ACTA ARITHMETICA
156.3 (2012)

On the diaphony of some finite hybrid point sets

by

Peter Hellekalek (Salzburg) and Peter Kritzer (Linz)

1. Introduction. This work continues the exploration of the b-adic method introduced in [6, 7]. It is motivated by recent advances on hybrid point sets in the theory of uniform distribution of sequences in the multidimensional unit cube $[0,1)^s$, in particular by [18].

By a *point set* we mean, here and in the following, a sequence of points (either finite or infinite) in the s-dimensional unit cube, i.e., points are allowed to occur repeatedly.

The b-adic method employs structural properties of the compact group of b-adic integers to derive techniques for the analysis of the uniform distribution of point sets in $[0,1)^s$ (see [6, 7, 8, 10]). Its central elements are particular function classes derived from the characters of the compact group $\mathbb{Z}_b$ of b-adic integers.

Hybrid sequences are sequences of points in $[0,1)^s$ where certain coordinates of the points stem from one lower-dimensional sequence and the remaining coordinates from a second lower-dimensional sequence. This idea was proposed by Spanier in [34], who suggested mixing quasi-Monte Carlo and Monte Carlo methods. Recently, considerable advances for the discrepancy of hybrid sequences have been achieved, in a series of papers by Niederreiter [25]–[29] (see also [30]).

Obviously, the idea of mixing different types of point sets can be extended to more than two components, an idea that was dealt with in the recent paper [8], where general new tools for the analysis of hybrid sequences were introduced, based on a hybrid function system involving trigonometric, p-adic, and Walsh functions. We are going to make use of crucial results from [8] in this work.

2010 *Mathematics Subject Classification*: Primary 11K06; Secondary 11K38, 11K45, 11K70, 11L03.

Key words and phrases: diaphony, hybrid diaphony, hybrid point set, Halton sequence, lattice point set, b-adic function systems.

DOI: 10.4064/aa156-3-4

In this paper, we study a new notion of diaphony, namely the hybrid diaphony (see [8]) of a special sort of a finite hybrid sequence that has first been introduced in [18], the mix of a Halton sequence in prime bases and a lattice point set modulo a prime. We derive a previously unknown upper bound on the diaphony of such point sets. Our technique shows how to employ the b-adic method for this kind of problems and exhibits, for the first time, the interplay between classical techniques for estimating particular exponential sums and the new hybrid approach.

Let us outline the problem under consideration in the next two sections.

1.1. Basic definitions and the $\boldsymbol{b}$-adic function system. We recall the following concepts from [7, 8, 10].

Throughout this paper, b denotes a positive integer, $b \geq 2$, and $\boldsymbol{b} = (b_1, \ldots, b_s)$ stands for a vector of not necessarily distinct integers $b_i \geq 2$, $1 \leq i \leq s$. Further, p denotes a prime, and $\boldsymbol{p} = (p_1, \ldots, p_s)$ represents a vector of not necessarily distinct primes p_i, $1 \leq i \leq s$. We write $\mathbb{N}$ for the positive integers, and we put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. We will use the standard convention that empty sums have the value 0 and empty products the value 1.

We consider the s-dimensional torus $\mathbb{R}^s/\mathbb{Z}^s$, which will be identified with the half-open interval $[0,1)^s$. We put $e(y) = e^{2\pi \mathtt{i} y}$ for $y \in \mathbb{R}$, where $\mathtt{i}$ is the imaginary unit.

For a nonnegative integer k, let $k = \sum_{j \geq 0} k_j b^j$, $k_j \in \{0, 1, \ldots, b-1\}$, be the unique b-adic representation of k in base b. With the exception of at most finitely many indices j, the digits k_j are equal to 0. Every real number $x \in [0,1)$ has a b-adic representation $x = \sum_{j \geq 0} x_j b^{-j-1}$, with digits $x_j \in \{0, 1, \ldots, b-1\}$. If x is a *b-adic rational*, which means that $x = ab^{-g}$, a and g integers, $0 \leq a < b^g$, $g \in \mathbb{N}$, and if $x \neq 0$, then there exist two such representations. The b-adic representation of x is uniquely determined under the condition that $x_j \neq b-1$ for infinitely many j. In the following, we will call this particular representation the *regular* (b-adic) representation of x.

Let $\mathbb{Z}_b$ denote the compact group of the b-adic integers. We refer the reader to Hewitt and Ross [11] and Mahler [23] for details. An element z of $\mathbb{Z}_b$ will be written in the form $z = \sum_{j \geq 0} z_j b^j$, with digits $z_j \in \{0, 1, \ldots, b-1\}$. The set $\mathbb{Z}$ of integers is embedded in $\mathbb{Z}_b$. If $z \in \mathbb{N}_0$, then at most finitely many digits z_j are different from 0. If $z \in \mathbb{Z}$, $z < 0$, then at most finitely many digits z_j are different from $b-1$. In particular, $-1 = \sum_{j \geq 0} (b-1) b^j$.

DEFINITION 1.1. The map $\varphi_b : \mathbb{Z}_b \to [0,1)$ given by $\varphi_b(\sum_{j \geq 0} z_j b^j) = \sum_{j \geq 0} z_j b^{-j-1} \pmod 1$ will be called the *b-adic Monna map.*

The restriction of φ_b to $\mathbb{N}_0$ is often called the *radical-inverse function* in base b. The Monna map is surjective, but not injective. It may be inverted in the following sense.

Definition 1.2. We define the *pseudoinverse* φ_b^+ of the b-adic Monna map φ_b by

$$\varphi_b^+ : [0,1) \to \mathbb{Z}_b, \qquad \varphi_b^+\Big(\sum_{j\ge 0} x_j b^{-j-1}\Big) = \sum_{j\ge 0} x_j b^j,$$

where $\sum_{j\ge 0} x_j b^{-j-1}$ stands for the regular b-adic representation of the element $x \in [0,1)$.

The image of $[0,1)$ under φ_b^+ is the set $\mathbb{Z}_b \setminus (-\mathbb{N})$. Furthermore, $\varphi_b \circ \varphi_b^+$ is the identity map on $[0,1)$, and $\varphi_b^+ \circ \varphi_b$ the identity on $\mathbb{N}_0 \subset \mathbb{Z}_b$. In general, $z \neq \varphi_b^+(\varphi_b(z))$ for $z \in \mathbb{Z}_b$. For example, if $z = -1$, then $\varphi_b^+(\varphi_b(-1)) = \varphi_b^+(0) = 0 \neq -1$.

A central point in the concept of $\boldsymbol{b}$-adic function systems introduced in [10] is the enumeration of the dual group $\hat{\mathbb{Z}}_b$. Namely, $\hat{\mathbb{Z}}_b$ can be written in the form $\hat{\mathbb{Z}}_b = \{\chi_{b,k} : k \in \mathbb{N}_0\}$, where $\chi_{b,k} : \mathbb{Z}_b \to \{c \in \mathbb{C} : |c| = 1\}$, $\chi_{b,k}(\sum_{j\ge 0} z_j b^j) = e(\varphi_b(k)(z_0 + z_1 b + \cdots))$. We note that $\chi_{b,k}$ depends only on a finite number of digits of z and, hence, this function is well defined.

As in [8, 10], we employ the function φ_b^+ to lift the characters $\chi_{b,k}$ to the torus.

Definition 1.3. For $k \in \mathbb{N}_0$, let $\gamma_{b,k} : [0,1) \to \{c \in \mathbb{C} : |c| = 1\}$, $\gamma_{b,k}(x) = \chi_{b,k}(\varphi_b^+(x))$, denote the kth *b-adic function.* We put $\mathit{\Gamma}_b = \{\gamma_{b,k} : k \in \mathbb{N}_0\}$ and call it the *b-adic function system* on $[0,1)$.

The preceding notions are easily generalized to the higher-dimensional case. Let $\boldsymbol{b} = (b_1,\dots,b_s)$ be a vector of not necessarily distinct integers $b_i \ge 2$, let $\boldsymbol{x} = (x_1,\dots,x_s) \in [0,1)^s$, let $\boldsymbol{z} = (z_1,\dots,z_s)$ denote an element of the compact product group $\mathbb{Z}_{\boldsymbol{b}} = \mathbb{Z}_{b_1} \times \cdots \times \mathbb{Z}_{b_s}$ of $\boldsymbol{b}$-adic integers, and let $\boldsymbol{k} = (k_1,\dots,k_s) \in \mathbb{N}_0^s$. We define $\varphi_{\boldsymbol{b}}(\boldsymbol{z}) = (\varphi_{b_1}(z_1),\dots,\varphi_{b_s}(z_s))$, and $\varphi_{\boldsymbol{b}}^+(\boldsymbol{x}) = (\varphi_{b_1}^+(x_1),\dots,\varphi_{b_s}^+(x_s))$. Moreover, let $\chi_{\boldsymbol{b},\boldsymbol{k}}(\boldsymbol{z}) = \prod_{i=1}^s \chi_{b_i,k_i}(z_i)$, where $\chi_{b_i,k_i} \in \hat{\mathbb{Z}}_{b_i}$, and define $\gamma_{\boldsymbol{b},\boldsymbol{k}}(\boldsymbol{x}) = \prod_{i=1}^s \gamma_{b_i,k_i}(x_i)$, where $\gamma_{b_i,k_i} \in \mathit{\Gamma}_{b_i}$, $1 \le i \le s$. Then $\gamma_{\boldsymbol{b},\boldsymbol{k}} = \chi_{\boldsymbol{b},\boldsymbol{k}} \circ \varphi_{\boldsymbol{b}}^+$. Let $\mathit{\Gamma}_{\boldsymbol{b}}^{(s)} = \{\gamma_{\boldsymbol{b},\boldsymbol{k}} : \boldsymbol{k} \in \mathbb{N}_0^s\}$ denote the $\boldsymbol{b}$*-adic function system* in dimension s. It was shown in [10] that $\mathit{\Gamma}_{\boldsymbol{b}}^{(s)}$ is an orthonormal basis of $L^2([0,1)^s)$.

Definition 1.4. Let $k \in \mathbb{Z}$. The kth *trigonometric function* e_k is defined as $e_k : [0,1) \to \mathbb{C}$, $e_k(x) = e(kx)$. For $\boldsymbol{k} = (k_1,\dots,k_d) \in \mathbb{Z}^d$, the $\boldsymbol{k}$*th trigonometric function* $e_{\boldsymbol{k}}$ is defined as $e_{\boldsymbol{k}} : [0,1)^d \to \mathbb{C}$, $e_{\boldsymbol{k}}(\boldsymbol{x}) = \prod_{i=1}^d e(k_i x_i)$, $\boldsymbol{x} = (x_1,\dots,x_d) \in [0,1)^d$. The *trigonometric function system* in dimension $d \ge 1$ is denoted by $\mathcal{T}^{(d)} = \{e_{\boldsymbol{k}} : \boldsymbol{k} \in \mathbb{Z}^d\}$.

