*J. Austral. Math. Soc.* (*Series A*) **60** (1996), 228–244

# ON IRREGULARITIES OF DISTRIBUTION III

W. W. L. CHEN

(Received 15 January 1991; revised 23 May 1994)

Communicated by J. H. Loxton

**Dedicated to the memory of Gerold Wagner**

**Abstract**

We study the $L^W$-norm ($2 \leq W < \infty$) of the discrepancy of a sequence of points in the unit cube relative to similar copies of a given convex polygon. In particular, we prove the rather surprising result that the estimates obtained have the same order of magnitude as the analogous question when the sequence of points is replaced by a set of points.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 11K38.
*Keywords and phrases*: Irregularities of distribution, discrepancy.

## 1. Introduction

Suppose that $\mathscr{P}$ is a distribution of $N$ points in the unit torus $U^L = [0, 1)^L$, where $L \geq 1$. For every $\mathbf{y} = (y_1, \ldots, y_L) \in U^L$, let

$$B(\mathbf{y}) = [0, y_1) \times \cdots \times [0, y_L),$$

and let

$$Z_L[\mathscr{P}; B(\mathbf{y})] = \#(\mathscr{P} \cap B(\mathbf{y})),$$

where $\#S$ denotes the cardinality of the set $S$. We are interested in the discrepancy function

$$D_L[\mathscr{P}; B(\mathbf{y})] = Z_L[\mathscr{P}; B(\mathbf{y})] - N\mu_L(B(\mathbf{y})),$$

where $\mu_L$ denotes the usual volume in $U^L$. The case $L = 1$ is trivial. For $L \geq 2$, the following results are well known.

THEOREM 1A. (Roth [6]) *Suppose that $\mathscr{P}$ is a distribution of $N$ points in $U^L$. Then*

$$\int_{U^L} |D_L[\mathscr{P}; B(\mathbf{y})]|^2 \, d\mathbf{y} \gg_L (\log N)^{L-1}.$$

THEOREM 1B. (Roth [7]) *For every natural number $N \geq 2$, there exists a distribution $\mathscr{P}$ of $N$ points in $U^L$ such that*

$$\int_{U^L} |D_L[\mathscr{P}; B(\mathbf{y})]|^2 \, d\mathbf{y} \ll_L (\log N)^{L-1}.$$

We also have the following more general results.

THEOREM 1C. (Schmidt [8]) *Let $W > 1$. Suppose that $\mathscr{P}$ is a distribution of $N$ points in $U^L$. Then*

$$\int_{U^L} |D_L[\mathscr{P}; B(\mathbf{y})]|^W \, d\mathbf{y} \gg_{L,W} (\log N)^{(L-1)W/2}.$$

THEOREM 1D. (Chen [4]) *Let $W > 0$. For every natural number $N \geq 2$, there exists a distribution $\mathscr{P}$ of $N$ points in $U^L$ such that*

$$\int_{U^L} |D_L[\mathscr{P}; B(\mathbf{y})]|^W \, d\mathbf{y} \ll_{L,W} (\log N)^{(L-1)W/2}.$$

Note that the above theorems remain true in the trivial case $L = 1$.

Suppose now that $\mathscr{P}$ is a distribution of $N$ points in the unit torus $U^K = [0, 1]^K$, where $K \geq 2$. Let $A$ be a compact and convex body in $U^K$. For any real number $\lambda \in (0, 1]$, any proper orthogonal transformation $\tau$ in $\mathbb{R}^K$ and any vector $\mathbf{u} \in U^K$, let

$$A(\lambda, \tau, \mathbf{u}) = \{\tau(\lambda \mathbf{x}) + \mathbf{u} : \mathbf{x} \in A\}$$

(note that $A(\lambda, \tau, \mathbf{u})$ and $A$ are similar to each other), and let

$$Z_K[\mathscr{P}; A(\lambda, \tau, \mathbf{u})] = \#(\mathscr{P} \cap A(\lambda, \tau, \mathbf{u})).$$

We are interested in the discrepancy function

$$D_K[\mathscr{P}; A(\lambda, \tau, \mathbf{u})] = Z_K[\mathscr{P}; A(\lambda, \tau, \mathbf{u})] - N\mu_K(A(\lambda, \tau, \mathbf{u})),$$

where $\mu_K$ denotes the usual volume in $U^K$. Corresponding to Theorem 1A, we have the following result. Let $\mathscr{T}$ be the group of all proper orthogonal transformations in $\mathbb{R}^K$, and let $d\tau$ be the volume element of the invariant measure on $\mathscr{T}$, normalized such that $\int_{\mathscr{T}} d\tau = 1$.

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

THEOREM 2A. (Beck [1]) *Suppose that $\mathscr{P}$ is a distribution of $N$ points in $U^K$, and that $A$ is a compact and convex body in $U^K$. Suppose further that $r(A) \geq N^{-1/K}$, where $r(A)$ denotes the radius of the largest inscribed ball of $A$. Then*

$$\int_0^1 \int_{\mathscr{T}} \int_{U^K} |D_K[\mathscr{P}; A(\lambda, \tau, \mathbf{u})]|^2 \, d\mathbf{u} \, d\tau \, d\lambda \gg_A N^{1-1/K}.$$

We comment here that Theorem 2A is sharp. The following analogue of Theorem 1B can be deduced using ideas in Beck and Chen [2].

THEOREM 2B. *Suppose that $A$ is a compact and convex body in $U^K$. Then for every natural number $N$, there exists a distribution $\mathscr{P}$ of $N$ points in $U^K$ such that*

$$\int_0^1 \int_{\mathscr{T}} \int_{U^K} |D_K[\mathscr{P}; A(\lambda, \tau, \mathbf{u})]|^2 \, d\mathbf{u} \, d\tau \, d\lambda \ll_A N^{1-1/K}.$$

On the other hand, the following is a trivial deduction from Theorem 2A.

