On irregularities of distribution IV

W.W.L. Chen

1. Introduction

Suppose that $\mathcal{P}$ 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

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

and let

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

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

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

where μ_L denotes the usual volume in U^L. The case $L = 1$ is trivial. For $L \geq 2$, we have the following result.

Theorem 1. *Suppose that $W > 1$ and the natural number $N \geq 2$.*
(a) For every distribution $\mathcal{P}$ of N points in U^L, we have

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

(b) There exists a distribution $\mathcal{P}$ of N points in U^L such that

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

Here the case $W = 2$ was established by Roth [**11**,**12**]. The general case was established by Schmidt [**13**] and Chen [**6**]. Note also that the conclusions remain true in the trivial case $L = 1$.

Suppose now that $\mathcal{P}$ 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 τ 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

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

We are interested in the discrepancy function

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

where μ_K denotes the usual volume in U^K. Let $\mathcal{T}$ be the group of all proper orthogonal transformations in $\mathbb{R}^K$, and let $\mathrm{d}\tau$ be the volume element of the invariant measure on $\mathcal{T}$, normalized such that $\int_{\mathcal{T}}\mathrm{d}\tau=1$. We have the following result.

Theorem 2. *Suppose that $W\geq 2$ and the natural number $N\geq 1$. Suppose further that A is a compact and convex body in U^K satisfying $r(A)\geq N^{-1/K}$, where $r(A)$ denotes the radius of the largest inscribed ball of A.*
(a) For every distribution $\mathcal{P}$ of N points in U^K, we have

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

(b) There exists a distribution $\mathcal{P}$ of N points in U^K such that

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

Here the lower bound was established by Beck [**3**]. The upper bound was established by Chen [**7**], although the case $W=2$ can be deduced using ideas in Beck and Chen [**4**].

Let us now combine these two problems. More precisely, suppose that $\mathcal{P}$ is a distribution of N points in the unit torus U^{K+L}, where $K\geq 2$ and $L\geq 1$. Let A be a compact and convex body in U^K. For any real number $\lambda\in(0,1]$, any proper orthogonal transformation τ in $\mathbb{R}^K$, any vectors $\mathbf{u}\in U^K$ and $\mathbf{y}\in U^L$, consider the cartesian product

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

where $A(\lambda,\tau,\mathbf{u})\subseteq U^K$ and $B(\mathbf{y})\subseteq U^L$ are defined as before, and let

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

We are interested in the discrepancy function

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

In this paper, we shall establish the following result.

Theorem 3. *Suppose that $W \geq 2$ and the natural number $N \geq 1$. Suppose further that A is a compact and convex body in U^K satisfying $r(A) \geq N^{-1/K}$, where $r(A)$ denotes the radius of the largest inscribed ball of A.*

(a) For every distribution $\mathcal{P}$ of N points in U^{K+L}, we have

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

(b) There exists a distribution $\mathcal{P}$ of N points in U^{K+L} such that

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

In fact, part (a) of Theorem 3 is easily deduced from part (a) of Theorem 2, while the special case $W = 2$ of part (b) was established by Beck and Chen [**5**]. It therefore remains to establish part (b) when W is an even positive integer. Note that the order of magnitude of the estimates is independent of L.

The author takes great pleasure in thanking the referee for his very careful reading of the original version of the paper, and for the many valuable comments and suggestions.

2. The basic idea

Given any natural number N, we need to show that there exists a set $\mathcal{P}$ of N points in U^{K+L} such that the inequality in Theorem 3(b) holds.

As in Beck and Chen [**5**], we shall in fact construct a sequence of more than N points in U^{K+L} and use only the first N terms of this sequence. The main ingredient in the construction of this sequence in U^{K+L} is the Chinese remainder theorem. This not only makes it possible for the determination of the first K coordinates of the points of the sequence to be carried out independently of the determination of the last L coordinates of these points, but also enables us to treat the discrepancy arising from $A(\lambda,\tau,\mathbf{u})$ quite separately from the discrepancy arising from $B(\mathbf{y})$. Furthermore, it ensures that important properties of the sequence are also present in many subsequences that arise from our argument.

Indeed, we shall show that the construction in Beck and Chen [**5**] used to established the special case $W = 2$ will be sufficient. However, the treatment of the discrepancy arising from $B(\mathbf{y})$ in Beck and Chen [**5**] is unnecessarily complicated due to an elementary oversight. Here we give a much simpler argument in §9.