Remark 1.5. For given s and d, let us write a point $\boldsymbol{x} \in [0,1)^{s+d}$ in the form $\boldsymbol{x} = (\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)})$ with $\boldsymbol{x}^{(1)} \in [0,1)^s$ and $\boldsymbol{x}^{(2)} \in [0,1)^d$. For a given index $\boldsymbol{k} = (\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)}) \in \mathbb{N}_0^s \times \mathbb{Z}^d$, the functions $\gamma_{\boldsymbol{b},\boldsymbol{k}^{(1)}} \otimes e_{\boldsymbol{k}^{(2)}} : [0,1)^{s+d} \to \mathbb{C}$,

$\boldsymbol{x} = (\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)}) \mapsto \gamma_{\boldsymbol{b},\boldsymbol{k}^{(1)}}(\boldsymbol{x}^{(1)}) e_{\boldsymbol{k}^{(2)}}(\boldsymbol{x}^{(2)})$, define the *hybrid function system*

$$\Gamma_{\boldsymbol{b}}^{(s)} \otimes \mathcal{T}^{(d)} = \{\gamma_{\boldsymbol{b},\boldsymbol{k}^{(1)}} \otimes e_{\boldsymbol{k}^{(2)}} : (\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)}) \in \mathbb{N}_0^s \times \mathbb{Z}^d\}.$$

This system is an orthonormal basis of the space $L^2([0,1)^{s+d})$. We refer to [8] for this kind of notions and generalizations.

1.2. The problem dealt with in this paper. In many applications of mathematics, such as numerical integration by means of quasi-Monte Carlo methods (see, e.g., [1, 2, 20, 22, 24, 33]), or function approximation (see, e.g, [21]), one is in need of point sets which are evenly distributed in the unit cube. There are several well-known types of point sets with this distribution property, one of the most important being the Halton sequences (cf. [4]).

Definition 1.6. Let $\boldsymbol{b} = (b_1, \ldots, b_s)$ be a vector of s not necessarily distinct integers $b_i \geq 2$. The s-dimensional *Halton sequence* to the bases $b_1, \ldots, b_s$ (or to the base $\boldsymbol{b}$) is defined to be the sequence $\boldsymbol{\omega} = (\boldsymbol{\omega}_n)_{n\geq 0}$ in $[0,1)^s$, where

$$\boldsymbol{\omega}_n = \varphi_{\boldsymbol{b}}(n), \qquad n \geq 0.$$

A Halton sequence is uniformly distributed if the bases $b_1, \ldots, b_s$ are coprime, which can, e.g., be conveniently achieved by choosing the bases as distinct primes (see, e.g., [20]). We shall use this assumption in this paper.

In addition to infinite point sets, such as Halton sequences, there are important finite sequences of, say, N elements in $[0,1)^d$, where N is fixed and their definition depends in some way on N. One prominent example is that of lattice point sets. We refer to [24] or [33] for excellent introductions to this topic. The definition of a lattice point set, introduced by Korobov [16] and Hlawka [12], is as follows.

Definition 1.7. Let N be a positive integer and let $\boldsymbol{g} = (g_1, \ldots, g_d)$ be a d-dimensional vector of positive integers. The *lattice point set* $\boldsymbol{\omega} = (\boldsymbol{\omega}_n)_{n=0}^{N-1}$ with generating vector $\boldsymbol{g}$, consisting of N points in $[0,1)^d$, is defined by

$$\boldsymbol{\omega}_n = \left(\left\{\frac{ng_1}{N}\right\}, \ldots, \left\{\frac{ng_d}{N}\right\}\right), \qquad 0 \leq n \leq N-1,$$

where $\{\cdot\}$ denotes the fractional part of a number. For short, we write

$$\boldsymbol{\omega}_n = \left(\left\{\frac{n\boldsymbol{g}}{N}\right\}\right), \qquad 0 \leq n \leq N-1.$$

It is of great interest to find out how well the points of a given point set are spread in the unit cube. There are different quality measures for assessing the uniformity of distribution of a point set. For example, there is the well-known concept of discrepancy (see, e.g., [1], [20], or [24]). Apart from discrepancy, there are other ways for assessing the quality of distribution of a point set, such as diaphony. The diaphony of a point set is one of the most common assessment criteria for the quality of distribution of a given point set, and it is closely related to the worst case integration error of a QMC integration rule based on this point set (see, e.g, [31]). The classical diaphony was first introduced by Zinterhof [35], and it was later modified to the concepts of dyadic (Walsh) diaphony by Hellekalek and Leeb [9], to the b-adic (Walsh) diaphony by Grozdanov and Stoilova [3], and to the so-called p-adic diaphony by Hellekalek [7]. For assessing the diaphony of hybrid point sets, we need the more general notion of *hybrid* diaphony, which was introduced in [8]. The following notation stems from [8] and has been adapted for our purposes.

For a given base $\boldsymbol{b} = (b_1, \ldots, b_s)$ of integers $b_i \geq 2$, and a vector $\boldsymbol{k} \in \mathbb{N}_0^s$, $\boldsymbol{k} = (k_1, \ldots, k_s)$, define

$$\rho_{b_i}(k_i) = \begin{cases} 1 & \text{if } k_i = 0, \\ b_i^{-2(j-1)} & \text{if } b_i^{j-1} \leq k_i < b_i^j \text{ for } j \in \mathbb{N}, \end{cases}$$

for $1 \leq i \leq s$, and put $\rho_{\boldsymbol{b}}(\boldsymbol{k}) = \prod_{i=1}^s \rho_{b_i}(k_i)$.

Furthermore, for a positive integer t and a vector $\boldsymbol{k} \in \mathbb{Z}^d$, define

$$r_t(k_i) = \begin{cases} 1 & \text{if } k_i = 0, \\ |k_i|^{-t} & \text{if } k_i \neq 0, \end{cases}$$

for $1 \leq i \leq d$ and put $r_t(\boldsymbol{k}) = \prod_{i=1}^d r_t(k_i)$.

For an integer vector $\boldsymbol{k} = (\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)}) \in \mathbb{N}_0^s \times \mathbb{Z}^d$, we define the weight function $\rho(\boldsymbol{k}) = \rho_{\boldsymbol{b}}(\boldsymbol{k}^{(1)}) r_2(\boldsymbol{k}^{(2)})$.

Moreover, we put

$$\sigma = \Bigl(\prod_{i=1}^{s}(1+b_i)\Bigr)\Bigl(1+\frac{\pi^2}{3}\Bigr)^{d}. \tag{1}$$

We are now ready to define the measure of uniform distribution that will be studied in this paper.

Definition 1.8. Let $\boldsymbol{\omega}^{(1)} = (\boldsymbol{\omega}_n^{(1)})_{n=0}^{N-1}$ be a point set in $[0,1)^s$, and let $\boldsymbol{\omega}^{(2)} = (\boldsymbol{\omega}_n^{(2)})_{n=0}^{N-1}$ be a point set in $[0,1)^d$. Furthermore, let $\boldsymbol{\omega} = (\boldsymbol{\omega}_n)_{n=0}^{N-1}$ be the $(s+d)$-dimensional point set defined by $\boldsymbol{\omega}_n = (\boldsymbol{\omega}_n^{(1)}, \boldsymbol{\omega}_n^{(2)})$, $0 \leq n \leq N-1$. Moreover, let $\boldsymbol{p} = (p_1, \ldots, p_s)$ be a vector of not necessarily distinct primes p_i. The *hybrid diaphony* of the $(s+d)$-dimensional sequence $\boldsymbol{\omega}$ with respect to the function system $\mathit{\Gamma}_{\boldsymbol{p}}^{(s)} \otimes \mathcal{T}^{(d)}$ is given by

$$F_N(\boldsymbol{\omega}) := \left(\frac{1}{\sigma - 1} \sum_{\substack{\boldsymbol{k}^{(1)} \in \mathbb{N}_0^s \\ \boldsymbol{k}^{(2)} \in \mathbb{Z}^d \\ (\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)}) \neq \boldsymbol{0}}} \rho(\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)}) \left| \frac{1}{N} \sum_{n=0}^{N-1} \gamma_{\boldsymbol{p}, \boldsymbol{k}^{(1)}}(\boldsymbol{\omega}_n^{(1)}) e_{\boldsymbol{k}^{(2)}}(\boldsymbol{\omega}_n^{(2)}) \right|^2 \right)^{1/2}.$$

REMARK 1.9. A more general version of the hybrid diaphony involving also Walsh functions can be found in [8]. There it was shown that the hybrid diaphony is a normalized measure of uniformity of distribution, i.e., it always takes on values in $[0, 1]$ and takes on low values if and only if a point set is evenly spread in the unit cube.

Let us, in the next step, introduce a special choice of a finite point set $\boldsymbol{\omega}$ that we are going to be concerned with in this paper. In what follows, let

- $\boldsymbol{\omega}^{(1)} = (\boldsymbol{\omega}_n^{(1)})_{n=0}^{\infty}$ be an s-dimensional Halton sequence to the base $\boldsymbol{p} = (p_1, \dots, p_s)$ (from now on we always assume that $p_1, \dots, p_s$ are s distinct primes),
- $\boldsymbol{\omega}^{(2)} = (\boldsymbol{\omega}_n^{(2)})_{n=0}^{N-1}$ be a d-dimensional lattice point set with N points, generated by a vector $\boldsymbol{g} \in \mathbb{Z}^s$, where we assume that $N > 2$ is a prime different from $p_1, \dots, p_s$, and
- $\boldsymbol{\omega} = (\boldsymbol{\omega}_n)_{n=0}^{N-1}$ be the $(s+d)$-dimensional finite hybrid point set defined by $(\boldsymbol{\omega}_n)_{n=0}^{N-1} = (\boldsymbol{\omega}_n^{(1)}, \boldsymbol{\omega}_n^{(2)})_{n=0}^{N-1}$.

We emphasize that we always assume $\boldsymbol{\omega}$ to be of the form above throughout the rest of the paper.

The logical question when dealing with $\boldsymbol{\omega}$ is how evenly it is distributed in the unit cube, and, as outlined above, one may consider different quality criteria for this purpose. For instance, the discrepancy of $\boldsymbol{\omega}$ was studied in [18], where it was shown that $\boldsymbol{\omega}$ is, for clever choices of the vector $\boldsymbol{g}$, a low discrepancy point set. Here we would like to further advance the results of [18] and study a different way of measuring the quality of distribution of $\boldsymbol{\omega}$. As $\boldsymbol{\omega}$ is a hybrid point set, it is near at hand to consider its hybrid diaphony with a particular choice of the underlying function systems, as described in Definition 1.8.

The rest of the paper is structured as follows. In Section 2, we show that there exist generating vectors $\boldsymbol{g} \in \mathbb{Z}^d$ such that the hybrid point set $\boldsymbol{\omega}$ obtained by mixing the first N points of a Halton sequence in prime bases with a lattice point set generated by $\boldsymbol{g}$ has low diaphony. In Section 3, we outline that one can even restrict oneself to very particular choices of $\boldsymbol{g}$ and still obtain strong diaphony bounds. Finally, we summarize our main findings in Section 4 and discuss the relation of our results to other problems.

2. The diaphony of the mixture of Halton and lattice point sets. Within this section, let $\boldsymbol{\omega}$, as defined in Section 1.2, be the mixture of the first N points of an s-dimensional Halton sequence and a d-dimensional lattice point set.

We are going to show the following theorem.

