MATHEMATICS OF COMPUTATION
VOLUME 58, NUMBER 197
JANUARY 1992, PAGES 305-314

THE EXISTENCE OF EFFICIENT LATTICE RULES FOR MULTIDIMENSIONAL NUMERICAL INTEGRATION

HARALD NIEDERREITER

Dedicated to Professor Edmund Hlawka on the occasion of his 75th birthday

ABSTRACT. In this contribution to the theory of lattice rules for multidimensional numerical integration, we first establish bounds for various efficiency measures which lead to the conclusion that in the search for efficient lattice rules one should concentrate on lattice rules with large first invariant. Then we prove an existence theorem for efficient lattice rules of rank 2 with prescribed invariants, which extends an earlier result of the author for lattice rules of rank 1.

1. INTRODUCTION

For $s \geq 2$ an s-dimensional *lattice* is the set of all linear combinations with integer coefficients of s linearly independent vectors in $\mathbf{R}^s$. We only consider lattices which contain $\mathbf{Z}^s$ as a sublattice. If L is such a lattice, then $L \cap [0, 1)^s$ is a finite set consisting, say, of the distinct points $\mathbf{x}_1, \ldots, \mathbf{x}_N$. The s-dimensional *lattice rule* corresponding to L (or, by a slight abuse of language, the lattice rule L) approximates the integral $I(f)$ of a function f over $[0, 1]^s$ by

$$Q(L; f) = \frac{1}{N} \sum_{n=1}^{N} f(\mathbf{x}_n).$$

We write $X(L) = L \cap [0, 1)^s = \{\mathbf{x}_1, \ldots, \mathbf{x}_N\}$ for the set of nodes in the lattice rule L. If we want to emphasize that the number of nodes in a lattice rule is N, then we speak of an *N-point lattice rule.* To avoid a trivial case, we always assume that $N \geq 2$.

Lattice rules were originally designed for the numerical integration of periodic functions having $[0, 1]^s$ as their period interval, and they were introduced by Sloan [15] and Sloan and Kachoyan [16]. Later, the applicability of lattice rules was extended to nonperiodic integrands by Niederreiter and Sloan [14]. A special class of lattice rules has been known for a long time as the *method of good lattice points*, which goes back to Korobov [5] and Hlawka [3]. We refer to Lyness [9] for a recent survey of lattice rules and to Hua and Wang [4] and Niederreiter [11, 13] for expository accounts of the method of good lattice points.

Received April 12, 1990; revised January 17, 1991.
1991 *Mathematics Subject Classification.* Primary 65D32; Secondary 11K45.

An important classification of lattice rules was established by Sloan and Lyness [18]. They showed that for any s-dimensional lattice rule L there exist a uniquely determined integer r (called the *rank*) with $1 \le r \le s$ and positive integers $n_1, \dots, n_r$ (called the *invariants*) with $n_{i+1} | n_i$ for $i = 1, \dots, r-1$ and $n_r > 1$ such that the node set $X(L)$ consists exactly of all fractional parts

$$\left\{ \sum_{i=1}^{r} \frac{k_i}{n_i} \mathbf{z}_i \right\} \quad \text{with } 1 \le k_i \le n_i \text{ for } 1 \le i \le r, \tag{1}$$

and with suitable $\mathbf{z}_1, \dots, \mathbf{z}_r \in \mathbf{Z}^s$. Here the fractional part $\{\mathbf{t}\}$ of $\mathbf{t} = (t_1, \dots, t_s) \in \mathbf{R}^s$ is defined by

$$\{\mathbf{t}\} = (\{t_1\}, \dots, \{t_s\}) \in [0, 1)^s,$$

where $\{t\} = t - \lfloor t \rfloor$ for $t \in \mathbf{R}$. The points listed in (1) are all distinct, and so the number N of nodes satisfies $N = n_1 \cdots n_r$. The lattice rules that are used in the method of good lattice points are precisely the lattice rules of rank 1.

In the present paper we will, first of all, present evidence that in the search for efficient lattice rules one should concentrate on lattice rules with large first invariant n_1 (see §2). Then we will prove an existence theorem for lattice rules of rank 2 which shows what kind of efficiency one can expect if the invariants n_1 and n_2 are prescribed (see §3). This theorem can be viewed as an extension of the existence theorem for efficient lattice rules of rank 1 in Niederreiter [12].

To assess the efficiency of lattice rules, we use a standard procedure in numerical integration, namely to consider the order of magnitude of error bounds (for suitable classes of integrands) in terms of the number N of nodes. To describe the most important error bounds, we introduce the following definitions and notations.

Definition 1. The *dual lattice* $L^\perp$ of a lattice L is defined by

$$L^\perp = \{\mathbf{h} \in \mathbf{R}^s : \mathbf{h} \cdot \mathbf{x} \in \mathbf{Z} \text{ for all } \mathbf{x} \in L\},$$

where $\mathbf{h} \cdot \mathbf{x}$ denotes the standard inner product of $\mathbf{h}$ and $\mathbf{x}$.

For a lattice rule L we have $L \supseteq \mathbf{Z}^s$, and so it follows that $L^\perp \subseteq \mathbf{Z}^s$. For $h \in \mathbf{Z}$ we put $r(h) = \max(1, |h|)$, and for $\mathbf{h} = (h_1, \dots, h_s) \in \mathbf{Z}^s$ we put $r(\mathbf{h}) = \prod_{i=1}^{s} r(h_i)$.

Definition 2. For any lattice rule L and for any real $\alpha > 1$ define

$$R_\alpha(L) = \sum_{\substack{\mathbf{h} \in L^\perp \\ \mathbf{h} \ne \mathbf{0}}} \frac{1}{r(\mathbf{h})^\alpha}.$$

Now suppose that the integrand f is periodic with period interval $[0, 1]^s$ and that f is represented by its absolutely convergent Fourier series with Fourier coefficients $\hat{f}(\mathbf{h})$ satisfying $\hat{f}(\mathbf{h}) = O(r(\mathbf{h})^{-\alpha})$ for some $\alpha > 1$. Then Sloan and Kachoyan [17] have shown the error bound

$$Q(L; f) - I(f) = O(R_\alpha(L)), \tag{2}$$

where the implied constant depends only on f. Thus, an efficient lattice rule should have a small value of $R_\alpha(L)$. To get a criterion independent of α, we

introduce the quantity $R_1(L)$. Put

$$C(N) = \{h \in \mathbf{Z}\colon -N/2 < h \le N/2\}, \qquad C^*(N) = C(N)\backslash\{0\},$$
$$C_s(N) = \{(h_1, \dots, h_s) \in \mathbf{Z}^s\colon h_i \in C(N) \text{ for } 1 \le i \le s\},$$
$$C_s^*(N) = C_s(N)\backslash\{\mathbf{0}\}.$$

Definition 3. For any N-point lattice rule L let

$$R_1(L) = \sum_{\mathbf{h}\in E(L)} \frac{1}{r(\mathbf{h})},$$

where $E(L) = C_s^*(N) \cap L^\perp$.

Note that $E(L)$ is nonempty by [14, Proposition 3]. We remark that in the definition of $R_1(L)$ we cannot use the same range of summation as in the definition of $R_\alpha(L)$, $\alpha > 1$, since the resulting infinite series would diverge. The advantage of $R_1(L)$ is that all quantities $R_\alpha(L)$, $\alpha > 1$, can be bounded in terms of $R_1(L)$. In fact, in Theorem 1 we will show that $R_\alpha(L) = O(R_1(L)^\alpha)$ for all $\alpha > 1$. Thus, a small value of $R_1(L)$ guarantees small values of $R_\alpha(L)$ for all $\alpha > 1$.

Definition 4. The *figure of merit* $\rho(L)$ of a lattice rule L is defined by

$$\rho(L) = \min_{\substack{\mathbf{h}\in L^\perp \\ \mathbf{h}\neq\mathbf{0}}} r(\mathbf{h}).$$

The quantities $R_\alpha(L)$, $\alpha \ge 1$, can be bounded in terms of the figure of merit $\rho(L)$. For $\alpha = 1$ we note first that we also have $\rho(L) = \min_{\mathbf{h}\in E(L)} r(\mathbf{h})$ with $E(L)$ as in Definition 3, according to [14, Proposition 1]. Hence, for any N-point lattice rule L we have

$$\frac{1}{\rho(L)} \le R_1(L) = O\left(\frac{(\log N)^s}{\rho(L)}\right), \tag{3}$$

where the upper bound was shown in the proof of [14, Theorem 2]. For $\alpha > 1$ we have

$$\frac{1}{\rho(L)^\alpha} \le R_\alpha(L) = O\left(\frac{(1+\log\rho(L))^{s-1}}{\rho(L)^\alpha}\right), \tag{4}$$

where the upper bound was shown in the proof of [17, Theorem 4]. The implied constants in (3) and (4) depend only on α and s. An error bound for nonperiodic integrands is based on the following notion.

Definition 5. The *discrepancy* $D(L)$ of the node set $X(L)$ of an N-point lattice rule L is defined by

$$D(L) = \sup_J \left|\frac{\operatorname{card}(X(L)\cap J)}{N} - \operatorname{Vol}(J)\right|,$$

where the supremum is extended over all half-open subintervals J of $[0, 1)^s$ of the form $J = \prod_{i=1}^s [u_i, v_i)$ and where $\operatorname{Vol}(J)$ denotes the volume of J.

Now let the integrand f be of bounded variation on $[0, 1]^s$ in the sense of Hardy and Krause. Then we have

$$Q(L; f) - I(f) = O(D(L)) \tag{5}$$

by the Koksma-Hlawka inequality (see [6, Chapter 2]), where the implied constant depends only on f. By combining Theorem 1 in [14] and inequality (4) in [14], we obtain

$$D(L) \leq s/N + \tfrac{1}{2}R_1(L) \tag{6}$$

for any N-point lattice rule L. Therefore, a small value of $R_1(L)$ guarantees a small discrepancy $D(L)$ and thus a small error bound in (5). The discrepancy $D(L)$ can also be bounded in terms of the figure of merit $\rho(L)$. According to results in [14] we have

$$\frac{c_s}{\rho(L)} \leq D(L) \leq \frac{c_s'(\log N)^s}{\rho(L)}$$

for any N-point lattice rule L, where the positive constants c_s and c_s' depend only on s.

In view of the results above, we see that an efficient lattice rule L can be characterized as having a small value of $R_1(L)$ or a large value of $\rho(L)$, and that these two characterizations are basically equivalent because of (3). For a detailed discussion of various ways of assessing the efficiency of integration rules such as lattice rules we refer to Lyness [8].

2. Some simple bounds

We show first that the quantities $R_\alpha(L)$, $\alpha > 1$, can be bounded in terms of $R_1(L)$. Let $\zeta(\alpha) = \sum_{h=1}^{\infty} h^{-\alpha}$, $\alpha > 1$, be the Riemann zeta-function.

