords: lattice points problem, low discrepancy sequences, totally real algebraic number field, central limit theorem.

[1]The results of this paper were announced in [Le1], [Le2].

According to [Be2, p. 41], the generalizations of this result to the multidimensional case for a Kronecker's lattice is very difficult because of problems connected to Littlewood's conjecture:

$$\varliminf_{n\to\infty} \quad n \ll n\alpha \gg\ll n\beta \gg= 0$$

for all reals α, β, where $\ll x \gg= \min(\{x\}, 1-\{x\})$.

In this paper, in order to avoid these problems, we consider a lattice Γ obtained from a module in a totally real algebraic number field. We prove the Central Limit Theorem (abbreviated CLT) for the number of points in a parallelepiped. We obtain also a similar result for low discrepancy sequences corresponding to Γ (see [Le2]). For related questions and generalizations, see [Le3]. In a forthcoming paper, we will generalize results from [Be2] to the cases of s-dimensional Halton's sequences (for 1-dimensional case see [LeMe]), (t, s)-sequences, and admissible lattices (see the definition below).

1.2. Lattice points

Let $\mathcal{O} \subset \mathbb{R}^s$ be a compact region, vol $\mathcal{O}$ its volume, $t\mathcal{O}$ its dilatation of $\mathcal{O}$ by a factor $t > 0$, and let $t\mathcal{O} + \mathbf{x}$ be the translation of $t\mathcal{O}$ by a vector $\mathbf{x} \in \mathbb{R}^s$. Let $\Gamma \subset \mathbb{R}^s$ be a lattice, i.e., a discrete subgroup of $\mathbb{R}^s$ with a compact fundamental set $\mathbb{R}^s/\Gamma$, and denote $\det\Gamma$=vol$(\mathbb{R}^s/\Gamma)$. Let

$$\mathcal{N}(\mathcal{O}, \Gamma) = \operatorname{card}(\mathcal{O} \cap \Gamma) = \sum_{\boldsymbol{\gamma}\in\Gamma} \mathbb{1}_{\mathcal{O}}(\boldsymbol{\gamma}) \tag{1.1}$$

be the number of points of Γ lying inside $\mathcal{O}$. We define the error $\mathcal{R}(\mathcal{O}+\mathbf{x}, \Gamma)$ by

$$\mathcal{N}(\mathcal{O}+\mathbf{x}, \Gamma) = \mathrm{vol}\mathcal{O} \cdot (\det\Gamma)^{-1} \; + \; \mathcal{R}(\mathcal{O}+\mathbf{x}, \Gamma). \tag{1.2}$$

We define the norm of $\mathbf{x} = (x_1, \dots, x_s)$ by $\mathrm{Nm}(\mathbf{x}) = x_1 x_2 \cdots x_s$. The lattice $\Gamma \subset \mathbb{R}^s$ is *admissible* if

$$\mathrm{Nm}\,\Gamma = \inf_{\boldsymbol{\gamma}\in\Gamma\setminus\{0\}} |\mathrm{Nm}(\boldsymbol{\gamma})| > 0.$$

Let $\mathcal{K}$ be a totally real algebraic number field of degree $s \geq 2$, and let σ be the canonical embedding of $\mathcal{K}$ in the Euclidean space $\mathbb{R}^s$, $\sigma : \mathcal{K} \ni \xi \to \sigma(\xi) = \big(\sigma_1(\xi), \dots, \sigma_s(\xi)\big) \in \mathbb{R}^s$, where $\{\sigma_j\}_{j=1}^s$ are the embeddings of $\mathcal{K}$ in $\mathbb{R}$. Let $N_{\mathcal{K}/\mathbb{Q}}(\xi)$ be the norm of $\xi \in \mathcal{K}$. By [BS, p. 404]

$$N_{\mathcal{K}/\mathbb{Q}}(\xi) = \sigma_1(\xi)\cdots\sigma_s(\xi), \quad \text{and} \quad |N_{\mathcal{K}/\mathbb{Q}}(\alpha)| \geq 1 \tag{1.3}$$

for all algebraic integers $\alpha \in \mathcal{K} \setminus \{0\}$. Thus $|\mathrm{Nm}(\sigma(\xi))| = |N_{\mathcal{K}/\mathbb{Q}}(\xi)|$. Let M be a full $\mathbb{Z}-$module in $\mathcal{K}$, and let Γ_M be the lattice corresponding to M under the embedding σ. It is known that the set $M^\perp$ of all $\beta \in \mathcal{K}$, for which $\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z}$ for all $\alpha \in M$, is also a full $\mathbb{Z}-$ module (*the dual of the module* M) of the field $\mathcal{K}$ (see [BS, p. 94]). Recall that the dual lattice $\Gamma_M^{\perp}$ consists of all vectors $\boldsymbol{\gamma}^{\perp} \in \mathbb{R}^s$ such that the inner product $\langle \boldsymbol{\gamma}^{\perp}, \boldsymbol{\gamma} \rangle$ belongs to $\mathbb{Z}$ for each $\boldsymbol{\gamma} \in \Gamma$. Hence $\Gamma_{M^{\perp}} = \Gamma_M^{\perp}$. Let $(C_M)^{-1} > 0$ be an integer such that $(C_M)^{-1}\gamma$ are algebraic integers for all $\gamma \in M \cup M^{\perp}$. Hence

$$\min(\mathrm{Nm}\,\Gamma_M, \mathrm{Nm}\,\Gamma_M^{\perp}) \geq C_M^s. \tag{1.4}$$

Therefore Γ_M and $\Gamma_{M^{\perp}}$ are admissible lattices. In the following we will use the notation $\Gamma = \Gamma_M$.

We note that the problem considered in this paper is closely connected with quantum chaos theory. By [Bl] and [Ma], the problem about the number of eigenvalues of an operator in a quantum system in a large interval $[0, t]$ leads to the problem of counting the number of lattice points in a domain $t\mathcal{O}$. For example, the particular case of the famous Berry-Tabor conjecture (see, e.g., [Ma]) consists of the assertion that the number of lattice points in the thin domain $(t + 1/t)\mathcal{O} \setminus t\mathcal{O}$ tends to the Poisson distribution (for the case of 'generic' lattice), where t is a uniformly distributed random variable in $[0, L]$ and $L \to \infty$ (see, e.g., [Bl], [Ma], and [Si]).

1.3. Low discrepancy sequences

Let $\big((\beta_{n,N})_{n=0}^{N-1}\big)$ be an N-point set in the s-dimensional unit cube $[0,1)^s$, $\mathcal{O} = [0, y_1) \times \cdots \times [0, y_s) \subseteq [0,1)^s$,

$$\Delta\big(\mathcal{O}, (\beta_{n,N})_{n=0}^{N-1}\big) = \sum_{0 \leq n \leq N-1} \mathbb{1}_{\mathcal{O}}(\beta_{n,N}) - y_1 y_2 \cdots y_s N. \tag{1.5}$$

We define the L^{∞} and L^2 *discrepancy* of an N-point set $(\beta_{n,N})_{n=0}^{N-1}$ by

$$D\big((\beta_{n,N})_{n=0}^{N-1}\big) = \sup_{0 < y_1, \dots, y_s \leq 1} \Big| \frac{1}{N} \Delta\big(\mathcal{O}, (\beta_{n,N})_{n=0}^{N-1}\big) \Big|,$$

$$D_2\big((\beta_{n,N})_{n=0}^{N-1}\big) = \left(\int_{[0,1]^s} \Big| \frac{1}{N} \Delta\big(\mathcal{O}, (\beta_{n,N})_{n=0}^{N-1}\big) \Big|^2 \mathrm{dy_1 \cdots dy_s} \right)^{1/2},$$

respectively. In 1954, Roth proved that there exists a constant $C > 0$, such that

$$N D_2\big((\beta_{n,N})_{n=0}^{N-1}\big) > C (\ln N)^{\frac{s-1}{2}} \tag{1.6}$$

for all N-point sets $(\beta_{n,N})_{n=0}^{N-1}$.

Definition. A sequence $(\beta_n)_{n \geq 0}$ is of low discrepancy (abbreviated l.d.s.) if

$$D\big((\beta_n)_{n=0}^{N-1}\big) = O\big(N^{-1} (\ln N)^s\big) \quad \text{as} \quad N \to \infty.$$

A sequence of point sets $\big((\beta_{n,N})_{n=0}^{N-1}\big)_{N=1}^{\infty}$ is of low discrepancy (abbreviated l.d.p.s.) if

$$D\big((\beta_{n,N})_{n=0}^{N-1}\big) = O\big(N^{-1}(\ln N)^{s-1}\big) \quad \text{as} \quad N \to \infty.$$

For examples of l.d.s. and l.d.p.s. see [BC] and [DrTi]. In [Fr], Frolov constructed a low discrepancy point set from a module in a totally real algebraic number field (see also [By],[Skr]). Using this approach, we proposed in [Le2] the following construction of l.d.s. :

According to (1.4), $|\mathrm{Nm}(\boldsymbol{\gamma}^{(1)} - \boldsymbol{\gamma}^{(2)})| \geq C_M^s$ for different points $\boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)} \in \Gamma$. Hence, there are no two different points $\boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)} \in \Gamma$ with $\gamma_s^{(1)} = \gamma_s^{(2)}$. It follows that the set $W_{\mathbf{x}} = ((\mathbf{x}, 0) + \Gamma) \cap [0,1)^{s-1} \times (-\infty, \infty)$ with $\mathbf{x} \in [0,1)^{s-1}$ can be enumerated by a sequence $(z_{\mathbf{x},k}, z_s(\mathbf{x}, k))_{k=-\infty}^{+\infty}$ in the following way:

$$z_{\mathbf{x},0} = \mathbf{x},\ z_s(\mathbf{x}, 0) = 0,\ \ z_{\mathbf{x},k} \in [0,1)^{s-1} \ \text{ and } \ z_s(\mathbf{x}, k) < z_s(\mathbf{x}, k+1) \in \mathbb{R}, \quad (1.7)$$

for $k \in \mathbb{Z}$. We see that there exists a unique $(w, y_s) \in W_{\mathbf{x}}$ with

$$y_s = \min\{v > 0 \mid \exists w \in [0,1)^{s-1}, \ \text{ such that } \ (w, v) \in W_{\mathbf{x}}\}.$$

Let $\mathcal{T}(\mathbf{x}) = w$. In [Le2], we proved that $\mathcal{T}(\mathbf{x})$ is an ergodic transformation with respect to the Lebesgue measure on $[0,1)^{s-1}$, $\mathcal{T}^k(\mathbf{x}) = z_k(\mathbf{x})$ for $k \in \mathbb{Z}$, and $\big(T^k(x)\big)_{n\geq 1}$ is of low discrepancy, i.e., $D_N\big(\big(T^k(x)\big)_{n\geq 1}\big) = O(\ln^s N)$. In [Le4], we proved that this estimate cannot be improved.

In Theorem 2, we will prove that there exists a sequence $(\beta_k)_{k\geq 0}$ such that the triangular array of random variables $(\mathbb{1}_{[0,y_1)\times\cdots\times[0,y_{s-1})}(\beta_k))_{k=0}^{[y_s N]-1}$ satisfies the CLT with an extremely small (by order of magnitude) standard deviation (see Roth's lower bound (1.6)). We will take $\beta_k = \mathcal{T}^k(\mathbf{x}),\ k = 0, 1, \ldots$

1.4. Statement of the results

We consider the probability space $([0,1]^s, \lambda, B([0,1]^s))$ with Lebesgue's measure λ. Hence, we have the following formula for the expectation:

$$\mathbf{E}[f(\boldsymbol{\theta})] = \int_{[0,1]^s} f(\boldsymbol{\theta}) \,\mathrm{d}\boldsymbol{\theta}. \quad (1.8)$$

We define the variation of f by $\mathbf{Var}(f) = \mathbf{E}[f^2] - (\mathbf{E}[f])^2$. Let $\mathbb{K}_s = [-1/2, 1/2)^s$,

$$\mathbf{N} = (N_1, \ldots, N_s),\ N_i > 0,\ (i = 1, \ldots, s),\ N = N_1 N_2 \cdots N_s,$$

$$(x_1, \ldots, x_s) \cdot (y_1, \ldots, y_s) = (x_1 y_1, \ldots, x_s y_s),$$

$$(x_1, \ldots, x_s) \cdot \mathcal{O} = \{(x_1, \ldots, x_s) \cdot (y_1, \ldots, y_s) \ : \ (y_1, \ldots, y_s) \in \mathcal{O}\}$$

and $n = [\log_2 N] + 1$.

Theorem 1. *With the notations as above, there exist $w_2 > w_1 > 0$ such that*

$$\sup_{t,\mathbf{x}} \left| \mathrm{vol}\left\{ \boldsymbol{\theta} \in \mathbf{I}^s : \frac{\mathcal{R}(\boldsymbol{\theta} \cdot \mathbf{N} \cdot \mathbb{K}_s + \mathbf{x}, \Gamma)}{w(\mathbf{N},\mathbf{x}) n^{(s-1)/2}} < t \right\} - \Phi(t) \right| = O(n^{-1/15})$$

as $N \to \infty$, with $w(\mathbf{N},\mathbf{x}) = \mathbf{Var}^{1/2}(\mathcal{R}(\boldsymbol{\theta} \cdot \mathbf{N} \cdot \mathbb{K}_s + \mathbf{x}, \Gamma)) n^{-(s-1)/2} \in [w_1, w_2]$, $\mathbf{I} = [0,1)$ for all $\mathbf{x} \in [0,1)^{s-1}$.

Theorem 2. *Let $\mathcal{O} = [0, y_1) \times \cdots \times [0, y_{s-1})$. Then there exist $w_2 > w_1 > 0$ such that*

$$\sup_{t} \left| \mathrm{vol}\left\{ \mathbf{y} \in \mathbf{I}^s, \mathbf{x} \in \mathbf{I}^{s-1} : \frac{\Delta\big(\mathcal{O}, \big(\mathcal{T}^k(\mathbf{x})\big)_{k=0}^{[y_s N]-1}\big)}{v(N,\mathbf{x}) n^{(s-1)/2}} < t \right\} - \Phi(t) \right| = O(n^{-1/15})$$

as $N \to \infty$, with $v(N,\mathbf{x}) = \mathbf{Var}^{1/2}\Big(\Delta\Big(\mathcal{O}, \big(\mathcal{T}^k(\mathbf{x})\big)_{k=0}^{[y_s N]-1}\Big)\Big) n^{-(s-1)/2} \in [w_1, w_2]$.

Throughout the paper, O-constants do not depend on $\mathbf{x}, \boldsymbol{\theta}$ and $\mathbf{N}$.

Remark. Let $K(r_1, r_2)$ be an algebraic number field with signature (r_1, r_2), $r_1 + 2r_2 = s$, $\Gamma = \Gamma(M, r_1, r_2) \subset \mathbb{R}^s$ a lattice obtained from a module M in $K(r_1, r_2)$, $\mathbf{N} = (N_1^{'}, \ldots, N_{r_1}^{'}, N_1, \ldots, N_{r_2}) \in \mathbb{Z}_+^{r_1+r_2}$, $\boldsymbol{\gamma} = (\gamma_1^{'}, \ldots, \gamma_{r_1}^{'}, \gamma_1, \ldots \ldots, \gamma_{r_2}) \in \mathbb{R}^s$ $(\gamma_i^{'} \in \mathbb{R},\ \gamma_j \in \mathbb{R}^2, i = 1, \ldots, r_1, j = 1, \ldots, r_2)$, $\mathbf{y} = (y_1^{'}, \ldots \ldots, y_{r_1}^{'}, y_1, \ldots, y_{r_2})$, $V = \mathbb{R}^s/\Gamma$, $(\mathbf{y}, \mathbf{x})$ a uniformly distributed random variable in $[0,1]^{r_1+r_2} \times V$,

$$G(\mathbf{N}) = \prod_{i=1}^{r_1} [-N_i y_i, N_i y_i] \prod_{j=1}^{r_2} \{ z \in \mathbb{R}^2 \quad |z| \le N_j y_j \},$$

and let

$$\xi_1(\mathbf{N}) = \sum_{\boldsymbol{\gamma} \in \Gamma + \mathbf{x}} \mathbf{1}_{G(\mathbf{N})}(\boldsymbol{\gamma}),$$

$$\xi_2(\mathbf{N}) = \sum_{\boldsymbol{\gamma} \in \Gamma + \mathbf{x}} \mathbf{1}_{G(\mathbf{N})}(\boldsymbol{\gamma}) \prod_{j=1}^{r_2} \sqrt{N_j^2 y_j^2 - \gamma_j^2}.$$

In a forthcoming paper, we will prove CLT for the multisequence $\xi_i(\mathbf{N})$, where $i = 1$ if $r_2 \ge 2$ and $i = 2$ if $r_2 = 1, r_1 \ge 1$. The case $r_2 = 1, r_1 = 0$ was investigated earlier by Hughes and Rudnick [HuRu].

Let us describe the main steps of the proof of Theorem 1:

In Subsection 2.1, we use the Poisson summation formula and the standard trick of 'smoothing'. This allows us to express the error $\dot{\mathcal{R}}$ in terms on absolutely convergent Fourier series. Let $\eta_1, \ldots, \eta_{s-1}$ be a set of fundamental units of the field $\mathcal{K}$, and let $A_1, \ldots, A_{s-1}$ be a set of the appropriate toral automorphisms. Let $F_1 \subset \mathbb{R}^s$ be a fundamental domain for the field $\mathcal{K}$.

According to [BS, p. 112] for all $\boldsymbol{\gamma} \in \Gamma^{\perp}$ there exist $\boldsymbol{\gamma}_1 \in F_1 \cap \Gamma^{\perp}$ such that $\boldsymbol{\gamma} = \boldsymbol{\gamma}_1 \eta_1^{k_1} \dots \eta_{s-1}^{k_{s-1}}$ for some $k_1, \dots k_{s-1} \in \mathbb{Z}$. By (2.1.2) and (2.1.6), we get that the main part of the error $\dot{\mathcal{R}}$ can be expressed as a sum of the form $\sum_{k_1=-n}^{n} \cdots \sum_{k_{s-1}=-n}^{n} f_{\mathbf{N},\tau,\mathbf{x}}(A_1^{k_1} \cdots A_{s-1}^{k_{s-1}} \boldsymbol{\theta})$. The function $f_{\mathbf{N},\tau,\mathbf{x}}$ does not comply with conditions of [Le3, Theorem 5]. Hence, we cannot apply [Le3, Theorem 5] to immediately obtain Theorem 1. Therefore, we should reprove [Le3, Theorem 5]. In [Le3, Theorem 5], we use the moment method. In this paper, we use the martingale method. But the main idea of this article is the same as in [Le3, Theorem 5] and is as follows:

In order to prove the central limit theorem, it is sufficient to calculate the upper bound of the number of solutions of the exponential Diophantine equation

$$\sum_{i=1}^{d} \beta_i \eta_1^{k_{i,1}} \cdots \eta_{s-1}^{k_{i,s-1}} = 0, \qquad k_{i,j} \in \{-n, \dots, 0, \dots, n\}, \quad \beta_i \in \mathcal{K}, \tag{1.9}$$

$i = 1, \dots, d,\ j = 1, \dots, s-1$, where $d \to \infty$ in [Le3, Theorem 5], and $d = 4$ in this paper. We apply the S-unit theorem to obtain this bound.

In Subsection 2.2, we consider a dyadic decomposition of the domain of summation $\Gamma^{\perp}$ of the Fourier series of the error $\dot{\mathcal{R}}$ in the regions $\Gamma^{\perp} \cap B_{\mathbf{k},j}$, where $B_{\mathbf{k},j} = [2^{k_1}, 2^{k_1}+1) \times \cdots \times [2^{k_{s-1}}, 2^{k_{s-1}}+1) \times [j2^{k_s}, j2^{k_s}+1)$ $\mathbf{k} \in \mathbb{Z}^s$, $k_1 + \cdots + k_s = 0$, $j \in \mathbb{Z}$. In [Le3], we used a more natural decomposition $\Gamma^{\perp} = \cup_{k_1,\dots,k_{s-1} \in \mathbb{Z}} (F_1 \cup \Gamma^{\perp}) \eta_1^{k_1} \cdots \eta_{s-1}^{k_{s-1}}$. However, the dyadic decomposition is more appropriate to construct the martingale difference area $(\big(\mathcal{A}(\dot{G}_k)\big)_{k=1}^{n}$, see (2.3.8), (2.4.1) and (2.8.1)). In addition, this allows us to compute the volume of the most important domains of the lattice $\Gamma^{\perp}$, such as $B_{\mathbf{k},j} \cap \{\boldsymbol{\gamma} \in \Gamma^{\perp} \mid \mathrm{Nm}(\boldsymbol{\gamma}) \le n^{1/2}\}$.

In Subsection 2.3, we cite two famous Diophantine results—the S-unit theorem [ESS] (see Theorem A) and lower bounds for linear forms in logarithms of algebraic numbers see [BW, Theorem B] We decompose the domain of summation $\Gamma^{\perp}$ to five parts: $\Gamma^{\perp} = G_1 \cup \cdots \cup G_5$. Next we apply Theorem B to the main part G_1.

In Subsection 2.4, we find upper bounds on the variance of the error $\dot{\mathcal{R}}$ ($\dot{\mathcal{R}} = \mathcal{A}(G_1) + \cdots + \mathcal{A}(G_5)$). It is clear that it is sufficient to compute separately the variance of $\mathcal{A}(G_i)$, $i = 1, \dots, 5$ (see Lemma 7 – Lemma 10).

In Subsection 2.5, we obtain (in Lemma 13) lower bounds on the variance of $\dot{\mathcal{R}}$. Lemma 13 is a simple consequence of Lemma 12. The proof of Lemma 12 is based on the admissibility property of the lattice $\Gamma^{\perp}$ and on Minkowski's convex body theorem.

In Subsections 2.6 and 2.7, we use the S-unit theorem to compute

$$\sum_{i=1}^{n} E\big[\mathcal{A}^4(\dot{G}_i)\big] \quad \text{and} \quad \sum_{i=1}^{n} E\big[\mathcal{A}^2\big(\dot{G}_i\big) - E\big(\mathcal{A}^2(\dot{G}_i)\big)\big]^2.$$

In Subsection 2.8, we prove the martingale property of the sequence

$$\big(\mathcal{A}(\dot{G}_i)\big)_{i\geq 1}.$$

Using Theorem C, we prove CLT for the main part $\mathbb{S}_n$ of $\dot{\mathcal{R}}$.