THEOREM 2.1. *Let $\boldsymbol{\omega}^{(1)} = (\boldsymbol{\omega}_n^{(1)})_{n=0}^{\infty}$ be an s-dimensional Halton sequence to the base $\boldsymbol{p} = (p_1, \ldots, p_s)$, where $p_1, \ldots, p_s$ are s distinct primes. Let N be a prime different from $p_1, \ldots, p_s$. Then there exists $\boldsymbol{g} \in \{1, \ldots, N-1\}^d$ such that the point set $\boldsymbol{\omega} = (\boldsymbol{\omega}_n)_{n=0}^{N-1} = (\boldsymbol{\omega}_n^{(1)}, \boldsymbol{\omega}_n^{(2)})_{n=0}^{N-1}$, where $\boldsymbol{\omega}_n^{(2)} = \{n\boldsymbol{g}/N\}$ for $0 \le n \le N-1$, satisfies*

$$F_N(\boldsymbol{\omega}) \le c\frac{(\log N)^{s+d+1}}{N},$$

where c is a positive constant that is independent of N.

Proof. We introduce some further notation. Choose positive integers $m_1, \ldots, m_s$, where each m_i is minimal such that $N^2 \le p_i^{m_i}$. We put

$$\Delta_{\boldsymbol{p},s}(N) := \{\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s : k_i < p_i^{m_i},\ 1 \le i \le s\},$$

and $\Delta^*_{\boldsymbol{p},s}(N) := \Delta_{\boldsymbol{p},s}(N) \setminus \{\boldsymbol{0}\}$. By $\Delta_{p_i,1}(N)$ and $\Delta^*_{p_i,1}(N)$ we mean the one-dimensional analogues of $\Delta_{\boldsymbol{p},s}(N)$ and $\Delta^*_{\boldsymbol{p},s}(N)$ with respect to the ith component.

Furthermore, we write

$$C_d(N^2) := \{\boldsymbol{k} \in \mathbb{Z}^d : \|\boldsymbol{k}\|_\infty \le N^2/2\} \quad \text{and} \quad C_d^*(N^2) := C_d(N^2) \setminus \{\boldsymbol{0}\}.$$

We also write

$$\Xi_{\boldsymbol{p},s,d}(N) := \Delta_{\boldsymbol{p},s}(N) \times C_d(N^2) \quad \text{and} \quad \Xi^*_{\boldsymbol{p},s,d}(N) := \Xi_{\boldsymbol{p},s,d}(N) \setminus \{\boldsymbol{0}\}.$$

Finally, let

$$\delta := \max\left\{\frac{2}{(1+\pi^2/3)N^2/2}, \max_{1\le i\le s} \frac{p_i}{(p_i+1)p_i^{m_i}}\right\}.$$

Using this notation, we invoke Corollary 5 of [8] to obtain

$$\begin{aligned} F_N^2(\boldsymbol{\omega}) \le{}& \frac{\sigma(s+d)\delta}{\sigma-1} \\ &+ \frac{1}{\sigma-1} \sum_{(\boldsymbol{k}^{(1)},\boldsymbol{k}^{(2)})\in\Xi^*_{\boldsymbol{p},s,d}(N)} \rho_{\boldsymbol{p}}(\boldsymbol{k}^{(1)}) r_2(\boldsymbol{k}^{(2)}) \Big|\sum(\boldsymbol{k}^{(1)},\boldsymbol{k}^{(2)})\Big|^2, \end{aligned}$$

where σ is defined as in (1), and

$$\Big|\sum(\boldsymbol{k}^{(1)},\boldsymbol{k}^{(2)})\Big| := \Big|\frac{1}{N}\sum_{n=0}^{N-1}\gamma_{\boldsymbol{p},\boldsymbol{k}^{(1)}}(\boldsymbol{\omega}_n^{(1)})e_{\boldsymbol{k}^{(2)}}(\boldsymbol{\omega}_n^{(2)})\Big|. \tag{2}$$

The above bound on $F_N^2(\boldsymbol{\omega})$ can be written in the form

$$F_N^2(\boldsymbol{\omega}) \le \frac{c_1}{N^2} + c_2 \sum_{(\boldsymbol{k}^{(1)},\boldsymbol{k}^{(2)})\in \varXi^*_{\boldsymbol{p},s,d}(N)} \rho_{\boldsymbol{p}}(\boldsymbol{k}^{(1)})r_2(\boldsymbol{k}^{(2)})\Big|\sum(\boldsymbol{k}^{(1)},\boldsymbol{k}^{(2)})\Big|^2, \tag{3}$$

where $c_1, c_2 > 0$ are constants that might depend on the p_i and s, but not on N. We shall frequently use constants c_l in our estimates, always tacitly assuming that the c_l are positive and independent of N. The indices $l = 1, 2, \ldots$ are used to indicate that the constants may be different from each other.

We now study the term

$$\begin{aligned}
&\sum_{(\boldsymbol{k}^{(1)},\boldsymbol{k}^{(2)})\in \varXi^*_{\boldsymbol{p},s,d}(N)} \rho_{\boldsymbol{p}}(\boldsymbol{k}^{(1)})r_2(\boldsymbol{k}^{(2)})\Big|\sum(\boldsymbol{k}^{(1)},\boldsymbol{k}^{(2)})\Big|^2 \\
&= \sum_{\boldsymbol{k}^{(1)}\in \varDelta^*_{\boldsymbol{p},s}(N)} \rho_{\boldsymbol{p}}(\boldsymbol{k}^{(1)})\Big|\sum(\boldsymbol{k}^{(1)},\boldsymbol{0})\Big|^2 + \sum_{\boldsymbol{k}^{(2)}\in C^*_d(N^2)} r_2(\boldsymbol{k}^{(2)})\Big|\sum(\boldsymbol{0},\boldsymbol{k}^{(2)})\Big|^2 \\
&\quad + \sum_{\substack{\boldsymbol{k}^{(1)}\in \varDelta^*_{\boldsymbol{p},s}(N)\\ \boldsymbol{k}^{(2)}\in C^*_d(N^2)}} \rho_{\boldsymbol{p}}(\boldsymbol{k}^{(1)})r_2(\boldsymbol{k}^{(2)})\Big|\sum(\boldsymbol{k}^{(1)},\boldsymbol{k}^{(2)})\Big|^2 =: \sum\nolimits_1 + \sum\nolimits_2 + \sum\nolimits_3 .
\end{aligned}$$

For $\sum_1$, we can write

$$\sum_1 = \sum_{\boldsymbol{k}^{(1)}\in \varDelta^*_{\boldsymbol{p},s}(N)} \rho_{\boldsymbol{p}}(\boldsymbol{k}^{(1)})\Big|\frac{1}{N}\sum_{n=0}^{N-1}\gamma_{\boldsymbol{p},\boldsymbol{k}^{(1)}}(\boldsymbol{\omega}_n^{(1)})\Big|^2.$$

This expression was studied in [31], where it was shown that

$$\sum\nolimits_1 \le \frac{\pi^2}{3}\frac{1}{N^2}\Big(-1+\prod_{j=1}^{s}\Big(1+(1+2\log_{b_j}N)b_j^2\Big)\Big) \le c_3\frac{(\log N)^s}{N^2}.$$

We therefore obtain

$$F_N^2(\boldsymbol{\omega}) \le \frac{c_1}{N^2} + c_2c_3\frac{(\log N)^s}{N^2} + c_2\sum\nolimits_2 + c_2\sum\nolimits_3 . \tag{4}$$

Let $\langle\cdot,\cdot\rangle$ denote the usual inner or dot product. For $\sum_2$ we have

$$\begin{aligned}
\sum\nolimits_2 &= \sum_{\boldsymbol{k}^{(2)}\in C^*_d(N^2)} r_2(\boldsymbol{k}^{(2)})\Big|\frac{1}{N}\sum_{n=0}^{N-1} e(\langle\boldsymbol{k}^{(2)},\boldsymbol{\omega}_n^{(2)}\rangle)\Big|^2 \\
&= \sum_{\boldsymbol{k}^{(2)}\in C^*_d(N^2)} r_2(\boldsymbol{k}^{(2)})\Big|\frac{1}{N}\sum_{n=0}^{N-1} e\Big(\frac{1}{N}\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle n\Big)\Big|^2 = \sum_{\substack{\boldsymbol{k}^{(2)}\in C^*_d(N^2)\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)}).
\end{aligned}$$

Finally, we deal with $\sum_3$. For every $\boldsymbol{k}^{(1)} = (k_1^{(1)}, \dots, k_s^{(1)}) \in \Delta^*_{\boldsymbol{p},s}(N)$, there is a unique subset $\mathfrak{u} \neq \emptyset$ of $[s] := \{1, \dots, s\}$ such that $k_i^{(1)} \in \Delta^*_{p_i,1}(N)$ if $i \in \mathfrak{u}$ and $k_i^{(1)} = 0$ otherwise. Let $\boldsymbol{p}_{\mathfrak{u}}$ denote the projection of $\boldsymbol{p}$ onto the components which are contained in $\mathfrak{u}$. Furthermore, define

$$\Delta^+_{\boldsymbol{p}_{\mathfrak{u}},|\mathfrak{u}|}(N) := \prod_{i\in\mathfrak{u}} \Delta^*_{p_i,1}(N),$$

and write $\sum_{\mathfrak{u}}(\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)})$ for the obvious adaption of $\sum(\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)})$ with respect to $\mathfrak{u}$.

Using this notation, we have

$$\begin{aligned}\sum\nolimits_3 &= \sum_{\substack{\boldsymbol{k}^{(1)}\in\Delta^*_{\boldsymbol{p},s}(N)\\ \boldsymbol{k}^{(2)}\in C^*_d(N^2)}} \rho_{\boldsymbol{p}}(\boldsymbol{k}^{(1)}) r_2(\boldsymbol{k}^{(2)}) \Big|\sum(\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)})\Big|^2 \\ &= \sum_{\boldsymbol{k}^{(2)}\in C^*_d(N^2)} r_2(\boldsymbol{k}^{(2)}) \sum_{\emptyset\neq\mathfrak{u}\subseteq[s]} \sum_{\boldsymbol{k}^{(1)}\in\Delta^+_{\boldsymbol{p}_{\mathfrak{u}},|\mathfrak{u}|}(N)} \rho_{\boldsymbol{p}_{\mathfrak{u}}}(\boldsymbol{k}^{(1)}) \Big|\sum\nolimits_{\mathfrak{u}}(\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)})\Big|^2,\end{aligned}$$

which yields

$$\sum\nolimits_3 = \sum_{\emptyset\neq\mathfrak{u}\subseteq[s]} \sum_{\boldsymbol{k}^{(2)}\in C^*_d(N^2)} r_2(\boldsymbol{k}^{(2)}) \sum_{\boldsymbol{k}^{(1)}\in\Delta^+_{\boldsymbol{p}_{\mathfrak{u}},|\mathfrak{u}|}(N)} \rho_{\boldsymbol{p}_{\mathfrak{u}}}(\boldsymbol{k}^{(1)}) \Big|\sum\nolimits_{\mathfrak{u}}(\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)})\Big|^2. \tag{5}$$