Theorem 1. *For any N-point lattice rule L and any $\alpha > 1$ we have*

$$R_\alpha(L) \leq (1 + 2\zeta(\alpha)N^{-\alpha})^s - 1 + (1 + 2\zeta(\alpha))^s R_1(L)^\alpha.$$

Proof. By [17, Lemma 1] we have $N\mathbf{x} \in \mathbf{Z}^s$ for all $\mathbf{x} \in L$, hence $L^\perp$ contains $N\mathbf{Z}^s$. We write

$$R_\alpha(L) = \sum_{\substack{\mathbf{h} \in N\mathbf{Z}^s \\ \mathbf{h} \neq \mathbf{0}}} r(\mathbf{h})^{-\alpha} + \sum_{\mathbf{h} \in L^\perp \setminus N\mathbf{Z}^s} r(\mathbf{h})^{-\alpha} =: \textstyle\sum_1 + \sum_2 . \tag{7}$$

Now

$$\begin{aligned}
\textstyle\sum_1 &= \sum_{\mathbf{h} \in N\mathbf{Z}^s} r(\mathbf{h})^{-\alpha} - 1 = \sum_{h_1, \ldots, h_s \in \mathbf{Z}} r(Nh_1)^{-\alpha} \cdots r(Nh_s)^{-\alpha} - 1 \\
&= \left(\sum_{h \in \mathbf{Z}} r(Nh)^{-\alpha} \right)^s - 1 = \left(1 + 2\sum_{h=1}^{\infty} (Nh)^{-\alpha} \right)^s - 1 \\
&= (1 + 2\zeta(\alpha)N^{-\alpha})^s - 1.
\end{aligned}$$

To bound $\sum_2$, we use that every $\mathbf{h} \notin N\mathbf{Z}^s$ can be uniquely represented in the form $\mathbf{h} = \mathbf{k} + N\mathbf{m}$ with $\mathbf{k} \in C_s^*(N)$ and $\mathbf{m} \in \mathbf{Z}^s$. We have $\mathbf{h} \in L^\perp$ if and only if $\mathbf{k} \in L^\perp$. Thus, the $\mathbf{h} \in L^\perp \setminus N\mathbf{Z}^s$ are exactly given by all points $\mathbf{k} + N\mathbf{m}$ with $\mathbf{k} \in E(L)$ and $\mathbf{m} \in \mathbf{Z}^s$, where $E(L)$ is as in Definition 3. Therefore,

$$\textstyle\sum_2 = \sum_{\mathbf{m} \in \mathbf{Z}^s} \sum_{\mathbf{k} \in E(L)} r(\mathbf{k} + N\mathbf{m})^{-\alpha}.$$

We claim that

$$r(\mathbf{k} + N\mathbf{m}) \geq r(\mathbf{k})r(\mathbf{m}) \quad \text{for } \mathbf{k} \in C_s(N),\ \mathbf{m} \in \mathbf{Z}^s. \tag{8}$$

It suffices to show

$$r(k+Nm) \geq r(k)r(m) \quad \text{for } k \in C(N),\, m \in \mathbf{Z}.$$

This inequality is trivial whenever $km = 0$. If $km \neq 0$, then

$$\begin{aligned} r(k+Nm) &= |k+Nm| \geq N|m| - |k| \geq N|m| - \frac{N}{2} \\ &= \frac{N}{2}(2|m|-1) \geq |k|\,|m| = r(k)r(m). \end{aligned}$$

Thus (8) is proved. Using (8), we get

$$\begin{aligned} \textstyle\sum_2 &\leq \sum_{\mathbf{m}\in\mathbf{Z}^s} \sum_{\mathbf{k}\in E(L)} r(\mathbf{m})^{-\alpha} r(\mathbf{k})^{-\alpha} \\ &= \left(\sum_{\mathbf{m}\in\mathbf{Z}^s} r(\mathbf{m})^{-\alpha}\right)\left(\sum_{\mathbf{k}\in E(L)} r(\mathbf{k})^{-\alpha}\right) = (1+2\zeta(\alpha))^s \sum_{\mathbf{k}\in E(L)} r(\mathbf{k})^{-\alpha} \\ &\leq (1+2\zeta(\alpha))^s \left(\sum_{\mathbf{k}\in E(L)} r(\mathbf{k})^{-1}\right)^{\alpha} = (1+2\zeta(\alpha))^s R_1(L)^{\alpha}. \end{aligned}$$

In view of (7), this establishes the result. □

We note that $(1+2\zeta(\alpha)N^{-\alpha})^s - 1 \leq c(s,\alpha)N^{-\alpha}$ with a constant $c(s,\alpha)$ depending only on s and α. Furthermore, we have $R_1(L) \geq \rho(L)^{-1} \geq N^{-1}$, where the first inequality is obtained from (3) and the second inequality follows from the bound $\rho(L) \leq N$ shown in [14, Proposition 2]. Hence, Theorem 1 yields $R_\alpha(L) = O(R_1(L)^\alpha)$ with an implied constant depending only on s and α.

We consider now lattice rules of arbitrary rank r and with invariants $n_1, \dots, n_r$ as described in §1. Note that n_1 is the largest invariant. The following result is an improvement on the bound $\rho(L) \leq N = n_1 \cdots n_r$ mentioned above.

Proposition 1. *We always have* $\rho(L) \leq n_1$.

Proof. Since the invariants $n_2, \dots, n_r$ are divisors of n_1, it follows from the description of the node set $X(L)$ in (1) that the coordinates of all points of L are rationals with denominator n_1. Therefore $L^\perp$ contains $n_1\mathbf{Z}^s$. In particular, we have $\mathbf{h}_0 = (n_1, 0, \dots, 0) \in L^\perp$, hence $\rho(L) \leq r(\mathbf{h}_0) = n_1$. □

The argument in the proof of Proposition 1 also yields general lower bounds for the quantities $R_\alpha(L)$, $\alpha \geq 1$. Here and later on, we use the expression

$$S(m) = \sum_{h\in C^*(m)} |h|^{-1} \quad \text{for integers } m \geq 1, \tag{9}$$

where for $m = 1$ we use the standard convention that an empty sum has the value 0. The following result is obtained from [12, Lemmas 1 and 2].

Lemma 1. *For any* $m \geq 1$ *we have*

$$S(m) = 2\log m + C + \varepsilon(m) \quad \textit{with } |\varepsilon(m)| < 4/m^2,$$

where $C = 2\gamma - \log 4 = -0.23\cdots$ *with* γ *being the Euler-Mascheroni constant.*

Proposition 2. *For any N-point lattice rule we have*

$$R_\alpha(L) \geq (1 + 2\zeta(\alpha)n_1^{-\alpha})^s - 1 \quad \textit{for } \alpha > 1,$$
$$R_1(L) \geq \left(1 + \frac{1}{n_1} S\left(\frac{N}{n_1}\right)\right)^s - 1.$$

Proof. We have shown in the proof of Proposition 1 that $L^\perp \supseteq n_1\mathbf{Z}^s$. Thus for $\alpha > 1$,

$$R_\alpha(L) \geq \sum_{\substack{\mathbf{h}\in n_1\mathbf{Z}^s \\ \mathbf{h}\neq\mathbf{0}}} r(\mathbf{h})^{-\alpha} = \sum_{\mathbf{h}\in n_1\mathbf{Z}^s} r(\mathbf{h})^{-\alpha} - 1 = (1 + 2\zeta(\alpha)n_1^{-\alpha})^s - 1,$$

where the last identity is shown like the formula for $\sum_1$ in the proof of Theorem 1. For $\alpha = 1$ we note that $E(L) \supseteq C_s^*(N) \cap (n_1\mathbf{Z}^s)$ and that the elements of the latter set are exactly all points $n_1\mathbf{h}$ with $\mathbf{h} \in C_s^*(N/n_1)$. Therefore,

$$\begin{aligned} R_1(L) &\geq \sum_{\mathbf{h}\in C_s^*(N/n_1)} r(n_1\mathbf{h})^{-1} = \sum_{\mathbf{h}\in C_s(N/n_1)} r(n_1\mathbf{h})^{-1} - 1 \\ &= \left(\sum_{h\in C(N/n_1)} r(n_1 h)^{-1}\right)^s - 1 = \left(1 + \frac{1}{n_1}\sum_{h\in C^*(N/n_1)} |h|^{-1}\right)^s - 1 \\ &= \left(1 + \frac{1}{n_1} S\left(\frac{N}{n_1}\right)\right)^s - 1. \quad \square \end{aligned}$$

It follows from Proposition 2 and Lemma 1 that if factors depending only on s and α are suppressed, then $R_\alpha(L)$ is at least of the order of magnitude $n_1^{-\alpha}$ for $\alpha > 1$ and at least of the order of magnitude $n_1^{-1}\log(N/n_1)$ for $\alpha = 1$. For the discrepancy $D(L)$ we have the following general lower bound.

Proposition 3. *We always have $D(L) \geq 1/n_1$.*

Proof. By the proof of Proposition 1, the coordinates of all points of $X(L)$ are rationals with denominator n_1. For $0 < \varepsilon < n_1^{-1}$ let J_ε be the interval $[\varepsilon, n_1^{-1}) \times [0, 1)^{s-1}$. Then J_ε contains no point of $X(L)$, and so

$$D(L) \geq \left|\frac{\operatorname{card}(X(L)\cap J_\varepsilon)}{N} - \operatorname{Vol}(J_\varepsilon)\right| = \operatorname{Vol}(J_\varepsilon) = \frac{1}{n_1} - \varepsilon.$$

Letting $\varepsilon \to 0+$ we get the desired result. $\square$

The bounds established in the propositions above basically carry the same information, but the consequences are displayed most clearly by Proposition 1. To assess the efficiency of a lattice rule, one has to relate the figure of merit $\rho(L)$ to the number $N = n_1 \cdots n_r$ of nodes. For lattice rules of rank $r \geq 2$, Proposition 1 says that the "relative" figure of merit $\rho(L)/N$ satisfies

$$\frac{\rho(L)}{N} \leq \frac{1}{n_2 \cdots n_r}. \tag{10}$$

We want $\rho(L)/N$ to be as large as possible for an efficient lattice rule, but (10) shows that this becomes more unlikely the larger the invariants $n_2, \ldots, n_r$. Indeed, (10) suggests that if we want to look for efficient lattice rules of rank ≥ 2, then our best bet is to consider lattice rules with large first invariant n_1. In

particular, we could consider lattice rules of rank 2 with small second invariant n_2. This is also supported by the results of the explicit search for efficient lattice rules carried out by Sloan and Walsh [20] which yielded lattice rules of precisely this type.

We will now concentrate on lattice rules of rank 2. In §3 we establish results which show the existence of lattice rules L of rank 2 for which the quantities $R_\alpha(L)$, $\alpha \geq 1$, are small, and these results are the better the smaller the invariant n_2.

3. Existence theorems for lattice rules of rank 2

We consider lattice rules which have a useful additional property, namely that of projection regularity. If L is an s-dimensional lattice rule with node set $X(L)$, then for $1 \leq d \leq s$ we define $X_d(L)$ to be the subset of $[0, 1)^d$ obtained by retaining only the first d coordinates of each point of $X(L)$. Then L is called *projection regular* if $\operatorname{card}(X_d(L)) = n_1 \cdots n_d$ for $1 \leq d \leq r$, where r is the rank and $n_1, \ldots, n_r$ are the invariants of L. A characterization of projection-regular lattice rules was given by Sloan and Lyness [19].

For lattice rules of rank 1 a general existence theorem for efficient lattice rules was established in Niederreiter [12]. It was shown that for every dimension $s \geq 2$ and every integer $N \geq 2$ there exists a projection-regular N-point lattice rule L of rank 1 with

$$R_1(L) = O(N^{-1}(\log N)^s), \tag{11}$$

where the implied constant depends only on s. This result is in fact best possible since it was proved by Larcher [7] that for any N-point lattice rule L of rank 1, $R_1(L)$ is at least of the order of magnitude $N^{-1}(\log N)^s$.