In Subsection 2.9, we prove that the difference $\dot{\mathcal{R}} - \mathbb{S}_n$ is very small, and Theorem 1 follows.

2. Proofs of theorems

We will prove Theorem 1 by using the martingale CLT [Mo] (see Theorem C). First we will find the upper and lower bounds of the variance of the error $\dot{\mathcal{R}}$. Next we approximate $\dot{\mathcal{R}}$ by a martingale difference area $\dot{\mathcal{R}} = \mathcal{A}(\dot{G}_1)+\cdots+\mathcal{A}(\dot{G}_n)$.

According to Theorem C, in order to prove the CLT, it is sufficient to show that $\mathbb{W}_n + \mathbb{A}_n = o(1)$ for $n \to \infty$. By Lemma 19, it is sufficient to calculate the upper bound of $E[\mathcal{A}^4(\dot{G}_i)]$ (resp. $E\big[\mathcal{A}^2(\dot{G}_i) - E\big(\mathcal{A}^2(\dot{G}_i)\big)\big]^2$) to get $\mathbb{W}_n$, see (2.8.13) (resp. $\mathbb{A}_n$, see (2.8.16) and (2.8.20)). We calculate $E[\mathcal{A}^4(\dot{G}_i)]$ in Lemma 14 and $E\big[\mathcal{A}^2(\dot{G}_i) - E\big(\mathcal{A}^2(\dot{G}_i)\big)\big]^2$ in Lemma 16.

The main part of evidence in both of these lemmas is to estimate the number of solutions of an exponential Diophantine equation similar to (1.9) (see (2.6.7), (2.7.1) and (2.7.7)). We get these estimates by using the S-unit theorem.

2.1. Poisson summation formula

We shall need the Poisson summation formula:

$$\det\Gamma \sum_{\boldsymbol{\gamma}\in\Gamma} f(\boldsymbol{\gamma} - X) = \sum_{\boldsymbol{\gamma}\in\Gamma^{\perp}} \widehat{f}(\boldsymbol{\gamma}) e(\langle\boldsymbol{\gamma}, \mathbf{x}\rangle), \tag{2.1.1}$$

where

$$\widehat{f}(Y) = \int_{\mathbb{R}^s} f(X) e(\langle\mathbf{y}, \mathbf{x}\rangle)\, \mathrm{d}\mathbf{x}$$

is the Fourier transform of $f(X)$, and

$$e(x) = exp(2\pi\sqrt{-1}x), \langle\mathbf{y}, \mathbf{x}\rangle = y_1x_1 + \cdots + y_sx_s.$$

Formula (2.1.1) holds for functions $f(\mathbf{x})$ with period lattice Γ if one of the functions f or $\widehat{f}$ is integrable and belongs to class C^{∞} (see, e.g., [SW, p. 251]).

Let $\mathbf{d} = (d_1, \dots, d_s)$, $d_i \geq 0$ $(i = 1, \dots, s)$, $\mathcal{O}_{\mathbf{d}} = [-d_1/2, d_1/2] \times \cdots \cdots \times [-d_s/2, d_s/2]$, and let $\widehat{\mathbb{1}}_{\mathcal{O}_{\mathbf{d}}}(\boldsymbol{\gamma})$ be the Fourier transform of the indicator function $\mathbb{1}_{\mathcal{O}_{\mathbf{d}}}(\boldsymbol{\gamma})$. It is easy to prove that $\widehat{\mathbb{1}}_{\mathcal{O}_{\mathbf{d}}}(\mathbf{0}) = d_1 d_2 \cdots d_s$ and

$$\widehat{\mathbb{1}}_{\mathcal{O}_{\mathbf{d}}}(\boldsymbol{\gamma}) = \prod_{i=1}^{s} \frac{e(d_i\gamma_i/2) - e(-d_i\gamma_i/2)}{2\pi\sqrt{-1}\gamma_i} = \prod_{i=1}^{s} \frac{\sin(\pi d_i \gamma_i)}{\pi\gamma_i} \tag{2.1.2}$$

for $\mathrm{Nm}(\boldsymbol{\gamma}) \neq 0$. We fix a nonnegative function $\omega(\mathbf{x})$, $\mathbf{x} \in \mathbb{R}^s$, of the class C^∞, with a support inside the unit ball $|\mathbf{x}| \leq 1$, such that

$$\int_{\mathbb{R}^s} \omega(\mathbf{x})\, \mathrm{d}\mathbf{x} = 1. \tag{2.1.3}$$

We set $\omega_\tau(\mathbf{x}) = \tau^{-s}\omega(\tau^{-1}\mathbf{x})$, $\tau > 0$, and

$$\hat{\omega}(\mathbf{y}) = \int_{\mathbb{R}^s} e(\langle \mathbf{y}, \mathbf{x}\rangle)\omega(\mathbf{x})\, \mathrm{d}\mathbf{x}. \tag{2.1.4}$$

Notice that the Fourier transform $\hat{\omega_\tau}(\mathbf{y}) = \hat{\omega}(\tau\mathbf{y})$ of the function $\omega_\tau(\mathbf{y})$ satisfies the bound

$$|\hat{\omega_\tau}(\mathbf{y})| < c_2(1 + \tau|\mathbf{y}|)^{-2s}. \tag{2.1.5}$$

Lemma 1. *There exists a constant $c > 0$, such that we have for $N > c$*

$$|\mathcal{R}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) - \ddot{\mathcal{R}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma)| \leq 2^s,$$

where

$$\ddot{\mathcal{R}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) = \frac{1}{\det\Gamma} \sum_{\boldsymbol{\gamma}\in\Gamma^\perp\setminus\mathbf{0}} \widehat{\mathbb{1}}_{\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}}}(\gamma)\widehat{\omega}(\tau\gamma)e(\langle\gamma, \mathbf{x}\rangle), \quad \tau = N^{-2}. \tag{2.1.6}$$

Proof. Let $\mathcal{O}^{\pm\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} = [0, \max(0, \theta_1 N_1 \pm \tau)) \times \cdots \times [0, \max(0, \theta_s N_s \pm \tau))$, and let $\mathbb{1}_{\mathcal{O}}(x)$ be the indicator function of $\mathcal{O}$. We consider the convolutions of the functions $\mathbb{1}_{\mathcal{O}^{\pm\tau}_{\mathbf{N}}}(\boldsymbol{\gamma})$ and $\omega_\tau(\mathbf{y})$:

$$\omega_\tau * \mathbb{1}_{\mathcal{O}^{\pm\tau}_{\mathbf{N}}}(\mathbf{x}) = \int_{\mathbb{R}^s} \omega_\tau(\mathbf{x} - \mathbf{y})\mathbb{1}_{\mathcal{O}^{\pm\tau}_{\mathbf{N}}}(\mathbf{y})\, \mathrm{d}\mathbf{y}. \tag{2.1.7}$$

It is obvious that the nonnegative functions (2.1.7) are of class C^∞ and are compactly supported in τ-neighborhoods of the bodies $\mathcal{O}^{\pm\tau}_{\mathbf{N}}$, respectively. We obtain

$$\mathbb{1}_{\mathcal{O}^{-\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}}}(\mathbf{x}) \leq \mathbb{1}_{\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}}}(\mathbf{x}) \leq \mathbb{1}_{\mathcal{O}^{+\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}}}(\mathbf{x}), \qquad \mathbb{1}_{\mathcal{O}^{-\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}}}(\mathbf{x}) \leq \omega_\tau * \mathbb{1}_{\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}}}(\mathbf{x}) \leq \mathbb{1}_{\mathcal{O}^{+\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}}}(\mathbf{x}). \tag{2.1.8}$$

Replacing $\mathbf{x}$ by $\boldsymbol{\gamma} - \mathbf{x}$ in (2.1.8) and summing these inequalities over $\boldsymbol{\gamma} \in \Gamma = \Gamma_M$, we find from (1.1), that

$$\mathcal{N}(\mathcal{O}^{-\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) \leq \mathcal{N}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) \leq \mathcal{N}(\mathcal{O}^{+\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma),$$

and

$$\mathcal{N}(\mathcal{O}^{-\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) \le \dot{\mathcal{N}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) \le \mathcal{N}(\mathcal{O}^{+\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma),$$

where

$$\dot{\mathcal{N}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) = \sum_{\boldsymbol{\gamma}\in\Gamma} \omega_\tau * \mathbb{1}_{\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}}}(\boldsymbol{\gamma} - \mathbf{x}). \tag{2.1.9}$$

Hence

$$\begin{aligned} -\mathcal{N}(\mathcal{O}^{+\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) + \mathcal{N}(\mathcal{O}^{-\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) &\le \dot{\mathcal{N}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) - \mathcal{N}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) \\ &\le \mathcal{N}(\mathcal{O}^{+\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) - \mathcal{N}(\mathcal{O}^{-\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma). \end{aligned}$$

Thus

$$\left|\mathcal{N}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) - \dot{\mathcal{N}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma)\right| \le \mathcal{N}(\mathcal{O}^{+\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) - \mathcal{N}(\mathcal{O}^{-\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma). \tag{2.1.10}$$

Consider the right side of this inequality. We have that $\mathcal{O}^{+\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}} \setminus \mathcal{O}^{-\tau}_{\boldsymbol{\theta}\cdot\mathbf{N}}$ is the union of boxes $\mathcal{O}^{(i)}$, $i = 1, \dots, 2^s - 1$, where

$$\begin{aligned} \mathrm{vol}(\mathcal{O}^{(i)}) \le \mathrm{vol}(\mathcal{O}^{+\tau}_{\mathbf{N}}) - \mathrm{vol}(\mathcal{O}^{-\tau}_{\mathbf{N}}) &\le \prod_{i=1}^{s}(N_i + \tau) - \prod_{i=1}^{s}(N_i - \tau) \\ &\le N\left(\prod_{i=1}^{s}(1+\tau) - \prod_{i=1}^{s}(1-\tau)\right) < \ddot{c}_s N\tau = \ddot{c}_s/N, \qquad \tau = N^{-2}, \end{aligned}$$

with some $\ddot{c}_s > 0$. From (1.4), we get $|\mathrm{Nm}(\boldsymbol{\gamma})| \ge C_M^s$ for $\boldsymbol{\gamma} \in \Gamma_M \setminus \mathbf{0}$. We see

$|\mathrm{Nm}(\boldsymbol{\gamma}_1 - \boldsymbol{\gamma}_2)| \le \mathrm{vol}(\mathcal{O}^{(i)} + \mathbf{x}) < C_M^s$ for $\boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2 \in \mathcal{O}^{(i)} + \mathbf{x}$ and $N > \ddot{c}_s / C_M^s$. Therefore, the box $\mathcal{O}^{(i)} + \mathbf{x}$ contains at most one point of Γ_M for $N > \ddot{c}/C_M^s$. By (2.1.10), we obtain

$$|\dot{\mathcal{N}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) - \mathcal{N}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma)| \le 2^s - 1, \quad \text{for} \quad N > \ddot{c}/C_M^s. \tag{2.1.11}$$

Let

$$\dot{\mathcal{R}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) = \dot{\mathcal{N}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) - \frac{\mathrm{vol}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}})}{\det \Gamma}. \tag{2.1.12}$$

By (2.1.9), we have that $\dot{\mathcal{N}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma)$ is a periodic function of $\mathbf{x} \in \mathbb{R}^n$ with the period lattice Γ. Applying the Poisson summation formula to the series (2.1.9), and bearing in mind that $\widehat{\omega}_\tau(\mathbf{y}) = \widehat{\omega}(\tau\mathbf{y})$, we obtain from (2.1.6)

$$\dot{\mathcal{R}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma) = \ddot{\mathcal{R}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x}, \Gamma).$$

Note that (2.1.5) ensures the absolute convergence of the series (2.1.6) over $\boldsymbol{\gamma} \in \Gamma^\perp \setminus \{0\}$. Using (1.2), (2.1.11) and (2.1.12), we get the assertion of Lemma 1. $\square$

2.2. Dyadic decomposition

Let $\mathfrak{D}_M$ be the ring of coefficients of the full module M, $\mathfrak{U}_M$ be the group of units of $\mathfrak{D}_M$, $M_1 = M$, $M_2 = M^{\perp}$, and let $\eta_{k,1}, \dots, \eta_{k,s-1}$ be the set of fundamental units of $\mathfrak{U}_{M_k}$ $(k = 1, 2)$. According to the Dirichlet's theorem (see, e.g., [BS, p. 112]), every unit $\eta \in \mathfrak{U}_{M_k}$ has a unique representation in the form

$$\eta = (-1)^a \eta_{k,1}^{a_1} \cdots \eta_{k,s-1}^{a_{s-1}}, \qquad k = 1, 2, \tag{2.2.1}$$

where $a_1, \dots a_{s-1}$ are rational integers and $a \in \{0, 1\}$. We will denote $\sigma(\mathfrak{U}_{M_k})$ by the same symbol $\mathfrak{U}_{M_k}$.

Lemma 2. *Let $y_1, \dots, y_s > 0$ be reals, $\mathbf{y} = (y_1, \dots, y_s)$, $y = \mathrm{Nm}(\mathbf{y}) = y_1 y_2 \cdots y_s$. Then there exists $\eta_k(\boldsymbol{y}) \in \mathfrak{U}_{M_k}$ with*

$$y_i y^{-1/s} |\sigma_i(\eta_k(\boldsymbol{y}))| \in [1/c_0, c_0], \tag{2.2.2}$$

where $i = 1, \dots, s,\ k = 1, 2,$ and

$$c_0 = \exp\left(\sum_{k=1,2} \sum_{1 \le i,j < s} |\ln |\sigma_i(\eta_{k,j})|| \right) > 1. \tag{2.2.3}$$

P r o o f. We fix $k \in \{1, 2\}$. The matrix $(\ln |\sigma_i(\eta_{k,j})|)_{1 \le i,j < s}$ is non singular [BS, pp. 104, 115]. Hence, there exist reals $b_1, \dots, b_{s-1}$ with

$$\sum_{1 \le j < s} b_j \ln |\sigma_i(\eta_{k,j})| = 1/s \ln y - \ln y_i, \qquad i = 1, \dots, s-1.$$

Taking $a_j = [b_j],\ j = 1, \dots, s-1$ and $\eta_k(\boldsymbol{y}) = \eta_{k,1}^{a_1} \cdots \eta_{k,s-1}^{a_{s-1}}$, we obtain for $i \in [1, s-1]$,

$$-\sum_{1 \le j < s} |\ln |\sigma_i(\eta_{k,j})|| \le \ln(y_i y^{-1/s} |\sigma_i(\eta_k(\boldsymbol{y}))|) \le \sum_{1 \le j < s} |\ln |\sigma_i(\eta_{k,j})||. \tag{2.2.4}$$

Hence

$$-\ln c_0 \le \ln\big(y_i y^{-1/s} |\sigma_i(\eta_k(\mathbf{y}))|\big) \le \ln c_0, \quad i = 1, \dots, s-1, \ \ k = 1, 2.$$

Bearing in mind that $|\mathrm{Nm}(\eta_k(\mathbf{y}))| = 1$ and $y = y_1 y_2 \cdots y_s$, we get from (2.2.4) and (2.2.3)

$$\ln\big(y_s y^{-1/s} |\sigma_s(\eta_k(\boldsymbol{y}))|\big) = -\sum_{1 \le i < s} \ln\big(y_i y^{-1/s} |\sigma_i(\eta_k(\boldsymbol{y}))|\big) \in [-\ln c_0, \ln c_0].$$

Therefore, the assertion (2.2.2) is true for $i \in [1, s],\ k = 1, 2$, and Lemma 2 is proved. $\square$

We apply this lemma to the vector $\mathbf{y} = \mathbf{N} = (N_1, \dots, N_s)$. Let $N_i^{'} = N_i|\sigma_i(\eta_1(\mathbf{N}))|$, $i = 1, \dots, s$, and let $\sigma(\eta_1(\mathbf{N})) = (\sigma_1(\eta_1(\mathbf{N})), \dots, \sigma_s(\eta_1(\mathbf{N})))$. We see that

$$\boldsymbol{\gamma} \in \Gamma_M \cap (\boldsymbol{\theta} \cdot \mathbf{N} \cdot \mathbb{K}^s + \mathbf{x}) \Leftrightarrow \boldsymbol{\gamma} \cdot \sigma(\eta_1(\mathbf{N})) \in \Gamma_M \cap \Big(\boldsymbol{\theta} \cdot \mathbf{N}^{'} \cdot \mathbb{K}^s + \mathbf{x} \cdot \sigma\big(\eta_1(\mathbf{N})\big)\Big).$$

Hence

$$\mathcal{N}(\boldsymbol{\theta} \cdot \mathbf{N} \cdot \mathbb{K}^s + \mathbf{x}, \Gamma_M) = \mathcal{N}\Big(\boldsymbol{\theta} \cdot \mathbf{N}' \cdot \mathbb{K}^s + \mathbf{x} \cdot \sigma\big(\eta_1(\mathbf{N})\big), \Gamma_M\Big).$$

By (1.2), we have

$$\mathcal{R}(\boldsymbol{\theta} \cdot \mathbf{N} \cdot \mathbb{K}^s + \mathbf{x}, \Gamma_M) = \mathcal{R}\Big(\boldsymbol{\theta} \cdot \mathbf{N}' \cdot \mathbb{K}^s + \mathbf{x} \cdot \sigma\big(\eta_1(\mathbf{N})\big), \Gamma_M\Big).$$

Therefore, without loss of generality, we can assume that

$$N_i N^{-1/s} \in [1/c_0, c_0], \quad i = 1, \dots, s. \tag{2.2.5}$$

Now, let $n = [\log_2 N] + 1$,

$$\mathbb{F}_n^{'} = \Big\{\boldsymbol{\gamma} \in \Gamma^{\perp} \setminus \{0\} : |\gamma_i||\mathrm{Nm}(\boldsymbol{\gamma})|^{-1/s} \in [1/c_0, c_0],\ i = 1, \dots, s,\ |\mathrm{Nm}(\boldsymbol{\gamma})| \leq n^{1/2}\Big\}$$

and

$$\mathbb{F}_n = \bigcup_{\boldsymbol{\gamma} \in \mathbb{F}_n^{'}} \Big\{\boldsymbol{\gamma}^{'} \in \mathbb{F}_n^{'} \ : \ \gamma_1^{'} = \max_{\eta \in \mathfrak{U}_{M^{\perp}},\ \boldsymbol{\gamma} \cdot \sigma(\eta) \in \mathbb{F}_n^{'}} (\boldsymbol{\gamma} \cdot \sigma(\eta))_1\Big\}. \tag{2.2.6}$$

By (1.4), we get that

$$\text{if} \quad \boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)} \in \mathbb{F}_n,\ \boldsymbol{\gamma}^{(1)} \neq \boldsymbol{\gamma}^{(2)}, \quad \text{then} \quad \boldsymbol{\gamma}^{(1)} \neq \boldsymbol{\gamma}^{(2)} \cdot \sigma(\eta) \quad \forall \eta \in \mathfrak{U}_{M^{\perp}}. \tag{2.2.7}$$

Lemma 3. *Let $a, b \geq 1$ be integers,*

$$\mathbb{G}(a,b) = \Big\{\boldsymbol{\gamma} \in \Gamma^{\perp} \setminus \{0\} \ : \ \max_{1 \leq i \leq s} |\gamma_i| \in (2^a, 2^{a+b}], \quad |\mathrm{Nm}(\boldsymbol{\gamma})| \leq n^{1/2}\Big\}, \tag{2.2.8}$$

$$\mathbb{G}^{'}(a,b) := \bigcup_{\boldsymbol{\gamma} \in \mathbb{F}_n} \bigcup_{\eta \in \mathfrak{U}(\boldsymbol{\gamma}, a, b)} \boldsymbol{\gamma} \cdot \sigma(\eta), \tag{2.2.9}$$

with

$$\dot{\mathfrak{U}}(\boldsymbol{\gamma}^{(0)}, a, b) = \Big\{\eta \in \mathfrak{U}_{M^{\perp}} \ : \ \boldsymbol{\gamma}^{(0)} \cdot \sigma(\eta) \in \mathbb{G}(a,b)\Big\}. \tag{2.2.10}$$

Then

$$\mathbb{G}(a,b) = \mathbb{G}^{'}(a,b), \quad \#\dot{\mathfrak{U}}(\boldsymbol{\gamma}^{(0)}, a, b) = O\big(b(a+b)^{s-2}\big) \ \text{ for } \ \boldsymbol{\gamma}^{(0)} \in \mathbb{F}_n, \tag{2.2.11}$$

$$\#\mathbb{G}(a,b) = O\big(n^{1/2} b (a+b)^{s-2}\big),$$

$$\sum_{\boldsymbol{\gamma} \in \mathbb{F}_n} \frac{1}{|\mathrm{Nm}(\boldsymbol{\gamma})|} = O(\ln n) \qquad \text{and} \qquad \sum_{\boldsymbol{\gamma} \in \mathbb{F}_n} \frac{1}{\mathrm{Nm}^2(\boldsymbol{\gamma})} = O(1). \tag{2.2.12}$$

P r o o f. It is easy to see that $\mathbb{G}(a,b) \supseteq \mathbb{G}^{'}(a,b)$. Let $\boldsymbol{\gamma} \in \mathbb{G}(a,b)$. By Lemma 2, there exists $\eta \in \mathfrak{U}_{M^\perp}$ with $\boldsymbol{\gamma} \cdot \sigma(\eta) \in \mathbb{F}_n^{'}$. From (2.2.6), we obtain that there exists $\eta_1 \in \mathfrak{U}_{M^\perp}$ with $\boldsymbol{\gamma}^{(1)} = \boldsymbol{\gamma} \cdot \sigma(\eta\eta_1) \in \mathbb{F}_n$. By (2.2.9) and (2.2.10), we get that $\boldsymbol{\gamma} = \boldsymbol{\gamma}^{(1)}\sigma((\eta\eta_1)^{-1}) \in \mathbb{G}^{'}(a,b)$ and $\mathbb{G}(a,b) = \mathbb{G}^{'}(a,b)$. Let $\mathbf{m} = (m_1,\dots,m_s) \in \mathbb{Z}^s$, $m_1 + \cdots + m_s = 0$, $\boldsymbol{\kappa} = (\kappa_1,\dots,\kappa_s)$, $\kappa_i \in \{-1,1\} (i = 1,\dots,s)$, $\nu(\mu) = s$ if $\mu \neq s$, $\nu(\mu) = 1$ if $\mu = s$, $j \geq 0$ and

$$B(\mathbf{m},\mu,\boldsymbol{\kappa},j) = \prod_{1\leq i<\nu(\mu)} \big(\kappa_i 2^{m_i},\ \kappa_i 2^{m_i+1}\big] \times \big(j\kappa_{\nu(\mu)}2^{-m_{\nu(\mu)}}C_M^s,\ (j+1)\kappa_{\nu(\mu)}2^{-m_{\nu(\mu)}}C_M^s\big] \prod_{\nu(\mu)<i\leq s} \big(\kappa_i 2^{m_i}, \kappa_i 2^{m_i+1}\big]. \quad (2.2.13)$$