For $\mathfrak{u} \subseteq [s]$, $\mathfrak{u} \neq \emptyset$, let us write

$$\sum\nolimits^*_{\mathfrak{u}} := \sum_{\boldsymbol{k}^{(2)}\in C^*_d(N^2)} r_2(\boldsymbol{k}^{(2)}) \sum_{\boldsymbol{k}^{(1)}\in\Delta^+_{\boldsymbol{p}_{\mathfrak{u}},|\mathfrak{u}|}(N)} \rho_{\boldsymbol{p}_{\mathfrak{u}}}(\boldsymbol{k}^{(1)}) \Big|\sum\nolimits_{\mathfrak{u}}(\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)})\Big|^2. \tag{6}$$

We first deal with the special case $\mathfrak{u} = [s]$ in (6), which simplifies notational issues. The other cases will be dealt with later. For this particular instance, the term under consideration simplifies to

$$\begin{aligned}\sum\nolimits^*_{[s]} &= \sum_{\boldsymbol{k}^{(2)}\in C^*_d(N^2)} r_2(\boldsymbol{k}^{(2)}) \sum_{\boldsymbol{k}^{(1)}\in\Delta^+_{\boldsymbol{p},s}(N)} \rho_{\boldsymbol{p}}(\boldsymbol{k}^{(1)}) \Big|\sum(\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)})\Big|^2 \\ &= \sum_{\boldsymbol{k}^{(2)}\in C^*_d(N^2)} r_2(\boldsymbol{k}^{(2)}) \sum_{j_1=1}^{m_1} \cdots \sum_{j_s=1}^{m_s} \Big(\prod_{i=1}^{s} p_i^{-2(j_i-1)}\Big) \sum_{r_1=1}^{p_1-1} \cdots \sum_{r_s=1}^{p_s-1} \sum\nolimits_A,\end{aligned} \tag{7}$$

where $\boldsymbol{k}^{(1)} = (k_1^{(1)}, \dots, k_s^{(1)})$ and where

$$\begin{aligned}\sum\nolimits_A &:= \sum_{k_1^{(1)}=r_1p_1^{j_1-1}}^{(r_1+1)p_1^{j_1-1}-1} \cdots \sum_{k_s^{(1)}=r_sp_s^{j_s-1}}^{(r_s+1)p_s^{j_s-1}-1} \Big|\sum(\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)})\Big|^2 \\ &= \sum_{k_1^{(1)}=r_1p_1^{j_1-1}}^{(r_1+1)p_1^{j_1-1}-1} \cdots \sum_{k_s^{(1)}=r_sp_s^{j_s-1}}^{(r_s+1)p_s^{j_s-1}-1} \bigg|\frac{1}{N}\sum_{n=0}^{N-1} e\Big(\frac{1}{N}\langle\boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle n\Big) e(\langle\varphi_{\boldsymbol{p}}(\boldsymbol{k}^{(1)}), \boldsymbol{1}\rangle n)\bigg|^2.\end{aligned}$$

Note that

$$e(\langle \varphi_{\boldsymbol{p}}(\boldsymbol{k}^{(1)}), \mathbf{1}\rangle n) = \prod_{i=1}^{s} e(\varphi_{p_i}(k_i^{(1)})n).$$

For $r_i \in \{1, \ldots, p_i - 1\}$ and $k_i^{(1)} \in \{r_i p_i^{j_i-1}, \ldots, (r_i+1)p_i^{j_i-1} - 1\}$, the base p_i expansion of $k_i^{(1)}$ has the form

$$k_i^{(1)} = k_{i,0}^{(1)} + k_{i,1}^{(1)} p_i + \cdots + k_{i,j_i-2}^{(1)} p_i^{j_i-2} + r_i p_i^{j_i-1}.$$

We then obtain

$$\begin{aligned}\varphi_{p_i}(k_i^{(1)}) &= \frac{1}{p_i^{j_i}}(r_i + k_{i,j_i-2}^{(1)} p_i + \cdots + k_{i,0}^{(1)} p_i^{j_i-1}) \\ &= \frac{1}{p_i^{j_i}}(r_i + p_i(k_{i,j_i-2}^{(1)} + \cdots + k_{i,0}^{(1)} p_i^{j_i-2})) = \frac{1}{p_i^{j_i}}(r_i + p_i a_{i,j_i}),\end{aligned}$$

where we write

$$a_{i,j_i} := k_{i,j_i-2}^{(1)} + \cdots + k_{i,0}^{(1)} p_i^{j_i-2}$$

for short. Note that the integer a_{i,j_i} runs through $\{0, 1, \ldots, p_i^{j_i-1} - 1\}$ if $k_i^{(1)}$ runs through the set $\{r_i p_i^{j_i-1}, \ldots, (r_i+1)p_i^{j_i-1} - 1\}$. Hence we obtain

$$\sum\nolimits_A = \sum_{a_{1,j_1}=0}^{p_1^{j_1-1}-1} \cdots \sum_{a_{s,j_s}=0}^{p_s^{j_s-1}-1} \left| \frac{1}{N} \sum_{n=0}^{N-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle n\Big) \prod_{i=1}^{s} e\Big(\frac{n(r_i + p_i a_{i,j_i})}{p_i^{j_i}}\Big)\right|^2.$$

Also note that, for any $i \in \{1, \ldots, s\}$ and any $j_i \in \{1, \ldots, m_i\}$, the term $r_i + p_i a_{i,j_i}$ is coprime to $p_i^{j_i}$. Plugging it into (7), we can therefore write

$$\begin{aligned}(8)\qquad \sum\nolimits_{[s]}^{*} &= \sum_{\boldsymbol{k}^{(2)} \in C_d^*(N^2)} r_2(\boldsymbol{k}^{(2)}) \sum_{j_1=1}^{m_1} \cdots \sum_{j_s=1}^{m_s} \Big(\prod_{i=1}^{s} p_i^{-2(j_i-1)}\Big) \sum_{r_1=1}^{p_1-1} \cdots \sum_{r_s=1}^{p_s-1} \\ &\quad \times \sum_{a_{1,j_1}=0}^{p_1^{j_1-1}-1} \cdots \sum_{a_{s,j_s}=0}^{p_s^{j_s-1}-1} \left| \frac{1}{N} \sum_{n=0}^{N-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle n\Big) \prod_{i=1}^{s} e\Big(\frac{n(r_i + p_i a_{i,j_i})}{p_i^{j_i}}\Big)\right|^2 \\ &= \sum_{\boldsymbol{k}^{(2)} \in C_d^*(N^2)} r_2(\boldsymbol{k}^{(2)}) \sum_{j_1=1}^{m_1} \cdots \sum_{j_s=1}^{m_s} \Big(\prod_{i=1}^{s} p_i^{-2(j_i-1)}\Big) \sum\nolimits_B,\end{aligned}$$

where

$$\sum\nolimits_B := \sum_{\substack{x_1=0 \\ (x_1, p_1^{j_1})=1}}^{p_1^{j_1}-1} \cdots \sum_{\substack{x_s=0 \\ (x_s, p_s^{j_s})=1}}^{p_s^{j_s}-1} \left| \frac{1}{N} \sum_{n=0}^{N-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle n\Big) \prod_{i=1}^{s} e\Big(\frac{n x_i}{p_i^{j_i}}\Big)\right|^2.$$

Let us now study

$$
\begin{aligned}
(9)\quad \sum\nolimits_B = \frac{1}{N^2} \sum_{\substack{x_1=0\\(x_1,p_1^{j_1})=1}}^{p_1^{j_1}-1} \cdots \sum_{\substack{x_s=0\\(x_s,p_s^{j_s})=1}}^{p_s^{j_s}-1} \Bigl(\sum_{n=0}^{N-1} e\Bigl(\frac{1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle n\Bigr) \prod_{i=1}^{s} e\Bigl(\frac{n x_i}{p_i^{j_i}}\Bigr)\Bigr) \\
\times \Bigl(\sum_{m=0}^{N-1} e\Bigl(\frac{-1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle m\Bigr) \prod_{i=1}^{s} e\Bigl(\frac{-m x_i}{p_i^{j_i}}\Bigr)\Bigr) \\
= \frac{1}{N^2} \sum_{n=0}^{N-1} e\Bigl(\frac{1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle n\Bigr) \sum_{m=0}^{N-1} e\Bigl(\frac{-1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle m\Bigr) \\
\times \sum_{\substack{x_1=0\\(x_1,p_1^{j_1})=1}}^{p_1^{j_1}-1} \cdots \sum_{\substack{x_s=0\\(x_s,p_s^{j_s})=1}}^{p_s^{j_s}-1} \prod_{i=1}^{s} e\Bigl(\frac{(n-m)x_i}{p_i^{j_i}}\Bigr) \\
= \frac{1}{N^2} \sum_{n=0}^{N-1} e\Bigl(\frac{1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle n\Bigr) \sum_{m=0}^{N-1} e\Bigl(\frac{-1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle m\Bigr) \\
\times \prod_{i=1}^{s} \sum_{\substack{x_i=0\\(x_i,p_i^{j_i})=1}}^{p_i^{j_i}-1} e\Bigl(\frac{(n-m)x_i}{p_i^{j_i}}\Bigr).
\end{aligned}
$$

For $1 \le i \le s$, we can write, using the fact that p_i is a prime,

$$
\begin{aligned}
\sum\nolimits_{B,i} := \sum_{\substack{x_i=0\\(x_i,p_i^{j_i})=1}}^{p_i^{j_i}-1} e\Bigl(\frac{(n-m)x_i}{p_i^{j_i}}\Bigr) \\
= \sum_{x_i=0}^{p_i^{j_i}-1} e\Bigl(\frac{(n-m)x_i}{p_i^{j_i}}\Bigr) - \sum_{\substack{x_i=0\\(x_i,p_i^{j_i})>1}}^{p_i^{j_i}-1} e\Bigl(\frac{(n-m)x_i}{p_i^{j_i}}\Bigr) \\
= \sum_{x_i=0}^{p_i^{j_i}-1} e\Bigl(\frac{(n-m)x_i}{p_i^{j_i}}\Bigr) - \sum_{x_i=0}^{p_i^{j_i-1}-1} e\Bigl(\frac{(n-m)x_i p_i}{p_i^{j_i}}\Bigr) \\
= \sum_{x_i=0}^{p_i^{j_i}-1} e\Bigl(\frac{(n-m)x_i}{p_i^{j_i}}\Bigr) - \sum_{x_i=0}^{p_i^{j_i-1}-1} e\Bigl(\frac{(n-m)x_i}{p_i^{j_i-1}}\Bigr).
\end{aligned}
$$

A short consideration shows that

$$\sum\nolimits_{B,i} = \begin{cases} p_i^{j_i} - p_i^{j_i-1} & \text{if } n-m \equiv 0 \ (p_i^{j_i}) \text{ (Case 1)}, \\ -p_i^{j_i-1} & \text{if } n-m \not\equiv 0 \ (p_i^{j_i}) \text{ and } n-m \equiv 0 \ (p_i^{j_i-1}) \text{ (Case 2)}, \\ 0 & \text{if } n-m \not\equiv 0 \ (p_i^{j_i}) \text{ and } n-m \not\equiv 0 \ (p_i^{j_i-1}) \text{ (Case 3)}. \end{cases}$$