3. The sequence: general discussion

Let h be a natural number, to be fixed later, and let $p_1, \ldots, p_L$ be the first L odd primes.

For every $p = 2, p_1, \ldots, p_L$, for every $s = 0, 1, \ldots, h$ and for every $c \in \mathbb{Z}$, let

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

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

We shall construct an infinite sequence of points $\mathbf{p}_0, \mathbf{p}_1, \mathbf{p}_2, \ldots$ in U^{K+L} such that the following is satisfied. For every $s_0, s_1, \ldots, s_L \in \{0, 1, \ldots, h\}$, every set of the form

$$I(2,s_0,a_1) \times \ldots \times I(2,s_0,a_K) \times I(p_1,s_1,b_1) \times \ldots \times I(p_L,s_L,b_L)$$

in U^{K+L}, where $a_1, \ldots, a_K, b_1, \ldots, b_L \in \mathbb{Z}$, contains exactly one point of

$$\{\mathbf{p}_n : c2^{Ks_0}p_1^{s_1} \ldots p_L^{s_L} \leq n < (c+1)2^{Ks_0}p_1^{s_1} \ldots p_L^{s_L}\},$$

where c is any non-negative integer.

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 the desired result. As in Beck and Chen [**5**], 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.

Unlike in Beck and Chen [**5**], we observe that we need only to apply probabilistic arguments to deal with the discrepancy arising from $A(\lambda, \tau, \mathbf{u})$. This is essentially similar to the probabilistic arguments in Beck and Chen [**5**], and has its origins from the work of Beck [**1**,**2**]. To deal with the discrepancy arising from $B(\mathbf{y})$, we shall use a simple counting argument which is sufficient to replace the complicated discrete probabilistic techniques used in Beck and Chen [**5**].

For every non-negative integer n, let $\mathbf{p}_n = (\mathbf{q}_n, \mathbf{y}_n) \in U^{K+L}$, where $\mathbf{q}_n \in U^K$ and $\mathbf{y}_n \in U^L$. We shall discuss the sequence $\mathbf{q}_n$ in §§4-6 and the sequence $\mathbf{y}_n$ in §7.

4. A combinatorial approach

In this section, we closely follow Beck and Chen [**5**]. In particular, Lemmas 1 – 4 below are precisely Lemmas 1 – 4 in [**5**], and we omit the proofs here.

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

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

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

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

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

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

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

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

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

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

We now write

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

and let

$$F(n) = (F_1(n), \ldots, F_k(n)). \tag{7}$$

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

$$S(n) = I(2, h, F_1(n)) \times \ldots \times I(2, h, F_k(n)), \tag{8}$$

where, for every $j = 1, \ldots, K$ and every $n = 0, 1, ..., 2^{Kh} - 1$, the interval $I(2, h, F_j(n))$ is defined by (1) and (3)–(6). We further extend the range of definition of $S(n)$ over the set $\mathbb{Z}$ by periodicity so as to ensure that

$$S(n + 2^{Kh}) = S(n) \tag{9}$$

for every integer n.

The following observation is a simple consequence of our definitions.

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

$$\bigcup_{\substack{0 \leq n < 2^{Kh} \\ n \equiv n_0 \pmod{2^{Ks}}}} S(n) \tag{10}$$

is a cube of the form

$$C(s,\mathbf{c}) = I(2,s,c_1) \times \ldots \times I(2,s,c_K) \subseteq U^K, \tag{11}$$

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* (11)*, where* $\mathbf{c} = (c_1,\ldots,c_K) \in \{0,1,\ldots,2^s-1\}^K$, *is a union of the form* (10) *for some integer* n_0.

A simple rescaling and congruence argument gives the following generalization.

Lemma 2. *Suppose that* s *is an integer satisfying* $0 \leq s \leq h$, *and that* q *is an odd natural number. Then for every integer* n_0, *the set*

$$\bigcup_{\substack{0 \leq n < 2^{Kh}q \\ n \equiv n_0 \pmod{2^{Ks}q}}} S(n)$$

is a cube of the form (11)*, where* $\mathbf{c} = (c_1,\ldots,c_K) \in \{0,1,\ldots,2^s-1\}^K$.