It is easy to see that

$$B(\mathbf{m}_1,\mu,\boldsymbol{\kappa}_1,j_1) \cap B(\mathbf{m}_2,\mu,\boldsymbol{\kappa}_2,j_2) = \emptyset \quad \text{for} \quad (\mathbf{m}_1,\mu,\boldsymbol{\kappa}_1,j_1) \neq (\mathbf{m}_2,\mu,\boldsymbol{\kappa}_2,j_2). \quad (2.2.14)$$

Applying (1.4), we have for every $\mu \in [1,s]$ that

$$\Gamma^\perp \setminus \{0\} = \bigcup_{\kappa_1,\dots,\kappa_s\in\{-1,1\}} \ \bigcup_{\substack{\mathbf{m}\in\mathbb{Z}^s,\\ m_1+\cdots+m_s=0}} \ \bigcup_{j\geq 0} \ \bigcup_{\boldsymbol{\gamma}\in B(\mathbf{m},\mu,\boldsymbol{\kappa},j)} \boldsymbol{\gamma}. \quad (2.2.15)$$

Let

$$\boldsymbol{\gamma}^{(1)},\ \boldsymbol{\gamma}^{(2)} \in \Gamma^\perp \cap B(\mathbf{m},\mu,\boldsymbol{\kappa},j).$$

From (2.2.13), we see that

$$|\mathrm{Nm}(\boldsymbol{\gamma}^{(1)} - \boldsymbol{\gamma}^{(2)})| < C_M^s.$$

By (1.4), we obtain that $\boldsymbol{\gamma}^{(1)} = \boldsymbol{\gamma}^{(2)}$ and

$$\#\Gamma^\perp \cap B(\mathbf{m},\mu,\boldsymbol{\kappa},j) \leq 1. \quad (2.2.16)$$

Suppose

$$\eta \in \mathfrak{U}_{M^\perp} \cap B(\mathbf{m},\mu,\boldsymbol{\kappa},j).$$

Using (2.2.13), we have that

$$1 = |\mathrm{Nm}(\eta)| = (j+z_1)C_M^s 2^{z_2(s-1)} \qquad \text{with} \qquad z_1,z_2 \in [0,1]. \quad (2.2.17)$$

Hence

$$-1 + 2^{1-s}/C_M^s \leq j \leq 1/C_M^s.$$

Applying (2.2.16), we get

$$\sum_{j\geq 0} \#\mathfrak{U}_{M^\perp} \cap B(m,\mu,\boldsymbol{\kappa},j) \leq 2 + 1/C_M^s. \quad (2.2.18)$$

We denote $\sigma^{-1}(B(m,\mu,\boldsymbol{\kappa},j))$ and $\sigma^{-1}(\dot{\mathfrak{U}}(\boldsymbol{\gamma}^{(0)},a,b))$ by the same symbols $B(m,\mu,\boldsymbol{\kappa},j)$ and $\dot{\mathfrak{U}}(\boldsymbol{\gamma}^{(0)},a,b)$. Now let

$$\ddot{\mathfrak{U}}_\mu(\boldsymbol{\gamma}^{(0)},a,b)=\Big\{\boldsymbol{\gamma}\in\dot{\mathfrak{U}}(\boldsymbol{\gamma}^{(0)},a,b)\ \ :\ \ |\gamma_i|\le|\gamma^{(0)}_\mu|,\quad i=1,\dots,s\Big\}.$$

It is easy to see that

$$\dot{\mathfrak{U}}(\boldsymbol{\gamma}^{(0)},a,b)=\bigcup_{\mu\in[1,s]}\ddot{\mathfrak{U}}_\mu(\boldsymbol{\gamma}^{(0)},a,b). \tag{2.2.19}$$

Let

$$\eta\in\ddot{\mathfrak{U}}_\mu(\boldsymbol{\gamma}^{(0)},a,b)\cap B(m,\mu,\boldsymbol{\kappa},j). \tag{2.2.20}$$

Denote $m_i\in\mathbb{Z}$ $(i=1,\dots,s)$ from the following condition:

$$\log_2|\sigma(\eta)_i|=m_i+z_i\qquad\text{with}\qquad z_i\in[0,1). \tag{2.2.21}$$

By (2.2.8) and (2.2.20), we obtain

$$\log_2|(\boldsymbol{\gamma}^{(0)}\sigma(\eta))_\mu|=\log_2|\gamma^{(0)}_\mu|+m_\mu+z_\mu\in(a,a+b],$$

and

$$m_\mu\in J_1:=\big(a-1-\log_2|\gamma^{(0)}_\mu|,a+b-\log_2|\gamma^{(0)}_\mu|\big]\cap\mathbb{Z}\quad\text{with}\quad\#J_1\le b+2. \tag{2.2.22}$$

From (2.2.8), (2.2.20) and (1.4), we get

$$\log_2|\gamma^{(0)}_i\sigma(\eta)_i|=\log_2|\gamma^{(0)}_i|+m_i+z_i\le a+b\qquad\text{and}\qquad m_i\le a+b-\log_2|\gamma^{(0)}_i|. \tag{2.2.23}$$

Using (2.2.23), (2.2.21) and (2.2.21), we derive that

$$\begin{aligned}\log_2|\gamma^{(0)}_i\sigma(\eta)_i|&=\log_2|\gamma^{(0)}_i|\ -\sum_{j\in[1,s],j\ne i}\log_2|\sigma(\eta)_i|\\&\ge\log_2|\gamma^{(0)}_i|\ -\sum_{j\in[1,s],j\ne i}(m_j+1)\\&\ge\sum_{j\in[1,s]}\log_2|\gamma^{(0)}_j|-(s-1)(a+b+1)\\&=-(s-1)(a+b+1)+\log_2|\mathrm{Nm}(\boldsymbol{\gamma}^{(0)})|\\&\ge-(s-1)(a+b+1)+\log_2 C_M^s.\end{aligned}$$

By (2.2.23), we have $m_i\in[\log_2|\gamma^{(0)}_i\sigma(\eta)_i|-\log_2|\gamma^{(0)}_i|-1,a+b-\log_2|\gamma^{(0)}_i|]$. Hence

$$m_i\in J_2:=\big[-1-(s-1)(a+b+1)+s\log_2 C_M\\ -\log_2|\gamma^{(0)}_i|,a+b-\log_2|\gamma^{(0)}_i|\big],$$

with $\#J_2\le s(a+b+1)+2+s|\log_2 C_M|$.

We fix $\mu \in [1,s]$ and we consider (2.2.15). For given $m_1,\dots,m_{\nu(\mu)-1}$, $m_{\nu(\mu)+1}, \dots, m_s$, we take $m_{\nu(\mu)} = -\sum_{i\in[1,s],i\neq\nu(\mu)} m_i$. By (2.2.15), we get

$$\#\ddot{\mathfrak{U}}_\mu(\boldsymbol{\gamma}^{(0)},a,b) \leq \sum_{\kappa_1,\dots,\kappa_s\in\{-1,1\}} \sum_{m_\mu\in J_1} \sum_{\substack{m_i\in J_2 \\ i\neq\mu,\nu(\mu)}} \sum_{j\geq 0} \#\big(\dot{\mathfrak{U}}(\boldsymbol{\gamma}^{(0)},a,b)\cap B(m,\mu,\boldsymbol{\kappa},j)\big).$$

Bearing in mind (2.2.18), (2.2.19) and (2.2.22), we obtain

$$\#\dot{\mathfrak{U}}(\boldsymbol{\gamma}^{(0)},a,b) = O\big(\#J_1(\#J_2)^{s-2}\big) = O\big(b(a+b)^{s-2}\big). \tag{2.2.24}$$

Hence, the assertion (2.2.11) is proved.

Let $F_1 \subset \mathbb{R}^s$ be a fundamental domain for the field $\mathcal{K}$, and let

$$F_2 = \{\boldsymbol{\gamma}\in\Gamma^\perp\setminus\{0\} \;:\; |\gamma_i||\mathrm{Nm}(\boldsymbol{\gamma})|^{-1/s}\in[1/c_0,c_0],\;\; i=1,\dots,s\} \quad \text{(see (2.2.2))}.$$

By [BS, pp. 312, 322], the points of F_1 can be arranged in a sequence $\dot{\boldsymbol{\gamma}}^{(k)}$ so that $0 < |\mathrm{Nm}(\dot{\boldsymbol{\gamma}}^{(1)})| \leq |\mathrm{Nm}(\dot{\boldsymbol{\gamma}}^{(2)})| \leq \cdots$ and $c^{(1)}k \leq |\mathrm{Nm}(\dot{\boldsymbol{\gamma}}^{(k)})| \leq c^{(2)}k$, $k=1,2,\dots$ for some $c^{(2)} > c^{(1)} > 0$. Therefore, the points of F_2 can be arranged in a sequence $\boldsymbol{\gamma}^{(k)}$ so that

$$0 < |\mathrm{Nm}(\boldsymbol{\gamma}^{(1)})| \leq |\mathrm{Nm}(\boldsymbol{\gamma}^{(2)})| \leq \cdots$$

and

$$c^{(3)}k \leq |\mathrm{Nm}(\boldsymbol{\gamma}^{(k)})| \leq c^{(4)}k, \quad k=1,2,\dots \quad \text{for some} \quad c^{(4)} > c^{(3)} > 0.$$

Using (2.2.6), we have that

$$\sum_{\boldsymbol{\gamma}\in\mathbb{F}_n} 1/|\mathrm{Nm}(\boldsymbol{\gamma})| = O(\ln(n)), \quad \sum_{\boldsymbol{\gamma}\in\mathbb{F}_n} 1/\mathrm{Nm}^2(\boldsymbol{\gamma}) = O(1), \quad \text{and} \quad \#\mathbb{F}_n = O(n^{1/2}).$$

By (2.2.9) and (2.2.24), we obtain

$$\#\mathbb{G}(a,b) \leq \sum_{\boldsymbol{\gamma}^{(0)}\in\mathbb{F}_n} \#\dot{\mathfrak{U}}(\boldsymbol{\gamma}^{(0)},a,b) = O\big(n^{1/2}b(a+b)^{s-2}\big).$$

Hence, Lemma 3 is proved. □

2.3. Diophantine inequalities

We consider the following simple variant of the ***S-unit theorem*** (see [ESS, Theorem 1.1, p. 808]): Let $\beta_1,\dots,\beta_d\in\mathcal{K}$, $\beta_i\neq 0$, $i=1,\dots,d$, $\deg(\mathcal{K})=s$. We consider the equation

$$\beta_1\eta_1+\cdots+\beta_d\eta_d = 1 \quad \text{with} \quad \boldsymbol{\eta}=(\eta_1,\dots,\eta_d)\in(\mathfrak{U}_{M^\perp})^d. \tag{2.3.1}$$

A solution $\boldsymbol{\eta}$ of (2.3.1) is called ***non-degenerate*** if $\sum_{i\in I}\beta_i\eta_i\neq 0$ for every nonempty subset I of $\{1,\dots,d\}$.

Theorem A. *The number $A(\beta_1, \dots, \beta_d)$ of non-degenerate solutions $\boldsymbol{\eta} \in (\mathfrak{U}_{M^\perp})^d$ of equation* (2.3.1) *satisfies the estimate*

$$A(\beta_1, \dots, \beta_d) \leq \exp\big((6d)^{3d} s\big). \tag{2.3.2}$$

Linear forms in logarithms. Write Λ for the linear form in logarithms,

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_k \log \alpha_k,$$

where $b_1, \dots, b_k$ are integers, $|b_i| \leq B$ $(i = 1, \dots, k)$, $B \geq e$. We shall assume that $\alpha_1, \dots, \alpha_k$ are non-zero algebraic numbers with heights at most $A_1, \dots, A_k$ (all $\geq e$), respectively.

Theorem B. [BW, Theorem 2.15, p. 42] *If $\Lambda \neq 0$, then*

$$|\Lambda| > \exp\Big(- \big(16kd\big)^{2(k+2)} \ln A_1 \cdots \ln A_k \ln B \Big), \tag{2.3.3}$$

where d denote the degrees of $\mathbb{Q}(\alpha_1, \dots, \alpha_k)$.

Let

$$G^{(1)} = \Big\{ \boldsymbol{\gamma} \in \Gamma^\perp : |\boldsymbol{\gamma}| \leq N,\ |\mathrm{Nm}(\boldsymbol{\gamma})| \leq n^{1/2} \ \text{ and } \ |N_i \gamma_i| > 2^{(\ln n)^4} \ \ \forall i \in [1, s] \Big\}, \tag{2.3.4}$$

$$G^{(2)} = \Big\{ \boldsymbol{\gamma} \in \Gamma^\perp : |\boldsymbol{\gamma}| > N^5 \Big\},$$

$$G^{(3)} = \Big\{ \boldsymbol{\gamma} \in \Gamma^\perp : |\boldsymbol{\gamma}| \leq N^5,\ |\mathrm{Nm}(\boldsymbol{\gamma})| > n^{1/2} \Big\}, \tag{2.3.5}$$

$$G^{(4)} = \Big\{ \boldsymbol{\gamma} \in \Gamma^\perp : N < |\boldsymbol{\gamma}| \leq N^5,\ |\mathrm{Nm}(\boldsymbol{\gamma})| \leq n^{1/2} \Big\} \quad \text{and}$$

$$G^{(5)} = \Big\{ \boldsymbol{\gamma} \in \Gamma^\perp \setminus \{0\} \ : |\boldsymbol{\gamma}| \leq N,\ |\mathrm{Nm}(\boldsymbol{\gamma})| \leq n^{1/2} \quad \text{and} \quad \exists i \in [1, s] \quad \text{with} \quad |N_i \gamma_i| \leq 2^{(\ln n)^4} \Big\}. \tag{2.3.6}$$

It is easy to see that $G^{(i)} \cap G^{(j)} = \emptyset$ for $i \neq j$, and

$$\Gamma^\perp \setminus \{0\} = G^{(1)} \cup G^{(2)} \cup G^{(3)} \cup G^{(4)} \cup G^{(5)}. \tag{2.3.7}$$

Let

$$\dot{G}_0 = \Big\{ \boldsymbol{\gamma} \in G^{(1)} \ : \ \max_{1 \leq j \leq s} |\gamma_i| \leq 2^{n^{4/9}} \Big\}, \tag{2.3.8}$$

$$\dot{G}_i = \Big\{ \boldsymbol{\gamma} \in G^{(1)} \ : \ \max_{1 \leq j \leq s} |\gamma_i| \in \Big(2^{i n^{4/9}}, 2^{(i+1) n^{4/9} - n^{2/9}} \Big] \Big\},$$

and

$$\ddot{G}_i = \Big\{ \boldsymbol{\gamma} \in G^{(1)} \ : \ \max_{1 \leq j \leq s} |\gamma_i| \in \Big(2^{(i+1) n^{4/9} - n^{2/9}}, 2^{(i+1) n^{4/9}} \Big] \Big\}, \quad i = 1, 2, \dots$$

By (2.3.4) and (2.3.8), we have that $\dot{G}_i \cap \dot{G}_j = \emptyset$ for $i \neq j$, $\dot{G}_i \cap \ddot{G}_j = \emptyset$ and

$$G^{(1)} = \dot{G}_0 \cup \bigcup_{i=1}^{[n^{5/9}]} \big(\dot{G}_i \cup \ddot{G}_i\big). \tag{2.3.9}$$

Lemma 4. *There exist $\dot{c}, \ddot{c} > 0$ such that for all $\nu \in [1, s]$ and $\kappa \in \{-1, 1\}$*

$$\min_{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)} \in G^{(1)}, \gamma_\nu^{(1)} \neq \kappa\gamma_\nu^{(2)}} N_\nu |\gamma_\nu^{(1)} - \kappa\gamma_\nu^{(2)}| \geq N_\nu |\gamma_\nu^{(2)}| \exp(-\ddot{c}(\ln n)^3) \geq \dot{c} n^{20s}.$$

P r o o f. Let $\gamma_\nu^{(1)}/\gamma_\nu^{(2)}\kappa < 0$. From (2.3.4), we obtain

$$\min_{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)} \in G^{(1)}, \gamma_\nu^{(1)} \neq \kappa\gamma_\nu^{(2)}} N_\nu |\gamma_\nu^{(1)} - \kappa\gamma_\nu^{(2)}| \geq N_\nu |\gamma_\nu^{(2)}| \geq 2^{(\ln n)^4}. \tag{2.3.10}$$

Now let $\gamma_\nu^{(1)}/\gamma_\nu^{(2)}\kappa > 0$. Taking into account that $|\exp(x) - 1| \geq |x|$ any real x, we get

$$|\gamma_\nu^{(1)} - \kappa\gamma_\nu^{(2)}| = |\gamma_\nu^{(2)}(\exp(\ln(\kappa\gamma_\nu^{(1)}/\gamma_\nu^{(2)})) - 1)| \geq |\gamma_\nu^{(2)} \ln(\kappa\gamma_\nu^{(1)}/\gamma_\nu^{(2)})|. \tag{2.3.11}$$

By (2.2.6), (2.2.8), (2.2.9) and (2.3.4), we have that there exists $(\dot{\gamma}_\nu^{(k)}, \eta_k)$ such that $\gamma_\nu^{(k)} = \dot{\gamma}_\nu^{(k)} \cdot \sigma_\nu(\eta_k)$, where $\dot{\gamma}^{(k)} \in \mathbb{F}_n$ and η_k is a unit in $\mathcal{K}$ $(k = 1, 2)$. Let $\dot{\gamma}^{(k)} = \sigma(\mathfrak{f}^{(k)})$ with some $\mathfrak{f}^{(k)} \in M^\perp$ $(k = 1, 2)$. Using (2.2.1), (2.2.6) and (2.3.4), we obtain

$$\gamma_\nu^{(k)} = \sigma_\nu(\mathfrak{f}^{(k)})(-1)^{a^{(k)}} \sigma_\nu(\eta_{2,1})^{a_1^{(k)}} \cdots\ \sigma_\nu(\eta_{2,s-1})^{a_{s-1}^{(k)}},$$
$$|\sigma_i(\mathfrak{f}^{(k)})| \leq c_0 n^{1/(2s)} \qquad \text{for} \quad i = 1, \dots, s, \tag{2.3.12}$$

and

$$\left| a_1^{(k)} \ln(\sigma_\nu(\eta_{2,1})) + \cdots + a_{s-1}^{(k)} \ln(\sigma_\nu(\eta_{2,s-1})) \right|$$
$$\leq |\ln|\gamma_\nu^{(k)}|| + |\ln|\sigma_\nu(\mathfrak{f}^{(k)})|| \leq \ln N + 1/(2s)\ln n + \ln(c_0).$$

Bearing in mind that $\det((\ln(\sigma_i(\eta_{2,j})))_{1\leq i,j\leq s-1}) \neq 0$ (see [BS, pp. 104, 115]), we get that there exists $\tilde{C}_1 > 0$ such that

$$|a_i^{(k)}| < \tilde{C}_1 n \quad \text{for} \quad i = 1, \dots, s-1, k = 1, 2 \quad \text{and} \quad n = [\log_2 N] + 1.$$

Let $\kappa_1 = \operatorname{sign}(\gamma_\nu^{(1)}/\gamma_\nu^{(2)})$, where $\operatorname{sign}(x) = 1$ for $x > 0$ and $\operatorname{sign}(x) = -1$ for $x < 0$. We see that

$$\ln|\gamma_\nu^{(1)}/\gamma_\nu^{(2)}| = \ln\big(\kappa_1\gamma_\nu^{(1)}/\gamma_\nu^{(2)}\big) = \ln\big(\kappa_1(-1)^{a^{(1)}}\sigma_\nu(\mathfrak{f}^{(1)})\big) - \ln\big((-1)^{a^{(2)}}\sigma_\nu(\mathfrak{f}^{(2)})\big)$$
$$+ (a_1^{(1)} - a_1^{(2)})\ln\big(\sigma_\nu(\eta_{2,1})\big) + \cdots + \big(a_{s-1}^{(1)} - a_{s-1}^{(2)}\big)\ln\big(\sigma_\nu(\eta_{2,s-1})\big).$$

Let $\tilde{C}_2 \max_{i\in[1,s-1]} H(\eta_{2,i})$, where $H(\alpha)$ is the height of α. By (1.4), $C_M^{-1}\mathfrak{f}^{(k)}$ is an algebraic integer ($k = 1, 2$). Thus

$$f(x) = x^s + f_{s-1}x^{s-1} + \cdots + f_0 = \big(x - \sigma_1(C_M^{-1}\mathfrak{f}^{(k)})\big)\cdots\big(x - \sigma_s(C_M^{-1}\mathfrak{f}^{(k)})\big)$$

is the characteristic polynomial of $C_M^{-1}\mathfrak{f}^{(k)}$. Hence

$$H(C_M^{-1}\mathfrak{f}^{(k)}) \leq \max_{i\in[0,s-1]} |f_i|.$$

From (2.3.12), we have that

$$H(C_M^{-1}\mathfrak{f}^{(k)}) \leq \Big(2C_M^{-1}c_0 n^{1/(2s)}\Big)^s$$

and

$$H(\mathfrak{f}^{(k)}) \leq \Big(2C_M^{-2}c_0 n^{1/(2s)}\Big)^s.$$

Applying Theorem B with $d = s$, $k = s+1$, $\alpha_1 = \kappa_1(-1)^{a^{(1)}}\sigma_\nu(\mathfrak{f}^{(1)})$, $\alpha_2 = (-1)^{a^{(2)}}\sigma_\nu(\mathfrak{f}^{(2)})$, $\alpha_3 = \sigma_\nu(\eta_{2,1})$, $\ldots$, $\alpha_{s+1} = \sigma_\nu(\eta_{2,s-1})$, $A_1 = A_2 = \big(2C_M^{-2}c_0 n^{1/(2s)}\big)^s, A_3 = \cdots = A_{s-1} = \tilde{C}_2$ and $B = 2\tilde{C}_1 n$, we obtain

$$|\ln(\kappa_1\gamma_\nu^{(1)}/\gamma_\nu^{(2)})| \geq \exp(-\ddot{c}_\nu(\ln n)^3),$$

with some $\ddot{c}_\nu > 0$. Taking into account (2.3.11) and that $N_\nu|\gamma_\nu^{(2)}| \geq 2^{(\ln n)^4}$, we have

$$\min_{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}\in G^{(1)},\gamma_\nu^{(1)}\neq\kappa\gamma_\nu^{(2)}} N_\nu|\gamma_\nu^{(1)} - \kappa\gamma_\nu^{(2)}| \geq N_\nu|\gamma_\nu^{(2)}|\exp(-\ddot{c}_\nu(\ln n)^3) \geq \dot{c}_\nu n^{20s},$$

with some $\dot{c}_\nu > 0$. Now using (2.3.10), we get the assertion of Lemma 4. □

2.4. Upper bound of the variance of $\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s + \mathbf{x}, \Gamma)$

In this subsection, we prove that $\mathcal{A}(G_1)$ is the main part of $\dot{\mathcal{R}}$. In (2.3.9), we decomposed G_1 to essential parts $(\dot{G}_i)_{i\in[1,n]}$ and to auxiliary parts $(\ddot{G}_i)_{i\in[1,n]}$. This allows us to obtain in Lemma 11 that the approximation of $\dot{\mathcal{R}}$ be the sum of essential elements $(\mathcal{A}(\dot{G}_i))$. The random variables $(\mathcal{A}(\dot{G}_i))$ are almost independents. Thus in Lemma 11 we do the main step to construct the martingale approximation for $\dot{\mathcal{R}}$.