We now establish an analogous existence theorem for lattice rules of rank 2. We recall that for such lattice rules we have two invariants $n_1 > 1$ and $n_2 > 1$ with $n_2 | n_1$, and the number N of nodes is given by $N = n_1 n_2$. For a detailed discussion of lattice rules of rank 2, see Lyness and Sloan [10]. We now fix the dimension $s \geq 2$ and the invariants n_1 and n_2, and we put

$$Z_i = \{z \in \mathbf{Z} \colon 0 \leq z < n_i \text{ and } \gcd(z, n_i) = 1\} \quad \text{for } i = 1, 2.$$

Let $\mathscr{L} = \mathscr{L}(s; n_1, n_2)$ be the family of all s-dimensional lattice rules L of rank 2 with prescribed invariants n_1 and n_2 for which the node set $X(L)$ consists exactly of all fractional parts

$$\left\{\frac{k_1}{n_1}\mathbf{z}_1 + \frac{k_2}{n_2}\mathbf{z}_2\right\} \quad \text{with } 1 \leq k_1 \leq n_1,\ 1 \leq k_2 \leq n_2$$

as in (1), where $\mathbf{z}_1$ and $\mathbf{z}_2$ have the special form

$$\mathbf{z}_1 = (z_1^{(1)}, \ldots, z_1^{(s)}), \qquad \mathbf{z}_2 = (0, z_2^{(2)}, \ldots, z_2^{(s)}) \tag{12}$$

with $z_1^{(j)} \in Z_1$, $1 \leq j \leq s$, and $z_2^{(j)} \in Z_2$, $2 \leq j \leq s$. It follows immediately from [19, Theorems 2.1 and 3.3] that every lattice rule $L \in \mathscr{L}$ is projection regular. For each $L \in \mathscr{L}$ the corresponding lattice in $\mathbf{R}^s$ consists exactly of all linear combinations with integer coefficients of the vectors

$$\mathbf{b}_i = \frac{1}{n_i}\mathbf{z}_i \quad \text{for } i = 1, 2, \qquad \mathbf{b}_i = \mathbf{e}_i \quad \text{for } 3 \leq i \leq s,$$

where $\mathbf{e}_i$ is the unit vector with 1 in the ith coordinate and 0 elsewhere. Let

$$M(\mathscr{L}) = \frac{1}{\operatorname{card}(\mathscr{L})} \sum_{L \in \mathscr{L}} R_1(L)$$

be the average value of $R_1(L)$ as L runs through $\mathscr{L}$. Note that $\operatorname{card}(\mathscr{L}) = \phi(n_1)^s \phi(n_2)^{s-1}$, where ϕ is Euler's totient function.

Theorem 2. *For every dimension $s \geq 2$ and any prescribed invariants n_1 and n_2 we have*

$$M(\mathscr{L}) < c_s \left(\frac{(\log N)^s}{N} + \frac{\log N}{n_1} \right)$$

with a constant c_s depending only on s. In particular, for every $s \geq 2$ and any n_1 and n_2 there exists a projection-regular s-dimensional lattice rule L of rank 2 with invariants n_1 and n_2 such that

$$R_1(L) < c_s \left(\frac{(\log N)^s}{N} + \frac{\log N}{n_1} \right).$$

Corollary 1. *For every $s \geq 2$ and any prescribed invariants n_1 and n_2 there exists a projection-regular s-dimensional lattice rule L of rank 2 with invariants n_1 and n_2 such that*

$$R_\alpha(L) < c(s, \alpha) \left(\frac{(\log N)^s}{N} + \frac{\log N}{n_1} \right)^\alpha \quad \textit{for all } \alpha > 1,$$

where the constant $c(s, \alpha)$ depends only on s and α.

Proof. This follows from Theorems 1 and 2. □

Corollary 2. *For every $s \geq 2$ and any prescribed invariants n_1 and n_2 there exists a projection-regular s-dimensional lattice rule L of rank 2 with invariants n_1 and n_2 such that the discrepancy of the node set satisfies*

$$D(L) < c_s \left(\frac{(\log N)^s}{N} + \frac{\log N}{n_1} \right)$$

with a constant c_s depending only on s.

Proof. This follows from (6) and Theorem 2. □

These results guarantee the existence of efficient lattice rules provided that the invariant n_1 is sufficiently large, or equivalently, that the invariant n_2 is sufficiently small (if lattice rules with the same number $N = n_1 n_2$ of nodes are compared). This is in accordance with a conclusion that was reached in §2 by different arguments, namely that among lattice rules of rank 2 the most likely candidates for efficient lattice rules are those with small second invariant n_2. In view of (2) and (5), the bounds in Corollaries 1 and 2 yield information on the error bounds that can be achieved for suitable lattice rules $L \in \mathscr{L}$.

If we consider the order of magnitude of the bound for $R_1(L)$ in Theorem 2, then we observe that the first term $N^{-1}(\log N)^s$ is the same as the best possible order of magnitude of $R_1(L)$ for lattice rules of rank 1 (compare with (11) and the remarks following it). The second term $n_1^{-1} \log N$ is nearly best possible since it follows from the remarks after Proposition 2 that $R_1(L)$ is at least of the order of magnitude $n_1^{-1} \log n_2$. If $n_1 \approx n_2$ (i.e., if n_1 and n_2 are of

the same order of magnitude), then the term $n_1^{-1} \log N$ is in fact best possible, since we then have $\log N = \log(n_1 n_2) \approx \log n_2^2 \approx \log n_2$. If powers of $\log N$ are ignored, then the bounds for $R_\alpha(L)$, $\alpha > 1$, and $D(L)$ in Corollaries 1 and 2, respectively, are best possible, since $R_\alpha(L)$ and $D(L)$ are at least of the order of magnitude $n_1^{-\alpha}$ and n_1^{-1}, respectively, by results in §2.

We emphasize that Theorem 2 provides an upper bound for the *average value* of $R_1(L)$ as L runs through the family $\mathscr{L}$. This means that the bound for $R_1(L)$ in Theorem 2 is met by "random" choices of $L \in \mathscr{L}$. This has the following practical implication when searching for efficient lattice rules of rank 2 with prescribed invariants: choose lattice rules $L \in \mathscr{L}$ "at random," then there is a good chance that after a reasonably small number of trials a lattice rule can be found for which the bounds in Theorem 2 and Corollaries 1 and 2 hold. For lattice rules of rank 1 this "randomized" search procedure was already suggested by Haber [1].

The rest of the paper, which can be found in the Supplement section of this issue, is devoted to the proof of Theorem 2. In §4 we establish some auxiliary results that are needed for the proof, and in §5 we complete the proof. The basic ideas of the proof would also work for lattice rules of rank > 2, but the details become exceedingly more complicated.

Bibliography

1. S. Haber, *Parameters for integrating periodic functions of several variables*, Math. Comp. **41** (1983), 115–129.
2. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Clarendon Press, Oxford, 1960.
3. E. Hlawka, *Zur angenäherten Berechnung mehrfacher Integrale*, Monatsh. Math. **66** (1962), 140–151.
4. L. K. Hua and Y. Wang, *Applications of number theory to numerical analysis*, Springer, Berlin, 1981.
5. N. M. Korobov, *The approximate computation of multiple integrals*, Dokl. Akad. Nauk SSSR **124** (1959), 1207–1210. (Russian)
6. L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley, New York, 1974.
7. G. Larcher, *A best lower bound for good lattice points*, Monatsh. Math. **104** (1987), 45–51.
8. J. N. Lyness, *Some comments on quadrature rule construction criteria*, Numerical Integration III (H. Braß and G. Hämmerlin, eds.), ISNM85, Birkhäuser, Basel, 1988, pp. 117–129.
9. ——, *An introduction to lattice rules and their generator matrices*, IMA J. Numer. Anal. **9** (1989), 405–419.
10. J. N. Lyness and I. H. Sloan, *Some properties of rank-2 lattice rules*, Math. Comp. **53** (1989), 627–637.
11. H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), 957–1041.
12. ——, *Existence of good lattice points in the sense of Hlawka*, Monatsh. Math. **86** (1978), 203–219.
13. ——, *Quasi-Monte Carlo methods for multidimensional numerical integration*, Numerical Integration III (H. Braß and G. Hämmerlin, eds.), ISNM85, Birkhäuser, Basel, 1988, pp. 157–171.
14. H. Niederreiter and I. H. Sloan, *Lattice rules for multiple integration and discrepancy*, Math. Comp. **54** (1990), 303–312.
15. I. H. Sloan, *Lattice methods for multiple integration*, J. Comput. Appl. Math. **12/13** (1985), 131–143.

16. I. H. Sloan and P. J. Kachoyan, *Lattices for multiple integration*, Proc. Centre Math. Anal. Austral. Nat. Univ., vol. 6, Austral. Nat. Univ., Canberra, 1984, pp. 147–165.

17. ——, *Lattice methods for multiple integration: theory, error analysis and examples*, SIAM J. Numer. Anal. **24** (1987), 116–128.

18. I. H. Sloan and J. N. Lyness, *The representation of lattice quadrature rules as multiple sums*, Math. Comp. **52** (1989), 81–94.

19. ——, *Lattice rules: projection regularity and unique representations*, Math. Comp. **54** (1990), 649–660.

20. I. H. Sloan and L. Walsh, *A computer search of rank-2 lattice rules for multidimensional quadrature*, Math. Comp. **54** (1990), 281–302.

INSTITUTE FOR INFORMATION PROCESSING, AUSTRIAN ACADEMY OF SCIENCES, SONNENFELSGASSE 19, A-1010 VIENNA, AUSTRIA

E-mail address: nied@qiinfo.oeaw.ac.at

MATHEMATICS OF COMPUTATION
VOLUME 58, NUMBER 197
JANUARY 1992, PAGES S7–S16

Supplement to
THE EXISTENCE OF EFFICIENT LATTICE RULES FOR MULTIDIMENSIONAL NUMERICAL INTEGRATION

HARALD NIEDERREITER

This supplement contains the proof of Theorem 2 in the main part of the paper. In §4 we establish some auxiliary number–theoretic results that are needed for the proof, and in §5 we complete the proof. The numbering of lemmas and equations is continued from the main part and the references are to the bibliography in the main part.

4. AUXILIARY RESULTS

We need various concepts and results from number theory (see [2] as a general reference). Recall that a function F on the set $\mathbf{N}$ of positive integers is called *multiplicative* if $F(mn) = F(m)F(n)$ whenever $\gcd(m,n) = 1$. We write $\sum_{d|n}$ for a sum over all positive divisors d of $n \in \mathbf{N}$. If F and G are multiplicative functions, then the summatory function $\sum_{d|n} F(d)$ of F and the Dirichlet convolution $\sum_{d|n} F(n/d)G(d)$ of F and G are multiplicative functions of $n \in \mathbf{N}$. Let μ be the Möbius function and note that μ is multiplicative. From now on we abbreviate $\gcd(m,n)$ by (m,n). The symbol p will always denote a prime number. For $n \in \mathbf{N}$ let $e_p(n)$ be the largest exponent such that $p^{e_p(n)}|n$ (if $p \nmid n$, then $e_p(n) = 0$).