Note that we need not deal with the situation where n and m are such that Case 3 holds for some i, since then $\sum_B$ is zero. Hence, we only need to deal with n and m such that either Case 1 or Case 2 holds for all i in $\{1,\dots,s\}$. Also note that we always have

$$\Big| \sum\nolimits_{B,i} \Big| \le p_i^{j_1} - p_i^{j_i-1}.$$

In order to shorten notation we write, for given $n \in \{0,\dots,N-1\}$ and given $i \in \{1,\dots,s\}$,

$$m \in \begin{cases} \Theta_1(n,i) & \text{if } n-m \equiv 0 \ (p_i^{j_i}) \text{ (Case 1)}, \\ \Theta_2(n,i) & \text{if } n-m \not\equiv 0 \ (p_i^{j_i}) \text{ and } n-m \equiv 0 \ (p_i^{j_i-1}) \text{ (Case 2)}. \end{cases}$$

Since $\sum_B$ is a nonnegative real, we have $\sum_B = |\sum_B|$. Hence, inserting this back into (9), we obtain

$$\begin{aligned} \sum\nolimits_B &\le \frac{1}{N^2} \Big(\prod_{i=1}^{s} (p_i^{j_i} - p_i^{j_i-1}) \Big) \\ &\qquad \times \sum_{\mathfrak{v} \subseteq [s]} \Bigg| \sum_{n=0}^{N-1} e\Big(\frac{1}{N} \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle n \Big) \sum_{\substack{m=0 \\ m \in \Theta_1(n,i),\, i \in \mathfrak{v} \\ m \in \Theta_2(n,i),\, i \notin \mathfrak{v}}}^{N-1} e\Big(\frac{-1}{N} \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle m \Big) \Bigg| \\ &\le \frac{1}{N^2} \prod_{i=1}^{s} (p_i^{j_i} - p_i^{j_i-1}) \sum_{\mathfrak{v} \subseteq [s]} \Bigg| \sum_{R_1=0}^{p_1^{j_1}-1} \cdots \sum_{R_s=0}^{p_s^{j_s}-1} \sum_{\substack{n=0 \\ \forall i: n \equiv R_i \ (p_i^{j_i})}}^{N-1} e\Big(\frac{1}{N} \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle n \Big) \\ &\qquad \times \sum_{\substack{m=0 \\ m \in \Theta_1(n,i),\, i \in \mathfrak{v} \\ m \in \Theta_2(n,i),\, i \notin \mathfrak{v}}}^{N-1} e\Big(\frac{-1}{N} \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle m \Big) \Bigg|. \end{aligned}$$

Consider now a fixed $\mathfrak{v} \subseteq [s]$. Note that, for given n, given $R_1,\dots,R_s$, and for $i \notin \mathfrak{v}$, the condition $m \in \Theta_2(n,i)$ is equivalent to

$$m \not\equiv R_i \ (p_i^{j_i}) \wedge m \equiv R_i \ (p_i^{j_i-1}). \tag{10}$$

Also note that for any $i \in [s] \setminus \mathfrak{v}$ there exists a set $\{\lambda_{i,1},\dots,\lambda_{i,p_i-1}\}$ of cardinality $p_i - 1$ such that (10) holds if and only if

$$m \equiv \lambda_{i,t_i} \ (p_i^{j_i})$$

for some $t_i \in \{1,\dots,p_i-1\}$. Hence we obtain

$$\sum\nolimits_B \leq \frac{1}{N^2}\prod_{i=1}^{s}(p_i^{j_i}-p_i^{j_i-1})\sum_{\mathfrak{v}\subseteq[s]}\sum_{R_1=0}^{p_1^{j_1}-1}\cdots\sum_{R_s=0}^{p_s^{j_s}-1}\Bigg|\sum_{\substack{n=0\\ \forall i: n\equiv R_i\ (p_i^{j_i})}}^{N-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle n\Big)\Bigg|$$
$$\times\sum_{t_1=1}^{p_1-1}\cdots\sum_{t_s=1}^{p_s-1}\Bigg|\sum_{\substack{m=0\\ m\equiv R_i\ (p_i^{j_i}),\, i\in\mathfrak{v}\\ m\equiv\lambda_{i,t_i}\ (p_i^{j_i}),\, i\notin\mathfrak{v}}}^{N-1} e\Big(\frac{-1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle m\Big)\Bigg|.$$

Let us now consider the term

$$\Bigg|\sum_{\substack{n=0\\ \forall i: n\equiv R_i(p_i^{j_i})}}^{N-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle n\Big)\Bigg| \tag{11}$$

for some fixed $R_1,\ldots,R_s$. Since $p_1,\ldots,p_s$ are coprime, there is exactly one residue ρ_1 modulo $Q=p_1^{j_1}\cdots p_s^{j_s}$ with the property that the index n satisfies the required congruences in (11). Consequently, the system of congruences $n\equiv R_i\ (p_i^{j_i})$, $1\leq i\leq s$, holds if and only if

$$n\in\{\nu Q+\rho_1,\ 0\leq\nu\leq\lfloor N/Q\rfloor-1+\theta_1\},$$

where $\theta_1\in\{0,1\}$. Therefore,

$$\Bigg|\sum_{\substack{n=0\\ n\equiv R_i\ (p_i^{j_i})}}^{N-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle n\Big)\Bigg| = \Bigg|\sum_{\nu=0}^{\lfloor N/Q\rfloor-1+\theta_1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle(\nu Q+\rho_1)\Big)\Bigg|$$
$$=\Bigg|\sum_{\nu=0}^{\lfloor N/Q\rfloor-1+\theta_1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q\Big)\Bigg| \leq \Bigg|\sum_{\nu=0}^{\lfloor N/Q\rfloor-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q\Big)\Bigg|+1.$$

In exactly the same fashion, we obtain

$$\Bigg|\sum_{\substack{m=0\\ m\equiv R_i\ (p_i^{j_i}),\, i\in\mathfrak{v}\\ m\equiv\lambda_{i,t_i}\ (p_i^{j_i}),\, i\notin\mathfrak{v}}}^{N-1} e\Big(\frac{-1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle m\Big)\Bigg| \leq \Bigg|\sum_{\nu=0}^{\lfloor N/Q\rfloor-1} e\Big(\frac{-1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q\Big)\Bigg|+1.$$

Since Q is independent of $\mathfrak{v}$, the R_i, and the t_i, we get

$$\sum\nolimits_B \leq \frac{1}{N^2}\Big(\prod_{i=1}^{s}p_i^{j_i}\Big)2^s\Big(\prod_{i=1}^{s}p_i^{j_i}\Big)\Big(\prod_{i=1}^{s}p_i\Big)\Bigg(\Bigg|\sum_{\nu=0}^{\lfloor N/Q\rfloor-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q\Big)\Bigg|+1\Bigg)^2$$
$$=c_4\frac{Q^2}{N^2}\Bigg(\Bigg|\sum_{\nu=0}^{\lfloor N/Q\rfloor-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q\Big)\Bigg|+1\Bigg)^2.$$

Now we insert this back into (8), which yields

$$
\begin{aligned}
(12)\qquad \textstyle\sum_{[s]}^{*} &\le c_4 \sum_{\boldsymbol{k}^{(2)}\in C_d^*(N^2)} r_2(\boldsymbol{k}^{(2)}) \sum_{j_1=1}^{m_1}\cdots\sum_{j_s=1}^{m_s}\Big(\prod_{i=1}^{s} p_i^{-2(j_i-1)}\Big)\\
&\quad\times \frac{Q^2}{N^2}\bigg(\bigg|\sum_{\nu=0}^{\lfloor N/Q\rfloor-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle \nu Q\Big)\bigg|+1\bigg)^2\\
&= \frac{c_5}{N^2}\sum_{\boldsymbol{k}^{(2)}\in C_d^*(N^2)} r_2(\boldsymbol{k}^{(2)}) \sum_{j_1=1}^{m_1}\cdots\sum_{j_s=1}^{m_s}\bigg(\bigg|\sum_{\nu=0}^{\lfloor N/Q\rfloor-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle \nu Q\Big)\bigg|+1\bigg)^2\\
&= \frac{c_5}{N^2}\sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)}) \sum_{j_1=1}^{m_1}\cdots\sum_{j_s=1}^{m_s}\bigg(\Big\lfloor\frac{N}{Q}\Big\rfloor+1\bigg)^2\\
&\quad+ \frac{c_5}{N^2}\sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)}) \sum_{j_1=1}^{m_1}\cdots\sum_{j_s=1}^{m_s}\bigg(\bigg|\sum_{\nu=0}^{\lfloor N/Q\rfloor-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle \nu Q\Big)\bigg|+1\bigg)^2\\
&\le c_6(\log N)^s \sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)})\\
&\quad+ \frac{c_5}{N^2}\sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}} \sum_{j_1=1}^{m_1}\cdots\sum_{j_s=1}^{m_s} r_2(\boldsymbol{k}^{(2)})\bigg(\bigg|\sum_{\nu=0}^{\lfloor N/Q\rfloor-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle \nu Q\Big)\bigg|+1\bigg)^2.
\end{aligned}
$$

Let us now return to the sums $\sum_{\mathfrak{u}}^{*}$ defined in (6). Let $\emptyset \neq \mathfrak{u} \subseteq [s]$ be arbitrarily chosen, and write

$$\mathfrak{u} = \{v_1,\ldots,v_{|\mathfrak{u}|}\}.$$

In analogy to the derivation of (12), we get

$$
\begin{aligned}
\textstyle\sum_{\mathfrak{u}}^{*} &\le c_7(\log N)^{|\mathfrak{u}|} \sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)})\\
&\quad+ \frac{c_7}{N^2}\sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}} \sum_{j_{v_1}=1}^{m_{v_1}}\cdots\sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r_2(\boldsymbol{k}^{(2)})\\
&\quad\times\bigg(\bigg|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor-1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle \nu Q_{\mathfrak{u}}\Big)\bigg|+1\bigg)^2
\end{aligned}
$$

$$\leq c_7(\log N)^s \sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)})$$

$$+\frac{c_7}{N^2} \sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}} \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r_2(\boldsymbol{k}^{(2)})$$

$$\times \Bigg(\Bigg|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor -1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle \nu Q_{\mathfrak{u}}\Big)\Bigg| + 1\Bigg)^2,$$

where $Q_{\mathfrak{u}} := \prod_{i=1}^{|\mathfrak{u}|} b_i^{j_{v_i}}$.