Let

$$\mathcal{A}(G) = (\det\Gamma)^{-1}\sum_{\boldsymbol{\gamma}\in G}\widehat{\mathbb{1}}_{\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}}}(\boldsymbol{\gamma})\hat{\omega}(\tau\boldsymbol{\gamma})e(\langle\boldsymbol{\gamma},\mathbf{x}\rangle), \tag{2.4.1}$$

$$\tilde{\mathcal{A}}(G) = (\det\Gamma)^{-1}\sum_{\boldsymbol{\gamma}\in G}|\widehat{\mathbb{1}}_{\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}}}(\boldsymbol{\gamma})\hat{\omega}(\tau\boldsymbol{\gamma})|, \tag{2.4.2}$$

and let

$$\mathcal{B}(G,\boldsymbol{\kappa}) = \sum_{\boldsymbol{\gamma}\in G} \frac{(\det\Gamma)^{-1}\hat{\omega}(\tau\boldsymbol{\gamma})}{(2\pi\sqrt{-1})^s \mathrm{Nm}(\boldsymbol{\gamma})} e\Bigg(\sum_{k=1}^{s} \gamma_k(\kappa_k(\theta_k N_k)/2 + x_k)\Bigg). \tag{2.4.3}$$

We obtain from (2.1.2)

$$\mathcal{A}(G) = \sum_{\kappa_1,\dots,\kappa_s\in\{-1,1\}} \kappa_1\kappa_2\cdots\kappa_s \mathcal{B}(G,\boldsymbol{\kappa}). \tag{2.4.4}$$

Using the Cauchy–Schwartz inequality, we get

$$|\mathcal{A}(G)|^2 \le 2^s \sum_{\kappa_1,\dots,\kappa_s\in\{-1,1\}} |\mathcal{B}(G,\boldsymbol{\kappa})|^2. \tag{2.4.5}$$

By (2.3.7) and (2.1.6), we see that

$$\ddot{\mathcal{R}}(\mathcal{O}_{\boldsymbol{\theta}\cdot\mathbf{N}} + \mathbf{x},\Gamma) = \mathcal{A}(G^{(1)}) + \cdots + \mathcal{A}(G^{(5)}). \tag{2.4.6}$$

Let

$$h(\boldsymbol{\gamma}) = \frac{(\det\Gamma)^{-1}\hat{\omega}(\tau\boldsymbol{\gamma})}{(2\pi\sqrt{-1})^s \mathrm{Nm}(\boldsymbol{\gamma})} e\Bigg(\sum_{k=1}^{s} \gamma_k x_k\Bigg). \tag{2.4.7}$$

It is easy to see that

$$\mathcal{B}(G,\boldsymbol{\kappa}) = \sum_{\boldsymbol{\gamma}\in G} h(\boldsymbol{\gamma}) e\Bigg(\sum_{k=1}^{s} \kappa_k\gamma_k\theta_k N_k/2\Bigg), \tag{2.4.8}$$

and

$$\mathcal{A}(G) = \sum_{\kappa_1,\dots,\kappa_s\in\{-1,1\}} \kappa_1\kappa_2\cdots\kappa_s \sum_{\boldsymbol{\gamma}\in G} h(\boldsymbol{\gamma}) e\Bigg(\sum_{k=1}^{s} \kappa_k\gamma_k\theta_k N_k/2\Bigg). \tag{2.4.9}$$

Lemma 5. *With the notations as above*

$$\mathcal{A}(G^{(2)}) = O(1/N).$$

P r o o f. By (2.4.3) and (2.1.5) we have that

$$|\mathcal{B}(G^{(2)},\boldsymbol{\kappa})| \le c_2 \sum_{\boldsymbol{\gamma}\in G^{(2)}} \frac{(\det\Gamma)^{-1}(\tau|\boldsymbol{\gamma}|)^{-2s}}{(2\pi)^s|\mathrm{Nm}(\boldsymbol{\gamma})|}, \quad \tau = N^{-2}. \tag{2.4.10}$$

Notice that for every lattice $\mathfrak{L} \in \mathbb{R}^s$, one has the bound (see, e.g., [GL, pp. 141–142])

$$\#\{\boldsymbol{\gamma}\in\mathfrak{L} \;:\; j \le |\boldsymbol{\gamma}| \le j+1\} = O(j^{s-1}).$$

Hence

$$\sum_{\boldsymbol{\gamma}\in\Gamma^{\perp}:|\boldsymbol{\gamma}|\ge N^5} |\boldsymbol{\gamma}|^{-2s} \le \sum_{j\ge N^5} \sum_{\boldsymbol{\gamma}\in\Gamma^{\perp}:|\boldsymbol{\gamma}|\in[j,j+1)} |\boldsymbol{\gamma}|^{-2s}$$
$$= O\Bigg(\sum_{j\ge N^5} j^{-s-1}\Bigg) = O(N^{-5s}).$$

By (1.4), (2.3.5) and (2.4.10), we obtain

$$|\mathcal{B}(G^{(2)},\boldsymbol{\kappa})| \leq c_2(C_M^s \det\Gamma(2\pi)^s)^{-1} \sum_{\boldsymbol{\gamma}\in\Gamma^\perp:|\boldsymbol{\gamma}|\geq N^5} N^{4s}|\boldsymbol{\gamma}|^{-2s} = O(N^{-s}).$$

Using (2.4.4), we get the assertion of Lemma 5. □

Lemma 6. *Let* $\boldsymbol{\gamma}^{(i)} \in \Gamma^\perp,\ i = 1,2,\ \boldsymbol{\gamma}^{(1)} \neq \boldsymbol{\gamma}^{(2)}$. *Then*

$$\left|\mathbf{E}\Big[e(\langle\boldsymbol{\gamma}^{(1)} - \boldsymbol{\gamma}^{(2)}, \boldsymbol{\theta}\cdot\mathbf{N}\rangle/2+\beta)\Big]\right| \leq \frac{1}{\pi^s C_M^s N}.$$

P r o o f. Bearing in mind that

$$\left|\int_0^1 e(xz)dx\right| = \left|\frac{e(z)-1}{2\pi z}\right| \leq \frac{1}{|\pi z|}, \quad \text{with} \quad z\neq 0, \tag{2.4.11}$$

(1.4) and that $N_1\cdots N_s = N$, we have

$$\left|\mathbf{E}\left[e(\langle\boldsymbol{\gamma}^{(1)} - \boldsymbol{\gamma}^{(2)}, \boldsymbol{\theta}\cdot\mathbf{N}\rangle/2+\beta)\right]\right| \leq \frac{1}{\pi^s N|\mathrm{Nm}(\boldsymbol{\gamma}^{(1)} - \boldsymbol{\gamma}^{(2)})|} \leq \frac{1}{\pi^s C_M^s N}.$$

□

Lemma 7. *With the notations as above*

$$\mathbf{E}[|\mathcal{A}(G^{(1)})|^2] = O(n^{s-1}), \qquad \mathbf{E}[|\mathcal{A}(G^{(3)})|^2] = O(n^{s-3/2}), \tag{2.4.12}$$

and

$$|\mathcal{A}(\dot{G})| \leq \tilde{\mathcal{A}}(\dot{G}) = O(n^s), \quad \textit{with} \quad G\subseteq G^{(1)}. \tag{2.4.13}$$

P r o o f. By (2.4.3), (2.4.5) and the Cauchy–Schwartz inequality, we obtain that

$$\begin{aligned}\mathbf{E}\big[|\mathcal{A}(G)|^2\big] \leq 2^s \sum_{\kappa_1,\dots,\kappa_s\in\{-1,1\}} \Bigg(&\sum_{\boldsymbol{\gamma}\in G} \frac{(\det\Gamma)^{-2}|\hat{\omega}(\tau\boldsymbol{\gamma})|^2}{(2\pi)^{2s}|\mathrm{Nm}(\boldsymbol{\gamma})|^2} \\ &+ \sum_{\substack{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}\in G\\ \boldsymbol{\gamma}^{(1)}\neq\boldsymbol{\gamma}^{(2)}}} \frac{(\det\Gamma)^{-2}|\hat{\omega}(\tau\boldsymbol{\gamma}^{(1)})||\hat{\omega}(\tau\boldsymbol{\gamma}^{(2)})|}{(2\pi)^{2s}|\mathrm{Nm}(\boldsymbol{\gamma}^{(1)})||\mathrm{Nm}(\boldsymbol{\gamma}^{(2)})|} \\ &\times \left|\mathbf{E}\big[e(\langle\boldsymbol{\gamma}^{(1)} - \boldsymbol{\gamma}^{(2)}, \boldsymbol{\kappa}\cdot\boldsymbol{\theta}\cdot N\rangle/2+\beta)\big]\right|\Bigg)\end{aligned}$$

with $\beta = \sum_{k=1}^s \big(\gamma_k^{(1)} - \gamma_k^{(2)}\big)x_k$.

Applying Lemma 6, we get

$$\mathbf{E}[|\mathcal{A}(G)|^2] \leq \quad 2^{2s}\sum_{\mu\in[1,s]} S_{1,\mu}(G) + \frac{2^{2s}}{\pi^s C_M^s N}\, S_2(G,G) \tag{2.4.14}$$

with

$$S_{1,\mu}(G) = \sum_{\boldsymbol{\gamma}\in G, |\gamma_i|\leq|\gamma_\mu|, i=1,\dots,s} \frac{(\det\Gamma)^{-2}|\hat{\omega}(\tau\boldsymbol{\gamma})|^2}{(2\pi)^{2s}|\mathrm{Nm}(\boldsymbol{\gamma})|^2} \tag{2.4.15}$$

and

$$S_2(\dot{G},\ddot{G}) = \sum_{\boldsymbol{\gamma}^{(1)}\in\dot{G}, \boldsymbol{\gamma}^{(2)}\in\ddot{G},\ \ \boldsymbol{\gamma}^{(1)}\neq\boldsymbol{\gamma}^{(2)}} \frac{(\det\Gamma)^{-2}|\hat{\omega}(\tau\boldsymbol{\gamma}^{(1)})||\hat{\omega}(\tau\boldsymbol{\gamma}^{(2)})|}{(2\pi)^{2s}|\mathrm{Nm}(\boldsymbol{\gamma}^{(1)})||\mathrm{Nm}(\boldsymbol{\gamma}^{(2)})|}. \tag{2.4.16}$$

We fix $\mu\in[1,s]$, and we consider $S_{1,\mu}(G)$. Let $\boldsymbol{\gamma}\in B(m,\mu,\boldsymbol{\kappa},j)$. According to (2.2.13) and (2.2.16), we have

$$|\mathrm{Nm}(\boldsymbol{\gamma})| = (j+z_1)C_M^s 2^{z_2(s-1)}, \quad \text{and} \quad \#\Gamma^\perp\cap B(\mathbf{m},\mu,\boldsymbol{\kappa},j)\leq 1 \tag{2.4.17}$$

with $z_1,z_2\in[0,1]$. By (2.3.5) and (2.4.17), we obtain

$$j+1\geq n^{1/2}(C_M^s 2^{s-1})^{-1} \quad \text{for} \quad \boldsymbol{\gamma}\in G^{(3)}.$$

Hence

$$\sum_{j\geq 0}\ \sum_{\boldsymbol{\gamma}\in G^{(3)}\cap B(m,\mu,\boldsymbol{\kappa},j)} \frac{1}{|\mathrm{Nm}(\boldsymbol{\gamma})|^2} = O\left(\sum_{j\geq n^{1/2}} 1/j^2\right) = O(n^{-1/2}), \tag{2.4.18}$$

$$\sum_{j\geq 0}\ \sum_{\boldsymbol{\gamma}\in G\cap B(m,\mu,\boldsymbol{\kappa},j)} \frac{1}{|\mathrm{Nm}(\boldsymbol{\gamma})|^2} = O\left(\sum_{j\geq 1} 1/j^2\right) = O(1),\ \text{for}\ G\subseteq G^{(1)}. \tag{2.4.19}$$

Bearing in mind that $\mathrm{Nm}(\boldsymbol{\gamma})\leq N^{5s}$ for $\boldsymbol{\gamma}\in G^{(1)}\cup G^{(3)}$ and $n=[\log_2 N]+1$, we get from (2.3.5) and (2.4.17) that

$$\sum_{j\geq 0}\ \sum_{\boldsymbol{\gamma}\in (G^{(1)}\cup G^{(3)})\cap B(m,\mu,\boldsymbol{\kappa},j)} \frac{1}{|\mathrm{Nm}(\boldsymbol{\gamma})|} = O\left(\sum_{1\leq j\leq N^{5s}} 1/j\right) = O(n). \tag{2.4.20}$$

By (2.2.13), (2.3.5) and (1.4), we have for $\boldsymbol{\gamma}\in(G^{(1)}\cup G^{(3)})\cap B(m,\mu,\boldsymbol{\kappa},j)$ that

$$\log_2|\gamma_i|\in[m_i,m_i+1), \quad i\in[1,s],\ i\neq\nu(\mu), \quad |\gamma_i|\leq N^5, \quad |\mathrm{Nm}(\boldsymbol{\gamma})|\geq C_M^s,$$

$$C_M^s N^{-5(s-1)}\leq|\gamma_i|, \ \ s\log_2 C_M - 5(s-1)\log_2 N\leq\log_2|\gamma_i|\leq 5\log_2 N, i\in[1,s].$$

Therefore

$$m_i\in J, \quad i\in[1,s],\ i\neq\nu(\mu) \quad \text{with} \quad J=[s\log_2 C_M - 5(s-1)n, 5n]. \tag{2.4.21}$$

From (2.2.15), (2.1.5) and (2.4.15), we derive

$$S_{1,\mu}(G) \leq \sum_{\kappa_1,\dots,\kappa_s\in\{-1,1\}} \sum_{\substack{m_1+\dots+m_s=0\\ \mathbf{m}\in\mathbb{Z}^s, j\geq 0}} \sum_{\substack{\boldsymbol{\gamma}\in G\cap B(\mathbf{m},\mu,\boldsymbol{\kappa},j)\\ |\gamma_i|\leq|\gamma_\mu|, i=1,\dots,s}} \frac{(\det\Gamma)^{-2}c_2^2}{(2\pi)^{2s}|\mathrm{Nm}(\boldsymbol{\gamma})|^2}. \tag{2.4.22}$$

Hence, we obtain for $i=1,3$ that

$$S_{1,\mu}(G^{(i)}) \leq \sum_{\kappa_1,\dots,\kappa_s\in\{-1,1\}} \sum_{\substack{m_k\in J, k\in[1,s],\ k\neq\nu(\mu)\\ m_1+\dots+m_s=0,\ j\geq 0}} \sum_{\boldsymbol{\gamma}\in G^{(i)}\cap B(\mathbf{m},\mu,\boldsymbol{\kappa},j)} \frac{(\det\Gamma)^{-2}c_2^2}{(2\pi)^{2s}|\mathrm{Nm}(\boldsymbol{\gamma})|^2}.$$

Applying (2.4.18), (2.4.19) and (2.4.21), we get that

$$S_{1,\mu}(G^{(1)}) = O(n^{s-1}), \qquad \text{and} \qquad S_{1,\mu}(G^{(3)}) = O(n^{s-1-1/2}). \tag{2.4.23}$$

Analogously, we have from (2.4.16) and (2.4.20) that for $\dot{G}, \ddot{G} \subset G^{(1)} \cup G^{(3)}$

$$S_2(\dot{G},\ddot{G}) = O\left(\left(\sum_{\kappa_1,\dots,\kappa_s\in\{-1,1\}} \sum_{\substack{m_k\in J, k\in[1,s]\\ k\neq\nu(\mu), m_1+\dots+m_s=0}} \sum_{j\geq 0}\sum_{\boldsymbol{\gamma}\in G_0} \frac{1}{\mathrm{Nm}(\boldsymbol{\gamma})}\right)^2\right) = O(n^{2s}), \tag{2.4.24}$$

where $G_0 = G^{(1)} \cup G^{(3)} \cap B(\mathbf{m},\mu,\boldsymbol{\kappa},j)$.
According to (2.4.14), we obtain (2.4.12). By (2.4.2) and (2.1.2), we have that

$$\tilde{\mathcal{A}}(G) \leq (\det\Gamma)^{-1}c_2 \sum_{\boldsymbol{\gamma}\in G} 1/|\mathrm{Nm}(\boldsymbol{\gamma})|.$$

Now using (2.4.20), similarly to (2.4.22)-(2.4.23), we get (2.4.13).

Hence, Lemma 7 is proved. □

Lemma 8. *With the notations as above*

$$S_{1,\mu}(\tilde{G}) = O(n^{s-11/9}), \quad \textit{with} \quad \tilde{G} = \dot{G}_0 \bigcup_{1\leq i\leq n^{5/9}+1} \ddot{G}_i, \quad \mu=1,\dots,s.$$

P r o o f. Let $\boldsymbol{\gamma} \in \ddot{G}_i \cap B(\mathbf{m},\mu,\boldsymbol{\kappa},j)$. By (2.2.13), we have that $\log_2|\gamma_k| \in [m_k, m_k+1)$ with $k\in[1,s]$, $k\neq\nu(\mu)$. From (2.3.8) and (1.4), we derive for $|\gamma_i|\leq|\gamma_\mu|, i=1,\dots,s$ that

$$\log_2|\gamma_k| \leq (i+1)n^{4/9}, \quad \log_2|\gamma_k| \geq s\log_2 C_M - \sum_{j\in[1,s],\ j\neq k} \log_2|\gamma_j|,\ k=1,\dots,s,$$

and

$$\log_2|\gamma_\mu| > (i+1)n^{4/9} - n^{2/9}.$$

Therefore

$$m_\mu \in J_1 \quad \text{with} \quad J_1 = \left((i+1)n^{4/9} - n^{2/9} - 1, (i+1)n^{4/9}\right], \quad \#J_1 \leq n^{2/9}+2,$$

and

$$m_k \in J_2 \quad \text{with} \quad J_2 = \left(-(s-1)(i+1)n^{4/9} + s\log_2 C_M - 1, (i+1)n^{4/9}\right],$$
$$k \in [1,s],\ k \neq \nu(\mu),\ \mu,\ \#J_2 = O\left((i+1)n^{4/9}\right),\ \ i = 1,2,\dots$$

By (2.4.22), we get that

$$S_1(\ddot{G}_i) \leq \sum_{\kappa_1,\dots,\kappa_s \in \{-1,1\}} \sum_{m_\mu \in J_1} \sum_{\substack{m_k \in J_2 \\ k \neq \mu,\nu(\mu)}} \sum_{j \geq 0} \sum_{\substack{\boldsymbol{\gamma} \in \ddot{G}_i \cap B(\mathbf{m},\mu,\boldsymbol{\kappa},j) \\ |\gamma_i| \leq |\gamma_\mu|, i=1,\dots,s}} \frac{(\det\Gamma)^{-2} c_2^2}{(2\pi)^{2s}|\mathrm{Nm}(\boldsymbol{\gamma})|^2}.$$

Using (2.4.19), we obtain

$$S_{1,\mu}(\ddot{G}_i) = O(\#J_1 \#J_2^{s-2}) = O\big(i^{s-2} n^{((s-2)4+2)/9}\big).$$

Similarly we get that $S_{1,\mu}(\dot{G}_0) = O(n^{4(s-1)/9})$. Now from (2.4.15) and (2.3.8), we have

$$\begin{aligned} S_{1,\mu}(\tilde{G}) &= S_{1,\mu}(\dot{G}_0) \ + \sum_{1 \leq i \leq n^{5/9}+1} S_{1,\mu}(\ddot{G}_i) \\ &= O\left(\sum_{1 \leq i \leq n^{5/9}} i^{s-2} n^{((s-2)4+2)/9} \right) = O(n^{s-1-2/9}). \end{aligned}$$

Hence, Lemma 8 is proved. □

Lemma 9. *With the notations as above*

$$\mathbf{E}\left[\left|\mathcal{A}\big(G^{(5)}\big)\right|^2\right] = O\left(n^{s-2}(\ln n)^4\right).$$

Proof. Let

$$G^{(5,\mu)} = \{\boldsymbol{\gamma} \in G^{(5)} : |N_\mu \gamma_\mu| \leq 2^{(\ln n)^4} \text{ and } |N_j\gamma_j| > 2^{(\ln n)^4} \text{ for } j < \mu\}. \quad (2.4.25)$$

By (2.3.6), we have that

$$G^{(5)} = \bigcup_{\mu \in [1,s]} G^{(5,\mu)}, \qquad G^{(5,\mu)} \cap G^{(5,j)} = \emptyset \ \text{ for } \ \mu \neq j.$$