THEOREM 2C. *Let $W \geq 2$. Suppose that $\mathscr{P}$ is a distribution of $N$ points in $U^K$, and that $A$ is a compact and convex body in $U^K$. Suppose further that $r(A) \geq N^{-1/K}$, where $r(A)$ denotes the radius of the largest inscribed ball of $A$. Then*

$$\int_0^1 \int_{\mathscr{T}} \int_{U^K} |D_K[\mathscr{P}; A(\lambda, \tau, \mathbf{u})]|^W \, d\mathbf{u} \, d\tau \, d\lambda \gg_{A,W} N^{(1-1/K)W/2}.$$

In Beck and Chen [2], a version of the following problem was investigated. Suppose that $\mathscr{P}$ is a distribution of $N$ points in the unit torus $U^{K+1}$, where $K \geq 2$. Let $A$ be a compact and convex body in $U^K$. For any real number $\lambda \in (0, 1]$, any proper orthogonal transformation $\tau$ in $\mathbb{R}^K$, any vector $\mathbf{u} \in U^K$ and any $y \in U$, we consider the cartesian product

$$A(\lambda, \tau, \mathbf{u}) \times [0, y),$$

where $A(\lambda, \tau, \mathbf{u}) \in U^K$ is defined as before, and let

$$Z[\mathscr{P}; A(\lambda, \tau, \mathbf{u}) \times [0, y)] = \#(\mathscr{P} \cap (A(\lambda, \tau, \mathbf{u}) \times [0, y))).$$

We are interested in the discrepancy function

$$D[\mathscr{P}; A(\lambda, \tau, \mathbf{u}) \times [0, y)] = Z[\mathscr{P}; A(\lambda, \tau, \mathbf{u}) \times [0, y)] - N\mu_K(A(\lambda, \tau, \mathbf{u}))y.$$

A simple corollary of Theorem 2A is the following lower bound result.

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

THEOREM 3A. *Suppose that $\mathscr{P}$ is a distribution of $N$ points in $U^{K+1}$, and that $A$ is a compact and convex body in $U^K$. Suppose further that $r(A) \geq N^{-1/K}$, where $r(A)$ denotes the radius of the largest inscribed ball of $A$. Then*

$$\int_0^1 \int_{\mathscr{T}} \int_{U^K} \int_U |D[\mathscr{P}; A(\lambda, \tau, \mathbf{u}) \times [0, y)]|^2 \, dy \, d\mathbf{u} \, d\tau \, d\lambda \gg_A N^{1-1/K}.$$

The argument in Beck and Chen [2] can be adapted to show that Theorem 3A is sharp. We therefore have the following complementary result.

THEOREM 3B. *Suppose that $A$ is a compact and convex body in $U^K$. Then for every natural number $N$, there exists a distribution $\mathscr{P}$ of $N$ points in $U^{K+1}$ such that*

$$\int_0^1 \int_{\mathscr{T}} \int_{U^K} \int_U |D[\mathscr{P}; A(\lambda, \tau, \mathbf{u}) \times [0, y)]|^2 \, dy \, d\mathbf{u} \, d\tau \, d\lambda \ll_A N^{1-1/K}.$$

As before, the following is a trivial deduction from Theorem 3A.

THEOREM 3C. *Let $W \geq 2$. Suppose that $\mathscr{P}$ is a distribution of $N$ points in $U^{K+1}$, and that $A$ is a compact and convex body in $U^K$. Suppose further that $r(A) \geq N^{-1/K}$, where $r(A)$ denotes the radius of the largest inscribed ball of $A$. Then*

$$\int_0^1 \int_{\mathscr{T}} \int_{U^K} \int_U |D[\mathscr{P}; A(\lambda, \tau, \mathbf{u}) \times [0, y)]|^W \, dy \, d\mathbf{u} \, d\tau \, d\lambda \gg_{A,W} N^{(1-1/K)W/2}.$$

The purpose of this paper is to prove the following generalizations of Theorems 2B and 3B. Theorems 2D and 3D below complement Theorems 2C and 3C respectively.

THEOREM 2D. *Let $W > 0$. Suppose that $A$ is a compact and convex body in $U^K$. Then for every natural number $N$, there exists a distribution $\mathscr{P}$ of $N$ points in $U^K$ such that*

$$\int_0^1 \int_{\mathscr{T}} \int_{U^K} |D_K[\mathscr{P}; A(\lambda, \tau, \mathbf{u})]|^W \, d\mathbf{u} \, d\tau \, d\lambda \ll_{A,W} N^{(1-1/K)W/2}.$$

THEOREM 3D. *Let $W > 0$. Suppose that $A$ is a compact and convex body in $U^K$. Then for every natural number $N$, there exists a distribution $\mathscr{P}$ of $N$ points in $U^{K+1}$ such that*

$$\int_0^1 \int_{\mathscr{T}} \int_{U^K} \int_U |D[\mathscr{P}; A(\lambda, \tau, \mathbf{u}) \times [0, y)]|^W \, dy \, d\mathbf{u} \, d\tau \, d\lambda \ll_{A,W} N^{(1-1/K)W/2}.$$

The author would like to thank the referee for his valuable comments and suggestions.

## 2. The basic idea

Let $A$ be given and fixed. Given any natural number $N$, we shall show that there exists a sequence $\mathbf{q}_0, \ldots, \mathbf{q}_{N-1}$ of $N$ points in $U^K$ such that

$$\frac{1}{N}\sum_{M=1}^{N}\int_0^1\int_{\mathscr{T}}\int_{U^K}|D_K[\mathscr{Q}_M; A(\lambda, \tau, \mathbf{u})]|^W\,d\mathbf{u}\,d\tau\,d\lambda \ll_{A,W} N^{(1-1/K)W/2}, \tag{1}$$

where $\mathscr{Q}_M = \{\mathbf{q}_0, \ldots, \mathbf{q}_{M-1}\}$ for $1 \leq M \leq N$. Theorem 3D follows easily. The proof of Theorem 2D is simpler.

The construction of the sequence $\mathbf{q}_0, \ldots, \mathbf{q}_{N-1}$ may be done in the same way as in Beck and Chen [2]. However, in view of further work, we follow the slightly different approach in Beck and Chen [3].

Let $h$ be a natural number, to be fixed later. For $s = 0, 1, \ldots, h$ and for every $c \in \mathbb{Z}$, let

$$I(s, c) = [c2^{-s}, (c+1)2^{-s}). \tag{2}$$

In other words, $I(s, c)$ is an interval of length $2^{-s}$ and whose endpoints are consecutive integer multiples of $2^{-s}$.

We shall construct a finite sequence $\mathbf{q}_n$ $(0 \leq n < 2^{Kh})$ of $2^{Kh} \geq N$ points in $U^K$ such that the following is satisfied. For every $s = 0, 1, \ldots, h$, every set of the form

$$I(s, a_1) \times \cdots \times I(s, a_K)$$

in $U^K$, where $a_1, \ldots, a_K \in \mathbb{Z}$, contains exactly one point of

$$\{\mathbf{q}_n : c2^{Ks} \leq n < (c+1)2^{Ks}\},$$

where $c$ is any non-negative integer satisfying $c < 2^{K(h-s)}$.