Putting all these estimates together and plugging them into (5), we obtain

$$\sum\nolimits_3 \leq \sum_{\emptyset\neq\mathfrak{u}\subseteq[s]} c_7(\log N)^s \sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)})$$

$$+ \sum_{\emptyset\neq\mathfrak{u}\subseteq[s]} \frac{c_7}{N^2} \sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}} \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r_2(\boldsymbol{k}^{(2)})$$

$$\times \Bigg(\Bigg|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor -1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle \nu Q_{\mathfrak{u}}\Big)\Bigg| + 1\Bigg)^2$$

$$= c_8(\log N)^s \sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)})$$

$$+ \sum_{\emptyset\neq\mathfrak{u}\subseteq[s]} \frac{c_7}{N^2} \sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}} \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r_2(\boldsymbol{k}^{(2)})$$

$$\times \Bigg(\Bigg|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor -1} e\Big(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle \nu Q_{\mathfrak{u}}\Big)\Bigg| + 1\Bigg)^2.$$

Plugging our results for $\sum_2$ and $\sum_3$ into (4), and simplifying the constants, we obtain the bound

$$F_N^2(\boldsymbol{\omega}) \leq c_9\frac{(\log N)^s}{N^2} + c_{10}(\log N)^s \sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)}) \tag{13}$$

$$+\frac{c_{11}}{N^2}\sum_{\emptyset\neq\mathfrak{u}\subseteq[s]}\sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}}\sum_{j_{v_1}=1}^{m_{v_1}}\cdots\sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r_2(\boldsymbol{k}^{(2)})$$

$$\times\left(\left|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor-1} e\left(\frac{1}{N}\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q_{\mathfrak{u}}\right)\right|+1\right)^2.$$

Let us now study

$$\sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)})$$

in greater detail. Let us define

$$E_d^*(N^2) := \{(k_1^{(2)},\dots,k_d^{(2)})\in C_d^*(N^2) : k_j^{(2)}\equiv 0\ (N) \text{ for all } j,\ 1\le j\le d\},$$

and $G_d^*(N^2) := C_d^*(N^2)\setminus E_d^*(N^2)$. Note that for $\boldsymbol{k}^{(2)}\in E_d^*(N^2)$ the condition $\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\ (N)$ is trivially fulfilled. Furthermore, the components of $\boldsymbol{k}^{(2)}\in E_d^*(N^2)$ must all be multiples of N. We then obviously have

$$\begin{aligned}\sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)}) &= \sum_{\boldsymbol{k}^{(2)}\in E_d^*(N^2)} r_2(\boldsymbol{k}^{(2)}) + \sum_{\substack{\boldsymbol{k}^{(2)}\in G_d^*(N^2)\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)})\\ &\le\left(1+2\sum_{z=1}^{\infty}\frac{1}{z^2N^2}\right)^d - 1 + \sum_{\substack{\boldsymbol{k}^{(2)}\in G_d^*(N^2)\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)})\\ &\le\frac{c_{12}}{N^2}+\sum_{\substack{\boldsymbol{k}^{(2)}\in G_d^*(N^2)\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)}).\end{aligned}$$

On the other hand, for $\boldsymbol{k}^{(2)}\in E_d^*(N^2)$, the condition $\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\ (N)$ can never be fulfilled, so

$$\sum_{\emptyset\neq\mathfrak{u}\subseteq[s]}\sum_{\substack{\boldsymbol{k}^{(2)}\in C_d^*(N^2)\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}}\sum_{j_{v_1}=1}^{m_{v_1}}\cdots$$

$$\cdots\sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r_2(\boldsymbol{k}^{(2)})\left(\left|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor-1} e\left(\frac{1}{N}\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q_{\mathfrak{u}}\right)\right|+1\right)^2$$

$$= \sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \sum_{\substack{\boldsymbol{k}^{(2)} \in G_d^*(N^2) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \not\equiv 0\,(N)}} \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r_2(\boldsymbol{k}^{(2)}) \biggl(\biggl| \sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}} \rfloor - 1} e\Bigl(\frac{1}{N} \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \nu Q_{\mathfrak{u}}\Bigr) \biggr| + 1 \biggr)^2,$$

and we arrive at

$$F_N^2(\boldsymbol{\omega}) \le c_{13} \frac{(\log N)^s}{N^2} + c_{10} (\log N)^s \sum_{\substack{\boldsymbol{k}^{(2)} \in G_d^*(N^2) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \equiv 0\,(N)}} r_2(\boldsymbol{k}^{(2)}) \tag{14}$$

$$+ \frac{c_{11}}{N^2} \sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \sum_{\substack{\boldsymbol{k}^{(2)} \in G_d^*(N^2) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \not\equiv 0\,(N)}} \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r_2(\boldsymbol{k}^{(2)})$$

$$\times \biggl(\biggl| \sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}} \rfloor - 1} e\Bigl(\frac{1}{N} \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \nu Q_{\mathfrak{u}}\Bigr) \biggr| + 1 \biggr)^2$$

$$= \Bigl(c_{14} \frac{(\log N)^{s/2}}{N} \Bigr)^2 + \sum_{\substack{\boldsymbol{k}^{(2)} \in G_d^*(N^2) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \equiv 0\,(N)}} (c_{15} (\log N)^{s/2} r_1(\boldsymbol{k}^{(2)}))^2$$

$$+ \sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \sum_{\substack{\boldsymbol{k}^{(2)} \in G_d^*(N^2) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \not\equiv 0\,(N)}}$$

$$\times \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} \biggl(\frac{c_{16} r_1(\boldsymbol{k}^{(2)})}{N} \biggl(\biggl| \sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}} \rfloor - 1} e\Bigl(\frac{1}{N} \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \nu Q_{\mathfrak{u}}\Bigr) \biggr| + 1 \biggr) \biggr)^2.$$

Since all summands in (14) are nonnegative, we can apply an inequality which is sometimes (incorrectly) referred to as Jensen's inequality ([5]) to obtain

$$F_N^2(\boldsymbol{\omega}) \le \biggl[c_{14} \frac{(\log N)^{s/2}}{N} + \sum_{\substack{\boldsymbol{k}^{(2)} \in G_d^*(N^2) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \equiv 0\,(N)}} c_{15} (\log N)^{s/2} r_1(\boldsymbol{k}^{(2)})$$

$$+ \sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \sum_{\substack{\boldsymbol{k}^{(2)} \in G_d^*(N^2) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \not\equiv 0\,(N)}} \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} \frac{c_{16} r_1(\boldsymbol{k}^{(2)})}{N}$$

$$\times \biggl(\biggl| \sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}} \rfloor - 1} e\Bigl(\frac{1}{N} \langle \boldsymbol{k}^{(2)}, \boldsymbol{g} \rangle \nu Q_{\mathfrak{u}}\Bigr) \biggr| + 1 \biggr) \biggr]^2.$$

Writing $r(\cdot)$ instead of $r_1(\cdot)$, we obtain

$$F_N(\boldsymbol{\omega}) \leq c_{14}\frac{(\log N)^{s/2}}{N} + c_{15}(\log N)^{s/2} \sum_{\substack{\boldsymbol{k}^{(2)}\in G_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r(\boldsymbol{k}^{(2)}) \tag{15}$$

$$+ c_{16}\frac{1}{N}\sum_{\emptyset\neq\mathfrak{u}\subseteq[s]}\ \sum_{\substack{\boldsymbol{k}^{(2)}\in G_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}}\ \sum_{j_{v_1}=1}^{m_{v_1}}\cdots\sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r(\boldsymbol{k}^{(2)})$$

$$\times\left(\left|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor-1} e\left(\frac{1}{N}\langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle \nu Q_{\mathfrak{u}}\right)\right|+1\right).$$

We would now like to show the existence of a generating vector $\boldsymbol{g}$ such that the above bound on $F_N(\boldsymbol{\omega})$ is small. To this end, we average over all $\boldsymbol{g} = (g_1, \ldots, g_d) \in \{1, \ldots, N-1\}^d$. We then first study

$$M_1 := \frac{1}{(N-1)^d}\sum_{g_1=1}^{N-1}\cdots\sum_{g_d=1}^{N-1}\ \sum_{\substack{\boldsymbol{k}^{(2)}\in G_d^*(N^2)\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}} r(\boldsymbol{k}^{(2)})$$

$$= \frac{1}{(N-1)^d}\sum_{\boldsymbol{k}^{(2)}\in G_d^*(N^2)} r(\boldsymbol{k}^{(2)})\sum_{g_1=1}^{N-1}\cdots\sum_{\substack{g_d=1\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}}^{N-1} 1.$$

Let now $\boldsymbol{k}^{(2)} \in G_d^*(N^2)$ be fixed. Due to the definition of $G_d^*(N^2)$, there must be at least one component of $\boldsymbol{k}^{(2)}$ which is not congruent 0 modulo N. Let $d_0 \in \{1, \ldots, d\}$ be the maximal index such that this is the case for $k_{d_0}^{(2)}$. We then have

$$\sum_{g_1=1}^{N-1}\cdots\sum_{\substack{g_d=1\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}}^{N-1} 1 = (N-1)^{d-d_0}\sum_{g_1=1}^{N-1}\cdots\sum_{\substack{g_{d_0}=1\\ k_1^{(2)}g_1+\cdots+k_{d_0}^{(2)}g_{d_0}\equiv 0\,(N)}}^{N-1} 1.$$

Given $\boldsymbol{k}^{(2)}$ and $g_1, \ldots, g_{d_0-1}$, there exists at most one solution $g_{d_0} \in \{1, \ldots, N-1\}$ to the congruence

$$k_1^{(2)}g_1 + \cdots + k_{d_0}^{(2)}g_{d_0} \equiv 0\ (N),$$

so we obtain

$$\sum_{g_1=1}^{N-1}\cdots\sum_{\substack{g_d=1\\ \langle \boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\equiv 0\,(N)}}^{N-1} 1 \leq (N-1)^{d-1},$$

and thus

$$M_1 \le c_{17}\frac{1}{N}\sum_{\boldsymbol{k}^{(2)}\in G_d^*(N^2)} r(\boldsymbol{k}^{(2)}) \le c_{18}\frac{(\log N)^d}{N},$$

where we used a well-known estimate for sums of the form $\sum_{k=1}^{K}|k|^{-1}$, which can be found, e.g., in [24].