Lemma 2. *For $k, m, n \in \mathbf{N}$ we have*

$$B(k,m,n) := \sum_{d|n} \mu\left(\frac{n}{d}\right)(d,k)\left(m, \frac{d}{(d,k)}\right) = \begin{cases} \phi(n) & \text{if } n|km, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For $d \in \mathbf{N}$ we have

$$(d, km) = (d,k)\left(\frac{d}{(d,k)}, \frac{k}{(d,k)}m\right) = (d,k)\left(\frac{d}{(d,k)}, m\right) \tag{13}$$

since $d/(d,k)$ and $k/(d,k)$ are coprime. Therefore,

$$B(k,m,n) = \sum_{d|n} \mu\left(\frac{n}{d}\right)(d, km).$$

For $b \in \mathbf{N}$ we have

$$B(k,m,p^b) = (p^b, km) - (p^{b-1}, km),$$

hence $B(k,m,p^b) = p^b - p^{b-1} = \phi(p^b)$ if $p^b | km$, and $B(k,m,p^b) = 0$ otherwise. For fixed $k, m \in \mathbf{N}$ we note that (d, km) is a multiplicative function of d, thus $B(k,m,n)$ is a multiplicative function of n as a Dirichlet convolution of multiplicative functions, and so the result follows. □

Lemma 3. *For $k_1, k_2, n_1, n_2 \in \mathbf{N}$ let*

$$T(k_1,k_2,n_1,n_2) = \sum_{d_1|n_1} \sum_{d_2|n_2} \mu\left(\frac{n_1}{d_1}\right)\mu\left(\frac{n_2}{d_2}\right)(d_1,k_1)(d_2,k_2)\left(\frac{d_1}{(d_1,k_1)}, \frac{d_2}{(d_2,k_2)}\right).$$

Put $Q_1 = n_1/(n_1,k_1)$ and $Q_2 = n_2/(n_2,k_2)$. Then

$$T(k_1,k_2,n_1,n_2) = \begin{cases} \frac{\phi(n_1)\phi(n_2)}{\phi(Q_1)} & \text{if } Q_1 = Q_2, \\ 0 & \text{if } Q_1 \neq Q_2. \end{cases}$$

Proof. Write T for $T(k_1,k_2,n_1,n_2)$. With the notation in Lemma 2 we get

$$T = \sum_{d_1|n_1} \mu\left(\frac{n_1}{d_1}\right)(d_1,k_1)B\left(k_2, \frac{d_1}{(d_1,k_1)}, n_2\right). \tag{14}$$

According to Lemma 2, we only get a contribution to this sum if n_2 divides $k_2 d_1/(d_1,k_1)$, or equivalently, if Q_2 divides $d_1/(d_1,k_1)$. For any $d_1|n_1$ and any p we have

$$e_p\left(\frac{d_1}{(d_1,k_1)}\right) = \max(e_p(d_1) - e_p(k_1), 0) \leq \max(e_p(n_1) - e_p(k_1), 0) = e_p(Q_1),$$

hence $d_1/(d_1,k_1)$ divides Q_1. Thus, if $Q_2 \nmid Q_1$, then there is no contribution to the sum in (14), and so $T = 0$. Since $T = T(k_2,k_1,n_2,n_1)$, it follows that $T = 0$ if $Q_1 \nmid Q_2$. The only remaining case is $Q_2|Q_1$ and $Q_1|Q_2$, i.e., $Q_1 = Q_2$. If $Q_1 = Q_2$, then we only get a contribution to the sum in (14) if Q_1 divides $d_1/(d_1,k_1)$, but since $d_1/(d_1,k_1)$ always divides Q_1, we must have $d_1/(d_1,k_1) = Q_1$. Put $a_p = e_p(n_1), b_p = e_p(k_1)$, and

$$m_1 = \prod_{\substack{p \\ a_p > b_p}} p^{a_p}, \quad m_2 = \prod_{\substack{p \\ a_p \leq b_p}} p^{a_p},$$

so that $n_1 = m_1 m_2$. Then the conditions $d_1|n_1$ and $d_1/(d_1,k_1) = Q_1$ hold if and only if $e_p(d_1) \leq a_p$ and

$$\max(e_p(d_1) - b_p, 0) = \max(a_p - b_p, 0)$$

for all p. These conditions are equivalent to the following: $e_p(d_1) \leq a_p$ for all p and $e_p(d_1) = a_p$ whenever $a_p > b_p$. This is in turn equivalent to $d_1 = m_1 d$ with $d|m_2$. We apply this information to (14). We also use Lemma 2 and the fact that $d_1/(d_1,k_1) = Q_1$ implies $(d_1,k_1) = d_1/Q_1$. Then

$$\begin{aligned} T &= \phi(n_2) \sum_{d|m_2} \mu\left(\frac{n_1}{m_1 d}\right)\frac{m_1 d}{Q_1} = \frac{\phi(n_2)n_1}{Q_1} \sum_{d|m_2} \mu\left(\frac{m_2}{d}\right)\frac{d}{m_2} \\ &= \frac{\phi(n_2)n_1}{Q_1} \sum_{d|m_2} \frac{\mu(d)}{d} = \frac{\phi(n_2)n_1}{Q_1} \prod_{p|m_2}\left(1 - \frac{1}{p}\right). \end{aligned}$$

Now $p|m_2$ if and only if $0 < a_p \leq b_p$, and the latter is equivalent to $p|n_1$ and $p \nmid Q_1$. Using $\prod_{p|n}(1 - p^{-1}) = \phi(n)/n$ for $n \in \mathbf{N}$, we get

$$\prod_{p|m_2}\left(1 - \frac{1}{p}\right) = \frac{\phi(n_1)Q_1}{n_1\phi(Q_1)},$$

whence the formula for T in the case $Q_1 = Q_2$. □

Recall that a function G on $\mathbf{N}$ is called ***additive*** if $G(mn) = G(m) + G(n)$ whenever $(m,n) = 1$. Note that if F is a multiplicative function which only attains positive values, then $\log F$ is additive.

Lemma 4. *Let F be a multiplicative and G an additive function, and put*

$$H(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right)F(d)G(d) \quad \text{for} \quad n \in \mathbf{N},$$

$$J(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right)F(d) \quad \text{for} \quad n \in \mathbf{N}.$$

Then for all $n \in \mathbf{N}$ we have

$$H(n) = \sum_{p|n} H(p^{e_p(n)})J(n/p^{e_p(n)}). \tag{15}$$

Proof. For $m, n \in \mathbf{N}$ with $(m,n) = 1$ we have

$$\begin{aligned} H(mn) &= \sum_{d|mn} \mu\left(\frac{mn}{d}\right)F(d)G(d) = \sum_{\substack{d_1|m \\ d_2|n}} \mu\left(\frac{mn}{d_1 d_2}\right)F(d_1 d_2)G(d_1 d_2) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} \mu\left(\frac{m}{d_1}\right)\mu\left(\frac{n}{d_2}\right)F(d_1)F(d_2)(G(d_1) + G(d_2)) \\ &= \sum_{d_1|m} \mu\left(\frac{m}{d_1}\right)F(d_1)G(d_1)\sum_{d_2|n} \mu\left(\frac{n}{d_2}\right)F(d_2) + \sum_{d_2|n} \mu\left(\frac{n}{d_2}\right)F(d_2)G(d_2)\sum_{d_1|m} \mu\left(\frac{m}{d_1}\right)F(d_1), \end{aligned}$$

and so

$$H(mn) = H(m)J(n) + H(n)J(m). \tag{16}$$

Now $H(1) = F(1)G(1) = 0$ since $G(1) = 0$, and so (15) holds for $n = 1$ (recall that an empty sum is 0 by convention). We obtain (15) for all $n \in \mathbf{N}$ by proceeding by induction on the number of distinct prime divisors of n and using (16) and the fact that J is multiplicative. □

Lemma 5. *For $k, n \in \mathbf{N}$ put*

$$H(k,n) = \sum_{d|n} \mu\left(\frac{n}{d}\right)(d,k)\log\frac{d}{(d,k)}.$$

If there is a unique prime q such that $e_q(n) > e_q(k)$, then

$$H(k,n) = q^{e_q(k)}\phi(n/q^{e_q(n)})\log q.$$

Otherwise we have $H(k,n) = 0$.

Proof. Fix k and note that (d,k) is a multiplicative and $\log(d/(d,k))$ an additive function of d. We have

$$\sum_{d|n} \mu\left(\frac{n}{d}\right)(d,k) = B(k,1,n)$$

with the notation in Lemma 2. Thus, Lemma 4 yields

$$H(k,n) = \sum_{p|n} H(k,p^{e_p(n)})B(k,1,n/p^{e_p(n)}). \tag{17}$$

For $b \in \mathbf{N}$ we obtain

$$H(k,p^b) = (p^b,k)\log\frac{p^b}{(p^b,k)} - (p^{b-1},k)\log\frac{p^{b-1}}{(p^{b-1},k)}.$$

If $b \le e_p(k)$, then $(p^b,k) = p^b$ and $(p^{b-1},k) = p^{b-1}$, hence $H(k,p^b) = 0$. If $b > e_p(k)$, then $(p^b,k) = (p^{b-1},k) = p^{e_p(k)}$, hence $H(k,p^b) = p^{e_p(k)}\log p$. Using also Lemma 2, (17) reduces to

$$H(k,n) = \sum_p p^{e_p(k)}\phi(n/p^{e_p(n)})\log p, \tag{18}$$

where the sum runs over all p satisfying the following two conditions: (i) $e_p(n) > e_p(k)$; (ii) $n/p^{e_p(n)}$ divides k. Note that (ii) means $e_{p_1}(n) \le e_{p_1}(k)$ for all primes $p_1 \ne p$. Therefore, (i) and (ii) can hold simultaneously only in the case where there is a unique prime q with $e_q(n) > e_q(k)$, and in this case (i) and (ii) hold for $p = q$ and for no other prime. Thus, if there is a unique prime q with $e_q(n) > e_q(k)$, then the sum in (18) reduces to a single term with $p = q$, and in all other cases the sum in (18) is empty. □

Lemma 6. *For $k, m, n \in \mathbf{N}$ put*

$$E(k,m,n) = \sum_{d|n} \mu\left(\frac{n}{d}\right)(d,km)\log(m,\frac{d}{(d,k)}).$$

Then $E(k,m,n) = 0$ if $n \nmid km$. If $n|km$, then

$$E(k,m,n) = \phi(n)\log\left(\prod_p p^{e_p(n)-e_p(k)}\right) + \phi(n)\sum_p \frac{\log p}{p-1},$$

where the product and the sum are extended over all p with $e_p(n) > e_p(k)$.