The construction of such a sequence involves ideas in combinatorics and poses no real difficulty. However, such a sequence alone is insufficient to give a proof of either Theorem 2B or Theorem 3B, let alone Theorems 2D and 3D. As in Beck and Chen [2, 3], we appeal to tools in probability theory. A natural consequence of this is that our proof will not give any explicit description of the well-distributed sets in question. This is a common phenomenon in most upper bound proofs in irregularities of distribution.

We shall describe the combinatorial part of the argument in §3 and the probabilistic part of the argument in §4.

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

## 3. A combinatorial approach

For every integer $s$ satisfying $1 \le s \le h$, integers $\tau_1, \dots, \tau_{s-1} \in \{0, 1, \dots, 2^K - 1\}$ and vectors $\mathbf{a}_1, \dots, \mathbf{a}_{s-1} \in \{0, 1\}^K$, let

$$G[\tau_1, \dots, \tau_{s-1}; \mathbf{a}_1, \dots, \mathbf{a}_{s-1}] : \{0, 1, \dots, 2^K - 1\} \to \{0, 1\}^K$$

be a bijective mapping, with the convention that the mapping in the case $s = 1$ is denoted by $G[\emptyset]$. Given these mappings, we can define a bijective mapping

$$F : \{0, 1, \dots, 2^{Kh} - 1\} \to \{0, 1, \dots, 2^h - 1\}^K$$

as follows. Suppose that $n$ is an integer satisfying $0 \le n < 2^{Kh}$. Write

$$n = \tau_h 2^{K(h-1)} + \tau_{h-1} 2^{K(h-2)} + \cdots + \tau_1, \tag{3}$$

where $\tau_1, \dots, \tau_h \in \{0, 1, \dots, 2^K - 1\}$. We now let $\mathbf{a}_1, \dots, \mathbf{a}_h \in \{0, 1\}^K$ be the solution of the following system of equations

$$\begin{cases} G[\emptyset](\tau_1) & = \mathbf{a}_1, \\ G[\tau_1; \mathbf{a}_1](\tau_2) & = \mathbf{a}_2, \\ G[\tau_1, \tau_2; \mathbf{a}_1, \mathbf{a}_2](\tau_3) & = \mathbf{a}_3, \\ \quad \vdots & \\ G[\tau_1, \dots, \tau_{s-1}; \mathbf{a}_1, \dots, \mathbf{a}_{s-1}](\tau_s) & = \mathbf{a}_s, \\ \quad \vdots & \\ G[\tau_1, \dots, \tau_{h-2}; \mathbf{a}_1, \dots, \mathbf{a}_{h-2}](\tau_{h-1}) & = \mathbf{a}_{h-1}, \\ G[\tau_1, \dots, \tau_{h-1}; \mathbf{a}_1, \dots, \mathbf{a}_{h-1}](\tau_h) & = \mathbf{a}_h. \end{cases} \tag{4}$$

Suppose now that for each integer $t = 1, \dots, h$,

$$\mathbf{a}_t = (a_{t,1}, \dots, a_{t,K}) \in \{0, 1\}^K. \tag{5}$$

We write

$$F_j(n) = a_{1,j} 2^{h-1} + a_{2,j} 2^{h-2} + \cdots + a_{h,j} \tag{6}$$

and let

$$F(n) = (F_1(n), \dots, F_K(n)). \tag{7}$$

We next partition $U^K$ into a sequence of $2^{Kh}$ smaller cubes

$$S(n) = I(h, F_1(n)) \times \cdots \times I(h, F_K(n)),$$

where, for every $j = 1, \dots, K$ and every $n = 0, 1, \dots, 2^{Kh} - 1$, the interval $I(h, F_j(n))$ is defined by (2)–(6).

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

LEMMA 1. *Suppose that $s$ is an integer satisfying $0 \le s \le h$. Then for every integer $n_0$, the set*

$$\bigcup_{\substack{0 \le n < 2^{Kh} \\ n \equiv n_0 \pmod{2^{Ks}}}} S(n) \tag{8}$$

*is a cube of the form*

$$C(s, \mathbf{c}) = I(s, c_1) \times \cdots \times I(s, c_K) \subset U^K, \tag{9}$$

*where $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^s - 1\}^K$. On the other hand, every cube of the form (9), where $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^s - 1\}^K$, is a union of the form (8) for some integer $n_0$.*

PROOF. Note that the condition $n \equiv n_0 \pmod{2^{Ks}}$ determines precisely the values of $\tau_1, \ldots, \tau_s$ in (3). We can therefore solve the system of equations

$$\begin{cases} G[\emptyset](\tau_1) & = \mathbf{a}_1 \\ G[\tau_1; \mathbf{a}_1](\tau_2) & = \mathbf{a}_2 \\ \quad \vdots & \\ G[\tau_1, \ldots, \tau_{s-1}; \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}](\tau_s) & = \mathbf{a}_s \end{cases} \tag{10}$$

for $\mathbf{a}_1, \ldots, \mathbf{a}_s$. On the other hand, $\tau_{s+1}, \ldots, \tau_h$ in (3) can take all possible values. It follows from

$$\begin{cases} G[\tau_1, \ldots, \tau_s; \mathbf{a}_1, \ldots, \mathbf{a}_s](\tau_{s+1}) & = \mathbf{a}_{s+1} \\ \quad \vdots & \\ G[\tau_1, \ldots, \tau_{h-1}; \mathbf{a}_1, \ldots, \mathbf{a}_{h-1}](\tau_h) & = \mathbf{a}_h \end{cases} \tag{11}$$

that $\mathbf{a}_{s+1}, \ldots, \mathbf{a}_h$ can take all possible values. The first assertion follows. To prove the second assertion, simply note that $\tau_1, \ldots, \tau_s$ are determined uniquely with given $\mathbf{a}_1, \ldots, \mathbf{a}_s$ by (10), and that if $\mathbf{a}_{s+1}, \ldots, \mathbf{a}_h$ take all possible values, then $\tau_{s+1}, \ldots, \tau_h$ take all possible values in view of (11).