In the next step, let us, for fixed $\mathfrak{u}\subseteq[s]$, $\mathfrak{u}\neq\emptyset$, study the expression

$$\begin{aligned}
M_{2,\mathfrak{u}} :=& \frac{1}{(N-1)^d}\sum_{g_1=1}^{N-1}\cdots\sum_{g_d=1}^{N-1}\sum_{\substack{\boldsymbol{k}^{(2)}\in G_d^*(N^2)\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}}\sum_{j_{v_1}=1}^{m_{v_1}}\cdots\sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r(\boldsymbol{k}^{(2)})\\
&\times\left(\left|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor-1} e\left(\frac{1}{N}\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q_{\mathfrak{u}}\right)\right|+1\right)\\
\le& \sum_{\boldsymbol{k}^{(2)}\in G_d^*(N^2)}\sum_{j_{v_1}=1}^{m_{v_1}}\cdots\sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r(\boldsymbol{k}^{(2)})\\
&+\frac{1}{(N-1)^d}\sum_{g_1=1}^{N-1}\cdots\sum_{g_d=1}^{N-1}\sum_{\substack{\boldsymbol{k}^{(2)}\in G_d^*(N^2)\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}}\sum_{j_{v_1}=1}^{m_{v_1}}\cdots\sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r(\boldsymbol{k}^{(2)})\\
&\times\left|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor-1} e\left(\frac{1}{N}\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q_{\mathfrak{u}}\right)\right|\\
\le& c_{19}(\log N)^{s+d}+\frac{1}{(N-1)^d}\sum_{j_{v_1}=1}^{m_{v_1}}\cdots\sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}}\sum_{\boldsymbol{k}^{(2)}\in G_d^*(N^2)} r(\boldsymbol{k}^{(2)})\\
&\times\sum_{g_1=1}^{N-1}\cdots\sum_{\substack{g_d=1\\ \langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\,(N)}}^{N-1}\left|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor-1} e\left(\frac{1}{N}\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q_{\mathfrak{u}}\right)\right|.
\end{aligned}$$

Note that, in the last line, $Q_{\mathfrak{u}}$ is coprime to N and $\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\not\equiv 0\ (N)$. Consequently, the remainder of $Q_{\mathfrak{u}}\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle$, which will be denoted by $f(Q_{\mathfrak{u}},\boldsymbol{k}^{(2)},\boldsymbol{g})$ in the following, is also incongruent 0 modulo N. Using a well-known result that is outlined, e.g., in [32, p. 334], we get

$$\begin{aligned}
\left|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor-1} e\left(\frac{1}{N}\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle\nu Q_{\mathfrak{u}}\right)\right| &= \left|\sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}}\rfloor-1} e\left(\frac{\langle\boldsymbol{k}^{(2)},\boldsymbol{g}\rangle Q_{\mathfrak{u}}}{N}\nu\right)\right|\\
&\le \frac{N}{\min\{f(Q_{\mathfrak{u}},\boldsymbol{k}^{(2)},\boldsymbol{g}),N-f(Q_{\mathfrak{u}},\boldsymbol{k}^{(2)},\boldsymbol{g})\}}.
\end{aligned}$$

Let now $\boldsymbol{k}^{(2)} \in G_d^*(N^2)$ be fixed. Again, due to the definition of $G_d^*(N^2)$, there must be a maximal index d_0 such that $k_{d_0}^{(2)} \not\equiv 0\ (N)$. Hence we can write

$$\sum_{g_1=1}^{N-1} \cdots \sum_{\substack{g_d=1 \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle \not\equiv 0\,(N)}}^{N-1} \frac{N}{\min\{f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g}), N - f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g})\}}$$
$$= (N-1)^{d-d_0} \sum_{g_1=1}^{N-1} \cdots$$
$$\cdots \sum_{\substack{g_{d_0}=1 \\ k_1^{(2)} g_1 + \cdots + k_{d_0}^{(2)} g_{d_0} \not\equiv 0\,(N)}}^{N-1} \frac{N}{\min\{f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g}), N - f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g})\}}.$$

As in the analysis of M_1, since $k_{d_0}^{(2)} \not\equiv 0\ (N)$, for given $g_1, \ldots, g_{d_0-1}$ there is exactly one integer $a \in \{0, \ldots, N-1\}$ such that

$$k_1^{(2)} g_1 + \cdots + k_{d_0-1}^{(2)} g_{d_0-1} + k_{d_0}^{(2)} a \equiv 0\ (N).$$

Hence,

$$k_1^{(2)} g_1 + \cdots + k_{d_0}^{(2)} g_{d_0} \not\equiv 0\ (N)$$

whenever $g_{d_0} \in \{0, 1 \ldots, N-1\} \setminus \{a\}$. Accordingly,

$$(N-1)^{d-d_0} \sum_{g_1=1}^{N-1} \cdots \sum_{\substack{g_{d_0}=1 \\ k_1^{(2)} g_1 + \cdots + k_{d_0}^{(2)} g_{d_0} \not\equiv 0\,(N)}}^{N-1} \frac{N}{\min\{f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g}), N - f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g})\}}$$
$$\leq (N-1)^{d-d_0} \sum_{g_1=1}^{N-1} \cdots \sum_{g_{d_0-1}=1}^{N-1} \sum_{\substack{g_{d_0}=0 \\ g_{d_0} \neq a}}^{N-1} \frac{N}{\min\{f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g}), N - f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g})\}}.$$

However, if g_{d_0} runs through all of $\{0, \ldots, N-1\} \setminus \{a\}$, the dot product $k_1^{(2)} g_1 + \cdots + k_{d_0}^{(2)} g_{d_0}$ runs, modulo N, through all of $\{1, \ldots, N-1\}$. Furthermore, as $Q_{\mathfrak{u}}$ is coprime to N, the values of $f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g})$ also run through the whole set $\{1, \ldots, N-1\}$. Hence,

$$(N-1)^{d-d_0} \sum_{g_1=1}^{N-1} \cdots \sum_{g_{d_0-1}=1}^{N-1} \sum_{\substack{g_{d_0}=0 \\ g_{d_0} \neq a}}^{N-1} \frac{N}{\min\{f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g}), N - f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g})\}}$$
$$\leq N^{d-d_0} \sum_{g_1=1}^{N-1} \cdots \sum_{g_{d_0-1}=1}^{N-1} \sum_{z=1}^{N-1} \frac{N}{\min\{z, N-z\}} \leq c_{20} N^d \log N,$$

where we used another well-known estimate that can be found in [32]. We obtain

$$\begin{aligned} M_{2,\mathfrak{u}} &\le c_{19}(\log N)^{s+d} + c_{20}\log N \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} \sum_{\boldsymbol{k}^{(2)}\in G_d^*(N^2)} r(\boldsymbol{k}^{(2)}) \\ &\le c_{21}(\log N)^{s+d+1}. \end{aligned}$$

Finally, combining our estimates for M_1 and $M_{2,\mathfrak{u}}$ shows the existence of a generating vector $\boldsymbol{g}$ such that the point set $\boldsymbol{\omega}$ satisfies

$$F_N(\boldsymbol{\omega}) \le c\frac{(\log N)^{s+d+1}}{N},$$

with a positive constant c not depending on N, as claimed. ∎

By Theorem 2.1 we have shown the existence of lattice point sets having, when combined with the first N points of Halton sequences, low diaphony and hence good uniform distribution properties. With Theorem 2.1, the search for a corresponding "good" generating vector is possible, but the search space is of cardinality $(N-1)^d$. In the next section, we show how to reduce the search space.

3. Korobov-type generating vectors. A cardinality $(N-1)^d$ of candidate vectors for $\boldsymbol{g}$ renders a practical search infeasible for high values of N and/or d. However, we can improve on this result by considering a very special choice of generating vectors only. These vectors $\boldsymbol{g}$ are of the form $\boldsymbol{g} = (g, g^2, \dots, g^d)$ for some $g \in \{1, \dots, N-1\}$, and are usually referred to as *Korobov-type* generating vectors (cf. [17]). Frequently, one deals with Korobov-type generating vectors of the form $\boldsymbol{g} = (1, g, g^2, \dots, g^{d-1})$, but it is for technical reasons more useful to consider the slightly modified form $\boldsymbol{g} = (g, g^2, \dots, g^d)$. In the next theorem, we are going to show the existence of Korobov-type generating vectors $\boldsymbol{g}$ such that for the mixture of a lattice point set generated by $\boldsymbol{g}$ with a Halton sequence, we still obtain low diaphony.

THEOREM 3.1. *Let $\boldsymbol{\omega}^{(1)} = (\boldsymbol{\omega}_n^{(1)})_{n=0}^{\infty}$ be an s-dimensional Halton sequence to the base $\boldsymbol{p} = (p_1, \dots, p_s)$, where $p_1, \dots, p_s$ are s distinct primes. Let N be a prime different from $p_1, \dots, p_s$. Then there exists a vector $\boldsymbol{g} = (g, g^2, \dots, g^d)$ with $g \in \{1, \dots, N-1\}$ such that the point set $\boldsymbol{\omega} = (\boldsymbol{\omega}_n)_{n=0}^{N-1} = (\boldsymbol{\omega}_n^{(1)}, \boldsymbol{\omega}_n^{(2)})_{n=0}^{N-1}$, where $\boldsymbol{\omega}_n^{(2)} = \{n\boldsymbol{g}/N\}$ for $0 \le n \le N-1$, satisfies*

$$F_N(\boldsymbol{\omega}) \le c\frac{(\log N)^{s+d+1}}{N},$$

where c is a constant that is independent of N.

Proof. The proof of the theorem is in many ways similar to that of Theorem 2.1. Thus, we only point out those passages different from the proof in Section 2. In the same way as above, we arrive at an inequality which is the same as (15), where we had

$$F_N(\boldsymbol{\omega}) \leq c_{14}\frac{(\log N)^{s/2}}{N} + c_{15}(\log N)^{s/2} \sum_{\substack{\boldsymbol{k}^{(2)} \in G_d^*(N^2) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle \equiv 0\,(N)}} r(\boldsymbol{k}^{(2)})$$

$$+ c_{16}\frac{1}{N} \sum_{\emptyset \neq \mathfrak{u} \subseteq [s]} \sum_{\substack{\boldsymbol{k}^{(2)} \in G_d^*(N^2) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle \not\equiv 0\,(N)}} \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r(\boldsymbol{k}^{(2)})$$

$$\times \left(\Bigg| \sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}} \rfloor - 1} e\left(\frac{1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle \nu Q_{\mathfrak{u}}\right) \Bigg| + 1 \right).$$

We average over the possible generating vectors $\boldsymbol{g} = \rho(g) := (g, g^2, \ldots, g^d)$ for $g \in \{1, \ldots, N-1\}$. To this end, let us first consider the quantity

$$M_{1,K} := \frac{1}{(N-1)} \sum_{\boldsymbol{k}^{(2)} \in G_d^*(N^2)} r(\boldsymbol{k}^{(2)}) \sum_{\substack{g=1 \\ \boldsymbol{g}=\rho(g) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle \equiv 0\,(N)}}^{N-1} 1.$$

For a given $\boldsymbol{k}^{(2)} = (k_1^{(2)}, \ldots, k_d^{(2)}) \in G_d^*(N)$, there exists a maximal d_0 such that $k_{d_0}^{(2)} \not\equiv 0\ (N)$, and so the congruence

$$g k_1^{(2)} + g^2 k_2^{(2)} + \cdots + g^d k_d^{(2)} \equiv 0\ (N)$$

has at most $d_0 \leq d$ solutions. Therefore,

$$M_{1,K} \leq c_{22}\frac{(\log N)^d}{N-1},$$

where $c_{22} > 0$ is another constant independent of N.