Proof. Fix k and m and note that (d,km) is a multiplicative and $\log(m, d/(d,k))$ an additive function of d. We have

$$\sum_{d|n} \mu\left(\frac{n}{d}\right)(d,km) = B(km,1,n)$$

with the notation in Lemma 2. Thus, Lemma 4 yields

$$E(k,m,n) = \sum_{p|n} E(k,m,p^{e_p(n)})B(km,1,n/p^{e_p(n)}). \tag{19}$$

For $b \in \mathbf{N}$ we have

$$E(k,m,p^b) = (p^b,km)\log\left(m,\frac{p^b}{(p^b,k)}\right) - (p^{b-1},km)\log\left(m,\frac{p^{b-1}}{(p^{b-1},k)}\right).$$

If $b \le e_p(k)$, then $(p^b,k) = p^b$ and $(p^{b-1},k) = p^{b-1}$, hence $E(k,m,p^b) = 0$. If $b > e_p(km)$, then $(p^b,k) = (p^{b-1},k) = p^{e_p(k)}$ and

$$\left(m,\frac{p^b}{(p^b,k)}\right) = \left(m,\frac{p^{b-1}}{(p^{b-1},k)}\right) = p^{e_p(m)},$$

hence

$$E(k,m,p^b) = p^{e_p(km)}\log p^{e_p(m)} - p^{e_p(km)}\log p^{e_p(m)} = 0.$$

If $e_p(k) < b \le e_p(km)$, then $(p^b,k) = (p^{b-1},k) = p^{e_p(k)}$ and

$$\left(m,\frac{p^b}{(p^b,k)}\right) = p^{b-e_p(k)}, \quad \left(m,\frac{p^{b-1}}{(p^{b-1},k)}\right) = p^{b-1-e_p(k)},$$

hence

$$\begin{aligned}E(k,m,p^b) &= p^b \log p^{b-e_p(k)} - p^{b-1}\log p^{b-1-e_p(k)}\\ &= (p^b - p^{b-1})\log p^{b-e_p(k)} + p^{b-1}(\log p^{b-e_p(k)} - \log p^{b-1-e_p(k)})\\ &= \phi(p^b)\log p^{b-e_p(k)} + p^{b-1}\log p\\ &= \phi(p^b)(\log p^{b-e_p(k)} + \frac{\log p}{p-1}).\end{aligned}$$

Using also Lemma 2, we conclude that (19) reduces to

$$\begin{aligned}E(k,m,n) &= \sum_p \phi(p^{e_p(n)})(\log p^{e_p(n)-e_p(k)} + \frac{\log p}{p-1})\phi(n/p^{e_p(n)})\\ &= \phi(n)\sum_p(\log p^{e_p(n)-e_p(k)} + \frac{\log p}{p-1}),\end{aligned}$$

where the sum is over all p satisfying the following two conditions: (i) $e_p(k) < e_p(n) \le e_p(km)$; (ii) $n/p^{e_p(n)}$ divides km. Note that (i) implies that $p^{e_p(n)}$ divides km. Thus, if there exists a p satisfying (i) and (ii), then we must have $n|\ddot{\cdot}m$. Therefore, $E(k,m,n) = 0$ if $n\not|km$. If $n|km$, then (i) reduces to $e_p(n) > e_p(k)$, whereas (ii) holds automatically. The desired result now follows. □

We write $[m,n]$ for the least common multiple of $m,n \in \mathbf{N}$ and note that $[m,n] = mn/(m,n)$.

Lemma 7. *For $k_1,k_2,n_1,n_2 \in \mathbf{N}$ let*

$$V(k_1,k_2,n_1,n_2) = \\ = \sum_{d_1|n_1}\sum_{d_2|n_2}\mu\left(\frac{n_1}{d_1}\right)\mu\left(\frac{n_2}{d_2}\right)(d_1,k_1)(d_2,k_2)\left(\frac{d_1}{(d_1,k_1)},\frac{d_2}{(d_2,k_2)}\right)\log\left[\frac{d_1}{(d_1,k_1)},\frac{d_2}{(d_2,k_2)}\right].$$

Let Q_1 and Q_2 be as in Lemma 3. Then

$$V(k_1,k_2,n_1,n_2) = \frac{\phi(n_1)\phi(n_2)}{\phi(Q_1)}(\log Q_1 - \sum_{p|Q_1}\frac{\log p}{p-1}) \quad if \quad Q_1 = Q_2.$$

If there is a unique prime q such that $e_q(Q_1) \ne e_q(Q_2)$, then

$$V(k_1,k_2,n_1,n_2) = \frac{\phi(n_1)\phi(n_2)}{\phi(Q_j)}\log q,$$

where $j \in \{1,2\}$ is such that $e_q(Q_j) = \max(e_q(Q_1),e_q(Q_2))$. In all other cases we have $V(k_1,k_2,n_1,n_2) = 0$.

Proof. Using $[m,n] = mn/(m,n)$, we get

$$V(k_1,k_2,n_1,n_2) = V_1(k_1,k_2,n_1,n_2) + V_2(k_1,k_2,n_1,n_2) - V_3(k_1,k_2,n_1,n_2), \tag{20}$$

where

$$V_1(k_1,k_2,n_1,n_2) = \\ = \sum_{d_1|n_1}\sum_{d_2|n_2}\mu\left(\frac{n_1}{d_1}\right)\mu\left(\frac{n_2}{d_2}\right)(d_1,k_1)(d_2,k_2)\left(\frac{d_1}{(d_1,k_1)},\frac{d_2}{(d_2,k_2)}\right)\log\frac{d_1}{(d_1,k_1)},$$

$$V_2(k_1,k_2,n_1,n_2) = V_1(k_2,k_1,n_2,n_1),$$

$$V_3(k_1,k_2,n_1,n_2) = \\ \sum_{d_1|n_1}\sum_{d_2|n_2}\mu\left(\frac{n_1}{d_1}\right)\mu\left(\frac{n_2}{d_2}\right)(d_1,k_1)(d_2,k_2)\left(\frac{d_1}{(d_1,k_1)},\frac{d_2}{(d_2,k_2)}\right)\log\left(\frac{d_1}{(d_1,k_1)},\frac{d_2}{(d_2,k_2)}\right).$$

Abbreviate $V_1(k_1,k_2,n_1,n_2)$ by V_1. Then

$$\begin{aligned}V_1 &= \sum_{d_1|n_1}\mu\left(\frac{n_1}{d_1}\right)(d_1,k_1)\left(\log\frac{d_1}{(d_1,k_1)}\right)\sum_{d_2|n_2}\mu\left(\frac{n_2}{d_2}\right)(d_2,k_2)\left(\frac{d_1}{(d_1,k_1)},\frac{d_2}{(d_2,k_2)}\right)\\ &= \sum_{d_1|n_1}\mu\left(\frac{n_1}{d_1}\right)(d_1,k_1)B\left(k_2,\frac{d_1}{(d_1,k_1)},n_2\right)\log\frac{d_1}{(d_1,k_1)}\end{aligned}$$

with the notation in Lemma 2. According to Lemma 2, we only get a contribution to the last sum if n_2 divides $k_2d_1/(d_1,k_1)$, or equivalently, if Q_2 divides $d_1/(d_1,k_1)$. In the proof of Lemma 3 we have seen that $d_1/(d_1,k_1)$ divides Q_1. Therefore, $V_1 = 0$ if $Q_2\not|Q_1$. Now let $Q_2|Q_1$. Using again Lemma 2, we obtain

$$V_1 = \phi(n_2)\sum_{d_1}\mu\left(\frac{n_1}{d_1}\right)(d_1,k_1)\log\frac{d_1}{(d_1,k_1)}, \tag{21}$$

where the sum is over all $d_1|n_1$ such that Q_2 divides $d_1/(d_1,k_1)$. Now Q_2 divides $d_1/(d_1,k_1)$ if and only if

$$e_p(Q_2) + e_p(k_1) \le e_p(d_1) \quad \text{for all} \quad p|Q_2.$$

This is equivalent to $t|d_1$ with

$$t = \prod_{p|Q_2} p^{e_p(Q_2)+e_p(k_1)}. \tag{22}$$

We note that

$$t_1 := \frac{n_1}{t} = \prod_{p\not|Q_2} p^{e_p(n_1)}\prod_{p|Q_2} p^{e_p(n_1)-e_p(k_1)-e_p(Q_2)} = \prod_{p\not|Q_2} p^{e_p(n_1)}\prod_{p|Q_2} p^{e_p(Q_1)-e_p(Q_2)} \tag{23}$$

is a positive integer. Therefore, the sum in (21) is over all $d_1 = td$ with $d|t_1$, hence

$$V_1 = \phi(n_2)\sum_{d|t_1}\mu\left(\frac{t_1}{d}\right)(td,k_1)\log\frac{td}{(td,k_1)}.$$

By (13) we can write

$$(td,k_1) = (t,k_1)\left(d,\frac{k_1}{(t,k_1)}\right),$$

so that with $k := k_1/(t,k_1)$ we get

$$\begin{aligned} V_1 &= \phi(n_2)(t,k_1)\sum_{d|t_1}\mu\left(\frac{t_1}{d}\right)(d,k)\left(\log\frac{t}{(t,k_1)}+\log\frac{d}{(d,k)}\right) \\ &= \phi(n_2)(t,k_1)B(k,1,t_1)\log\frac{t}{(t,k_1)} + \phi(n_2)(t,k_1)H(k,t_1) =: V_4 + V_5 \end{aligned}$$

with the notation in Lemma 5. By Lemma 2 we have $B(k,1,t_1) \neq 0$ if and only if $t_1|k$. Now from (22),

$$k = \frac{k_1}{(t,k_1)} = \prod_{p\nmid Q_2} p^{e_p(k_1)}, \tag{24}$$

and so a comparison with (23) shows that $t_1|k$ if and only if $e_p(Q_1) = e_p(Q_2)$ for all $p|Q_2$ and $e_p(n_1) \le e_p(k_1)$ for all $p\nmid Q_2$. But $e_p(n_1) \le e_p(k_1)$ is equivalent to $e_p(Q_1) = 0$, and so $t_1|k$ if and only if $Q_1 = Q_2$. Thus, $V_4 = 0$ if $Q_1 \neq Q_2$. If $Q_1 = Q_2$, then

$$V_4 = \phi(n_2)(t,k_1)\phi(t_1)\log\frac{t}{(t,k_1)} = \phi(n_2)(t,k_1)\phi(t_1)\log Q_1,$$

and from (22) and (23) we get

$$\begin{aligned} (t,k_1)\phi(t_1) &= \prod_{p|Q_1} p^{e_p(k_1)}\cdot\phi\left(\prod_{p\nmid Q_1} p^{e_p(n_1)}\right) \\ &= \frac{1}{Q_1}\prod_{p|Q_1} p^{e_p(n_1)}\prod_{p\nmid Q_1} p^{e_p(n_1)}\prod_{p|n_1, p\nmid Q_1}\left(1-\frac{1}{p}\right) = \frac{n_1}{Q_1}\prod_{p|m_2}\left(1-\frac{1}{p}\right), \end{aligned}$$

where m_2 is as in the proof of Lemma 3. In that proof we have shown that

$$\prod_{p|m_2}\left(1-\frac{1}{p}\right) = \frac{\phi(n_1)Q_1}{n_1\phi(Q_1)},$$

and so it follows that

$$(t,k_1)\phi(t_1) = \frac{\phi(n_1)}{\phi(Q_1)}. \tag{25}$$

Thus, we have

$$V_4 = \begin{cases} \frac{\phi(n_1)\phi(n_2)}{\phi(Q_1)}\log Q_1 & \text{if } Q_1 = Q_2, \\ 0 & \text{if } Q_2|Q_1, Q_1 \neq Q_2. \end{cases} \tag{26}$$