For every $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^h - 1\}^K$, let $\mathbf{q}(\mathbf{c})$ be a point in the cube

$$C(h; \mathbf{c}) = I(h, c_1) \times \cdots \times I(h, c_K) \subset U^K.$$

Using $F$, we can define a permutation $\mathbf{q}_n$ $(0 \le n < 2^{Kh})$ of the $\mathbf{q}(\mathbf{c})$ as follows. For $n = 0, 1, \ldots, 2^{Kh} - 1$, let

$$\mathbf{q}_n = \mathbf{q}(F(n)) = \mathbf{q}(F_1(n), \ldots, F_K(n)).$$

Clearly $\mathbf{q}_n \in S(n)$ for every $n = 0, 1, \ldots, 2^{Kh} - 1$. Then it follows from Lemma 1 that

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

LEMMA 2. *Suppose that $s$ and $H$ are integers satisfying $0 \le s \le h$ and $0 \le H \le 2^{K(h-s)}$. Then every cube of the form (9), where $\mathbf{c} = (c_1, \dots, c_K) \in \{0, 1, \dots, 2^s - 1\}^K$, contains exactly one element of the set*

$$\{\mathbf{q}_n : H2^{Ks} \le n < (H+1)2^{Ks}\}.$$

PROOF. The restriction $H2^{Ks} \le n < (H+1)2^{Ks}$ determines precisely the values of $\tau_{s+1}, \dots, \tau_h$ in (3) with no restriction on $\tau_1, \dots, \tau_s$. On the other hand, the restriction $\mathbf{q}_n \in C(s; \mathbf{c})$ for a given $\mathbf{c}$ determines precisely the values of $\mathbf{a}_1, \dots, \mathbf{a}_s$ with no restriction on $\mathbf{a}_{s+1}, \dots, \mathbf{a}_h$. The system of equations (10) now determines precisely the values of $\tau_1, \dots, \tau_s$. Hence $n$ is uniquely determined.

We denote this element obtained by Lemma 2 by $\mathbf{q}(s; \mathbf{c}; H)$. In other words, for integers $s, c_1, \dots, c_K, H$ satisfying the hypotheses of Lemma 2,

$$\mathbf{q}(s; \mathbf{c}; H) = \{\mathbf{q}_n : H2^{Ks} \le n < (H+1)2^{Ks}\} \cap C(s; \mathbf{c}).$$

## 4. Some probabilistic lemmas

As in Beck and Chen [2, 3], we now use some elementary concepts and facts from probability theory (see, for example, Chung [5]), and define a 'randomization' of the deterministic points $\mathbf{q}(\mathbf{c}) = \mathbf{q}(c_1, \dots, c_K)$, mappings $G[\tau_1, \dots, \tau_{s-1}; \mathbf{a}_1, \dots, \mathbf{a}_{s-1}]$ and $F$, and the sequence $\mathbf{q}_n$ as follows.

(A) For $\mathbf{c} = (c_1, \dots, c_K) \in \{0, 1, \dots, 2^h - 1\}^K$, let $\tilde{\mathbf{q}}(\mathbf{c})$ be a random point uniformly distributed in the cube $C(h; \mathbf{c})$. More precisely,

$$\text{Prob}(\tilde{\mathbf{q}}(\mathbf{c}) \in \mathscr{S}) = \frac{\mu_K(C(h; \mathbf{c}) \cap \mathscr{S})}{\mu_K(C(h; \mathbf{c}))}$$

for all Borel sets $\mathscr{S} \subset \mathbb{R}^K$.

(B) For every integer $s$ satisfying $1 \le s \le h$, integers $\tau_1, \dots, \tau_{s-1} \in \{0, 1, \dots, 2^K - 1\}$ and vectors $\mathbf{a}_1, \dots, \mathbf{a}_{s-1} \in \{0, 1\}^K$, let $\tilde{G}[\tau_1, \dots, \tau_{s-1}; \mathbf{a}_1, \dots, \mathbf{a}_{s-1}]$ be a uniformly distributed random bijective mapping from $\{0, 1, ..., 2^K - 1\}$ to $\{0, 1\}^K$. More precisely, if $\pi : \{0, 1, ..., 2^K - 1\} \to \{0, 1\}^K$ is one of the $(2^K)!$ different (deterministic) bijective mappings, then

$$\text{Prob}(\tilde{G}[\tau_1, \dots, \tau_{s-1}; \mathbf{a}_1, \dots, \mathbf{a}_{s-1}] = \pi) = \frac{1}{(2^K)!}.$$

(C) Let $\tilde{F}$ be the random bijective mapping from $\{0, 1, \dots, 2^{Kh} - 1\}$ to $\{0, 1, \dots, 2^h - 1\}^K$ defined by (3), $\tilde{(4)}$ and (5)–(7), where $\tilde{(4)}$ denotes that in the system

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

(4) of equations, we replace each deterministic mapping by its corresponding random mapping.

(D) Let $\widetilde{\mathbf{q}}_n$ $(0 \le n < 2^{Kh})$ denote the random sequence defined by $\widetilde{F}$, i.e. for $n = 0, 1, \ldots, 2^{Kh} - 1$,

$$\widetilde{\mathbf{q}}_n = \mathbf{q}(\widetilde{F}(n)).$$

(E) Let $\widetilde{\mathbf{q}}(s; \mathbf{c}; H)$ denote the randomization of $\mathbf{q}(s; \mathbf{c}; H)$, i.e. for integers $s, c_1, \ldots, c_K, H$ satisfying the hypotheses of Lemma 2,

$$\widetilde{\mathbf{q}}(s; \mathbf{c}; H) = \{\widetilde{\mathbf{q}}_n : H2^{Ks} \le n < (H+1)2^{Ks}\} \cap C(s; \mathbf{c}). \tag{12}$$

(F) Finally, we may assume that the random variables

$$\widetilde{\mathbf{q}}(\mathbf{c}) \qquad (\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^h - 1\}^K)$$

and

$$\widetilde{G}[\tau_1, \ldots, \tau_{s-1}; \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}] \qquad (1 \le s \le h \text{ and } \tau_1, \ldots, \tau_{s-1} \in \{0, 1, \ldots, 2^K - 1\} \text{ and } \mathbf{a}_1, \ldots, \mathbf{a}_{s-1} \in \{0, 1\}^K)$$

are independent of each other. In fact, the existence of such a set of random variables follows immediately from the Kolmogorov extension theorem in probability theory.