In the next step, let us, for fixed $\mathfrak{u} \subseteq [s]$, $\mathfrak{u} \neq \emptyset$, study the expression

$$M_{2,\mathfrak{u},K} := \frac{1}{N-1} \sum_{\substack{g=1 \\ \boldsymbol{g}=\rho(g)}}^{N-1} \sum_{\substack{\boldsymbol{k}^{(2)} \in G_d^*(N^2) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle \not\equiv 0\,(N)}} \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} r(\boldsymbol{k}^{(2)})$$

$$\times \left(\Bigg| \sum_{\nu=0}^{\lfloor N/Q_{\mathfrak{u}} \rfloor - 1} e\left(\frac{1}{N}\langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle \nu Q_{\mathfrak{u}}\right) \Bigg| + 1 \right).$$

In exactly the same way as in the proof of Theorem 2.1, we see that

$$M_{2,\mathfrak{u},K} \le c_{23}(\log N)^{s+d} + \frac{1}{(N-1)} \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} \sum_{\boldsymbol{k}^{(2)} \in G_d^*(N^2)} r(\boldsymbol{k}^{(2)}) \times \sum_{\substack{g=1 \\ \boldsymbol{g}=\rho(g) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle \not\equiv 0\,(N)}}^{N-1} \frac{N}{\min\{f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g}), N - f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g})\}}$$

$$= c_{23}(\log N)^{s+d} + \frac{1}{(N-1)} \sum_{j_{v_1}=1}^{m_{v_1}} \cdots \sum_{j_{v_{|\mathfrak{u}|}}=1}^{m_{v_{|\mathfrak{u}|}}} \sum_{\boldsymbol{k}^{(2)} \in G_d^*(N^2)} r(\boldsymbol{k}^{(2)}) \times \sum_{a=1}^{N-1} \sum_{\substack{g=1 \\ \boldsymbol{g}=\rho(g) \\ \langle \boldsymbol{k}^{(2)}, \boldsymbol{g}\rangle \equiv a\,(N)}}^{N-1} \frac{N}{\min\{f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g}), N - f(Q_{\mathfrak{u}}, \boldsymbol{k}^{(2)}, \boldsymbol{g})\}}.$$

Similar to what we outlined for $M_{1,K}$, the congruence

$$g k_1^{(2)} + g^2 k_2^{(2)} + \cdots + g^d k_d^{(2)} \equiv a\ (N),$$

which is equivalent to

$$-a + g k_1^{(2)} + g^2 k_2^{(2)} + \cdots + g^d k_d^{(2)} \equiv 0\ (N), \tag{16}$$

has at most $d_0 \le d$ solutions g. Therefore, using the same methods as in the proof of Theorem 2.1, we obtain

$$M_{2,\mathfrak{u},K} = c_{24}((\log N)^{s+d+1}).$$

The rest of the proof follows exactly the lines of that of Theorem 2.1. ∎

Remark 3.2. We remark that bounding $M_{2,\mathfrak{u},K}$ in the proof of Theorem 3.1 would not work if we considered generating vectors $\boldsymbol{g} = (1, g, g^2, \ldots, g^{d-1})$ instead of those considered here, since in this case (16) might have $N-1$ solutions g if $k_1^{(2)} = a$ and $k_2^{(2)} = \cdots = k_d^{(2)} = 0$.

4. Remarks and conclusion. In this paper, we have considered hybrid point sets $\boldsymbol{\omega}$, which are built from Halton sequences and lattice point sets. Under some fairly general assumptions on the bases of the Halton sequence and on the cardinality of the lattice point set, we have shown that there always exist generating vectors $\boldsymbol{g}$ of a d-dimensional lattice point set, such that, if we combine the lattice point set with the first N points of an s-dimensional Halton sequence, we obtain a diaphony of order

$$\mathcal{O}\left(\frac{(\log N)^{s+d+1}}{N}\right),$$

where the implied constant is independent of N. For non-hybrid point sets, such as s-dimensional (pure) Halton sequences or (t, s)-sequences, it is known that one can achieve a diaphony of order $N^{-1}(\log N)^{s/2}$ (cf. [19] and [31]). Therefore, we see that the hybrid sequences considered here can have a diaphony which is close to that of non-hybrid quasi-Monte Carlo point sets, up to $\log N$-terms. On the other hand, it seems that there is no easy way to obtain a diaphony of order, say, $N^{-1}(\log N)^{(s+d)/2}$, as our additional $\log N$-terms were caused by having to apply "Jensen's inequality" before averaging over $\boldsymbol{g}$ (see the step after (14)).

Furthermore, similarly to what is stated in the conclusion of [18], it would be beneficial to not only have existence results for good generating vectors or existence results for good Korobov-type generating vectors, but also construction algorithms, e.g., component-wise constructions, for such generating vectors. This problem will be pursued in future research work.

Finally, we would like to point out that our Theorems 2.1 and 3.1 imply the existence of vectors $\boldsymbol{g}$ such that if we mix the lattice point set generated by $\boldsymbol{g}$ with a Halton sequence, we obtain low diaphony. Note, however, that $\sum_2$ in the proof of our results is essentially the usual diaphony of a pure lattice point set. Therefore, we can conclude that any vector $\boldsymbol{g}$ that guarantees low diaphony of our hybrid point sets, automatically guarantees low diaphony of the pure lattice point sets contained in the hybrid point sets.

Acknowledgements. P. Kritzer would like to thank P. Hellekalek for his hospitality during his visits to the Department of Mathematics at the University of Salzburg, and he would also like to thank F. Pillichshammer for discussions and comments.

Research of P. Hellekalek was supported by the University of Salzburg, projects P1884/5-2009 and P1884/4-2010.

P. Kritzer gratefully acknowledges the support of the Austrian Science Fund (Project P23389-N18).

References

[1] J. Dick and F. Pillichshammer, *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge Univ. Press, Cambridge, 2010.

[2] M. Drmota and R. F. Tichy, *Sequences, Discrepancies and Applications*, Lecture Notes in Math. 1651, Springer, Berlin, 1997.

[3] V. S. Grozdanov and S. S. Stoilova, *On the theory of b-adic diaphony*, C. R. Acad. Bulgare Sci. 54 (2001), no. 3, 31–34.

[4] J. H. Halton, *On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals*, Numer. Math. 2 (1960), 84–90.

[5] G. H. Hardy, J. E. Littlewood and G. Pólya, *Inequalities*, Cambridge Univ. Press, Cambridge, 1934.

[6] P. Hellekalek, *A general discrepancy estimate based on p-adic arithmetics*, Acta Arith. 139 (2009), 117–129.

[7] P. Hellekalek, *A notion of diaphony based on p-adic arithmetic*, Acta Arith. 145 (2010), 273–284.

[8] P. Hellekalek, *Hybrid function systems in the theory of uniform distribution of sequences*, in: Monte Carlo and Quasi-Monte Carlo Methods 2010, Springer, Berlin, 2012, to appear.

[9] P. Hellekalek and H. Leeb, *Dyadic diaphony*, Acta Arith. 80 (1997), 187–196.

[10] P. Hellekalek and H. Niederreiter, *Constructions of uniformly distributed sequences using the* b*-adic method*, Unif. Distrib. Theory 6 (2011), no. 1, 185–200.

[11] E. Hewitt and K. A. Ross, *Abstract Harmonic Analysis. Vol. I*, Grundlehren Math. Wiss. 115, Springer, Berlin, 2nd ed., 1979.

[12] E. Hlawka, *Zur angenäherten Berechnung mehrfacher Integrale*, Monatsh. Math. 66 (1962), 140–151.

[13] R. Hofer and P. Kritzer, *On hybrid sequences built from Niederreiter–Halton sequences and Kronecker sequences*, Bull. Austral. Math. Soc. 84 (2011), 238–254.

[14] R. Hofer, P. Kritzer, G. Larcher and F. Pillichshammer, *Distribution properties of generalized van der Corput–Halton sequences and their subsequences*, Int. J. Number Theory 5 (2009), 719–746.

[15] R. Hofer and G. Larcher, *Metrical results on the discrepancy of Halton–Kronecker sequences*, Math. Z. 271, 1–11, 2012.

[16] N. M. Korobov, *Approximate evaluation of repeated integrals*, Dokl. Akad. Nauk SSSR 124 (1959), 1207–1210 (in Russian).

[17] N. M. Korobov, *Properties and calculation of optimal coefficients*, Dokl. Akad. Nauk SSSR 132 (1960), 1009–1012 (in Russian).

[18] P. Kritzer, *On an example of finite hybrid quasi-Monte Carlo point sets*, Monatsh. Math., to appear.

[19] P. Kritzer and F. Pillichshammer, *The weighted dyadic diaphony of digital sequences*, in: A. Keller, S. Heinrich and H. Niederreiter (eds.), Monte Carlo and Quasi-Monte Carlo Methods 2006, Springer, Berlin, 2008, 549–560.

[20] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974.

[21] F. Y. Kuo, I. H. Sloan and H. Woźniakowski, *Lattice rules for multivariate approximation in the worst case setting*, in: H. Niederreiter and D. Talay (eds.), Monte Carlo and Quasi-Monte Carlo Methods 2004, Springer, Berlin, 2006, 289–330.

[22] C. Lemieux, *Monte Carlo and Quasi-Monte Carlo Sampling*, Springer Ser. Statist., Springer, New York, 2009.

[23] K. Mahler, *Lectures on Diophantine Approximations. Part I: g-Adic Numbers and Roth's Theorem*, Univ. of Notre Dame Press, Notre Dame, 1961.

[24] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Reg. Conf. Ser. Appl. Math. 63, SIAM, Philadelphia, 1992.

[25] H. Niederreiter, *On the discrepancy of some hybrid sequences*, Acta Arith. 138 (2009), 373–398.

[26] H. Niederreiter, *A discrepancy bound for hybrid sequences involving digital explicit inversive pseudorandom numbers*, Unif. Distrib. Theory 5 (2010), no. 1, 53–63.

[27] H. Niederreiter, *Further discrepancy bounds and an Erdős–Turán–Koksma inequality for hybrid sequences*, Monatsh. Math. 161 (2010), 193–222.

[28] H. Niederreiter, *Discrepancy bounds for hybrid sequences involving matrix-method pseudorandom vectors*, Publ. Math. Debrecen 79 (2011), 589–603.

[29] H. Niederreiter, *Improved discrepancy bounds for hybrid sequences involving Halton sequences*, Acta Arith. 155 (2012), to appear.

[30] H. Niederreiter and A. Winterhof, *Discrepancy bounds for hybrid sequences involving digital explicit inversive pseudorandom numbers*, Unif. Distrib. Theory 6 (2011), no. 1, 33–56.

[31] F. Pillichshammer, *The p-adic diaphony of the Halton sequence*, Funct. Approx. Comment. Math., to appear.

[32] I. E. Shparlinski, *Exponential sums in coding theory, cryptology and algorithms*, in: H. Niederreiter (ed.), Coding Theory and Cryptology (Singapore, 2001), Lect. Notes Ser. Inst. Math. Sci. Nat. Univ. Singap. 1, World Sci., River Edge, NJ, 2002, 323–383.

[33] I. H. Sloan and S. Joe, *Lattice Methods for Multiple Integration*, Oxford Univ. Press, New York, 1994.

[34] J. Spanier, *Quasi-Monte Carlo methods for particle transport problems*, in: H. Niederreiter and P. J.-S. Shiue (eds.), Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, Lecture Notes in Statist. 106, Springer, New York, 1995, 121–148.

[35] P. Zinterhof, *Über einige Abschätzungen bei der Approximation von Funktionen mit Gleichverteilungsmethoden*, Österreich Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II 185 (1976), 121–132.

Peter Hellekalek
Fachbereich Mathematik
Universität Salzburg
Hellbrunnerstr. 34
5020 Salzburg, Austria
E-mail: peter.hellekalek@sbg.ac.at

Peter Kritzer
Institut für Finanzmathematik
Universität Linz
Altenbergerstr. 69
4040 Linz, Austria
E-mail: peter.kritzer@jku.at

Received on 22.12.2011
and in revised form on 11.6.2012 (6916)