Similarly to (2.4.14)-(2.4.16), using the Cauchy–Schwartz inequality, we obtain from (2.1.2) and (2.4.1) that

$$\mathbf{E}\left[\left|\mathcal{A}(G^{(5)})\right|^2\right] \leq s2^{s-1} \sum_{\mu \in [1,s]} \sum_{\substack{\kappa_j \in \{-1,1\} \\ j \in [1,s], j \neq \mu}} \sum_{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)} \in G^{(5,\mu)}} \dot{\psi}(\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}),$$

with

$$\dot{\psi}(\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}) = \frac{(\det\Gamma)^{-2}|\hat{\omega}(\tau\boldsymbol{\gamma}^{(1)})||\hat{\omega}(\tau\boldsymbol{\gamma}^{(2)})|}{(2\pi)^{2s}|\mathrm{Nm}(\boldsymbol{\gamma}^{(1)})||\mathrm{Nm}(\boldsymbol{\gamma}^{(2)})|}\tilde{\psi}(\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}) \tag{2.4.26}$$

and

$$\tilde{\psi}\big(\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}\big) = \Bigg|\mathbf{E}\Bigg[\sin\big(\pi\theta_\mu N_\mu\gamma_\mu^{(1)}\big)\times\sin\big(\pi\theta_\mu N_\mu\gamma_\mu^{(2)}\big) \times e\Bigg(\sum_{1\le j\le s,\ j\neq\mu}(\gamma_j^{(1)}-\gamma_j^{(2)})\theta_j N_j\kappa_j/2\Bigg)\Bigg]\Bigg|. \tag{2.4.27}$$

Hence

$$\mathbf{E}[|\mathcal{A}(G^{(5)})|^2] \le s2^s\sum_{\mu\in[1,s]}\ \sum_{\kappa_j\in\{-1,1\},j\in[1,s],\ j\neq\mu}\big(\dot{S}_1(\mu)+\dot{S}_2(\mu)\big) \tag{2.4.28}$$

with

$$\dot{S}_1(\mu) = \sum_{\boldsymbol{\gamma}\in G^{(5,\mu)}}\dot{\psi}(\boldsymbol{\gamma},\boldsymbol{\gamma}) \quad\text{and}\quad \dot{S}_2(\mu) = \sum_{\substack{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}\in G^{(5,\mu)},\\ \boldsymbol{\gamma}^{(1)}\neq\boldsymbol{\gamma}^{(2)}}}\dot{\psi}(\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}). \tag{2.4.29}$$

Bearing in mind that $|\sin(x)|\le|x|$, we derive from (2.4.27) that

$$\tilde{\psi}(\boldsymbol{\gamma},\boldsymbol{\gamma}) \le \min(1,|2\pi N_\mu\gamma_\mu|^2). \tag{2.4.30}$$

Consider $\dot{S}_2(\mu)$. By (2.4.11), we get for $\boldsymbol{\gamma}^{(1)}\neq\boldsymbol{\gamma}^{(2)}$ that

$$\begin{aligned}\tilde{\psi}(\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}) &\le \prod_{j\in[1,s],j\neq\mu}\frac{1}{\pi N_j|\gamma_j^{(1)}-\gamma_j^{(2)}|}\\ &= \frac{N_\mu|\gamma_\mu^{(1)}-\gamma_\mu^{(2)}|}{\pi^{s-1}N|\mathrm{Nm}(\boldsymbol{\gamma}^{(1)}-\boldsymbol{\gamma}^{(2)})|} \le \frac{2^{(\ln n)^4+1}}{\pi^{s-1}C_M^s N}.\end{aligned}$$

According to (2.2.8), (2.3.6) and (1.4), we have

$$G^{(5)}\subset\mathbb{G}(s\log_2 C_M-(s-1)(n+1),n+1).$$

Using Lemma 3, we obtain $\#G^{(5)} = O(n^s)$. Applying (2.4.26) and (2.4.29), we get

$$\dot{S}_2(\mu) = O(n^{2s}N^{-1}2^{(\ln n)^4+1}) = O(1). \tag{2.4.31}$$

Now we fix $\mu\in[1,s]$, and we consider $\dot{S}_1(\mu)$. Let

$$\boldsymbol{\gamma}\in\Gamma^\perp\cap B(\mathbf{m},\mu,\boldsymbol{\kappa}^{(1)},j).$$

According to (2.2.13) and (2.4.25), we have that

$$\log_2|N_\mu\gamma_\mu| = \log_2 N_\mu + m_\mu + z_1 \le (\ln n)^4,\quad z_2\in[0,1).$$

Hence

$$m_\mu \in \dot{J}, \quad \text{with} \quad \dot{J} = (-\infty, (\ln n)^4 - \log_2 N_\mu].$$

By (2.4.17) and (1.4), we obtain that $C_M^s \max(1, j) \leq \mathrm{Nm}(\boldsymbol{\gamma}) \leq (j+1) C_M^s 2^{s-1}$ and

$$\sum_{\substack{m_\mu \in \dot{J} \\ j \geq 0}} \sum_{\boldsymbol{\gamma} \in G^{(5,\mu)} \cap B(\mathbf{m}, \mu, \boldsymbol{\kappa}^{(1)}, j)} \frac{\min(1, |N_\mu \gamma_\mu|^2)}{|\mathrm{Nm}(\boldsymbol{\gamma})|^2} = O\biggl(\sum_{m_\mu \in \dot{J}} \sum_{j \geq 1} \frac{\min(1, N_\mu^2 2^{2m_\mu})}{j^2} \biggr)$$

$$= O\Biggl(\sum_{\substack{m_\mu \leq -\log_2 N_\mu \\ j \geq 1}} \frac{N_\mu^2 2^{2m_\mu}}{j^2} + \sum_{m_\mu \in [-\log_2 N_\mu, (\ln n)^4 - \log_2 N_\mu]} \sum_{j \geq 1} \frac{1}{j^2} \Biggr) = O((\ln n)^4). \tag{2.4.32}$$

Bearing in mind (2.2.13) and that $|\boldsymbol{\gamma}| \leq N$, we have for $k \neq \mu, \nu(\mu)$ that

$$m_k + z_1 = \log_2 |\gamma_k| = \log_2 \mathrm{Nm}(\boldsymbol{\gamma}) - \sum_{j \in [1,s], j \neq k} \log_2 |\gamma_j| \geq \log_2 C_M^s - (s-1)(n+1),$$

with $z_1 \in [0, 1)$ and

$$m_k \in \ddot{J} \quad \text{with} \quad \ddot{J} = [\log_2 C_M^s - (s-1)(n+1) - 1, n+1]. \tag{2.4.33}$$

By (2.2.15), (2.4.26), (2.4.29), (2.4.30) and (2.1.5), we get

$$\begin{aligned} \dot{S}_1(\mu) &\leq \bigcup_{\boldsymbol{\kappa}^{(1)} \in \{-1,1\}^s} \bigcup_{\substack{\mathbf{m} \in \mathbb{Z}^s, \\ m_1 + \cdots + m_s = 0}} \bigcup_{j \geq 0} \sum_{\boldsymbol{\gamma} \in G^{(5,\mu)} \cap B(\mathbf{m}, \mu, \boldsymbol{\kappa}^{(1)}, j)} \dot{\psi}(\boldsymbol{\gamma}, \boldsymbol{\gamma}) \\ &\leq \sum_{\boldsymbol{\kappa}^{(1)} \in \{-1,1\}^s} \sum_{m_\mu \in \dot{J}} \sum_{\substack{m_k \in \ddot{J}, \\ k \in [1,s], k \neq \mu, \nu(\mu)}} \sum_{j \geq 0} \sum_{\boldsymbol{\gamma} \in G^{(5,\mu)} \cap B(\mathbf{m}, \mu, \boldsymbol{\kappa}^{(1)}, j)} \\ &\quad \times \frac{(\det \Gamma)^{-2} c_2^2 \min(1, |2\pi N_\mu \gamma_\mu|^2)}{(2\pi)^{2s} |\mathrm{Nm}(\boldsymbol{\gamma})|^2}. \end{aligned}$$

Applying (2.4.32) and (2.4.33), we derive

$$\dot{S}_1(\mu) = O\bigl(\# \ddot{J}^{s-2} (\ln n)^4\bigr) = O(n^{s-2} (\ln n)^4).$$

By (2.4.28) and (2.4.31), Lemma 9 is proved. □

Lemma 10. *With the notations as above*

$$\mathcal{A}(G^{(4)}) = O(1). \tag{2.4.34}$$

P r o o f. By (2.1.5), (2.1.2) and (2.4.1), we have

$$|\mathcal{A}(G^{(4)})| \leq (\det\Gamma)^{-1} c_2 \sum_{\boldsymbol{\gamma}\in G^{(4)}} \prod_{i=1}^{s} \frac{|\sin(\pi(\theta_i N_i \gamma_i)|}{2\pi|\gamma_i|}.$$

From (2.3.5), we get for $\boldsymbol{\gamma} \in G^{(4)}$ that $|\boldsymbol{\gamma}| > N$,

$$\exists \nu \in [1,s] \qquad \text{with} \qquad \log_2(|\gamma_\nu|) \geq \log_2(|\boldsymbol{\gamma}|/s) \geq n - 1 - \log_2 s,$$

and

$$\log_2(|\gamma_1|) + \cdots + \log_2(|\gamma_s|) \leq 1/2 \log_2 n, \qquad n = [\log_2 N] + 1.$$

Hence, there exists $\mu \in \{1,\dots,s\} \setminus \{\nu\}$ with

$$\begin{aligned}\log_2(|\gamma_\mu|) &\leq \frac{1}{s-1} \sum_{i\in[1,s], i\neq\nu} \log_2(|\gamma_i|)\\ &= \frac{1}{s-1}\Bigg(\sum_{i\in[1,s]} \log_2(|\gamma_i|) - \log_2(|\gamma_\nu|)\Bigg),\\ &\leq (-n + 1 + \log_2 s + 1/2\log_2 n)/(s-1),\end{aligned}$$

and

$$|\gamma_\mu| \leq 4N^{-\frac{1}{s-1}} n^{1/2}.$$

Bearing in mind that $N_\mu N^{-1/s} \in [1/c_0, c_0]$, we obtain

$$|\sin(\pi(\theta_\mu N_\mu \gamma_\mu))| \leq \pi|\theta_\mu N_\mu \gamma_\mu| \leq \pi|N_\mu\gamma_\mu| = O(N^{\frac{1}{s}-\frac{1}{s-1}} n^{1/2}) = O(n^{-s}).$$

Therefore

$$|\mathcal{A}(G^{(4)})| = O\Bigg(n^{-s} \sum_{\boldsymbol{\gamma}\in G^{(4)}} 1/\big|\mathrm{Nm}(\boldsymbol{\gamma})\big|\Bigg) = O(n^{-s} \# G^{(4)}).$$

Taking into account that $G^{(4)} \in \mathbb{G}(0, 10n)$, we get from Lemma 3 the assertion of Lemma 10. $\square$

Lemma 11. *There exists a real $w_2 > 0$ such that*

$$\mathbf{E}\Big[\big(\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s + \mathbf{x}, \Gamma)\big)^2\Big] \leq w_2 n^{s-1}, \tag{2.4.35}$$

$$\mathbf{E}\Big[|\mathcal{R}\big(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s + \mathbf{x}, \Gamma\big) - \mathcal{A}\big(G^{(1)}\big)|^2\Big] = O(n^{s-1-1/2}), \tag{2.4.36}$$

and

$$\mathbf{E}\Big[\big(\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s + \mathbf{x}, \Gamma) - \sum_{i\in[1,n^{5/9}]} \mathcal{A}(\dot{G}_i)\big)^2\Big] = O(n^{s-1-2/9}). \tag{2.4.37}$$

P r o o f. By (2.4.6) and Lemma 1, we get

$$\left|\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s+\mathbf{x},\Gamma)-\sum_{i=1}^{5}\mathcal{A}(G^{(i)})\right|\le 2^s.$$

It is easy to see that

$$|\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s+\mathbf{x},\Gamma)-\mathcal{A}(G^{(1)})|\le\sum_{i=2}^{5}|\mathcal{A}(G^{(i)})|+2^s.$$

Using the Cauchy–Schwartz inequality, we obatain

$$\mathbf{E}\big[|\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s+\mathbf{x},\Gamma)-\mathcal{A}(G^{(1)})|^2\big]\le 5\left(\sum_{i=2}^{5}\mathbf{E}[|\mathcal{A}(G^{(i)})|^2]+2^{2s}\right).$$

Applying Lemma 5–Lemma 10, we have (2.4.36). By Lemma 7, the triangle inequality and the Cauchy-Schwartz inequality, we get (2.4.35).

Now consider the statement (2.4.37). From (2.3.9) and (2.4.1) we obtain, that

$$\mathcal{A}(G^{(1)})=\sum_{i=1}^{[n^{5/9}]}\mathcal{A}(\dot{G}_i)+\mathcal{A}(\tilde{G}),\quad\text{with}\quad\tilde{G}=\dot{G}_0\bigcup_{i=1}^{[n^{5/9}]}\ddot{G}_i. \tag{2.4.38}$$

According to (2.4.14), we have

$$\mathbf{E}\big[|\mathcal{A}(\tilde{G})|^2\big]\le 2^{2s}\sum_{\mu\in[1,s]}S_{1,\mu}(\tilde{G})+\frac{2^{2s}}{\pi^s C_M^s N}S_2(\tilde{G},\tilde{G}).$$

Using Lemma 8 and (2.4.24), we derive

$$\mathbf{E}\big[|\mathcal{A}(\tilde{G})|^2\big]=O(n^{s-1-2/9}).$$

From (2.4.36) and the triangle inequality, we get (2.4.37). Therefore, Lemma 11 is proved. □

2.5. Lower bound of variance of $\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s+\mathbf{x},\Gamma)$

The main idea of the proof of Lemma 12 is to choose in G_1 c_0n^{s-1} different blocks $\mathcal{D}(\mathbf{m})$ of volume $2\det(\Gamma)$ and lying under the hyperbole $\{\mathbf{x}\in\mathbb{R}^s \mid |x_1\cdots x_s|<\det(\Gamma)\}$. The next step is to prove that for given $\boldsymbol{\gamma}\in\mathcal{D}(\mathbf{m})$ the corresponding summands in (2.5.1) are sufficiently large. This follows from the statement $\min_i|N_i\gamma_i|\ge 1$ and the obvious inequality

$$\max(|\cos(y)|,|\cos 2y|)\ge 1/2\quad\text{for all}\quad y.$$

Lemma 12. *There exist reals $w_3, c_5>0$ such that for $N>c_5$ and for all $\mathbf{x}$*

$$\check{\psi} := \sum_{\boldsymbol{\gamma}\in G^{(1)}} \frac{(\det\Gamma)^{-2}}{(2\pi)^{2s}|\mathrm{Nm}(\boldsymbol{\gamma})|^2} \mathbf{E}\left[\prod_{i=1}^{s} \sin^2(\pi\theta_i N_i \gamma_i)\right]$$
$$\times\, 2\cos^2(2\pi\langle\boldsymbol{\gamma},\mathbf{x}\rangle) \geq w_3 n^{s-1}. \quad (2.5.1)$$

P r o o f. Let $\mathbf{m}\in\mathbb{Z}^s, m_1+\cdots+m_s=0$, $q=2+[\det\Gamma^{\perp}/C_M^s]$, and

$$\mathcal{D}(\mathbf{m}) = \prod_{i=1}^{s}[-q^{m_i}, q^{m_i}] \times [-\det\Gamma^{\perp} q^{m_s}, \det\Gamma^{\perp} q^{m_s}].$$

According to Minkowsky's theorem, there exists

$$\boldsymbol{\gamma}(\mathbf{m})\in\Gamma^{\perp}\setminus\{0\} \quad \text{with} \quad \boldsymbol{\gamma}(\mathbf{m})\in\mathcal{D}(\mathbf{m}).$$

We see that

$$|\mathrm{Nm}(\boldsymbol{\gamma}(\mathbf{m}))| \leq \det\Gamma^{\perp}. \quad (2.5.2)$$

Suppose $|\gamma(\mathbf{m})_i| \leq q^{m_i-1}$ for some $i\in[1,s-1]$. By (1.4) we get

$$C_M^s \leq |\mathrm{Nm}(\boldsymbol{\gamma}(\mathbf{m}))| \leq \det\Gamma^{\perp}/q < C_M^s.$$

We arrive at a contradiction. Hence

$$|\gamma(\mathbf{m})_i\ | \ \in (q^{m_i-1}, q^{m_i}] \text{ for } i\in[1,s-1], \quad \text{and} \quad \boldsymbol{\gamma}(\mathbf{m}^{(1)}) \neq \boldsymbol{\gamma}(\mathbf{m}^{(2)}), \quad (2.5.3)$$

for $\mathbf{m}^{(1)}\neq\mathbf{m}^{(2)}$. Let

$$\bar{G} = \{\boldsymbol{\gamma}(\mathbf{m})\ |\ -n/(4s)\log_q 2 \leq m_i \leq -2s, \quad i=1,\cdots,s-1\}. \quad (2.5.4)$$

We see for sufficiently large N that

$$\#\bar{G} \geq n^{s-1}\big((5s)^{-1}\log_q 2\big)^{s-1}. \quad (2.5.5)$$

By (2.2.5) $N_i N^{1/s}\in[1/c_0, c_0]$. From (2.5.4), we obtain for sufficiently large N that

$$N_i 2^{-2s} \geq |N_i\gamma_i| \geq c_0^{-1} 2^{n/s - n/(4s)\log_q 2 - 2} \geq 2^{ln^4 n}, \quad i\in[1,s-1], \quad \boldsymbol{\gamma}\in\bar{G}.$$

Consider γ_s with $\boldsymbol{\gamma}\in\bar{G}$. By (2.5.2), we have

$$|\gamma_s| = |\mathrm{Nm}(\boldsymbol{\gamma})(\gamma_1\cdots\gamma_{s-1})^{-1}| \in |\gamma_1\cdots\gamma_{s-1}|^{-1}[C_M^s, \det\Gamma^{\perp}].$$

Now using (2.5.3) and (2.5.4), we obtain for sufficiently large N that

$$\log_q|N_s\gamma_s| \leq n/s\log_q 2 + \log_q(c_0\det\Gamma^{\perp}) - m_1 - \cdots m_{s-1} \leq 3/4n\log_q 2,$$

and

$$\log_q|N_s\gamma_s| \geq (n-1)/s\log_q 2 - \log_q c_0 + \log_q C_M^s - m_1 - \cdots - m_{s-1} - s \geq \frac{n(\log_q 2)}{2s}.$$

Therefore, we get for sufficiently large N and for $\boldsymbol{\gamma}\in\bar{G}$

$$|\boldsymbol{\gamma}| < N/2,\ |\mathrm{Nm}(\boldsymbol{\gamma})| \leq \det\Gamma^{\perp},\ |N_i\gamma_i| \geq 2^{ln^4 n},\ i=1,\ldots,s. \quad (2.5.6)$$

So $\bar{G} \cup 2\bar{G} \subset G_1$ (see (2.3.4)).

Let $\boldsymbol{\gamma} \in \bar{G}$. Taking into account that $|N_i \gamma_i| \geq 4$ $(i = 1, \dots, s)$, we obtain

$$\int_0^1 \sin^2(\pi\theta_i N_i \gamma_i)\, \mathrm{d}\theta_\mathrm{i} = 1/2 - 1/2 \int_0^1 \cos(2\pi\theta_\mathrm{i} \mathrm{N_i} \gamma_\mathrm{i})\, \mathrm{d}\theta_\mathrm{i} \geq 1/4. \tag{2.5.7}$$

Let $I = [1/6, 1/3] \cup [2/3, 5/6]$. If $\{\langle \boldsymbol{\gamma}, \mathbf{x} \rangle\} \notin I$, then $|\cos(2\pi\{\langle \boldsymbol{\gamma}, \mathbf{x} \rangle\})| \geq 1/2$. Let $\{\langle \boldsymbol{\gamma}, \mathbf{x} \rangle\} \in I$. Then we take $2\boldsymbol{\gamma}$ instead of $\boldsymbol{\gamma}$. We see that

$$|\cos(2\pi\{\langle 2\boldsymbol{\gamma}, \mathbf{x} \rangle\})| \geq 1/2,$$

and

$$\max\Big(\cos^2\big(2\pi\langle \boldsymbol{\gamma}(\mathbf{m}), \mathbf{x} \rangle\big), \cos^2\big(2\pi\langle 2\boldsymbol{\gamma}(\mathbf{m}), \mathbf{x} \rangle\big)\Big) \geq 1/4. \tag{2.5.8}$$

By (2.5.1)–(2.5.8), we have

$$\breve{\psi} \geq \sum_{\substack{\boldsymbol{\gamma}(\mathbf{m}) \in \bar{G} \\ \mathbf{m} \in \mathbb{Z}^{s-1}}} \frac{(\det\Gamma)^{-2}}{(2\pi)^{2s} C_M^{2s}} (1/4)^{s-1} \max\Big(\cos^2\big(2\pi\langle \boldsymbol{\gamma}(\mathbf{m}), \mathbf{x} \rangle\big), \cos^2\big(2\pi\langle 2\boldsymbol{\gamma}(\mathbf{m}), \mathbf{x} \rangle\big)\Big)$$

$$\geq w_4 \# \bar{G}, \quad \text{with} \quad w_4 = (\det\Gamma)^{-2}((2\pi)^{2s} C_M^{2s})^{-1} 4^{-s}.$$

Applying (2.5.5), we get the assertion of Lemma 12. □

Lemma 13. *There exist reals $c_6, w_1 > 0$ such that for $N > c_6$*

$$\mathbf{E}[(\mathcal{R}(\boldsymbol{\theta} \cdot \mathbf{N} \cdot \mathbb{K}^s + \mathbf{x}, \Gamma))^2] \geq w_1 n^{s-1}. \tag{2.5.9}$$