Let $(\Omega, \mathscr{F}, \mathrm{Prob})$ denote the underlying probability measure space. We have

LEMMA 3. *Suppose that $s$ and $H$ are integers satisfying $0 \le s \le h$ and $0 \le H < 2^{K(h-s)}$. Then for every $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^s - 1\}^K$, the random point $\widetilde{\mathbf{q}}(s; \mathbf{c}; H)$ is uniformly distributed in the cube $C(s; \mathbf{c})$.*

PROOF. Suppose that for $j = 1, \ldots, K$,

$$c_j = a_{1,j}2^{s-1} + a_{2,j}2^{s-2} + \cdots + a_{s,j}.$$

For $t = 1, \ldots, s$, let

$$\mathbf{a}_t = (a_{t,1}, \ldots, a_{t,K}).$$

Since the random mapping $\widetilde{G}[\emptyset]$ is uniformly distributed, it follows that the (random) solution $\widetilde{\tau}_1$ of the equation

$$\widetilde{G}[\emptyset](\widetilde{\tau}_1) = \mathbf{a}_1$$

has the property that for any $\delta \in \{0, 1, \ldots, 2^K - 1\}$,

$$\mathrm{Prob}(\widetilde{\tau}_1 = \delta) = 2^{-K}.$$

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

Now let $\tilde{\tau}_1 = \tau_1$ (i.e. fix the value of this random variable), and consider the (random) equation

$$\tilde{G}[\tau_1; \mathbf{a}_1](\tilde{\tau}_2) = \mathbf{a}_2.$$

Since $\tilde{G}[\tau_1; \mathbf{a}_1]$ is also uniformly distributed, we have, for any $\delta = \{0, 1, \dots, 2^K - 1\}$, that

$$\text{Prob}(\tilde{\tau}_2 = \delta | \tau_1 = \tau) = 2^{-K}.$$

In other words, the random variables $\tilde{\tau}_1$ and $\tilde{\tau}_2$ are independent of each other. Repeating this argument, we conclude that $\tilde{\tau}_1, \dots, \tilde{\tau}_s$, obtained from

$$\begin{cases} \tilde{G}[\emptyset](\tilde{\tau}_1) & = \mathbf{a}_1, \\ \tilde{G}[\tau_1; \mathbf{a}_1](\tilde{\tau}_2) & = \mathbf{a}_2, \\ \quad \vdots & \\ \tilde{G}[\tau_1, \dots, \tau_{s-1}; \mathbf{a}_1, \dots, \mathbf{a}_{s-1}](\tilde{\tau}_s) & = \mathbf{a}_s, \end{cases}$$

are independent random variables with common distribution function

$$\text{Prob}(\tilde{\tau}_t = \delta) = 2^{-K}$$

for every $t = 1, \dots, s$ and $\delta \in \{0, 1, \dots, 2^K - 1\}$. Let

$$\tilde{n}_0 = \tilde{\tau}_s 2^{K(s-1)} + \tilde{\tau}_{s-1} 2^{K(s-2)} + \cdots + \tilde{\tau}_1.$$

Then $\tilde{n}_0$ is uniformly distributed in the set $\{0, 1, \dots, 2^{Ks} - 1\}$. Write

$$\tilde{n} = \tau_h 2^{K(h-1)} + \cdots + \tau_{s+1} 2^{Ks} + \tilde{n}_0,$$

where

$$H 2^{Ks} = \tau_h 2^{K(h-1)} + \cdots + \tau_{s+1} 2^{Ks}.$$

Then

$$\tilde{\mathbf{q}}(s; \mathbf{c}; H) = \tilde{\mathbf{q}}_{\tilde{n}}.$$

Suppose now that $H 2^{Ks} \leq n < (H+1) 2^{Ks}$. Then

$$\text{Prob}(\tilde{\mathbf{q}}(s; \mathbf{c}; H) = \tilde{\mathbf{q}}_n) = \text{Prob}(\tilde{n} = n) = 2^{-Ks}.$$

Since $\tilde{\mathbf{q}}_n$ is uniformly distributed in $S(n)$ for every $n$ satisfying $H 2^{Ks} \leq n < (H+1) 2^{Ks}$, the result follows from the independence of $\tilde{n}$ and $\tilde{\mathbf{q}}_n$.

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

Let $\mathscr{S}$ be a fixed compact and convex set in $U^K$. For integers $s$ and $H$ satisfying $0 \le s \le h$ and $0 \le H < 2^{K(h-s)}$, consider the random set

$$\widetilde{\mathscr{P}}(s, H) = \{\widetilde{\mathbf{q}}(s; \mathbf{c}; H) : \mathbf{c} = (c_1, \dots, c_K) \in \{0, 1, \dots, 2^s - 1\}^K\}, \tag{13}$$

and write

$$Z_K[\widetilde{\mathscr{P}}(s, H); \mathscr{S}] = \#(\widetilde{\mathscr{P}}(s, H) \cap \mathscr{S})$$

and

$$\widetilde{D}_K(s, H) = Z_K[\widetilde{\mathscr{P}}(s, H); \mathscr{S}] - 2^{Ks}\mu_K(\mathscr{S}). \tag{14}$$

Note that $\widetilde{D}_K(s, H)$ depends on $\mathscr{S}$. Let

$$T(s, H) = \{\mathbf{c} \in \{0, 1, \dots, 2^s - 1\}^K : C(s; \mathbf{c}) \cap \mathscr{S} \neq \emptyset \text{ and } C(s; \mathbf{c}) \setminus \mathscr{S} \neq \emptyset\}.$$

It is easy to see that

$$\#T(s, H) \le 2K2^{(K-1)s}. \tag{15}$$

Since every cube $C(s; \mathbf{c})$ contains exactly one element (namely $\widetilde{\mathbf{q}}(s; \mathbf{c}; H)$) of the (random) set $\widetilde{\mathscr{P}}(s, H)$, we have

$$\widetilde{D}_K(s, H) = \sum_{\substack{\mathbf{c} \in T(s,H) \\ \widetilde{\mathbf{q}}(s;\mathbf{c};H) \in \mathscr{S}}} 1 - 2^{Ks} \sum_{\mathbf{c} \in T(s,H)} \mu_K(C(s; \mathbf{c}) \cap \mathscr{S}).$$

For every $\mathbf{c} \in T(s, H)$, let

$$\xi(s; \mathbf{c}; H) = \begin{cases} 1 & \widetilde{\mathbf{q}}(s; \mathbf{c}; H) \in \mathscr{S}, \\ 0 & \text{otherwise.} \end{cases} \tag{16}$$

By Lemma 3, we have, writing $\mathbb{E}$ for 'expected value',

$$\mathbb{E}\xi(s; \mathbf{c}; H) = \frac{\mu_K(C(s; \mathbf{c}) \cap \mathscr{S})}{\mu_K(C(s; \mathbf{c}))} = 2^{Ks}\mu_K(C(s; \mathbf{c}) \cap \mathscr{S}),$$

so that writing

$$\eta(s; \mathbf{c}; H) = \xi(s; \mathbf{c}; H) - \mathbb{E}\xi(s; \mathbf{c}; H), \tag{17}$$

we have

$$\widetilde{D}_K(s, H) = \sum_{\mathbf{c} \in T(s,H)} \eta(s; \mathbf{c}; H). \tag{18}$$

Note that $\mathbb{E}\eta = 0$ and $|\eta| \le 1$.