Now we consider V_5 for $Q_2|Q_1$. By Lemma 5 we have $H(k,t_1) \neq 0$ if and only if there is a unique prime q such that $e_q(t_1) > e_q(k)$. A comparison of (23) and (24) shows that if $p|Q_2$, then $e_p(t_1) > e_p(k)$ if and only if $e_p(Q_1) - e_p(Q_2) > 0$, and if $p\nmid Q_2$, then $e_p(t_1) > e_p(k)$ if and only if $e_p(n_1) > e_p(k_1)$. Note that $e_p(n_1) > e_p(k_1)$ is equivalent to $e_p(Q_1) > 0$. Therefore, for any p it is true that $e_p(t_1) > e_p(k)$ if and only if $e_p(Q_1) > e_p(Q_2)$. Consequently, the condition that there is a unique prime q such that $e_q(t_1) > e_q(k)$ is equivalent to the existence of a unique prime q (indeed, the same prime q) such that $e_q(Q_1) > e_q(Q_2)$. Thus, if this condition is not met, then $V_5 = 0$. If this condition is met, then the formula for $H(k,t_1)$ in Lemma 5 yields

$$V_5 = \phi(n_2)(t,k_1)q^{e_q(k)}\phi(t_1/q^{e_q(t_1)})\log q.$$

In the case under consideration we have $e_q(Q_1) > e_q(Q_2)$ and $e_p(Q_1) \le e_p(Q_2)$ for all $p \neq q$, but since $Q_2|Q_1$, it follows that $e_p(Q_1) = e_p(Q_2)$ for all $p \neq q$. By distinguishing the cases $q|Q_2$ and $q\nmid Q_2$, we deduce from (22), (23), and (24) that

$$(t,k_1)q^{e_q(k)} = \prod_{p|Q_1} p^{e_p(k_1)},$$

$$t_1/q^{e_q(t_1)} = \prod_{p\nmid Q_1} p^{e_p(n_1)}.$$

Thus, by the calculation leading to (25) we obtain

$$(t,k_1)q^{e_q(k)}\phi(t_1/q^{e_q(t_1)}) = \prod_{p|Q_1} p^{e_p(k_1)}\cdot\phi\left(\prod_{p\nmid Q_1} p^{e_p(n_1)}\right) = \frac{\phi(n_1)}{\phi(Q_1)},$$

and so

$$V_5 = \frac{\phi(n_1)\phi(n_2)}{\phi(Q_1)}\log q$$

if there is a unique prime q such that $e_q(Q_1) > e_q(Q_2)$. We recall that $V_5 = 0$ if this condition is not satisfied, and we combine this information with (26). Then we get the following formulas for $V_1 = V_4 + V_5$, where we also recall that $V_1 = 0$ if $Q_2\nmid Q_1$:

$$V_1 = \frac{\phi(n_1)\phi(n_2)}{\phi(Q_1)}\log Q_1 \quad \text{if} \quad Q_1 = Q_2,$$

$$V_1 = \frac{\phi(n_1)\phi(n_2)}{\phi(Q_1)} \log q$$

if there is a (unique) prime q such that $e_q(Q_1) > e_q(Q_2)$ and $e_p(Q_1) = e_p(Q_2)$ for all $p \neq q$, and $V_1 = 0$ in all other cases. Using $V_2(k_1, k_2, n_1, n_2) = V_1(k_2, k_1, n_2, n_1)$ and abbreviating $V_2(k_1, k_2, n_1, n_2)$ by V_2, we get the following formulas:

$$V_2 = \frac{\phi(n_1)\phi(n_2)}{\phi(Q_1)} \log Q_1 \quad \text{if} \quad Q_1 = Q_2,$$

$$V_2 = \frac{\phi(n_1)\phi(n_2)}{\phi(Q_2)} \log q$$

if there is a (unique) prime q such that $e_q(Q_2) > e_q(Q_1)$ and $e_p(Q_1) = e_p(Q_2)$ for all $p \neq q$, and $V_2 = 0$ in all other cases.

We consider now $V_3(k_1, k_2, n_1, n_2)$, which we abbreviate by V_3. Using (13), we can write

$$\begin{aligned} V_3 &= \sum_{d_1|n_1} \mu\left(\frac{n_1}{d_1}\right)(d_1, k_1) \sum_{d_2|n_2} \mu\left(\frac{n_2}{d_2}\right)\left(d_2, \frac{k_2 d_1}{(d_1, k_1)}\right) \log\left(\frac{d_1}{(d_1, k_1)}, \frac{d_2}{(d_2, k_2)}\right) \\ &= \sum_{d_1|n_1} \mu\left(\frac{n_1}{d_1}\right)(d_1, k_1) E\left(k_2, \frac{d_1}{(d_1, k_1)}, n_2\right) \end{aligned}$$

with the notation in Lemma 6. According to Lemma 6, we only get a contribution to the last sum if n_2 divides $k_2 d_1/(d_1, k_1)$, or equivalently, if Q_2 divides $d_1/(d_1, k_1)$. In the proof of Lemma 3 we have shown that $d_1/(d_1, k_1)$ divides Q_1. Therefore, $V_3 = 0$ if $Q_2 \nmid Q_1$. From the definition of V_3 at the beginning of the proof of Lemma 7 we see that $V_3 = V_3(k_2, k_1, n_2, n_1)$, thus $V_3 = 0$ if $Q_1 \nmid Q_2$. Hence $V_3 = 0$ if $Q_1 \neq Q_2$, and it remains to consider the case $Q_1 = Q_2$. In this case we only get a contribution to the last sum if $d_1/(d_1, k_1) = Q_1$, and noting that then $(d_1, k_1) = d_1/Q_1$, we obtain

$$V_3 = \frac{1}{Q_1} E(k_2, Q_1, n_2) \sum_{d_1} \mu\left(\frac{n_1}{d_1}\right) d_1,$$

where the sum is over all $d_1|n_1$ with $d_1/(d_1, k_1) = Q_1$. In the proof of Lemma 3 we have shown that these conditions on d_1 are equivalent to $d_1 = m_1 d$ with $d|m_2$. Therefore,

$$\begin{aligned} V_3 &= \frac{m_1}{Q_1} E(k_2, Q_1, n_2) \sum_{d|m_2} \mu\left(\frac{m_2}{d}\right) d \\ &= \frac{m_1}{Q_1} E(k_2, Q_1, n_2) \sum_{d|m_2} \mu(d) \frac{m_2}{d} \\ &= \frac{n_1}{Q_1} E(k_2, Q_1, n_2) \prod_{p|m_2} \left(1 - \frac{1}{p}\right). \end{aligned}$$

The last product was evaluated in the proof of Lemma 3, hence

$$V_3 = \frac{\phi(n_1)}{\phi(Q_1)} E(k_2, Q_1, n_2).$$

By Lemma 6 we have

$$E(k_2, Q_1, n_2) = \phi(n_2) \log\left(\prod_p p^{e_p(n_2) - e_p(k_2)}\right) + \phi(n_2) \sum_p \frac{\log p}{p-1},$$

where the product and the sum run over all p with $e_p(n_2) > e_p(k_2)$. Note that $e_p(n_2) > e_p(k_2)$ if and only if $p|Q_2 = Q_1$, and that

$$\prod_p p^{e_p(n_2) - e_p(k_2)} = \prod_{p|Q_2} p^{e_p(Q_2)} = Q_2 = Q_1.$$

Thus, we have shown

$$V_3 = \frac{\phi(n_1)\phi(n_2)}{\phi(Q_1)} \left(\log Q_1 + \sum_{p|Q_1} \frac{\log p}{p-1}\right) \quad \text{if} \quad Q_1 = Q_2$$

and $V_3 = 0$ if $Q_1 \neq Q_2$. Using (20) and the formulas for V_1, V_2, and V_3 above, we get the desired result. □

Lemma 8. *For $k_1, k_2, n_1, n_2 \in \mathbf{N}$ with $n_2|n_1$ let*

$$Y(k_1, k_2, n_1, n_2) = \sum_{d_1|n_1} \sum_{d_2|n_2} |\mu\left(\frac{n_1}{d_1}\right) \mu\left(\frac{n_2}{d_2}\right)| d_1 d_2 \left[\frac{d_1}{(d_1, k_1)}, \frac{d_2}{(d_2, k_2)}\right].$$

Then we have

$$Y(k_1, k_2, n_1, n_2) \leq \frac{n_1^3 n_2^2}{\phi(n_1)\phi(n_2)}.$$

Proof. It is clear that $[d_1/(d_1, k_1), d_2/(d_2, k_2)]$ divides n_1; therefore,

$$\begin{aligned} Y(k_1, k_2, n_1, n_2) &\leq n_1 \sum_{d_1|n_1} \sum_{d_2|n_2} |\mu\left(\frac{n_1}{d_1}\right) \mu\left(\frac{n_2}{d_2}\right)| d_1 d_2 \\ &= n_1^2 n_2 F(n_1) F(n_2) \end{aligned}$$

with

$$F(n) = \sum_{d|n} \frac{|\mu(d)|}{d} \quad \text{for} \quad n \in \mathbf{N}.$$

Now F is a multiplicative function as the summatory function of a multiplicative function. For $b \in \mathbf{N}$ we have

$$F(p^b) = \frac{p+1}{p} \leq \frac{p}{p-1} = \frac{p^b}{\phi(p^b)},$$

hence $F(n) \leq n/\phi(n)$ for all $n \in \mathbf{N}$. This implies the desired result. □

5. PROOF OF THEOREM 2

We fix the dimension $s \geq 2$ and the invariants $n_1, n_2 \in \mathbf{N}$ with $n_1 > 1, n_2 > 1$, and $n_2 | n_1$. For the family $\mathcal{L} = \mathcal{L}(s; n_1, n_2)$ we then have

$$M(\mathcal{L}) = \frac{1}{\operatorname{card}(\mathcal{L})} \sum_{L \in \mathcal{L}} R_1(L) = \frac{1}{\operatorname{card}(\mathcal{L})} \sum_{L \in \mathcal{L}} \sum_{\mathbf{h} \in E(L)} r(\mathbf{h})^{-1},$$

where $E(L)$ is as in Definition 3. Interchanging the order of summation, we get

$$M(\mathcal{L}) = \frac{1}{\operatorname{card}(\mathcal{L})} \sum_{\mathbf{h} \in C_s^*(N)} A(\mathbf{h}) r(\mathbf{h})^{-1},$$

where $N = n_1 n_2$ and $A(\mathbf{h})$ is the number of $L \in \mathcal{L}$ with $\mathbf{h} \in L^\perp$. Since $A(\mathbf{0}) = \operatorname{card}(\mathcal{L})$, we obtain

$$M(\mathcal{L}) = \frac{1}{\operatorname{card}(\mathcal{L})} \sum_{\mathbf{h} \in C_s(N)} A(\mathbf{h}) r(\mathbf{h})^{-1} - 1. \tag{27}$$

We write $e(t) = e^{2\pi\sqrt{-1}t}$ for real t. Then by [17, Theorem 1] we have for $\mathbf{h} \in \mathbf{Z}^s$:

$$\frac{1}{N} \sum_{\mathbf{x} \in X(L)} e(\mathbf{h} \cdot \mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{h} \in L^\perp, \\ 0 & \text{if } \mathbf{h} \notin L^\perp. \end{cases}$$