Proof. Applying (2.1.2) and (2.4.1), we have

$$\mathbf{E}[|\mathcal{A}(G^{(1)}, 0)|^2] = \ddot{S}_1 + \ddot{S}_2, \tag{2.5.10}$$

with

$$\ddot{S}_1 = \sum_{\substack{\boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)} \in G^{(1)}, \\ \boldsymbol{\gamma}^{(1)} = \pm \boldsymbol{\gamma}^{(2)}}} \ddot{\psi}(\boldsymbol{\gamma}^{(1)}, -\boldsymbol{\gamma}^{(2)}), \qquad \ddot{S}_2 = \sum_{\substack{\boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)} \in G^{(1)}, \\ \boldsymbol{\gamma}^{(1)} \neq \pm \boldsymbol{\gamma}^{(2)}}} \ddot{\psi}(\boldsymbol{\gamma}^{(1)}, -\boldsymbol{\gamma}^{(2)}), \tag{2.5.11}$$

where

$$\ddot{\psi}(\boldsymbol{\gamma}^{(1)}, -\boldsymbol{\gamma}^{(2)}) = \frac{(\det\Gamma)^{-2} \hat{\omega}(\tau\boldsymbol{\gamma}^{(1)}) \hat{\omega}(-\tau\boldsymbol{\gamma}^{(2)})}{(2\pi)^{2s} \mathrm{Nm}(\boldsymbol{\gamma}^{(1)}) \mathrm{Nm}(-\boldsymbol{\gamma}^{(2)})}\, e\big(\langle \boldsymbol{\gamma}^{(1)} - \boldsymbol{\gamma}^{(2)} \rangle, x\big) \breve{\boldsymbol{\psi}}(\boldsymbol{\gamma}^{(1)} - \boldsymbol{\gamma}^{(2)}).$$

and

$$\breve{\boldsymbol{\psi}}(\boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)}) = \mathbf{E}\left[\prod_{i=1}^{s} \sin\big(\pi\theta_i N_i \gamma_i^{(1)}\big) \sin\big(-\pi\theta_i N_i \gamma_i^{(2)}\big)\right]. \tag{2.5.12}$$

We consider $\ddot{S}_1$. Bearing in mind (2.1.3), (2.1.4), that

$$|e(z) - 1| = 2|\sin(\pi z)| \leq 2\pi|z|$$

and that $\omega(\mathbf{x})$ is supported inside the unit ball $B = \{\mathbf{x} \ : \ |\mathbf{x}| \leq 1\}$, we obtain for $\tau = 1/N^2$ and $|\boldsymbol{\gamma}| \leq N$ that

$$\begin{aligned} |\hat{\omega}(\tau\boldsymbol{\gamma}) - 1| &= \left| \int_{\mathbb{R}^s} e(\langle \tau\boldsymbol{\gamma}, \mathbf{x}\rangle)\omega(\mathbf{x})\,\mathrm{d}\mathbf{x} - 1 \right| = \left| \int_{\mathrm{B}} \big(\mathrm{e}(\langle \boldsymbol{\gamma}, \mathbf{x}\rangle/\mathrm{N}^2) - 1\big)\omega(\mathbf{x})\,\mathrm{d}\mathbf{x} \right| \\ &\leq \left| \int_B |e(\langle \boldsymbol{\gamma}, \mathbf{x}\rangle/N^2) - 1|\omega(\mathbf{x})\,\mathrm{d}\mathbf{x} \right| \\ &\leq 2\pi/N \int_B \omega(\mathbf{x})\,\mathrm{d}\mathbf{x} = 2\pi/\mathrm{N}. \end{aligned} \tag{2.5.13}$$

By (2.5.12), we see that

$$\breve{\boldsymbol{\psi}}(\boldsymbol{\gamma}^{(1)}, -\boldsymbol{\gamma}^{(2)})\big(\mathrm{Nm}(\boldsymbol{\gamma}^{(1)})\mathrm{Nm}(-\boldsymbol{\gamma}^{(2)})\big)^{-1} = \breve{\boldsymbol{\psi}}(\boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)})\big(\mathrm{Nm}(\boldsymbol{\gamma}^{(1)})\mathrm{Nm}(\boldsymbol{\gamma}^{(2)})\big)^{-1}. \tag{2.5.14}$$

Taking into account that $1 + \cos(2z) = 2\cos^2(z)$, we get from (2.5.1), (2.5.11), (2.5.13) and (2.5.14) that

$$\ddot{S}_1 = \breve{\psi} + O\left(1/N \sum_{\boldsymbol{\gamma} \in G^{(1)}} \frac{1}{|\mathrm{Nm}(\boldsymbol{\gamma})|^2} \right). \tag{2.5.15}$$

By (2.4.15), (2.4.23), (2.5.13) and Lemma 12, we have for sufficiently large N

$$\ddot{S}_1 \geq 0.5 w_3 n^{s-1}. \tag{2.5.16}$$

Now we consider $\ddot{S}_2$. We see from (2.5.12) and (2.4.11)

$$\begin{aligned} &\left| \breve{\boldsymbol{\psi}}(\boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)}) \right| \\ &= \left| 2^{-2s} \sum_{\kappa_1^{(1)}, \dots, \kappa_s^{(2)} \in \{-1,1\}} \kappa_1^{(1)}\kappa_2^{(1)} \cdots \kappa_s^{(2)} \mathbf{E}\left[e\left(\sum_{1 \leq i \leq s, j=1,2} \theta_i \times N_i \kappa_i^{(j)} \gamma_i^{(j)}/2 \right) \right] \right| \\ &\leq \ 2^{-s} \sum_{\kappa_1, \dots, \kappa_s \in \{-1,1\}} \left| \mathbf{E}\left[e\left(\sum_{i=1}^s \theta_i N_i \Big(\gamma_i^{(1)} + \kappa_i \gamma_i^{(2)}\Big)/2 \right) \right] \right| \\ &\leq \ 2^{-s} \sum_{\kappa_1, \dots, \kappa_s \in \{-1,1\}} \prod_{i=1}^s \min\left(1, \frac{1}{\pi |N_i(\gamma_i^{(1)} + \kappa_i \gamma_i^{(2)})|} \right). \end{aligned} \tag{2.5.17}$$

Applying Lemma 4, we get that $\psi(\boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)}) = O(n^{-20s})$. By (2.4.16), (2.4.24) and (2.5.11), we derive that

$$\ddot{S}_2 = O\big(n^{-20s} S_2\Big(G^{(1)}, G^{(1)}\Big)\Big) = O(n^{-2s}).$$

From (2.5.10) and (2.5.16), we have for sufficiently large N that

$$\mathbf{E}\Big[\big|\mathcal{A}\big(G^{(1)},0\big)\big|^2\Big] \geq 0.25 w_3 n^{s-1}. \tag{2.5.18}$$

By the triangle inequality, we obtain

$$\begin{aligned}&\left(\mathbf{E}\Big[\big(\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s+\mathbf{x},\Gamma)\big)^2\Big]\right)^{1/2} \\ &\geq \left(\mathbf{E}\Big[\big|\mathcal{A}\big(G^{(1)},0\big)\big|^2\Big]\right)^{1/2} - \left(\mathbf{E}\Big[\big|\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s+\mathbf{x},\Gamma)-\mathcal{A}\big(G^{(1)},0\big)\big|^2\Big]\right)^{1/2}.\end{aligned}$$

Using (2.5.18) and Lemma 11, we get the assertion of Lemma 13. □

2.6. Four moments estimates for $\mathcal{A}(\dot{G}_i)$

Let

$$\delta(\mathfrak{T}) = \begin{cases} 1, & \text{if } \mathfrak{T} \text{ is true,} \\ 0, & \text{otherwise.}\end{cases}$$

Lemma 14. *With the notations as above, we have*

$$\mathbf{E}[|\mathcal{A}(\dot{G}_i)|^4] = O(i^{2(s-2)} n^{8/9(s-1)}). \tag{2.6.1}$$

P r o o f. Using the following simple inequality

$$\Big|\sum_{1\leq i\leq 2^s} a_i\Big|^4 \leq \Big(2^s \max_{1\leq i\leq 2^s} |a_i|\Big)^4 \leq 2^{4s} \sum_{1\leq i\leq 2^s} |a_i|^4,$$

we obtain from (2.4.4)

$$\mathbf{E}[|\mathcal{A}(\dot{G}_i,\tau)|^4] \leq 2^{4s} \sum_{\kappa_1,\dots,\kappa_s\in\{-1,1\}} |\mathcal{B}(\dot{G}_i,\boldsymbol{\kappa},\tau)|^4. \tag{2.6.2}$$

Applying (2.4.8) and Lemma 6, we get

$$\mathbf{E}[|\mathcal{B}((\dot{G}_i,\boldsymbol{\kappa})|^4)] = \prod_{1\leq j\leq 4} \sum_{\boldsymbol{\gamma}^{(j)}\in\dot{G}_i} |h(\boldsymbol{\gamma}^{(j)})| \Big(\delta(\hat{\boldsymbol{\gamma}}=\mathbf{0}) + \big(1-\delta(\hat{\boldsymbol{\gamma}}=\mathbf{0})\big)N^{-1}O(1)\Big),$$

where $\hat{\boldsymbol{\gamma}} = \boldsymbol{\gamma}^{(1)} - \boldsymbol{\gamma}^{(2)} + \boldsymbol{\gamma}^{(3)} - \boldsymbol{\gamma}^{(4)}$. From (2.4.7), (2.4.16), (2.4.24) and Lemma 3, we derive that

$$\mathbf{E}[|\mathcal{B}((\dot{G}_i,\boldsymbol{\kappa},\tau)|^4)] = V_1 + V_2 + O(n^{8s}/N), \tag{2.6.3}$$

where

$$V_k = \prod_{1\leq j\leq 4} \sum_{\boldsymbol{\gamma}^{(j)}\in\dot{G}_i} \frac{(\det\Gamma)^{-1}|\hat{\omega}(\tau\boldsymbol{\gamma}^{(j)})|}{(2\pi)^s|\mathrm{Nm}(\boldsymbol{\gamma}^{(j)})|}\delta(\hat{\boldsymbol{\gamma}}=\mathbf{0})\delta_k(\bar{\boldsymbol{\gamma}}), \quad k=1,2, \tag{2.6.4}$$

with $\bar{\boldsymbol{\gamma}} = (\boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)}, \boldsymbol{\gamma}^{(3)}, \boldsymbol{\gamma}^{(4)})$,

$$\delta_1(\bar{\gamma}) = \delta\big(\nexists j, l \in [1,4],\ j \neq l \mid \boldsymbol{\gamma}^{(j)} = (-1)^{l-j+1}\boldsymbol{\gamma}^{(l)}\big), \quad \text{and} \quad \delta_2(\bar{\gamma}) = 1 - \delta_1(\bar{\gamma}). \tag{2.6.5}$$

By (2.2.6) and (2.2.10), we have that

$$\boldsymbol{\gamma}^{(j)} = \tilde{\boldsymbol{\gamma}}^{(j)} \cdot \sigma(\eta^{(j)}) \quad \text{with} \quad \tilde{\boldsymbol{\gamma}}^{(j)} = (\tilde{\gamma}_1^{(j)}, \dots, \tilde{\gamma}_s^{(j)}), \tilde{\boldsymbol{\gamma}}^{(j)} \in \mathbb{F}_n$$

and

$$\eta^{(j)} \in \dot{\mathfrak{U}}(\boldsymbol{\gamma}^{(j)}, a, b), (j = 1, \dots, 4).$$

Using (2.2.10) and (2.3.8), we obtain that

$$a = in^{4/9} \quad \text{and} \quad b = n^{4/9} - n^{2/9}.$$

Hence

$$V_k = O\Bigg(\prod_{1\leq j\leq 4} \sum_{\tilde{\boldsymbol{\gamma}}^{(j)}\in\mathbb{F}_n} \sum_{\eta^{(j)}\in\dot{\mathfrak{U}}(\tilde{\boldsymbol{\gamma}}^{(j)},a,b)} \frac{1}{|\mathrm{Nm}(\tilde{\boldsymbol{\gamma}}^{(j)})|}\delta_k(\bar{\gamma})\Bigg) \tag{2.6.6}$$
$$\times\, \delta\big(\tilde{\boldsymbol{\gamma}}^{(1)} \cdot \sigma(\eta^{(1)}) - \tilde{\boldsymbol{\gamma}}^{(2)} \cdot \sigma(\eta^{(2)}) + \tilde{\boldsymbol{\gamma}}^{(3)} \cdot \sigma(\eta^{(3)}) - \tilde{\boldsymbol{\gamma}}^{(4)} \cdot \sigma(\eta^{(4)}) = \mathbf{0}\big).$$

It is easy to see that

$$\tilde{\boldsymbol{\gamma}}^{(1)} \cdot \sigma(\eta^{(1)}) - \tilde{\boldsymbol{\gamma}}^{(2)} \cdot \sigma(\eta^{(2)}) + \tilde{\boldsymbol{\gamma}}^{(3)} \cdot \sigma(\eta^{(3)}) - \tilde{\boldsymbol{\gamma}}^{(4)} \cdot \sigma(\eta^{(4)}) = \mathbf{0}$$

if and only if

$$\big(\tilde{\gamma}_1^{(1)}\sigma_1(\eta^{(1)}) - \tilde{\gamma}_1^{(2)}\sigma_1(\eta^{(2)}) + \tilde{\gamma}_1^{(3)}\sigma_1(\eta^{(3)})\big)/\tilde{\gamma}_1^{(4)}\sigma_1(\eta^{(4)}) = 1. \tag{2.6.7}$$

First we consider V_1. We fix $\tilde{\boldsymbol{\gamma}}^{(1)}, \tilde{\boldsymbol{\gamma}}^{(2)}, \tilde{\boldsymbol{\gamma}}^{(3)}, \tilde{\boldsymbol{\gamma}}^{(4)}$ and $\eta^{(4)}$. From (2.2.6) and (2.6.5), we get that there is no degenerate solutions $(\eta^{(1)}, \eta^{(2)}, \eta^{(3)})$ of the equation (2.6.7). Applying Theorem A, we have that the number of non-degenerate solutions $(\eta^{(1)}, \eta^{(2)}, \eta^{(3)})$ of (2.6.7) is finite. Hence

$$V_1 = O\left(\sum_{\tilde{\boldsymbol{\gamma}}^{(j)}\in\mathbb{F}_n, 1\leq j\leq 4} \sum_{\eta^{(4)}\in\dot{\mathfrak{U}}(\tilde{\boldsymbol{\gamma}}^{(4)},a,b)} \frac{1}{|\mathrm{Nm}(\tilde{\boldsymbol{\gamma}}^{(1)})| \cdots |\mathrm{Nm}(\tilde{\boldsymbol{\gamma}}^{(4)})|}\right). \tag{2.6.8}$$

By (2.2.11) and (2.2.12), we derive

$$V_1 = O\Big((\ln\ n)^4 b(a+b)^{s-2}\Big) = O\Big(i^{s-2} n^{4/9(s-1)} (\ln\ n)^4\Big). \tag{2.6.9}$$

Now we consider V_2. Let $\boldsymbol{\gamma}^{(j_0)} = (-1)^{l_0-j_0+1}\boldsymbol{\gamma}^{(l_0)}$. Bearing in mind that $\hat{\boldsymbol{\gamma}} = \boldsymbol{\gamma}^{(1)} - \boldsymbol{\gamma}^{(2)} + \boldsymbol{\gamma}^{(3)} - \boldsymbol{\gamma}^{(4)} = \mathbf{0}$, we obtain that $\boldsymbol{\gamma}^{(j_1)} = (-1)^{l_1-j_1+1}\boldsymbol{\gamma}^{(l_1)}$

with $\{j_1, l_1\} = \{1,2,3,4\} \setminus \{j_0, l_0\}$. Hence, from (2.6.4), we get

$$V_2 = O\left(\left(\sum_{\tilde{\gamma}^{(1)} \in \mathbb{F}_n} \sum_{\eta^{(1)} \in \dot{\mathfrak{U}}(\tilde{\gamma}^{(1)},a,b)} \frac{1}{\mathrm{Nm}^2(\tilde{\gamma}^{(1)})}\right)^2\right).$$

By (2.2.11) and (2.2.12), we have

$$V_2 = O\Big(b^2(a+b)^{2(s-2)}\Big) = O\Big(i^{2(s-2)} n^{8/9(s-1)}\Big).$$

Using (2.6.2), (2.6.3) and (2.6.9), we obtain (2.6.1) and the assertion of Lemma 14. $\square$

2.7. Conditional variance estimate

From (2.8.8) and (2.8.9), we get that the bound in the martingale CLT depends on $\mathbb{A}_n = E(|\mathbb{V}_n^2 - 1|)$, where $\mathbb{V}_n^2$ is a Lévy conditional variance. By (2.8.16) and (2.8.20), in order to obtain $\mathbb{A}_n$, it is sufficient to find the upper bound of $\varkappa$ (see (2.7.12)). We will obtain this bound in Lemma 17 by using the auxiliary variables $H_{i,j}, \dot{H}_{i,j}$ and $\ddot{H}_{i,j}$, with $H_{i,j} = \dot{H}_{i,j} + \ddot{H}_{i,j}$. In Lemma 15, we prove that $\ddot{H}_{i,j}$ is the essential part of $H_{i,j}$. In order to obtain the upper bound of $\ddot{H}_{i,j}$, we decompose the domain of the summation by using the auxiliary functions $\delta_i(l)$ (see (2.7.1)-(2.7.2)) Next we use Diophantine inequalities (2.3.2) and (2.3.3) (see Lemma 16).

Let

$$\bar{\gamma} = \big(\boldsymbol{\gamma}^{(1)}, \boldsymbol{\gamma}^{(2)}, \boldsymbol{\gamma}^{(3)}, \boldsymbol{\gamma}^{(4)}\big),$$

and

$$\begin{aligned}
\dot{\boldsymbol{\gamma}} &= \dot{\gamma} = (\dot{\gamma}_1, \dots, \dot{\gamma}_s) = \boldsymbol{\kappa}^{(1)} \cdot \boldsymbol{\gamma}^{(1)} + \dots + \boldsymbol{\kappa}^{(4)} \cdot \boldsymbol{\gamma}^{(4)},\\
\ddot{\boldsymbol{\gamma}} &= \boldsymbol{\kappa}^{(3)} \cdot \boldsymbol{\gamma}^{(1)} + \boldsymbol{\kappa}^{(4)} \cdot \boldsymbol{\gamma}^{(2)},\\
\ddot{\boldsymbol{\gamma}} &= \ddot{\gamma} = (\ddot{\gamma}_1, \dots, \ddot{\gamma}_s) = \boldsymbol{\kappa}^{(3)} \cdot \boldsymbol{\gamma}^{(1)} + \boldsymbol{\kappa}^{(4)} \cdot \boldsymbol{\gamma}^{(2)},
\end{aligned} \tag{2.7.1}$$

$$\begin{aligned}
\dot{\delta}_1(\bar{\gamma}) &= \delta(\dot{\boldsymbol{\gamma}} = \mathbf{0},\ \ddot{\boldsymbol{\gamma}} = \mathbf{0}),\\
\dot{\delta}_2(\bar{\gamma}) &= \delta(\dot{\boldsymbol{\gamma}} = \mathbf{0},\ \ddot{\boldsymbol{\gamma}} \neq 0),\\
\dot{\delta}_3(\bar{\gamma}) &= \delta(\dot{\boldsymbol{\gamma}} \neq \mathbf{0},\ \ddot{\boldsymbol{\gamma}} = \mathbf{0}),\\
\dot{\delta}_4(\bar{\gamma}) &= \delta(\dot{\boldsymbol{\gamma}} \neq \mathbf{0},\ \ddot{\boldsymbol{\gamma}} \neq \mathbf{0},\ \exists \nu \in [1,s] \dot{\gamma}_\nu = 0 \text{ and } \quad \ddot{\gamma}_\nu = 0),\\
\dot{\delta}_5(\bar{\gamma}) &= \delta(\dot{\boldsymbol{\gamma}} \neq \mathbf{0},\ \ddot{\boldsymbol{\gamma}} \neq \mathbf{0},\ \exists \nu \in [1,s] \dot{\gamma}_\nu = 0 \text{ and } \nexists \nu \in [1,s] \quad \dot{\gamma}_\nu = 0,\ \ddot{\gamma}_\nu = 0),\\
\dot{\delta}_6(\bar{\gamma}) &= \delta(\dot{\boldsymbol{\gamma}} \neq \mathbf{0},\ \ddot{\boldsymbol{\gamma}} \neq \mathbf{0},\ \forall \nu \in [1,s] \dot{\gamma}_\nu \neq 0 \text{ and } \quad \ddot{\gamma}_\nu \neq 0),\\
\dot{\delta}_7(\bar{\gamma}) &= \delta(\dot{\boldsymbol{\gamma}} \neq \mathbf{0},\ \ddot{\boldsymbol{\gamma}} \neq \mathbf{0},\ \forall \nu \in [1,s] \dot{\gamma}_\nu \neq 0 \text{ and } \exists \nu \in [1,s] \quad \ddot{\gamma}_\nu = 0).
\end{aligned}$$

It is easy to verify that

$$\sum_{1\le k\le 7} \dot{\delta}_k(\bar{\gamma}) = 1. \tag{2.7.2}$$

Lemma 15. *Let $l \ge 2$, $i,j = 1,2,\dots,$ and let*

$$\dot{H}_{i,j}(l) = \sum_{\boldsymbol{\kappa}^{(1)},\dots,\boldsymbol{\kappa}^{(4)}\in\{-1,1\}^s} \sum_{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}\in\dot{G}_i} \sum_{\boldsymbol{\gamma}^{(3)},\boldsymbol{\gamma}^{(4)}\in\dot{G}_j} h(\boldsymbol{\gamma}^{(1)})\cdots h(\boldsymbol{\gamma}^{(4)}) \tag{2.7.3}$$
$$\times \dot{\delta}_l(\bar{\gamma})\mathbf{E}\left[e\left(\sum_{k\in[1,s]} \sum_{\nu\in[1,2]} \theta_k \kappa_k^{(\nu)} \gamma_k^{(\nu)} N_k/2 \right)\right]$$
$$\times \mathbf{E}\left[e\left(\sum_{k\in[1,s]} \sum_{\nu\in[3,4]} \theta_k \kappa_k^{(\nu)} \gamma_k^{(\nu)} N_k/2 \right)\right].$$

Then

$$\dot{H}_{i,j}(l) = O(n^{-10s}). \tag{2.7.4}$$

P r o o f. Applying (2.4.7) and Lemma 6, we get

$$\dot{H}_{i,j}(l) = O\Bigg(\sum_{\boldsymbol{\kappa}^{(1)},\dots,\boldsymbol{\kappa}^{(4)}\in\{-1,1\}^s} \sum_{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}\in\dot{G}_i} \sum_{\boldsymbol{\gamma}^{(3)},\boldsymbol{\gamma}^{(4)}\in\dot{G}_j} |\mathrm{Nm}(\boldsymbol{\gamma}^{(1)}\cdots\boldsymbol{\gamma}^{(4)})|^{-1} \dot{\delta}_l(\bar{\gamma})$$
$$\times \prod_{k\in[1,s]} \min\left(1, \frac{1}{N_k|\dot{\gamma}_k - \ddot{\gamma}_k|}\right) \min\left(1, \frac{1}{N_k|\ddot{\gamma}_i|}\right)\Bigg).$$