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

$$C(h;\mathbf{c}) = I(2,h,c_1) \times \ldots \times I(2,h,c_K) \subseteq U^K.$$

Using F, we can define a permutation $\mathbf{q}_n$ $(0 \leq n < 2^{Kh})$ 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 $n = 0,1,\ldots,2^{Kh}-1$. Again, we extend the range of definition of $\mathbf{q}_n$ over the set $\mathbb{Z}$ by periodicity with period 2^{Kh} so as to ensure that

$$\mathbf{q}_n \in S(n)$$

for every integer n. Then it follows from Lemma 1 that

Lemma 3. *Suppose that* s *and* H *are integers satisfying* $0 \leq s \leq h$ *and* $H \geq 0$. *Then every cube of the form* (11)*, where* $\mathbf{c} = (c_1,\ldots,c_K) \in \{0,1,\ldots,2^s-1\}^K$, *contains exactly one element of the set*

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

We denote this element obtained by Lemma 3 by $\mathbf{q}(s;\mathbf{c};H)$. In other words, for integers $s,c_1,\ldots,c_K,H$ satisfying the hypotheses of Lemma 3,

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

Lemma 4. *Let q be an odd natural number and let n_0 be an integer satisfying $0 \leq n_0 < q$. Then for every bijective mapping F of the form* (2) *defined by* (3)–(7)*, there exists a corresponding bijective mapping F' of the same type such that $S(n_0 + qn) = S'(n)$ for every $n \in \mathbb{Z}$, where S' is defined in terms of F' in the same way as S is defined in terms of F by* (7)–(9)*.*

In other words, the good distribution properties of the functions F and G can be extended to the more general situation first alluded to in Lemma 2.

5. Some probabilistic lemmas

As in Beck and Chen [**4**,**5**] and Chen [**7**], we now use some elementary concepts and facts from probability theory (see, for example, Chung [**8**]), and define a "randomization" of the deterministic points $\mathbf{q}(\mathbf{c}) = \mathbf{q}(c_1, \ldots, c_K)$, mappings $G[\tau_1, \ldots, \tau_{s-1}; \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}]$ and F, and the sequence $\mathbf{q}_n$ as follows.

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

$$\mathrm{Prob}(\widetilde{\mathbf{q}}(\mathbf{c}) \in \mathcal{S}) = \frac{\mu_K(C(h; \mathbf{c}) \cap \mathcal{S})}{\mu_K(C(h; \mathbf{c}))}$$

for all Borel sets $\mathcal{S} \subseteq \mathbb{R}^K$.

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

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

(C) Let $\widetilde{F}$ be the random bijective mapping from $\{0, 1, \ldots, 2^{Kh} - 1\}$ to $\{0, 1, \ldots, 2^h - 1\}^K$ defined by (3), $\widetilde{(5)}$ and (5)–(7), where $\widetilde{(4)}$ denotes that in the system (4) of equations, we replace each deterministic mapping by its corresponding random mapping.

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

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

again, we extend $\widetilde{\mathbf{q}}_n$ over the set $\mathbb{Z}$ by periodicity with period 2^{Kh}.

(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 3,

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

(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

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

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 $(\Omega, \mathcal{F}, \mathrm{Prob})$ denote the underlying probability measure space.

We shall first state that the independence and uniformity of the original random variables lead to uniformity of the distribution of random points in special cubes. The following is precisely Lemma 5 of [**5**], and we omit the proof here.

Lemma 5. *Suppose that s and H are integers satisfying $0 \leq s \leq h$ and $H \geq 0$. 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 $C(s; \mathbf{c})$.*

Let $\mathcal{S}$ be a fixed compact and convex set in U^K. For integers s and H satisfying $0 \leq s \leq h$ and $H \geq 0$, consider the random set

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

and write

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

and

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

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

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

It is easy to see that

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

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

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

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

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

By Lemma 5, we have, writing $\mathbb{E}$ for "expected value",

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

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 shall next state that the independence and uniformity of the original random variables also lead to independence properties concerning the random points discussed in Lemma 5.

Lemma 6. *Suppose that $0 \le s \le h$. Suppose further that H is an integer satisfying $H \ge 0$ 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.*

This is essentially Lemma 4 of Chen [**7**] on noting that, as in Lemma 3, we may assume that $H < 2^{K(h-s)}$, in view of periodicity.