Therefore,

$$A(\mathbf{h}) = \frac{1}{N} \sum_{L \in \mathcal{L}} \sum_{\mathbf{x} \in X(L)} e(\mathbf{h} \cdot \mathbf{x}).$$

For $L \in \mathcal{L}$ the node set $X(L)$ has the special form described in §3. Using also the special form of $\mathbf{z}_1$ and $\mathbf{z}_2$ in (12), we get

$$\begin{aligned} \sum_{\mathbf{x} \in X(L)} e(\mathbf{h} \cdot \mathbf{x}) &= \sum_{k_1=1}^{n_1} \sum_{k_2=1}^{n_2} e\left(\mathbf{h} \cdot \left(\frac{k_1}{n_1}\mathbf{z}_1 + \frac{k_2}{n_2}\mathbf{z}_2\right)\right) \\ &= \sum_{k_1=1}^{n_1} \sum_{k_2=1}^{n_2} e\left(\sum_{i=1}^{2} \sum_{j=i}^{s} \frac{k_i}{n_i} h_j z_i^{(j)}\right), \end{aligned}$$

where $\mathbf{h} = (h_1, \ldots, h_s)$. It follows that

$$\begin{aligned} A(\mathbf{h}) &= \frac{1}{N} \sum_{z_1^{(1)}, \ldots, z_1^{(s)} \in Z_1} \sum_{z_2^{(2)}, \ldots, z_2^{(s)} \in Z_2} \sum_{k_1=1}^{n_1} \sum_{k_2=1}^{n_2} e\left(\sum_{i=1}^{2} \sum_{j=i}^{s} \frac{k_i}{n_i} h_j z_i^{(j)}\right) \\ &= \frac{1}{N} \sum_{k_1=1}^{n_1} \sum_{k_2=1}^{n_2} \sum_{z_1^{(1)}, \ldots, z_1^{(s)} \in Z_1} \sum_{z_2^{(2)}, \ldots, z_2^{(s)} \in Z_2} \prod_{i=1}^{2} \prod_{j=i}^{s} e\left(\frac{k_i}{n_i} h_j z_i^{(j)}\right) \\ &= \frac{1}{N} \sum_{k_1=1}^{n_1} \sum_{k_2=1}^{n_2} \prod_{i=1}^{2} \prod_{j=i}^{s} \left(\sum_{z \in Z_i} e\left(\frac{k_i}{n_i} h_j z\right)\right) \\ &= \frac{1}{N} \sum_{k_1=1}^{n_1} \sum_{k_2=1}^{n_2} \prod_{j=1}^{s} \prod_{i=1}^{\min(j,2)} \left(\sum_{z \in Z_i} e\left(\frac{k_i}{n_i} h_j z\right)\right). \end{aligned}$$

Therefore,

$$\begin{aligned} \sum_{\mathbf{h} \in C_s(N)} \frac{A(\mathbf{h})}{r(\mathbf{h})} &= \frac{1}{N} \sum_{k_1=1}^{n_1} \sum_{k_2=1}^{n_2} \sum_{h_1, \ldots, h_s \in C(N)} \frac{1}{r(h_1) \ldots r(h_s)} \prod_{j=1}^{s} \prod_{i=1}^{\min(j,2)} \left(\sum_{z \in Z_i} e\left(\frac{k_i}{n_i} h_j z\right)\right) \\ &= \frac{1}{N} \sum_{k_1=1}^{n_1} \sum_{k_2=1}^{n_2} \prod_{j=1}^{s} \left(\sum_{h \in C(N)} \frac{1}{r(h)} \prod_{i=1}^{\min(j,2)} \left(\sum_{z \in Z_i} e\left(\frac{k_i}{n_i} h z\right)\right)\right). \end{aligned} \tag{28}$$

Now we use

$$\sum_{d | n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1, \end{cases}$$

and we obtain

$$\begin{aligned} \sum_{z \in Z_i} e\left(\frac{k_i}{n_i} h z\right) &= \sum_{z=0}^{n_i - 1} e\left(\frac{k_i}{n_i} h z\right) \sum_{d | (z, n_i)} \mu(d) = \sum_{d | n_i} \mu(d) \sum_{\substack{z=0 \\ d | z}}^{n_i - 1} e\left(\frac{k_i}{n_i} h z\right) \\ &= \sum_{d | n_i} \mu(d) \sum_{a=0}^{(n_i/d) - 1} e\left(\frac{k_i}{n_i} h d a\right) = \sum_{d | n_i} \mu\left(\frac{n_i}{d}\right) \sum_{a=0}^{d-1} e\left(\frac{k_i}{d} h a\right), \end{aligned}$$

where in the last step we changed the summation variable from d to n_i/d. The last inner sum has the value d if $d | k_i h$ and the value 0 otherwise. Thus,

$$\sum_{z \in Z_i} e\left(\frac{k_i}{n_i} h z\right) = \sum_{\substack{d | n_i \\ d | k_i h}} \mu\left(\frac{n_i}{d}\right) d.$$

If $h = 0$, then the sum on the left-hand side trivially has the value $\phi(n_i)$. Therefore, we get

(29)
$$\sum_{h\in C(N)} \frac{1}{r(h)} \prod_{i=1}^{\min(j,2)} \left(\sum_{z\in Z_i} e\left(\frac{k_i}{n_i}hz\right)\right) = \prod_{i=1}^{\min(j,2)} \phi(n_i) + \sum_{h\in C^*(N)} \frac{1}{|h|} \prod_{i=1}^{\min(j,2)} \left(\sum_{\substack{d|n_i \\ d|k_ih}} \mu\left(\frac{n_i}{d}\right) d\right).$$

Now let $j \geq 2$. Then (29) yields

$$\begin{aligned} &\sum_{h\in C(N)} \frac{1}{r(h)} \prod_{i=1}^{2} \left(\sum_{z\in Z_i} e\left(\frac{k_i}{n_i}hz\right)\right) = \\ (30)\qquad &= \phi(n_1)\phi(n_2) + \sum_{d_1|n_1}\sum_{d_2|n_2} \mu\left(\frac{n_1}{d_1}\right)\mu\left(\frac{n_2}{d_2}\right) d_1d_2 \sum_{\substack{h\in C^*(N) \\ d_1|k_1h,\, d_2|k_2h}} \frac{1}{|h|}. \end{aligned}$$

For $i = 1, 2$ we have $d_i|k_ih$ if and only if $d_i/(d_i, k_i)$ divides h. Therefore, the conditions $d_1|k_1h$ and $d_2|k_2h$ hold simultaneously if and only if the least common multiple $W(d_1, d_2, k_1, k_2) := [d_1/(d_1, k_1), d_2/(d_2, k_2)]$ divides h. Thus,

$$\begin{aligned} \sum_{\substack{h\in C^*(N) \\ d_1|k_1h,\, d_2|k_2h}} \frac{1}{|h|} &= \sum_{\substack{h\in C^*(N) \\ W(d_1,d_2,k_1,k_2)|h}} \frac{1}{|h|} = \frac{1}{W(d_1,d_2,k_1,k_2)} S\left(\frac{N}{W(d_1,d_2,k_1,k_2)}\right) \\ &= \frac{1}{W(d_1,d_2,k_1,k_2)} \left(2\log N + C - 2\log W(d_1,d_2,k_1,k_2) + \varepsilon\left(\frac{N}{W(d_1,d_2,k_1,k_2)}\right)\right) \end{aligned}$$

by Lemma 1. Since $[m, n] = mn/(m, n)$, it follows from (30) that

$$\begin{aligned} &\sum_{h\in C(N)} \frac{1}{r(h)} \prod_{i=1}^{2} \left(\sum_{z\in Z_i} e\left(\frac{k_i}{n_i}hz\right)\right) = \phi(n_1)\phi(n_2) + (2\log N + C)T(k_1,k_2,n_1,n_2) \\ &- 2V(k_1,k_2,n_1,n_2) + \sum_{d_1|n_1}\sum_{d_2|n_2} \mu\left(\frac{n_1}{d_1}\right)\mu\left(\frac{n_2}{d_2}\right) \frac{d_1d_2}{W(d_1,d_2,k_1,k_2)} \varepsilon\left(\frac{N}{W(d_1,d_2,k_1,k_2)}\right) \end{aligned}$$

with the notation in Lemmas 3 and 7. Since $|\varepsilon(m)| < 4/m^2$ by Lemma 1, we get

$$\begin{aligned} &\left|\sum_{d_1|n_1}\sum_{d_2|n_2} \mu\left(\frac{n_1}{d_1}\right)\mu\left(\frac{n_2}{d_2}\right) \frac{d_1d_2}{W(d_1,d_2,k_1,k_2)} \varepsilon\left(\frac{N}{W(d_1,d_2,k_1,k_2)}\right)\right| \leq \\ &\leq \frac{4}{N^2} \sum_{d_1|n_1}\sum_{d_2|n_2} \left|\mu\left(\frac{n_1}{d_1}\right)\mu\left(\frac{n_2}{d_2}\right)\right| d_1d_2W(d_1,d_2,k_1,k_2) \\ &= \frac{4}{N^2} Y(k_1,k_2,n_1,n_2) \leq \frac{4n_1}{\phi(n_1)\phi(n_2)} \end{aligned}$$

according to Lemma 8. It follows that

$$\begin{aligned} (31)\qquad &\left|\sum_{h\in C(N)} \frac{1}{r(h)} \prod_{i=1}^{2} \left(\sum_{z\in Z_i} e\left(\frac{k_i}{n_i}hz\right)\right)\right| \leq \\ &\leq |\phi(n_1)\phi(n_2) + (2\log N + C)T(k_1,k_2,n_1,n_2) - 2V(k_1,k_2,n_1,n_2)| + \frac{4n_1}{\phi(n_1)\phi(n_2)}. \end{aligned}$$

Let $Q_1 = n_1/(n_1, k_1)$ and $Q_2 = n_2/(n_2, k_2)$. If $Q_1 = Q_2$, then using

$$0 \leq \log Q_1 - \sum_{p|Q_1} \frac{\log p}{p-1} \leq \log n_1,$$

we obtain from Lemmas 3 and 7,

$$|\phi(n_1)\phi(n_2) + (2\log N + C)T(k_1,k_2,n_1,n_2) - 2V(k_1,k_2,n_1,n_2)| \leq \phi(n_1)\phi(n_2) + \frac{2\phi(n_1)\phi(n_2)}{\phi(Q_1)} \log N.$$

If there is a unique prime q such that $e_q(Q_1) \neq e_q(Q_2)$, then using the fact that $q|n$ implies $\phi(n) \geq q - 1 > \log q$, we obtain from Lemmas 3 and 7,

$$|\phi(n_1)\phi(n_2) + (2\log N + C)T(k_1,k_2,n_1,n_2) - 2V(k_1,k_2,n_1,n_2)| \leq \phi(n_1)\phi(n_2).$$

In all other cases we have $T(k_1, k_2, n_1, n_2) = V(k_1, k_2, n_1, n_2) = 0$ by Lemmas 3 and 7, and so the last inequality holds trivially. By [2, Theorem 328] we have

$$(32)\qquad \frac{n}{\phi(n)} < c\log\log(n+1) \quad \text{for all} \quad n \geq 2$$

with an absolute constant $c > 0$. In the following we denote by c a positive absolute constant which may have different values in different occurrences. In view of (31) we then get

$$(33)\qquad \left|\sum_{h\in C(N)} \frac{1}{r(h)} \prod_{i=1}^{2} \left(\sum_{z\in Z_i} e\left(\frac{k_i}{n_i}hz\right)\right)\right| < \phi(n_1)\phi(n_2) + \frac{c\phi(n_1)\phi(n_2)}{\phi(Q_1)} \log N$$

if $Q_1 = Q_2$, where we also used (32) and the fact that $Q_1|n_1$ implies $\phi(Q_1) \leq \phi(n_1)$. From (31) and (32) we get

$$(34)\qquad \left|\sum_{h\in C(N)} \frac{1}{r(h)} \prod_{i=1}^{2} \left(\sum_{z\in Z_i} e\left(\frac{k_i}{n_i}hz\right)\right)\right| < \phi(n_1)\phi(n_2) + c\,\log\log(n_1+1)$$

if $Q_1 \neq Q_2$.