We need the following analogue of Lemma 3 of Beck and Chen [2].

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

LEMMA 4. *Suppose that* $0 \leq s \leq h$. *Suppose further that* $H$ *is an integer satisfying* $0 \leq H < 2^{K(h-s)}$ *and that* $\mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(W)} \in \{0, 1, \ldots, 2^s - 1\}^K$ *are distinct. Then the random variables* $\eta(s; \mathbf{c}^{(1)}; H), \ldots, \eta(s; \mathbf{c}^{(W)}; H)$ *are independent.*

Note that Lemma 4 here covers only one very special case of Lemma 3 of [2]. In fact, the analogue of the remaining cases of Lemma 3 of [2] is replaced by applications of Hölder's inequality later in the argument here.

PROOF OF LEMMA 4. It follows from (16) and (17) that it is sufficient to prove that $\widetilde{\mathbf{q}}(s; \mathbf{c}^{(1)}; H), \ldots, \widetilde{\mathbf{q}}(s; \mathbf{c}^{(W)}; H)$ are independent. For every $w = 1, \ldots, W$, let $\mathbf{c}^{(w)} = (c_1^{(w)}, \ldots, c_K^{(w)})$, where for every $j = 1, \ldots, K$,

$$c_j^{(w)} 2^{h-s} = c_{1,j}^{(w)} 2^{h-1} + c_{2,j}^{(w)} 2^{h-2} + \cdots + c_{s,j}^{(w)} 2^{h-s},$$

where $c_{1,j}^{(w)}, \ldots, c_{s,j}^{(w)} \in \{0, 1\}$. For every $t = 1, \ldots, s$, let

$$\mathbf{c}_t^{(w)} = (c_{t,1}^{(w)}, \ldots, c_{t,K}^{(w)}).$$

Furthermore, let

$$H 2^{Ks} = \lambda_h 2^{K(h-1)} + \cdots + \lambda_{s+1} 2^{Ks},$$

where $\lambda_{s+1}, \ldots, \lambda_h \in \{0, 1, \ldots, 2^K - 1\}$. Then the random variable $\widetilde{\mathbf{q}}(s; \mathbf{c}^{(w)}; H)$ depends only on the following random variables: the random mappings

$$(19w) \qquad \begin{cases} \widetilde{G}[\lambda_1, \ldots, \lambda_s; \mathbf{c}_1^{(w)}, \ldots, \mathbf{c}_s^{(w)}], \\ \widetilde{G}[\lambda_1, \ldots, \lambda_s, \lambda_{s+1}; \mathbf{c}_1^{(w)}, \ldots, \mathbf{c}_s^{(w)}, \mathbf{d}_{s+1}], \\ \quad \vdots \\ \widetilde{G}[\lambda_1, \ldots, \lambda_s, \lambda_{s+1}, \ldots, \lambda_{h-1}; \mathbf{c}_1^{(w)}, \ldots, \mathbf{c}_s^{(w)}, \mathbf{d}_{s+1}, \ldots, \mathbf{d}_{h-1}], \end{cases}$$

where $\lambda_1, \ldots, \lambda_s \in \{0, 1, \ldots, 2^K - 1\}$ and $\mathbf{d}_{s+1}, \ldots, \mathbf{d}_{h-1} \in \{0, 1\}^K$; and the random points

$$(20w) \qquad \{\widetilde{\mathbf{q}}(\mathbf{c}) : C(h; \mathbf{c}) \subset C(s; \mathbf{c}^{(w)})\}.$$

Note that $\lambda_1, \ldots, \lambda_s$ are random variables, and the random functions in $(19w)$ for $w = 1, \ldots, W$ all have the same common distribution function for different values of $\lambda_1, \ldots, \lambda_s$ (see proof of Lemma 3). On the other hand, $\mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(W)}$ are distinct, and so $(\mathbf{c}_1^{(1)}, \ldots, \mathbf{c}_s^{(1)}), \ldots, (\mathbf{c}_1^{(W)}, \ldots, \mathbf{c}_s^{(W)})$ are also distinct. It follows that the random mappings and random points in $(19w)$ and $(20w)$ for $w = 1, \ldots, W$ are independent, and the lemma follows.

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

## 5. Proof of Theorems 2D and 3D

For every natural number $M$ satisfying $1 \le M \le 2^{Kh}$, let

$$\widetilde{\mathscr{Q}}_M = \{\widetilde{\mathbf{q}}_0, \widetilde{\mathbf{q}}_1, \dots, \widetilde{\mathbf{q}}_{M-1}\} \tag{21}$$

and, for every compact and convex set $\mathscr{S} \subset U^K$, let

$$Z_K[\widetilde{\mathscr{Q}}_M; \mathscr{S}] = \#(\widetilde{\mathscr{Q}}_M \cap \mathscr{S}),$$

and write

$$D_K[\widetilde{\mathscr{Q}}_M; \mathscr{S}] = Z_K[\widetilde{\mathscr{Q}}_M; \mathscr{S}] - M\mu_K(\mathscr{S}).$$

LEMMA 5. *Let $W$ be an even natural number. For every natural number $M$ satisfying $1 \le M \le 2^{Kh}$, we have*

$$\mathbb{E}\Big(D_K[\widetilde{\mathscr{Q}}_M; \mathscr{S}]\Big)^W \ll_{K,W} M^{(1-1/K)W/2}.$$

Lemma 5 follows easily from the lemma below, which is stated in a form suitable for proof by induction.