6. An intermediate result

For every natural number N, let

$$\widetilde{\mathcal{Q}}_N = \{\widetilde{\mathbf{q}}_0, \widetilde{\mathbf{q}}_1, \ldots, \widetilde{\mathbf{q}}_{N-1}\}. \tag{19}$$

For every compact and convex set $S \subset U^K$, let

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

and write

$$D_K[\widetilde{\mathcal{Q}}_N;\mathcal{S}] = Z_K[\widetilde{\mathcal{Q}}_N;\mathcal{S}] - N\mu_K(\mathcal{S}).$$

Lemma 7. *Let W be an even natural number. There exists a positive constant $C_0(K,W)$, depending at most on K and W, such that for every natural number N satisfying $1 \le N \le 2^{Kh}$, we have*

$$\mathbb{E}\Big(D_K[\widetilde{\mathcal{Q}}_N;\mathcal{S}]\Big)^W \le C_0(K,W)N^{(1-1/K)W/2}.$$

This is Lemma 5 of Chen [**7**], and we omit the technical proof here. In essence, Lemma 7 asserts that the probabilistic model gives estimates that are of the order of magnitude of the square root of the trivial estimate of the type

$$|D_K[\mathcal{Q}_N;\mathcal{S}]| \ll_K N^{1-1/K}.$$

Lemma 7 is sufficient for the study of the case $L = 1$. For $L \geq 2$, we need a stronger version of Lemma 7. For every natural number N and every residue class R of integers modulo q, let

$$\widetilde{\mathcal{Q}}_N(R) = \{\widetilde{\mathbf{q}}_n : 0 \leq n < N \text{ and } n \in R\}.$$

For every compact and convex set $S \subset U^K$, let

$$Z_K[\widetilde{\mathcal{Q}}_N(R);\mathcal{S}] = \#(\widetilde{\mathcal{Q}}_N(R) \cap \mathcal{S}),$$

and write

$$D_K[\widetilde{\mathcal{Q}}_N(R);\mathcal{S}] = Z_K[\widetilde{\mathcal{Q}}_N(R);\mathcal{S}] - N'\mu_K(\mathcal{S}),$$

where $N' = \#\widetilde{\mathcal{Q}}_N(R) = \#(R \cap [0, N))$.

Lemma 8. *Let W be an even natural number, and let R be any residue class of integers modulo q, where q is an odd natural number. For every natural number N satisfying $1 \leq N \leq 2^{Kh}q$, we have*

$$\mathbb{E}\Big(D_K[\widetilde{\mathcal{Q}}_N(R);\mathcal{S}]\Big)^W \leq C_0(K,W)(Nq^{-1}+1)^{(1-1/K)W/2},$$

where the positive constant $C_0(K,W)$ is the same as in Lemma 7.

Proof. Let R be the residue class n_0 modulo q, where $0 \leq n_0 < q$. Then

$$\widetilde{\mathcal{Q}}_N(R) = \{\widetilde{\mathbf{q}}_{n_0+qn} : 0 \leq n < N'\},$$

where

$$N' \leq [(N-n_0)q^{-1}] + 1 \leq Nq^{-1} + 1. \tag{20}$$

In view of Lemma 4 and the independence between the randomization of F and the randomization of the point $\mathbf{q}(\mathbf{c})$, we have

$$\mathbb{E}\Big(D_K[\widetilde{\mathcal{Q}}_N(R);\mathcal{S}]\Big)^W = \mathbb{E}\Big(D_K[\widetilde{\mathcal{Q}}_{N'};\mathcal{S}]\Big)^W. \tag{21}$$

Lemma 8 now follows on combining (20), (21) and Lemma 7. ♣

7. The van der Corput–Halton–Hammersley sequence

Let p_j denote the j–th odd prime. For any integer n satisfying $0 \leq n < p_j^h$, write

$$n = \sigma_{h,j} p_j^{h-1} + \sigma_{h-1,j} p_j^{h-2} + \ldots + \sigma_{1,j},$$

where $\sigma_{1,j}, \ldots, \sigma_{h,j} \in \{0, 1, \ldots, p_j - 1\}$, and let

$$y_j(n) = \sigma_{1,j} p_j^{-1} + \ldots + \sigma_{h,j} p_j^{-h}.$$

We extend the range of definition of $y_j(n)$ over the set $\mathbb{Z}$ by periodicity so as to ensure that $y_j(n + p_j^h) = y_j(n)$ for every $n \in \mathbb{Z}$. Then the following result is almost trivial.