From (2.7.1), we have that for $l \ge 2$ there exists $k_0 \in [1,s]$ such that

$$\max(|\dot{\gamma}_{k_0} - \ddot{\gamma}_{k_0}|, |\ddot{\gamma}_{k_0}|) > 0.$$

Using Lemma 4, we derive that $N_i \max(|\dot{\gamma}_{k_0} - \ddot{\gamma}_{k_0}|, |\ddot{\gamma}_{k_0}|) > \dot{c}n^{20s}$. Thus

$$\dot{H}_{i,j}(l) = O\left(n^{-20s} \left(\sum_{\boldsymbol{\gamma}\in G^{(1)}} (\mathrm{Nm}(\boldsymbol{\gamma}))^{-1} \right)^4 \right). \tag{2.7.5}$$

By (2.2.8) and (2.3.4) $G^{(1)} = \mathbb{G}(0,2n)$. Similarly to (2.6.8) and (2.6.9), we obtain from Lemma 3 that

$$\dot{H}_{i,j}(l) = O(n^{-20s} n^{8s}) = O(n^{-10s}). \tag{2.7.6}$$

Hence, Lemma 15 is proved. □

Lemma 16. *Let $l \geq 2$, $i < j$, and*

$$\ddot{H}_{i,j}(l) = \sum_{\boldsymbol{\kappa}^{(1)},\dots,\boldsymbol{\kappa}^{(4)} \in \{-1,1\}^s} \; \sum_{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)} \in \dot{G}_i} \; \sum_{\boldsymbol{\gamma}^{(3)},\boldsymbol{\gamma}^{(4)} \in G_j} h(\boldsymbol{\gamma}^{(1)}) \cdots h(\boldsymbol{\gamma}^{(4)})$$
$$\times \dot{\delta}_l(\bar{\boldsymbol{\gamma}}) \mathbf{E}\left[e\left(\sum_{k \in [1,s]} \sum_{\nu \in [1,4]} \theta_k \kappa_k^{(\nu)} \gamma_k^{(\nu)} N_k/2 \right) \right]. \quad (2.7.7)$$

Then

$$\dot{H}_{i,j}(l) = O\big(j^{s-2} n^{4/9(s-1)+2/45}\big). \quad (2.7.8)$$

P r o o f. Applying (2.4.7) and Lemma 6, we get

$$\ddot{H}_{i,j}(l) = O\left(\sum_{\boldsymbol{\kappa}^{(1)},\dots,\boldsymbol{\kappa}^{(4)} \in \{-1,1\}^s} \; \sum_{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)} \in \dot{G}_i} \; \sum_{\boldsymbol{\gamma}^{(3)},\boldsymbol{\gamma}^{(4)} \in \dot{G}_j} \right.$$
$$\left. \times \left| \mathrm{Nm}\Big(\boldsymbol{\gamma}^{(1)} \dots \boldsymbol{\gamma}^{(4)} \Big) \right|^{-1} \dot{\delta}_l(\bar{\boldsymbol{\gamma}}) \prod_{\nu \in [1,s]} \min\left(1, \frac{1}{N_\nu |\dot{\gamma}_\nu|}\right) \right). \quad (2.7.9)$$

We will prove Lemma 16 separately for each $l \in [2,7]$:

Case $l \in \{2,5\}$**:** We will consider the case $l = 2$. The proof for the case $l = 5$ is similar. By (2.7.1) and (2.7.9), we have

$$\dot{H}_{i,j}(2) = O\left(\sum_{1 \leq \nu \leq s} \tilde{H}_{i,j,\nu} \right).$$

with

$$\tilde{H}_{i,j,\nu} = \sum_{\boldsymbol{\kappa}^{(1)},\dots,\boldsymbol{\kappa}^{(4)} \in \{-1,1\}^s} \; \sum_{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)} \in \dot{G}_i} \; \sum_{\boldsymbol{\gamma}^{(3)},\boldsymbol{\gamma}^{(4)} \in G_j} \frac{|\mathrm{Nm}(\boldsymbol{\gamma}^{(1)} \cdots \boldsymbol{\gamma}^{(4)})|}{\delta(\dot{\gamma}_\nu = 0, \ddot{\gamma}_\nu \neq 0)}.$$

Let

$$\boldsymbol{\gamma}^{(j)} = \tilde{\boldsymbol{\gamma}}^{(j)} \cdot \sigma(\eta^{(j)}) \quad \text{with} \quad \tilde{\boldsymbol{\gamma}}^{(j)} \in \mathbb{F}_n$$

and

$$\eta^{(j)} \in \dot{\mathfrak{U}}\,(\boldsymbol{\gamma}^{(j)}, a_j, b_j) \; (j = 1, \dots, 4), \; a_1 = a_2 = i n^{4/9}, \; a_3 = a_4 = j n^{4/9}$$

and

$$b_1 = \cdots = b_4 = n^{4/9} - n^{2/9}.$$

We fix $\tilde{\boldsymbol{\gamma}}^{(1)}, \tilde{\boldsymbol{\gamma}}^{(2)}, \tilde{\boldsymbol{\gamma}}^{(3)}, \tilde{\boldsymbol{\gamma}}^{(4)}$ and $\eta^{(4)}$. Bearing in mind that $\ddot{\gamma}_\nu \neq 0$ and $i < j$, we obtain that there is no degenerate solutions $(\eta^{(1)}, \eta^{(2)}, \eta^{(3)})$ (see (2.3.1)) of the equation

$$\dot{\gamma}_\nu = \sum_{1 \leq k \leq 4} \kappa_\nu^{(k)} \tilde{\gamma}_\nu^{(k)} \sigma_\nu(\eta^{(k)}) = 0.$$

Similarly to (2.6.8) and (2.6.9), we derive from Theorem A, (2.2.11) and (2.2.12) that

$$\tilde{H}_{i,j,\nu} = O\left(\sum_{\substack{\tilde{\boldsymbol{\gamma}}^{(j)} \in \mathbb{F}_n \\ 1 \leq j \leq 4}} \sum_{\boldsymbol{\eta}^{(4)} \in \dot{\mathfrak{U}}(\tilde{\boldsymbol{\gamma}}^{(4)}, a_4, b_4)} \frac{1}{\mathrm{Nm}(\tilde{\boldsymbol{\gamma}}^{(j)})} \right) = O\Big(j^{s-2} n^{4/9(s-1)} (\ln\ n)^4 \Big).$$

Hence, the assertion (2.7.8) is proved.

Case $l \in \{3, 7\}$**:** We have from (2.7.1) for both cases $l = 3$ and $l = 7$ that there exists $\nu \in [1, s]$ such that $\dot{\gamma}_\nu \neq 0$, $\ddot{\gamma}_\nu = 0$ and $\dot{\gamma}_\nu = \kappa_\nu^{(1)} \gamma_\nu^{(1)} + \kappa_\nu^{(2)} \gamma_\nu^{(2)}$. Applying Lemma 4, we get $|N_\nu \dot{\gamma}_\nu| \geq \dot{c} n^{20s}$. Now using (2.7.5), (2.7.6) and (2.7.9), we obtain (2.7.8).

Case $l = 4$**:** By (2.7.1), we have that there exist $\mu, \nu \in [1, s]$ with $\ddot{\gamma}_\nu = 0$, $\dot{\gamma}_\nu = 0$, and $\dot{\gamma}_\mu \neq 0$. It is easy to derive that $\boldsymbol{\gamma}^{(1)} = \pm \boldsymbol{\gamma}^{(2)}$, $\boldsymbol{\gamma}^{(3)} = \pm \boldsymbol{\gamma}^{(4)}$ and $\dot{\gamma}_\mu = \tilde{\kappa}_1 \gamma_\mu^{(1)} + \tilde{\kappa}_2 \gamma_\mu^{(3)}$ with $\tilde{\kappa}_i \in \{-2, 0, 2\}$, $i = 1, 3$. Hence

$$|\dot{\gamma}_\mu| = 2|\gamma_\mu^{(1)}| \quad \text{or} \quad |\dot{\gamma}_\mu| = 2|\gamma_\mu^{(3)}| \quad \text{or} \quad |\dot{\gamma}_\mu| = 2|\gamma_\mu^{(1)} \pm \gamma_\mu^{(3)}| \neq 0.$$

Applying (2.3.4) and Lemma 4, we get $|N_\mu \dot{\gamma}_\mu| \geq \dot{c} n^{20s}$ for sufficiently large N. By (2.7.5), (2.7.6) and (2.7.9), we obtain (2.7.8).

Case $l = 6$**:** By (2.3.8), we have that there exists $\nu \in [1, s]$ such that $\gamma_\nu^{(4)} \geq 2^{jn^{4/9}}$. Using Lemma 4, we obtain for sufficiently large N that

$$|\ddot{\gamma}_\nu| = |\kappa_\nu^{(3)} \gamma_\nu^{(3)} + \kappa_\nu^{(4)} \gamma_\nu^{(4)}| \geq |\gamma_\nu^{(4)}| \exp(-\ddot{c}(\ln n)^3) \geq 2^{jn^{4/9}} \exp(-\ddot{c}(\ln n)^3)|$$

$$\geq 2^{(i+1)n^{4/9} - n^{2/9} + 2} \geq 2|\kappa_\nu^{(1)} \gamma_\nu^{(1)} + \kappa_\nu^{(2)} \gamma_\nu^{(2)}|.$$

Hence, we get for sufficiently large N that

$$N_\nu |\dot{\gamma}_\nu| = N_\nu |\kappa_\nu^{(1)} \gamma_\nu^{(1)} + \kappa_\nu^{(2)} \gamma_\nu^{(2)} + \kappa_\nu^{(3)} \gamma_\nu^{(3)} + \kappa_\nu^{(4)} \gamma_\nu^{(4)}| \geq N_\nu |\ddot{\gamma}_\nu|/2 \geq n^{20s}.$$

Now from (2.7.5), (2.7.6) and (2.7.9), we obtain (2.7.8). Thus, Lemma 16 is proved. $\square$

Let

$$H_{i,j} = \sum_{1 \leq l \leq 7} (\ddot{H}_{i,j}(l) - \dot{H}_{i,j}(l)). \tag{2.7.10}$$

By (2.7.2), (2.7.3) and (2.7.7), we get

$$H_{i,j} = \sum_{\boldsymbol{\kappa}^{(1)},\dots,\boldsymbol{\kappa}^{(4)}\in\{-1,1\}^s} \ \sum_{\boldsymbol{\gamma}^{(1)},\boldsymbol{\gamma}^{(2)}\in\dot{G}_i} \ \sum_{\boldsymbol{\gamma}^{(3)},\boldsymbol{\gamma}^{(4)}\in G_j} h(\boldsymbol{\gamma}^{(1)})\cdots h(\boldsymbol{\gamma}^{(4)}) \tag{2.7.11}$$
$$\times\Bigg(\mathbf{E}\Bigg[e\Bigg(\sum_{k\in[1,s]}\sum_{l\in[1,4]}\phi_{k,l}\Bigg)\Bigg]-\mathbf{E}\Bigg[e\Bigg(\sum_{k\in[1,s]}\sum_{l\in[1,2]}\phi_{k,l}\Bigg)\Bigg]\mathbf{E}\Bigg[e\Bigg(\sum_{k\in[1,s]}\sum_{l\in[3,4]}\phi_{k,l}\Bigg)\Bigg]\Bigg)$$

with $\phi_{k,l} = \theta_k \kappa_k^{(l)} \gamma_k^{(l)} N_k/2$.

Lemma 17. *With the notations as above, we have*

$$\varkappa := \mathbf{E}\left[\left(\sum_{i\in[1,n^{5/9}]}(\mathcal{A}^2(\dot{G}_i)-\mathbf{E}[\mathcal{A}^2(\dot{G}_i)])\right)^2\right] = O\big(n^{2(s-1)-2/5}\big). \tag{2.7.12}$$

P r o o f. Let

$$\varkappa_{i,j} = \mathbf{E}\big[\big(\mathcal{A}^2(\dot{G}_i)-\mathbf{E}[\mathcal{A}^2(\dot{G}_i)]\big)\times\big(\mathcal{A}^2(\dot{G}_j)-\mathbf{E}[\mathcal{A}^2(\dot{G}_j)]\big)\big].$$

It is easy to see that

$$\varkappa_{i,j} = \mathbf{E}\big[\mathcal{A}^2(\dot{G}_i)\mathcal{A}^2(\dot{G}_j)\big] - \mathbf{E}[\mathcal{A}^2(\dot{G}_i)]\mathbf{E}[\mathcal{A}^2(\dot{G}_j)],$$

and

$$\varkappa \le \dot{\varkappa} + \ddot{\varkappa}, \quad \text{with} \quad \dot{\varkappa} = \sum_{i\in[0,n^{5/9}]}\varkappa_{i,i} \quad \text{and} \quad \ddot{\varkappa} = 2\sum_{i,j\in[1,n^{5/9}],\ i<j}|\varkappa_{i,j}|. \tag{2.7.13}$$

By Lemma 14, we obtain

$$\varkappa_{i,i} \le \mathbf{E}[|\mathcal{A}(\dot{G}_i)|^4] = O(i^{2(s-2)}n^{8/9(s-1)}),$$

and

$$\dot{\varkappa} = O\left(\sum_{i\in[0,n^{5/9}]} i^{2(s-2)}n^{8/9(s-1)}\right) = O\big(n^{2(s-1)-5/9}\big). \tag{2.7.14}$$

Using (2.4.9) and (2.7.11), we get

$$\varkappa_{i,j} = H_{i,j}. \tag{2.7.15}$$

From (2.7.1), (2.7.3) and (2.7.7), we derive

$$\ddot{H}_{i,j}(1) - \dot{H}_{i,j}(1) = 0.$$

By Lemma 15 and Lemma 16, we have

$$\dot{H}_{i,j}(l) = O(n^{-10s}) \ \text{ and } \ \ddot{H}_{i,j}(l) = O(j^{s-2}n^{4/9(s-1)+2/45}),\ l=2,3,\dots,7,\ i<j.$$

Applying (2.7.10), we obtain $H_{i,j} = O(j^{s-2} n^{4/9(s-1)})$. Now from (2.7.13) and (2.7.15), we get

$$\ddot{\varkappa} = O\Bigg(\sum_{j \in [1, n^{5/9}]} j^{s-1} n^{4/9(s-1)+2/45} \Bigg) = O\big(n^{5s/9+(s-1)4/9+2/45}\big) = O(n^{s-2/5}).$$

By (2.7.13) and (2.7.14), Lemma 17 is proved. □

2.8. Martingale approximation

Denote by $\dot{\mathcal{F}}(l)$ the sigma field on $[0,1)^s$ generated by

$$\left\{ \left[\frac{k_1}{2^l}, \frac{k_1+1}{2^l} \right) \times \cdots \times \left[\frac{k_s}{2^l}, \frac{k_s+1}{2^l} \right) \; : \; k_1, \ldots, k_s = 0, \ldots, 2^l - 1 \right\}.$$

Let

$$l(0) = 0, l(i) = (i+1)[n^{4/9}] + [n/s - n^{1/9}],$$

$$\mathcal{F}_i = \dot{\mathcal{F}}(l(i)) \quad \text{and} \quad \xi_i = \mathbf{E}[\mathcal{A}(\dot{G}_i) \mid \mathcal{F}_i] - \mathbf{E}[\mathcal{A}(\dot{G}_i) \mid \mathcal{F}_{i-1}],\ i = 1, 2, \ldots \tag{2.8.1}$$

Then $(\xi_i)_{i \geq 1}$ is the martingale difference array satisfying

$$\mathbf{E}[\xi_i | \mathcal{F}_{i-1}] = 0, \quad i = 1, 2, \ldots$$

Lemma 18. *With the notations as above*

$$\mathbf{E}[\mathcal{A}(\dot{G}_i) \mid \mathcal{F}_{i-1}] = O(n^{-10s}), \qquad \mathcal{A}(\dot{G}_i) - \xi_i = O(n^{-10s}), \tag{2.8.2}$$

$$\mathcal{A}(\dot{G}_i)^2 - \xi_i^2 = O(n^{-8s}) \quad \textit{and} \quad |\xi_i|^4 \leq 8 |\mathcal{A}(\dot{G}_i)|^4 + O(n^{-6s}). \tag{2.8.3}$$

P r o o f. It is easy to see that

$$\Big|2^l \int_{k/2^l}^{(k+1)/2^l} \sin(\lambda\theta)\, \mathrm{d}\theta \Big| = 2^{\mathrm{l}}/\lambda |\cos\big(\lambda(\mathrm{k}+1)/2^{\mathrm{l}}\big) - \cos(\lambda \mathrm{k}/2^{\mathrm{l}})| \leq 2^{\mathrm{l}+1}/\lambda \quad \text{with} \ \ \lambda > 0.$$

Hence, we obtain for $|\gamma_j| \geq 2^{i[n^{4/9}]}$ and $|N_j| \geq c_0^{-1} 2^{(n-1)/s}$ that

$$\left| 2^{l_{i-1}} \int_{k/2^{l_{i-1}}}^{(k+1)/2^{l_{i-1}}} \sin(N_j \gamma_j \theta)\, \mathrm{d}\theta \right| \leq \mathrm{c}_0 2^{-[\mathrm{n}^{1/9}]+5}. \tag{2.8.4}$$

Bearing in mind that

$$\mathbf{E}[\phi_1(\theta_1) \cdot \cdots \cdot \phi_s(\theta_s) \mid \mathcal{F}_{i-1}] = \prod_{j=1}^{s} 2^{l_i} \int_{k_j/2^{l_{i-1}}}^{(k_j+1)/2^{l_{i-1}}} \phi_j(\theta_j)\, \mathrm{d}\theta_{\mathrm{j}}$$

on $\left[\frac{k_1}{2^{l_{i-1}}}, \frac{k_1+1}{2^{l_{i-1}}}\right) \times \cdots \times \left[\frac{k_s}{2^{l_{i-1}}} \frac{k_s+1}{2^{l_{i-1}}}\right)$, we have from (2.3.8), (2.1.2), (2.4.1), Lemma 3 and (2.8.4), that

$$\mathbf{E}\big[\mathcal{A}(\dot{G}_i) \mid \mathcal{F}_{i-1}\big] = O(n^s 2^{-[n^{1/9}]}) = O(n^{-10s}). \tag{2.8.5}$$

Now let

$$|\gamma_j| \leq 2^{(i+1)[n^{4/9}]-[n^{2/9}]} \quad \text{and} \quad \theta_j^{(1,2)} \in \left[\frac{k}{2^{l_i}}, \frac{k+1}{2^{l_i}}\right),$$

then

$$\left|\sin\bigl(N_j\gamma_j\theta_j^{(1)}\bigr) - \sin\bigl(N_j\gamma_j\theta_j^{(2)}\bigr)\right| = \left|N_j\gamma_j\bigl(\theta_j^{(1)} - \theta_j^{(2)}\bigr)\cos\bigl(N_j\gamma_j\theta_j^{(3)}\bigr)\right|$$
$$\leq 2^{\left[n^{1/9}\right]-\left[n^{2/9}\right]+2}c_0,$$

with

$$\theta_j^{(3)} \in \left[\frac{k}{2^{l_i}}, \frac{k+1}{2^{l_i}}\right).$$

Therefore

$$\prod_{j=1}^{s}\sin\bigl(N_j\gamma_j\theta_j^{(1)}\bigr) = \prod_{j=1}^{s}\sin\bigl(N_j\gamma_j\theta_j^{(2)}\bigr) + O\left(2^{\left[n^{1/9}\right]-\left[n^{2/9}\right]}\right).$$

Thus

$$\prod_{j=1}^{s}\sin\left(N_j\gamma_j\theta_j\right) = \mathbf{E}\left[\prod_{j=1}^{s}\sin(N_j\gamma_j\theta) \mid \mathcal{F}_i\right] + O\left(2^{\left[n^{1/9}\right]-\left[n^{2/9}\right]}\right). \tag{2.8.6}$$

Taking into account (2.3.8), (2.1.2), (2.4.1) and (2.8.5), we get (2.8.2). It is easy to see that

$$|\mathcal{A}(\dot{G}_i)^2 - \xi_i^2| \leq (2|\mathcal{A}(\dot{G}_i)| + |\mathcal{A}(\dot{G}_i) - \xi_i|)|\mathcal{A}(\dot{G}_i) - \xi_i|,$$
$$|\xi_i|^4 \leq 8|\mathcal{A}(\dot{G}_i)|^4 + 8|\mathcal{A}(\dot{G}_i) - \xi_i|^4.$$

Applying (2.4.13), we obtain (2.8.3). Hence, Lemma 18 is proved. □

We shall use the following variant of the *martingale central limit theorem* (see [Mo, p. 414]):

Let $(\Omega, \mathcal{F}, P)$ be a probability space and $\{(\zeta_{n,k}, F_{n,k}) \mid n = 1, 2, \dots, k = 1, \dots, k_n\}$ be a martingale difference array with $\mathbf{E}[\zeta_{n,k}|F_{n,k-1}] = 0$ a.s. ($F_{n,0}$ is the trivial field).

Theorem C. *Let* $L(n,\epsilon) = \sum_{1\leq k\leq k_n}\mathbf{E}[\zeta_{n,k}^2\delta(|\zeta_{n,k}| > \epsilon)]$,

$$\mathbb{S}_n = \sum_{1\leq k\leq i}\zeta_{n,k}, \qquad \textit{and} \qquad \mathbb{V}_n^2 = \sum_{1\leq k\leq k_n}\mathbf{E}[\zeta_{n,k}^2|F_{n,k-1}], \tag{2.8.7}$$

$$\mathbb{A}_n = \mathbf{E}[|\mathbb{V}_n^2 - 1|], \quad \mathbb{W}_n = \int_0^1 L(n,\epsilon)\,\mathrm{d}\epsilon, \quad \text{and} \quad \sum_{1\leq \mathrm{k}\leq \mathrm{k_n}}\mathbf{E}[\zeta_{\mathrm{n,k}}^2] = 1. \tag{2.8.8}$$

Then

$$\sup_t |P(\mathbb{S}_n < t) - \Phi(t)| \leq 7(\mathbb{W}_n^{1/4} + \mathbb{A}_n^{1/3}). \tag{2.8.9}$$

Now we apply Theorem C to the martingale difference array (2.8.1) with $F_{n,k} = \mathcal{F}_k$, $\zeta_{n,i} = \xi_i/\varrho$, $\varrho = (\sum_{i\in[1,k_n]} \mathbf{E}[\xi_i^2])^{1/2}$, and $k_n = [n^{5/9}]$.