LEMMA 6. *Let $W$ be an even natural number. Suppose that $M$ is a natural number satisfying $1 \le M \le 2^{Kh}$, and that*

$$M - 1 = \tau_h 2^{K(h-1)} + \tau_{h-1} 2^{K(h-2)} + \cdots + \tau_1, \tag{22}$$

*where $\tau_1, \dots, \tau_h \in \{0, 1, \dots, 2^K - 1\}$. Suppose further that exactly $s$ of the coefficients $\tau_1, \dots, \tau_h$ are non-zero, and that $\tau_{k+1} = \cdots = \tau_h = 0$ and $\tau_k \ne 0$. Then*

$$\mathbb{E}\Big(D_K[\widetilde{\mathscr{Q}}_M; \mathscr{S}]\Big)^W \ll_{K,W} \left\{1 + \frac{1}{\sqrt{2}} + \cdots + \left(\frac{1}{\sqrt{2}}\right)^{s-1}\right\}^W (\sqrt{2})^{W(K-1)(k-1)}. \tag{23}$$

We shall prove Lemma 6 by induction on the number of non-zero coefficients when $M - 1$ is written in the form (22). The following lemma is a summary of the case $s = 1$. However, it is stated in a form more general than is necessary to prove Lemma 6 in the case $s = 1$. This generality is necessary in order that we may handle the inductive step in the proof of Lemma 6. For ease of notation, we write $\widetilde{\mathscr{Q}}_0 = \emptyset$.

LEMMA 7. *Let $W$ be an even natural number. Suppose either that $M = 0$, or that in the expression (22) for $M - 1$, the coefficients $\tau_1 = \cdots = \tau_j = 0$. Suppose further that $\overline{M} = M + \mu_j 2^{K(j-1)}$, where $0 < \mu_j < 2^K$. Then*

$$\mathbb{E}\Big(D_K[(\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M); \mathscr{S}]\Big)^W \ll_{K,W} (\sqrt{2})^{W(K-1)(j-1)}, \tag{24}$$

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

*where*

$$D_K[(\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M); \mathscr{S}] = \#\left((\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M) \cap \mathscr{S}\right) - (\overline{M} - M)\mu_K(\mathscr{S}). \tag{25}$$

Note that Lemma 6 in the case $s = 1$ is the special case $M = 0$ and $j = k$ of Lemma 7.

PROOF OF LEMMA 7. Note first of all that $M$ is a multiple of $2^{K(j-1)}$. By (12), (13) and (21),

$$\begin{aligned}\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M &= \left\{\widetilde{\mathbf{q}}_n : M \le n < M + \mu_j 2^{K(j-1)}\right\} \\ &= \bigcup_{m_j=0}^{\mu_j-1} \left\{\widetilde{\mathbf{q}}_n : M + m_j 2^{K(j-1)} \le n < M + (m_j+1)2^{K(j-1)}\right\} \\ &= \bigcup_{m_j=0}^{\mu_j-1} \widetilde{\mathscr{P}}(j-1, H(j, m_j)),\end{aligned}$$

where

$$H(j, m_j) = 2^{-K(j-1)}M + m_j.$$

It follows from (14), (18), (21) and (25) that

$$D_K[(\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M); \mathscr{S}] = \sum_{m_j=0}^{\mu_j-1} \sum_{\mathbf{c} \in T(j-1, H(j,m_j))} \eta(j-1; \mathbf{c}; H(j, m_j)). \tag{26}$$

Applying Hölder's inequality on the sum on the right–hand side of (26), we have

$$\begin{aligned}&\mathbb{E}\left(D_K[(\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M); \mathscr{S}]\right)^W \\ &\le \mu_j^{W-1} \sum_{m_j=0}^{\mu_j-1} \left(\sum_{\mathbf{c} \in T(j-1, H(j,m_j))} \mathbb{E}\eta(j-1; \mathbf{c}; H(j, m_j))\right)^W \\ &\le 2^{K(W-1)} \sum_{m_j=0}^{\mu_j-1} \left(\sum_{\mathbf{c} \in T(j-1, H(j,m_j))} \mathbb{E}\eta(j-1; \mathbf{c}; H(j, m_j))\right)^W.\end{aligned} \tag{27}$$

Let

$$X_{m_j} = \{\eta(j-1; \mathbf{c}; H(j, m_j)) : \mathbf{c} \in T(j-1, H(j, m_j))\}. \tag{28}$$

Combining (27) and (28), we have

$$\mathbb{E}\left(D_K[(\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M); \mathscr{S}]\right)^W \le 2^{K(W-1)} \sum_{m_j=0}^{\mu_j-1} \left(\sum_{\eta_1 \in X_{m_j}} \cdots \sum_{\eta_W \in X_{m_j}} \mathbb{E}(\eta_1 \ldots \eta_W)\right). \tag{29}$$

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

Consider any particular summand on the right-hand side of (29). Clearly

$$|\mathbb{E}(\eta_1 \dots \eta_W)| \le 1$$

always. Suppose further that one of the terms among $\eta_1, \dots, \eta_W$ is distinct from all the others, i.e. suppose that $\eta_i$ is distinct from any of $\eta_1, \dots, \eta_{i-1}, \eta_{i+1}, \dots, \eta_W$. Then by Lemma 4, we have

$$\mathbb{E}(\eta_1 \dots \eta_W) = \mathbb{E}(\eta_i)\mathbb{E}(\eta_1 \dots \eta_{i-1}\eta_{i+1} \dots \eta_W) = 0.$$

It follows that the only non-zero contribution to the sum in (29) arises from terms of the form

$$\mathbb{E}\left(\eta_{i_1}^{n_1} \dots \eta_{i_r}^{n_r}\right), \tag{30}$$

where $\eta_{i_1}, \cdots, \eta_{i_r}$ are distinct, $\min\{n_1, \dots, n_r\} \ge 2$ and $n_1 + \cdots + n_r = W$. In this case, we clearly have $r \le W/2$. Furthermore, if $r = W/2$, then we must have $n_1 = \cdots = n_r = 2$. Hence the number of terms in the sum

$$\sum_{\eta_1 \in X_{m_j}} \dots \sum_{\eta_W \in X_{m_j}} \mathbb{E}(\eta_1 \dots \eta_W) \tag{31}$$

of the form (30) with $r = W/2$ is

$$\ll_W \binom{|X_{m_j}|}{W/2} \ll_W |X_{m_j}|^{W/2}.$$

On the other hand, if $r < W/2$, then $r \le W/2 - 1$. It is easy to see that the number of terms in the sum in (31) of the form (30) with $r < W/2$ is $\ll_W |X_{m_j}|^{W/2-1}$. Hence

$$\mathbb{E}\Big(D_K[(\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M); \mathscr{S}]\Big)^W \ll_{K,W} \sum_{m_j=0}^{\mu_j - 1} |X_{m_j}|^{W/2}. \tag{32}$$

Finally, note from (15) and (28) that

$$|X_{m_j}| \le 2K2^{(K-1)(j-1)}. \tag{33}$$

(24) now follows on combining (32) and (33).