Lemma 9. *Let $s_j \in \{0, 1, \ldots, h\}$. If $b_j \in \mathbb{Z}$ and $I(p_j, s_j, b_j) \subseteq U$, then*

$$\{n \in \mathbb{Z} : y_j(n) \in I(p_j, s_j, b_j)\}$$

is a residue class modulo $p_j^{s_j}$.

Let $p_1, \ldots, p_L$ denote the first L odd primes, and let

$$\mathbf{y}_n = (y_1(n), \ldots, y_L(n))$$

for every $n \in \mathbb{Z}$. Then the result below follows immediately from Lemma 9 and the Chinese remainder theorem.

Lemma 10. *Let $s_1, \ldots, s_L \in \{0, 1, \ldots, h\}$. If $b_1, \ldots, b_L \in \mathbb{Z}$ and*

$$I(p_1, s_1, b_1) \times \ldots \times I(p_L, s_L, b_L) \subseteq U^L, \tag{22}$$

then

$$\{n \in \mathbb{Z} : \mathbf{y}_n \in I(p_1, s_1, b_1) \times \ldots \times I(p_L, s_L, b_L)\}$$

is a residue class modulo $p_1^{s_1} \ldots p_L^{s_L}$.

The van der Corput–Halton–Hammersley sequence $\mathbf{y}_n$ has been used on many occasions to give upper bound results in irregularities of distribution (see Halton [**9**], Hammersley [**10**], Roth [**12**], Chen [**6**] and Beck and Chen [**5**]).

8. The randomized sequence in the cube

We summarize our argument thus far. For any non–negative integer n, we write

$$\mathbf{p}_n = (\mathbf{q}_n, \mathbf{y}_n) \in U^{K+L},$$

where $\mathbf{q}_n \in U^K$ is defined in §4 and where $\mathbf{y}_n \in U^L$ is the van der Corput–Halton–Hammersley sequence defined in §7. We randomize the sequence $\mathbf{q}_n$ in §5 to obtain the sequence $\widetilde{\mathbf{q}}_n$. Consequently, we obtain a partly randomized version of $\mathbf{p}_n$, namely

$$\widetilde{\mathbf{p}}_n = (\widetilde{\mathbf{q}}_n, \mathbf{y}_n).$$

Note that the sequence $\widetilde{\mathbf{q}}_n$ satisfies Lemmas 7 and 8, while the sequence $\mathbf{y}_n$ satisfies Lemma 10. We shall combine these in the next section.

We shall write

$$\widetilde{\mathcal{P}}_N = \{\widetilde{\mathbf{p}}_0, \widetilde{\mathbf{p}}_1, \ldots, \widetilde{\mathbf{p}}_{N-1}\}. \tag{23}$$

9. Subdivision of the rectangular box

In this section, we follow the argument in Roth [**12**] and simplify the argument in Beck and Chen [**5**]. Let

$$B^* = [0, \eta_1) \times \ldots \times [0, \eta_L) \subseteq U^L, \tag{24}$$

where, for every $j = 1, \ldots, L$, the number $\eta_j \neq 1$ and is an integer multiple of p_j^{-h}, so that there exist unique integers $\nu_{1,j}, \ldots, \nu_{h,j} \in \{0, 1, \ldots, p_j - 1\}$ such that

$$\eta_j = \nu_{1,j} p_j^{-1} + \ldots + \nu_{h,j} p_j^{-h}.$$

For every $j = 1, \ldots, L$ and $s = 1, \ldots, h$, let

$$\xi_{s,j} = \nu_{1,j} p_j^{-1} + \ldots + \nu_{s,j} p_j^{-s}$$

denote the greatest integer multiple of p_j^{-s} not exceeding η_j, and write

$$I_{s,j} = [\xi_{s-1,j} - \xi_{s,j}),$$

with the convention that $\xi_{0,j} = 0$, so that

$$[0, \eta_j) = \bigcup_{s=1}^{h} J_{s,j}. \tag{25}$$

For every $j = 1, \ldots, L$, $s = 1, \ldots, h$ and $\alpha = 1, \ldots, \nu_{s,j}$, let

$$J_{s,j,\alpha} = [\xi_{s-1,j} + (\alpha - 1) p_j^{-s}, \xi_{s-1,j} + \alpha p_j^{-s}),$$

so that

$$J_{s,j} = \bigcup_{\alpha=1}^{\nu_{s,j}} J_{s,j,\alpha}. \tag{26}$$

Combining (25) and (26), we obtain

$$[0,\eta_j) = \bigcup_{s=1}^{h} \bigcup_{\alpha=1}^{\nu_{s,j}} J_{s,j,\alpha}. \tag{27}$$