Now we consider the expression on the left-hand side of (29) for $j = 1$. If $k_1 = n_1$, then it is clear from Lemma 1 that

$$(35)\qquad \Big|\sum_{h\in C(N)} \frac{1}{r(h)} \sum_{x\in Z_1} e\left(\frac{k_1}{n_1}hx\right)\Big| < c\phi(n_1)\log N.$$

If $1 \le k_1 < n_1$, then we apply (34) with $k_2 = n_2$ to obtain

$$(36)\qquad \Big|\sum_{h\in C(N)} \frac{1}{r(h)} \sum_{x\in Z_1} e\left(\frac{k_1}{n_1}hx\right)\Big| < \phi(n_1) + \frac{c\log\log(n_1+1)}{\phi(n_2)}.$$

Now we combine the information in (33), (34), (35), and (36) to obtain bounds for the product

$$\prod_{j=1}^{s}\Big|\sum_{h\in C(N)} \frac{1}{r(h)} \prod_{i=1}^{\min(j,2)}\left(\sum_{x\in Z_i} e\left(\frac{k_i}{n_i}hx\right)\right)\Big|,$$

which we abbreviate by $\prod$. If $k_1 = n_1$ and $k_2 = n_2$, then $Q_1 = Q_2 = 1$, and so it follows from (33) and (35) that

$$(37)\qquad \prod < c_s\phi(n_1)^s\phi(n_2)^{s-1}(\log N)^s,$$

where here and in the sequel, c_s denotes a positive constant which depends only on s and which may have different values in different occurrences. If $k_1 = n_1$ and $1 \le k_2 < n_2$, then $Q_1 = 1$ and $Q_2 > 1$, hence it follows from (34) and (35) that

$$(38)\qquad \begin{aligned}\prod &< c(\phi(n_1)\phi(n_2) + c\log\log(n_1+1))^{s-1}\phi(n_1)\log N\\ &= c\phi(n_1)^s\phi(n_2)^{s-1}\left(1+\frac{c\log\log(n_1+1)}{\phi(n_1)\phi(n_2)}\right)^{s-1}\log N < c_s\phi(n_1)^s\phi(n_2)^{s-1}\log N,\end{aligned}$$

where we used (32) in the last step. If $1 \le k_1 < n_1$ and $Q_1 = Q_2$, then (33) and (36) yield

$$(39)\qquad \begin{aligned}\prod &< \left(\phi(n_1) + \frac{c\log\log(n_1+1)}{\phi(n_2)}\right)\left(\phi(n_1)\phi(n_2) + \frac{c\phi(n_1)\phi(n_2)}{\phi(Q_1)}\log N\right)^{s-1}\\ &= \phi(n_1)^s\phi(n_2)^{s-1}\left(1+\frac{c\log\log(n_1+1)}{\phi(n_1)\phi(n_2)}\right)\left(1+\frac{c\log N}{\phi(Q_1)}\right)^{s-1}.\end{aligned}$$

If $1 \le k_1 < n_1$ and $Q_1 \ne Q_2$, then (34) and (36) yield

$$(40)\qquad \begin{aligned}\prod &< \left(\phi(n_1) + \frac{c\log\log(n_1+1)}{\phi(n_2)}\right)(\phi(n_1)\phi(n_2) + c\log\log(n_1+1))^{s-1}\\ &= \phi(n_1)^s\phi(n_2)^{s-1}\left(1+\frac{c\log\log(n_1+1)}{\phi(n_1)\phi(n_2)}\right)^{s}\\ &< \phi(n_1)^s\phi(n_2)^{s-1}\left(1+\frac{c_s\log\log(n_1+1)}{\phi(n_1)}\right) < \phi(n_1)^s\phi(n_2)^{s-1}\left(1+\frac{c_s\log N}{n_1}\right),\end{aligned}$$

where we also used (32). From (27), (28), (37), (38), (39), and (40) and the fact that $\mathrm{card}(\mathcal{L}) = \phi(n_1)^s\phi(n_2)^{s-1}$ we obtain

$$\begin{aligned}M(\mathcal{L})+1 &\le \frac{1}{\mathrm{card}(\mathcal{L})N}\sum_{k_1=1}^{n_1}\sum_{k_2=1}^{n_2}\prod_{j=1}^{s}\Big|\sum_{h\in C(N)}\frac{1}{r(h)}\prod_{i=1}^{\min(j,2)}\left(\sum_{x\in Z_i} e\left(\frac{k_i}{n_i}hx\right)\right)\Big|\\ &< c_s\frac{(\log N)^s}{N} + c_s(n_2-1)\frac{\log N}{N} + \frac{1}{N}\left(1+\frac{c\log\log(n_1+1)}{\phi(n_1)\phi(n_2)}\right)\cdot\\ &\quad\cdot\sum_{k_1=1}^{n_1-1}\sum_{\substack{k_2=1\\ Q_1=Q_2}}^{n_2}\left(1+\frac{c\log N}{\phi(Q_1)}\right)^{s-1}\\ &\quad+\frac{1}{N}\left(1+\frac{c_s\log N}{n_1}\right)\sum_{k_1=1}^{n_1-1}\sum_{\substack{k_2=1\\ Q_1\ne Q_2}}^{n_2}1\\ &< c_s\frac{(\log N)^s}{N} + c_s\frac{\log N}{n_1} + \frac{1}{N}\left(1+\frac{c\log\log(n_1+1)}{\phi(n_1)\phi(n_2)}\right)\sum_{k_1=1}^{n_1}\sum_{\substack{k_2=1\\ Q_1=Q_2}}^{n_2}\left(1+\frac{c\log N}{\phi(Q_1)}\right)^{s-1}\\ &\quad+\frac{1}{N}\left(1+\frac{c_s\log N}{n_1}\right)\sum_{k_1=1}^{n_1}\sum_{\substack{k_2=1\\ Q_1\ne Q_2}}^{n_2}1.\end{aligned}$$

Consider the condition $Q_1 = Q_2$, i.e., $n_1/(n_1,k_1) = n_2/(n_2,k_2)$, with $1 \le k_1 \le n_1$ and $1 \le k_2 \le n_2$. If d is the common value of Q_1 and Q_2, then necessarily $d|n_2$ and $(n_2,k_2) = n_2/d$, and the last condition holds for exactly $\phi(d)$ values of k_2. Furthermore, $(n_1,k_1) = n_1/d$, and this condition holds for exactly $\phi(d)$ values of k_1. Thus, for fixed d we have $Q_1 = Q_2 = d$ for exactly $\phi(d)^2$ choices of k_1, k_2. The total number of solutions k_1, k_2 of $Q_1 = Q_2$ is given by

$$g(n_2) := \sum_{d|n_2}\phi(d)^2.$$

Therefore, we get

$$\begin{aligned}M(\mathcal{L})+1 <{} & c_s\frac{(\log N)^s}{N} + c_s\frac{\log N}{n_1} + \frac{1}{N}\left(1+\frac{c\log\log(n_1+1)}{\phi(n_1)\phi(n_2)}\right)\sum_{d|n_2}\phi(d)^2\left(1+\frac{c\log N}{\phi(d)}\right)^{s-1}\\ &+\frac{1}{N}\left(1+\frac{c_s\log N}{n_1}\right)(n_1n_2 - g(n_2)),\end{aligned}$$

and since $n_1n_2 = N$, we obtain

$$(41)\qquad M(\mathcal{L}) < c_s\frac{(\log N)^s}{N} + c_s\frac{\log N}{n_1} - \frac{g(n_2)}{N} + \frac{1}{N}\left(1+\frac{c\log\log(n_1+1)}{\phi(n_1)\phi(n_2)}\right)\sum_{d|n_2}\phi(d)^2\left(1+\frac{c\log N}{\phi(d)}\right)^{s-1}$$

Now

$$\sum_{d|n_2} \phi(d)^2 \left(1 + \frac{c \log N}{\phi(d)}\right)^{s-1} = \sum_{d|n_2} \phi(d)^2 \sum_{m=0}^{s-1} \binom{s-1}{m} \frac{c^m (\log N)^m}{\phi(d)^m}$$

$$\leq g(n_2) + c_s(\log N) \sum_{d|n_2} \phi(d) + \sum_{m=2}^{s-1} c_s (\log N)^m \sum_{d|n_2} 1$$

$$\leq g(n_2) + c_s n_2 \log N + c_s \tau(n_2)(\log N)^{s-1},$$

where $\tau(n)$ is the number of positive divisors of $n \in \mathbf{N}$. Together with (41) we get

$$M(\mathcal{L}) < c_s \frac{(\log N)^s}{N} + c_s \frac{\log N}{n_1} + c_s \tau(n_2) \frac{(\log N)^{s-1}}{N} + \\ + \frac{c \log\log(n_1+1)}{N\phi(n_1)\phi(n_2)} \left(g(n_2) + c_s n_2 \log N + c_s \tau(n_2)(\log N)^{s-1}\right).$$

Since

$$g(n_2) = \sum_{d|n_2} \phi(d)^2 \leq \phi(n_2) \sum_{d|n_2} \phi(d) = \phi(n_2) n_2,$$

it follows that

$$M(\mathcal{L}) < c_s \frac{(\log N)^s}{N} + c_s \frac{\log N}{n_1} + c_s \tau(n_2) \frac{(\log N)^{s-1}}{N}. \tag{42}$$

By [2, Theorem 315] we have $\tau(n) = O(n^\varepsilon)$ for every $\varepsilon > 0$. In particular, $\tau(n_2) \leq c_s n_2^{1/(s-1)}$. Suppose that with this value of c_s we had

$$\tau(n_2) > \log N \quad \text{and} \quad \tau(n_2) > c_s^{s-1} \frac{n_2}{(\log N)^{s-2}}.$$

Then,

$$\tau(n_2) = \tau(n_2)^{(s-2)/(s-1)} \tau(n_2)^{1/(s-1)} > (\log N)^{(s-2)/(s-1)} c_s \frac{n_2^{1/(s-1)}}{(\log N)^{(s-2)/(s-1)}} = c_s n_2^{1/(s-1)},$$

a contradiction. Thus we have either $\tau(n_2) \leq \log N$ or $\tau(n_2) \leq c_s^{s-1} n_2/(\log N)^{s-2}$. This means that the last term on the right-hand side of (42) can be incorporated into the other two terms on the right-hand side of (42). Hence,

$$M(\mathcal{L}) < c_s \frac{(\log N)^s}{N} + c_s \frac{\log N}{n_1},$$

which completes the proof of Theorem 2.