PROOF OF LEMMA 6. We shall use induction on the number $s$ of non-zero coefficients $\tau_1, \dots, \tau_h$ in (22). The case $s = 1$ is proved in Lemma 7. Suppose now that (23) holds for fixed $s$ and $k$, and that $\tau_1 = \cdots = \tau_j = 0$. Now let $\overline{M} = M + \mu_j 2^{K(j-1)}$,

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

where $1 \le \mu_j < 2^K$. Then in the expression of $\overline{M} - 1$ analogous to (22), the number of non-zero coefficients is now exactly $s + 1$. Also

$$D_K[\widetilde{\mathscr{Q}}_{\overline{M}}; \mathscr{S}] = D_K[\widetilde{\mathscr{Q}}_M; \mathscr{S}] + D_K[(\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M); \mathscr{S}],$$

so that if $W$ is an even natural number, then

$$\Big(D_K[\widetilde{\mathscr{Q}}_{\overline{M}}; \mathscr{S}]\Big)^W = \sum_{w=0}^{W} \binom{W}{w} \Big(D_K[\widetilde{\mathscr{Q}}_M; \mathscr{S}]\Big)^{W-w} \Big(D_K[(\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M); \mathscr{S}]\Big)^w.$$

Applying Hölder's inequality, we have

$$\mathbb{E}\Big(D_K[\widetilde{\mathscr{Q}}_{\overline{M}}; \mathscr{S}]\Big)^W \le \sum_{w=0}^{W} \binom{W}{w} \Big\{\mathbb{E}\Big(D_K[\widetilde{\mathscr{Q}}_M; \mathscr{S}]\Big)^W\Big\}^{(W-w)/W} \Big\{\mathbb{E}\Big(D_K[(\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M); \mathscr{S}]\Big)^W\Big\}^{w/W}.$$

We now apply the induction hypothesis to the term $\mathbb{E}(D_K[\widetilde{\mathscr{Q}}_M; \mathscr{S}])^W$ and apply Lemma 7 to the term $\mathbb{E}(D_K[(\widetilde{\mathscr{Q}}_{\overline{M}} \setminus \widetilde{\mathscr{Q}}_M); \mathscr{S}])^W$, and so

$$\begin{aligned}
&\mathbb{E}\Big(D_K[\widetilde{\mathscr{Q}}_{\overline{M}}; \mathscr{S}]\Big)^W \\
&\quad \ll_{K,W} \sum_{w=0}^{W} \binom{W}{w} \left(\left\{1 + \frac{1}{\sqrt{2}} + \cdots + \left(\frac{1}{\sqrt{2}}\right)^{s-1}\right\} (\sqrt{2})^{(K-1)(k-1)}\right)^{W-w} \times \\
&\qquad \times \left((\sqrt{2})^{(K-1)(j-1)}\right)^w \\
&\quad = \left(\left\{1 + \frac{1}{\sqrt{2}} + \cdots + \left(\frac{1}{\sqrt{2}}\right)^{s-1}\right\} (\sqrt{2})^{(K-1)(k-1)} + (\sqrt{2})^{(K-1)(j-1)}\right)^W \\
&\quad = \left(1 + \frac{1}{\sqrt{2}} + \cdots + \left(\frac{1}{\sqrt{2}}\right)^{s-1} + \left(\frac{1}{\sqrt{2}}\right)^{(K-1)(k-j)}\right)^W (\sqrt{2})^{W(K-1)(k-1)} \\
&\quad \le \left(1 + \frac{1}{\sqrt{2}} + \cdots + \left(\frac{1}{\sqrt{2}}\right)^{s-1} + \left(\frac{1}{\sqrt{2}}\right)^{s}\right)^W (\sqrt{2})^{W(K-1)(k-1)}
\end{aligned}$$

since clearly $(K-1)(k-j) \ge s$.

Let $A$ be a given compact and convex body in $U^K$. It now follows from Lemma 5 that for any real number $\lambda \in (0, 1]$, any proper orthogonal transformation $\tau$ in $\mathbb{R}^K$ and any vector $\mathbf{u} \in U^K$, we have

$$\mathbb{E}\Big(D_K[\widetilde{\mathscr{Q}}_M; A(\lambda, \tau, \mathbf{u})]\Big)^W \ll_{K,W} M^{(1-1/K)W/2}$$

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press

for every $M$ satisfying $1 \leq M \leq 2^{Kh}$. If we now choose $h$ to satisfy

$$2^{K(h-1)} < N \leq 2^{Kh},$$

then

$$\mathbb{E}\left(\frac{1}{N}\sum_{M=1}^{N}\int_0^1\int_{\mathscr{T}}\int_{U^K}|D_K[\widetilde{\mathscr{Q}}_M; A(\lambda,\tau,\mathbf{u})]|^W\,d\mathbf{u}\,d\tau\,d\lambda\right) \ll_{K,W} N^{(1-1/K)W/2}.$$

(1) follows immediately. This proves Theorem 3D. Note also the simpler inequality

$$\mathbb{E}\left(\int_0^1\int_{\mathscr{T}}\int_{U^K}|D_K[\widetilde{\mathscr{Q}}_N; A(\lambda,\tau,\mathbf{u})]|^W\,d\mathbf{u}\,d\tau\,d\lambda\right) \ll_{K,W} N^{(1-1/K)W/2}.$$

Theorem 2D follows.

## References

[1] J. Beck, 'Irregularities of distribution I', *Acta Math.* **159** (1987), 1–49.
[2] J. Beck and W. W. L. Chen, 'Note on irregularities of distribution', *Mathematika* **33** (1986), 148–163.
[3] ———, 'Note on irregularities of distribution II', *Proc. London Math. Soc.* **61** (1990), 251–272.
[4] W. W. L. Chen, 'On irregularities of distribution', *Mathematika* **27** (1980), 153–170.
[5] K. L. Chung, *A course in probability theory* (Academic Press, New York, 1974).
[6] K. F. Roth, 'On irregularities of distribution', *Mathematika* **1** (1954), 73–79.
[7] ———, 'On irregularities of distribution IV', *Acta Arith.* **37** (1980), 67–75.
[8] W. M. Schmidt, 'Irregularities of distribution X', in: *Number theory and algebra* (Academic Press, New York, 1977) pp. 311–329.

School of MPCE
Macquarie University
Sydney NSW 2109
Australia
e-mail: wchen@mpce.mq.edu.au

https://doi.org/10.1017/S1446788700037629 Published online by Cambridge University Press