Hence it follows from (24) and (27) that

$$B^* = \bigcup_{s_1=1}^{h} \cdots \bigcup_{s_L=1}^{h} \bigcup_{\alpha_1=1}^{\nu_{s,1}} \cdots \bigcup_{\alpha_L=1}^{\nu_{s,L}} (J_{s_1,1,\alpha_1} \times \ldots \times J_{s_L,L,\alpha_L}). \tag{28}$$

Consider now the distribution $\widetilde{\mathcal{P}}_N$ of N points in U^{K+L} given by (23). For any sets $\mathcal{S} \subseteq U^K$ and $\mathcal{B} \subseteq U^L$, let

$$D[\widetilde{\mathcal{P}}_N; \mathcal{S} \times \mathcal{B}] = \#(\widetilde{\mathcal{P}}_N \cap (\mathcal{S} \times \mathcal{B})) - N\mu_K(\mathcal{S})\mu_L(\mathcal{B}).$$

Since the union in (28) is pairwise disjoint, it follows that

$$D[\widetilde{\mathcal{P}}_N; \mathcal{S} \times B^*] = \sum_{s_1=1}^{h} \cdots \sum_{s_L=1}^{h} \sum_{\alpha_1=1}^{\nu_{s,1}} \cdots \sum_{\alpha_L=1}^{\nu_{s,L}} D[\widetilde{\mathcal{P}}_N; \mathcal{S} \times J_{s_1,1,\alpha_1} \times \ldots \times J_{s_L,L,\alpha_L}]. \tag{29}$$

If we write $\mathbf{s} = (s_1, \ldots, s_L)$ and $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_L)$, and let

$$D(\widetilde{\mathcal{P}}_N; \mathcal{S}; \mathbf{s}, \boldsymbol{\alpha}) = D[\widetilde{\mathcal{P}}_N; \mathcal{S} \times J_{s_1,1,\alpha_1} \times \ldots \times J_{s_L,L,\alpha_L}],$$

then it follows from (29) that

$$D[\widetilde{\mathcal{P}}_N; \mathcal{S} \times B^*] = \sum_{\mathbf{s}} \sum_{\boldsymbol{\alpha}} D(\widetilde{\mathcal{P}}_N; \mathcal{S}; \mathbf{s}, \boldsymbol{\alpha}), \tag{30}$$

where, for simplicity, we write

$$\sum_{\mathbf{s}} = \sum_{s_1=1}^{h} \cdots \sum_{s_L=1}^{h} \qquad \text{and} \qquad \sum_{\boldsymbol{\alpha}} = \sum_{\alpha_1=1}^{\nu_{s,1}} \cdots \sum_{\alpha_L=1}^{\nu_{s,L}}.$$

Suppose that W is an even natural number. Then it follows from (30) and Minkowski's inequality that

$$\mathbb{E}\left(|D[\widetilde{\mathcal{P}}_N; \mathcal{S} \times B^*]|^W\right) \leq \left(\sum_{\mathbf{s}} \sum_{\boldsymbol{\alpha}} \mathbb{E}\left(|D(\widetilde{\mathcal{P}}_N; \mathcal{S}; \mathbf{s}, \boldsymbol{\alpha})|^W\right)^{1/W}\right)^W. \tag{31}$$

Note next that

$$J_{s_1,1,\alpha_1} \times \ldots \times J_{s_L,L,\alpha_L}$$

is of the form (22), and so it follows from Lemma 10 that

$$D(\widetilde{\mathcal{P}}_N;\mathcal{S};\mathbf{s},\boldsymbol{\alpha}) = D_K[\widetilde{\mathcal{Q}}_N(R);\mathcal{S}]$$

for some residue class modulo $p_1^{s_1}\dots p_L^{s_L}$. It therefore follows from Lemma 8 that

$$\mathbb{E}\left(|D(\widetilde{\mathcal{P}}_N;\mathcal{S};\mathbf{s},\boldsymbol{\alpha})|^W\right) \leq C_0(K,W)(Np_1^{-s_1}\dots p_L^{-s_L}+1)^{(1-1/K)W/2}.$$