Lemma 19. *Let*

$$\mathbb{S}_n = \sum_{1\le i\le k_n} \xi_i/\varrho. \tag{2.8.10}$$

Then

$$\sup_t |P(\mathbb{S}_n < t) - \Phi(t)| = O(n^{-1/15}).$$

P r o o f. By (2.8.1), $(\xi_i)_{i\ge1}$ is the martingale difference sequence (and consequently orthogonal). Using the triangle inequality, Lemma 11, Lemma 13 and Lemma 18, we obtain

$$\begin{aligned}\varrho^2 &= \sum_{i\in[1,k_n]} \mathbf{E}[\xi_i^2] = \mathbf{E}\left[\left(\sum_{i\in[1,k_n]} \xi_i\right)^2\right] = \mathbf{E}\left[\sum_{i\in[1,k_n]} \mathcal{A}(\dot{G}_i)^2\right] + O(1)\\ &= \mathbf{E}\left[\big(\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}^s + \mathbf{x},\Gamma)\big)^2\right] + O(n^{s-1-2/9}) \in n^{s-1}[w_3, w_4],\end{aligned} \tag{2.8.11}$$

with some $w_4 > w_3 > 0$.

Let $\dot{\mathcal{F}}$ be a sub-σ-algebra of $\mathcal{F}$. By Jensen's inequality, we get

$$\mathbf{E}[|\vartheta|^\alpha] \le (\mathbf{E}[|\vartheta|^\beta])^{\alpha/\beta} \quad\text{and}\quad \mathbf{E}[|\vartheta|^\alpha \mid \dot{\mathcal{F}}] \le (\mathbf{E}[|\vartheta|^\beta \mid \dot{\mathcal{F}}])^{\alpha/\beta}, \;\text{ with }\; \beta > \alpha > 0. \tag{2.8.12}$$

Consider $\mathbb{W}_n$. We derive from (2.8.8) that

$$\begin{aligned}\mathbb{W}_n = \sum_{1\le i\le k_n} \int_0^1 \int |\xi_i/\varrho|^2 \delta\big(\xi_i/\varrho| > \epsilon\big)\,\mathrm{dP}\,\mathrm{d}\epsilon \le \sum_{1\le \mathrm{i}\le \mathrm{k_n}} \int_0^1 \int_{\{|\xi_\mathrm{i}/\varrho|>\epsilon\}} |\xi_\mathrm{i}/\varrho|^2\\ \times |\xi_i/(\varrho\epsilon)|^{24/25}\,\mathrm{dP}\,\mathrm{d}\epsilon \le \sum_{1\le \mathrm{i}\le \mathrm{k_n}} \int |\xi_\mathrm{i}/\varrho|^{74/25}\,\mathrm{dP} \int_0^1 \epsilon^{-24/25}\,\mathrm{d}\epsilon.\end{aligned}$$

Applying (2.8.11) and (2.8.12) with $\alpha = 74/25$, $\beta = 4$, we have

$$\mathbb{W}_n \le 25 \sum_{i=1}^{k_n} \left(\int |\xi_i/\varrho|^4\,\mathrm{dP}\right)^{37/50} = O\left(n^{-(s-1)37/25} \sum_{i=1}^{k_n} (\mathbf{E}[\mathcal{A}^4(\dot{G}_i)])^{37/50}\right). \tag{2.8.13}$$

By Lemma 14, we get

$$\begin{aligned}
\mathbb{W}_n &= O\Big(n^{-(s-1)37/100} \sum_{1\leq i\leq k_n} i^{2(s-2)\frac{37}{25}} n^{\frac{8}{9}(s-1)\frac{37}{50}}\Big) \\
&= O\left(n^{-(s-1)\frac{37}{25}+\frac{5}{9}(2(s-2)\frac{37}{50}+1)+\frac{8}{9}(s-1)\frac{37}{50}}\right) \\
&= O\left(n^{-4/15}\right) \text{ and } \mathbb{W}_n^{1/4} = O(n^{-1/15}). \qquad (2.8.14)
\end{aligned}$$

Next consider $\mathbb{A}_n$. Let

$$\mathbb{U}_n^2 = \sum_{1\leq k\leq k_n} (\xi_i/\varrho)^2. \qquad (2.8.15)$$

Using (2.8.11), (2.8.15) and Lemma 18, we derive

$$\begin{aligned}
\mathbf{E}[|\mathbb{U}_n^2 - 1|^2] = & \ \varrho^{-4}\mathbf{E}\left[\left|\sum_{1\leq k\leq k_n} (\xi_i^2 - \mathbf{E}[\xi_i^2])\right|^2\right] \qquad (2.8.16) \\
& \leq 2\varrho^{-4}\mathbf{E}\left[\left(\sum_{1\leq k\leq k_n} (\mathcal{A}^2(\dot{G}_i) - \mathbf{E}[\mathcal{A}^2(\dot{G}_i)])\right)^2\right] + O(n^{-5}).
\end{aligned}$$

By Lemma 17, we obtain

$$\mathbf{E}[|\mathbb{U}_n^2 - 1|^2] = O\big(n^{-2(s-1)+2(s-1)-5/9}\big) = O(n^{-5/9}). \qquad (2.8.17)$$

Let

$$\varsigma_i = (\xi_i/\varrho)^2 - \mathbf{E}[(\xi_i/\varrho)^2|\mathcal{F}_{i-1}] \quad \text{and} \quad \mathbb{V}_n^2 = \sum_{1\leq i\leq k_n} \mathbf{E}[(\xi_i/\varrho)^2|\mathcal{F}_{i-1}]. \quad (2.8.18)$$

By (2.8.1), we see that $(\varsigma_i)_{i\geq 1}$ is the martingale difference array satisfying $\mathbf{E}[\varsigma_i|\mathcal{F}_{i-1}] = 0,\ i = 1, 2, \ldots$ From (2.8.15), we have

$$\mathbf{E}[|\mathbb{V}_n^2 - \mathbb{U}_n^2|^2] = \mathbf{E}\Big[\Big|\sum_{1\leq i\leq k_n} \varsigma_i\Big|^2\Big] = \sum_{1\leq i\leq k_n} \mathbf{E}[\varsigma_i^2].$$

Using (2.8.18) and (2.8.12), we get

$$\mathbf{E}[\varsigma_i^2] \leq 2\varrho^{-4}(\mathbf{E}[\xi_i^4] + \mathbf{E}[(\mathbf{E}[\xi_i^2|\mathcal{F}_{i-1}])^2]) \leq 4\varrho^{-4}\mathbf{E}[\xi_i^4].$$

By Lemma 14, Lemma 18 and (2.8.11), we have

$$\begin{aligned}\mathbf{E}[|\mathbb{V}_n^2-\mathbb{U}_n^2|^2] &= O\left(n^{-2(s-1)}\sum_{i=1}^{k_n}\mathbf{E}[\mathcal{A}^4(\dot{G}_i)]+n^{-7s}\right)\\ &= O\left(n^{-2(s-1)}\sum_{i=1}^{k_n} i^{2(s-2)}\times n^{8/9(s-1)}\right)\\ &= O\left(n^{-2(s-1)+5/9(2s-3)+8/9(s-1)}\right)=O(n^{-5/9}). \qquad (2.8.19)\end{aligned}$$

By (2.8.8) and (2.8.12), we get

$$\begin{aligned}\mathbb{A}_n^2 = (\mathbf{E}[|\mathbb{V}_n^2-1|])^2 &\le \mathbf{E}[|\mathbb{V}_n^2-1|^2]\\ &= \mathbf{E}[|\mathbb{V}_n^2-\mathbb{U}_n^2+\mathbb{U}_n^2-1|^2]\\ &\le 2\mathbf{E}[|\mathbb{V}_n^2-\mathbb{U}_n^2|^2]+2\mathbf{E}[|\mathbb{U}_n^2-1|^2]. \qquad (2.8.20)\end{aligned}$$

From (2.8.17) and (2.8.19), we derive

$$\mathbb{A}_n^2=O(n^{-2/5}), \quad \text{and} \quad \mathbb{A}_n^{1/3}=O(n^{-1/15}).$$

Applying (2.8.14) and Theorem C, we obtain the assertion of Lemma 19. □

2.9. End of the proof of Theorem 1

Let $\dot{\mathbb{S}}_n=\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}_s+\mathbf{x},\Gamma)/\dot{\varrho}$ and $\dot{\varrho}=\left(\mathbf{E}[\mathcal{R}^2(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}_s+\mathbf{x},\Gamma)]\right)^{1/2}$. Using Lemma 11 and Lemma 18, we obtain

$$\begin{aligned}&\mathbf{E}\left[\left(\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}_s+\mathbf{x},\Gamma)-\sum_{1\le i\le k_n}\xi_i\right)^2\right]\\ &\le 2\mathbf{E}\left[\left(\mathcal{R}(\boldsymbol{\theta}\cdot\mathbf{N}\cdot\mathbb{K}_s+\mathbf{x},\Gamma)-\sum_{1\le i\le k_n}\mathcal{A}(\dot{G}_i)\right)^2\right]\\ &\quad+2\mathbf{E}\left[\left(\sum_{1\le i\le k_n}(\mathcal{A}(\dot{G}_i)-\xi_i)\right)^2\right]=O(n^{s-1-2/9}). \qquad (2.9.1)\end{aligned}$$

By (2.8.11), we get $\dot{\varrho}^2-\varrho^2=O(n^{s-1-2/9})$, $\dot{\varrho}^2\ge w_2 n^{s-1}$ for some $w_2>0$, and

$$\left|\frac{1}{\varrho}-\frac{1}{\dot{\varrho}}\right|=\frac{|\varrho-\dot{\varrho}|}{\varrho\dot{\varrho}}=\frac{|\varrho^2-\dot{\varrho}^2|}{\varrho\dot{\varrho}|\varrho+\dot{\varrho}|}=O(n^{-3/2(s-1)-2/9}). \qquad (2.9.2)$$

Applying (2.8.10), (2.8.11), (2.9.2) and (2.9.1), we derive

$$\mathbf{E}[(\mathbb{S}_n - \dot{\mathbb{S}}_n)^2] \leq 2\mathbf{E}\left[\Big(\sum_{1 \leq k \leq k_n} \xi_i - \mathcal{R}(\boldsymbol{\theta} \cdot \mathbf{N} \cdot \mathbb{K}_s + \mathbf{x}, \Gamma)\Big)^2 / \varrho^2\right]$$
$$+ 2(1/\varrho - 1/\dot{\varrho})^2 \mathbf{E}[\mathcal{R}^2(\boldsymbol{\theta} \cdot \mathbf{N} \cdot \mathbb{K}_s + \mathbf{x}, \Gamma)] = O(n^{-2/9}).$$

By Chebyshev's inequality, we have

$$P\big(|\dot{\mathbb{S}}_n - \mathbb{S}_n| \geq n^{-1/15}\big) = O(n^{-2/9+2/15}) = O(n^{-1/15}). \tag{2.9.3}$$

It is easy to see that

$$\{\dot{\mathbb{S}}_n < t\} \subseteq \big(\{\mathbb{S}_n < t + n^{-1/15}\} \cap \{|\dot{\mathbb{S}}_n - \mathbb{S}_n| \leq n^{-1/15}\}\big) \cup \big\{|\dot{\mathbb{S}}_n - \mathbb{S}_n| \geq n^{-1/15}\big\}$$

and

$$\{\mathbb{S}_n < t - n^{-1/15}\} \subseteq \big(\{\dot{\mathbb{S}}_n < t\} \cap \{|\dot{\mathbb{S}}_n - \mathbb{S}_n| \leq n^{-1/15}\}\big) \cup \{|\dot{\mathbb{S}}_n - \mathbb{S}_n| \geq n^{-1/15}\}.$$

Hence

$$P\big(\{\mathbb{S}_n < t - n^{-1/15}\}\big) - P\big(\{|\dot{\mathbb{S}}_n - \mathbb{S}_n| \geq n^{-1/15}\}\big)$$
$$\leq P\big(\{\dot{\mathbb{S}}_n < t\}\big) \leq P\big(\{\mathbb{S}_n < t + n^{-1/15}\}\big) + P\big(\{|\dot{\mathbb{S}}_n - \mathbb{S}_n| \geq n^{-1/15}\}\big). \tag{2.9.4}$$

We note for $|u| \leq n^{-1/15}$ that

$$|\Phi(t+u) - \Phi(t)| < \frac{1}{\sqrt{2\pi}} \int_{t-|u|}^{t+|u|} e^{-u^2/2}\,\mathrm{du} \leq \frac{1}{\sqrt{2\pi}} \int_{\mathrm{t-n^{-1/15}}}^{\mathrm{t+n^{-1/15}}} \mathrm{du} = \frac{2}{\sqrt{2\pi}} \mathrm{n}^{-1/15}.$$

Using Lemma 19, we get

$$\sup_t \Big| P\big(\{\mathbb{S}_n < t + u\}\big) - \Phi(t) \Big|$$
$$\leq \sup_t \Big(\big|P\big(\{\mathbb{S}_n < t + u\}\big) - \Phi(t+u)\big| + |\Phi(t+u) - \Phi(t)| \Big)$$
$$= O(n^{-1/15}), \qquad |u| \leq n^{-1/15}.$$

By (2.9.4) and (2.9.3), we derive

$$\sup_t |P(\dot{\mathbb{S}}_n < t) - \Phi(t)| = O(n^{-1/15}).$$

Bearing in mind that throughout the paper O-constants does not depend on $\mathbf{x}$, we obtain the assertion of Theorem 1. □

2.10. Sketch of the proof of Theorem 2

We use notations from §1.3. Let

$$
\begin{aligned}
&I_0 = [0, y_1) \times \cdots \times [0, y_{s-1}),\\
&I_1 = [-y_1/2, y_1/2) \times \cdots \times [-y_{s-1}/2, y_{s-1}/2),\\
&I_2 = [-1/2, 1/2)^{s-1},\\
&I_3 = [-y_s N \det \Gamma/2, y_s N \det \Gamma/2),\\
&I_4 = [-z_s(\mathbf{x}, [y_s N])/2, z_s(\mathbf{x}, [y_s N])/2),\\
&\mathbf{u}_1 = (y_1/2, \cdots, y_{s-1}/2, z_s(\mathbf{x}, [y_s N])/2) - \dot{\mathbf{x}},\\
&\mathbf{u}_2 = (1/2, \cdots, 1/2, z_s(\mathbf{x}, [y_s N])/2) - \dot{\mathbf{x}}\\
&\qquad \text{with } \mathbf{x} = (x_1, \cdots, x_{s-1}),\ \dot{\mathbf{x}} = (x_1, \cdots, x_{s-1}, 0).
\end{aligned}
$$

By (1.1), (1.5) and (1.7), we obtain

$$\Delta(I_0, (\mathcal{T}^l(\mathbf{x}))_{l=0}^{[y_s N]-1}) = \mathcal{N}(I_1 \times I_3 + \mathbf{u}_1, \Gamma) - y_1 \cdots y_{s-1} \mathcal{N}(I_3 \times I_2 + \mathbf{u}_2, \Gamma).$$

Let $a = z_s(\mathbf{x}, [y_s N])$, $b = y_s N \det \Gamma$, and let

$$(\kappa, I) = \begin{cases} (1, [-a/2, -b/2) \cup [b/2, a/2), & \text{if } a > b,\\ (-1, [-b/2, -a/2) \cup [a/2, b/2, & \text{otherwise.} \end{cases}$$

By (1.5) and (1.7), we get

$$\Delta(I_0, (\mathcal{T}^l(\mathbf{x}))_{l=0}^{[y_s N]-1}) = \dot{R}_1 + \kappa \ddot{R}_1 - y_1 y_2 \cdots y_{s-1} (\dot{R}_2 + \kappa \ddot{R}_2)$$

with

$$\dot{R}_i = \mathcal{R}(I_i \times I_3 + \mathbf{u}_k, \Gamma), \quad \text{and} \quad \ddot{R}_i = \mathcal{R}(I_i \times I_4 + \mathbf{u}_k, \Gamma), \quad i = 1, 2.$$

It is easy to verify (see also [Le2, p. 86]) that

$$\ddot{R}_i = O\big((\ln(n))^{s-1}\big), \quad i = 1, 2.$$

Thus $\dot{R}_1 - y_1 y_2 \cdots y_{s-1} \dot{R}_2$ is the essential part of $\Delta(I_0, (\mathcal{T}^l(\mathbf{x}))_{l=0}^{[y_s N]-1})$. Repeating the proofs of §2.4, we have the upper bound of the variance of $\dot{R}_1 - y_1 \cdots y_{s-1} \dot{R}_2$. Using Roth's inequality (1.6), we get the lower bound of the variance $\dot{R}_1 - y_1 \cdots y_{s-1} \dot{R}_2$. Next repeating the proofs of §2.5 – §2.8, we obtain the assertion of Theorem 2. □

Acknowledgements. I am very grateful to the referee for corrections and suggestions which improved this paper.

REFERENCES

[BW] BAKER, A.— WUSTHOLZ, G.: *Logarithmic Forms and Diophantine Geometry*, Cambridge University Press, Cambridge, 2007.

[Be1] BECK, J.: *Randomness of* $n\sqrt{2}$ mod 1 *and a Ramsey property of the hyperbola. Sets, graphs and numbers* (G. Halsz ed. et al.), Sets, graphs and numbers. A birthday salute to Vera T.Ss and Andrs Hajnal. Colloq. Math. Soc. Jnos Bolyai. **60**, (1992) 23–66.

[Be2] BECK, J.: *Randomness in lattice point problems*, Discrete Math. **229** (2001), no. 1–3, 29–55.

[Be3] BECK, J.: *Probabilistic Diophantine Approximation: Randomness in Lattice Point Counting*, Springer, New York, 2014.

[BC] BECK, J.—CHEN, W. W. L.: *Irregularities of Distribution*. Cambridge Univ. Press, Cambridge, 1987.

[Bl] BLEHER, P.: *Trace formula for quantum integrable systems, lattice-point problem, and small divisors* (D. A. Hejhal ed. et al.), in: Emerging Applications of Number Theory. Based on the proceedings of the IMA summer program, Minneapolis, MN, USA, July 15-26, 1996. IMA Vol. Math. Appl. **109** (1999), pp. 1–38.

[BS] BOREVICH, A. I.—SHAFEREVITCH, I. R.: *Number Theory*, Academic Press, New York, 1966.

[By] BYKOVSKIĬ, V. A.: *On the right order of error of optimal cubature formulas in the spaces with dominating derivation and* L^2 *discrepancy of nets*, Dalnevost. Science Center of the USSR Acad. of Sciences, Vladivostok, 1985. (In Russian)

[DrTi] DRMOTA, M. — TICHY, R.: *Sequences, Discrepancies and Applications*, in: Lecture Notes in Mathematics Vol. 1651, Springer-Verlag, Berlin, 1997.

[ESS] EVERTSE, J. H.—SCHLICKEWEI, H. P.—SCHMIDT, W. M.: *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. (2) **155** (2002), no. 3, 807–836.

[Fr] FROLOV, K. K.: *Upper bound of the discrepancy in metric* L_p, $2 \leq p < \infty$. Dokl. Akad. Nauk SSSR **252** (1980), no. 4, 805–807 (In Russian); English translation: Soviet Math. Dokl. **21** (1980), no. 3, 840–842.

[GL] GRUBER, P. M.—LEKKERKERKER, C. G.: *Geometry of Numbers*, North-Holland, New-York, 1987.

[HuRu] HUGHES, C. P.—RUDNICK, Z.: *On the distribution of lattice points in thin annuli*, Int. Math. Res. Not. **13** (2004), 637–658.

[Le1] LEVIN, M. B.: *The multidimensional generalization of J.Beck 'Randomness of $n\sqrt{2} \mod 1 \dots$' and a.s. invariance principle for $\mathbb{Z}^d$-actions of toral automorphisms*, Abstracts of Annual Meeting of the Israel Mathematical Union (2002), `http://imu.org.il/Meetings/IMUmeeting2002/ergodic.txt`

[Le2] LEVIN, M. B.: *On low discrepancy sequences and low discrepancy ergodic transformations of the multidimensional unit cube*, Israel J. Math. **178** (2010), 61–106.

[Le3] LEVIN, M. B.: *Central Limit Theorem for $\mathbb{Z}_+^d$-actions by toral endomorphisms*, Electronic Journal of Probability **18** (2013), no. 35, 42 pp.

[Le4] LEVIN, M. B.: *On the lower bound in the lattice point remainder problem for a parallelepiped*, Discrete Comput. Geom. **54** (2015), no. 4, 826–870.

[LeMe] LEVIN, M. B.—MERZBACH, E.: *Central limit theorems for the ergodic adding machine*, Israel J. Math. **134** (2003), 61–92.

[Ma] MARKLOF, J.: *Energy level statistics, lattice point problems, and almost modular functions*, Frontiers in Number Theory, Physics, and Geometry. I, Springer, Berlin, 2006, pp. 163–181.

[Mo] MORI, T.: *On the rate of convergence in the martingale central limit theorem.* Studia Sci. Math. Hungar. **12** (1977), no. 3–4, 413–417.

[Si] SINAĬ, YA. G.: *Poisson distribution in a geometric problem. Dynamical systems and statistical mechanics (Moscow, 1991)*, Adv. Soviet Math. **3**, Amer. Math. Soc., Providence, RI, 1991. pp. 199–214.

[Skr] SKRIGANOV, M. M.: *Construction of uniform distributions in terms of geometry of numbers*, Algebra i Analiz **6** (1994), no. 3 200–230; Reprinted in: St. Petersburg Math. J. **6**(1995), no. 3 635–664.

[SW] STEIN, E.—WEISS, G.: *Introduction to Fourier Analysis on Euclidean Spaces*, Princeton University Press, New-York, 1971.

Received September 10, 2015
Accepted October 19, 2015

Mordechay B. Levin
Department of Mathematics
Bar-Ilan University
Ramat-Gan, 52900
ISRAEL
E-mail: mlevin@math.biu.ac.il