Combining this with (31), we obtain

$$\begin{aligned}\mathbb{E}\left(|D[\widetilde{\mathcal{P}}_N;\mathcal{S}\times B^*]|^W\right) &\leq C_0(K,W)\left(\sum_{\mathbf{s}}\sum_{\boldsymbol{\alpha}}(Np_1^{-s_1}\dots p_L^{-s_L}+1)^{(1-1/K)/2}\right)^W \\ &\leq C_1(K,W)(p_1\dots p_L)^W(N^{(1-1/K)W/2}+h^{LW}), \qquad (32)\end{aligned}$$

noting that there are no more than $p_1\dots p_L$ summands in the summation $\sum_{\boldsymbol{\alpha}}$ and no more than h^L summands in the summation $\sum_{\mathbf{s}}$. Here $C_1(K,W)$ is a suitably chosen positive constant not less than $C_0(K,W)$, and depends at most on K and W.

10. Completion of the proof

Suppose now that $\mathbf{y}=(y_1,\dots,y_L)\in U^L$. For every $j=1,\dots,L$, let

$$\eta_j=\eta_j(y_j)=p_j^{-h}[p_j^h y_j]$$

denote the greatest integer multiple of p_j^{-h} not exceeding y_j. Let $\boldsymbol{\eta}=(\eta_1,\dots,\eta_L)$. Writing $h=[\log_2 N]+1$, we clearly have $N\leq p_j^h$ for every $j=1,\dots,L$. Furthermore, as in Lemma 15 of Beck and Chen [**5**], one can show easily that for every $\mathcal{S}\subseteq U^K$, we have

$$|D[\widetilde{\mathcal{P}}_N;\mathcal{S}\times B(\mathbf{y})]-D[\widetilde{\mathcal{P}}_N;\mathcal{S}\times B(\boldsymbol{\eta})]|\leq L. \qquad (33)$$

Since $h=[\log_2 N]+1$, it follows from (32) and (33) that

$$\mathbb{E}\left(\int_0^1\int_{\mathcal{T}}\int_{U^K}\int_{U^L}|D[\widetilde{\mathcal{P}}_N;A(\lambda,\tau,\mathbf{u})\times B(\mathbf{y})]|^W\mathrm{d}\mathbf{y}\mathrm{d}\mathbf{u}\mathrm{d}\tau\mathrm{d}\lambda\right)\ll_{A,L,W} N^{(1-1/K)W/2}.$$

This completes the proof of Theorem 3.

References

1. J.Beck, ‘Balanced two-colorings of finite sets in the square I’, *Combinatorica*, **1** (1981), 327–335.

2. J.Beck, ‘Some upper bounds in the theory of irregularities of distribution’, *Acta Arith.*, **43** (1984), 115–130.

3. J.Beck, ‘Irregularities of distribution I’, *Acta Math.*, **159** (1987), 1–49.

4. J.Beck and W.W.L.Chen, ‘Note on irregularities of distribution’, *Mathematika*, **33** (1986), 148–163.

5. J.Beck and W.W.L.Chen, ‘Note on irregularities of distribution II’, *Proc. London Math. Soc.*, **61** (1990), 251–272.

6. W.W.L.Chen, ‘On irregularities of distribution’, *Mathematika*, **27** (1980), 153–170.

7. W.W.L.Chen, ‘On irregularities of distribution III’, *J. Australian Math. Soc. (A)*, **60** (1996), 228–244.

8. K.L.Chung, *A course in probability theory* (Academic Press, New York, 1974).

9. J.H.Halton, ‘On the efficiency of certain quasirandom sequences of points in evaluating multidimensional integrals’, *Num. Math.*, **2** (1960), 84–90.

10. J.M.Hammersley, ‘Monte Carlo methods for solving multivariable problems’, *Ann. New York Acad. Sci.*, **86** (1960), 844–874.

11. K.F.Roth, ‘On irregularities of distribution’, *Mathematika*, **1** (1954), 73–79.

12. K.F.Roth, ‘On irregularities of distribution IV’, *Acta Arith.*, **37** (1980), 67–75.

13. W.M.Schmidt, ‘Irregularities of distribution X’, *Number Theory and Algebra*, pp. 311–329 (Academic Press, New York, 1977).

Department of Mathematics
Macquarie University
Sydney NSW 2109