

A Negative Answer to a Question of Novak on Randomly Shifted Lattices and the Expected p -th Power of the L_p Discrepancy

Alper Ferudun*

October 14, 2026

Abstract

In an Oberwolfach report of 2004, E. Novak (joint work with A. Hinrichs) considered the generalized lattices with shift $M_n^{z,\Delta} = \{jz + \Delta \bmod 1 : 0 \leq j < n\}$, with z and Δ independent and uniformly distributed in $[0, 1]^d$, and asked whether, for even p , the expectation of $\text{disc}_p^p(M_n^{z,\Delta})$, the p -th power of the L_p discrepancy, is at most the corresponding expectation for n independent uniformly distributed points. We show that the answer is negative. Equality holds for $p = 2$, because the lattice points are pairwise independent (in substance a known fact, which underlies random Weyl sampling), and for $n \leq 2$. For $n = 3$ and $p = 4$ the difference of the two expectations is $\frac{8}{9} 2^{-d} ((\frac{2}{5})^d - (\frac{19}{48})^d) > 0$ in every dimension d ; for $d = 1$ the two values are $19/1620$ and $16/1620$. A closed formula shows that $n = 4, p = 4$ fails in every dimension as well. For every d and every even $p \geq 4$ the inequality fails for all $n \geq N(d, p)$, with $N(d, p)$ explicit: with probability of order $1/n$ the points form a short arithmetic progression, which gives $\mathbb{E} \text{disc}_p^p \geq 4/((p+1)^d(p+2)(p+3)(n-1))$ for the lattices, against order $n^{-p/2}$ for independent points. For thirteen pairs (p, d) , among them $p = 4$ with $d \leq 4$, the inequality fails for every $n \geq 3$; this part is computer-assisted (exact rational arithmetic and a certified polynomial inequality). We conjecture failure for all $n \geq 3, d \geq 1$ and even $p \geq 4$. The answer concerns the p -th power, as in the source; for the expectation of disc_p itself, which the wording of the corpus record also allows, all computed cases go the other way. The results are asymptotic in n for fixed d and p and do not exclude bounds of the i.i.d. type when n grows polynomially with d . The question is Novak's; no answer to it was found in the literature accessible to us. This is an unrefereed note.

1 Introduction

1.1 The question

For points $t_0, \dots, t_{n-1} \in [0, 1]^d$ (repetitions allowed) and $x \in [0, 1]^d$ let $V(x) = x_1 \cdots x_d$, let $A(x)$ be the number of indices i with $t_i \in [0, x] = [0, x_1] \times \cdots \times [0, x_d]$, and let $D(x) = V(x) - A(x)/n$ be the local discrepancy. For $1 \leq p < \infty$ the L_p discrepancy (the p -discrepancy of [Nov04, p. 697]) is

$$\text{disc}_p(t_0, \dots, t_{n-1}) = \left(\int_{[0,1]^d} |D(x)|^p dx \right)^{1/p}.$$

We compare two random point sets. In the first, the n points are independent and uniformly distributed in $[0, 1]^d$, and we write $E_{\text{iid}}(n, d, p) = \mathbb{E} \text{disc}_p^p(t_0, \dots, t_{n-1})$; this is the expectation E_λ of

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: <https://github.com/AlperTheKing>.
Unrefereed preprint. CC BY 4.0.

[Nov04], with respect to Lebesgue measure on $[0, 1]^{nd}$. The second is the *generalized lattice with shift* of [Nov04, p. 698],

$$M_n^{z, \Delta} = \{t_j = jz + \Delta \pmod{1} : j = 0, \dots, n-1\}, \quad z, \Delta \in [0, 1]^d,$$

where the reduction modulo 1 is taken in each coordinate and z and Δ are independent and uniformly distributed in $[0, 1]^d$; we write

$$E_{\text{lat}}(n, d, p) = \int_{[0, 1]^{2d}} \text{disc}_p^p(M_n^{z, \Delta}) dz d\Delta,$$

which is $E_{z, \Delta}(\text{disc}_p^p(M_n^{z, \Delta}))$ in [Nov04]. The generator z is a real vector, uniformly distributed in the whole cube; for fixed z , the set $M_n^{z, \Delta}$ consists of the first n points of the Kronecker sequence $(jz)_{j \geq 0}$, shifted by Δ . For even p , Novak expanded disc_p^p as a finite sum of products (Lemma 2.1 below), computed E_{iid} from it, and asked:

Question (Novak [Nov04, p. 698]). *For even p , is it true that*

$$E_{z, \Delta}(\text{disc}_p^p(M_n^{z, \Delta})) \leq E_{\lambda}(\text{disc}_p^p(M_n)), \quad \text{that is,} \quad E_{\text{lat}}(n, d, p) \leq E_{\text{iid}}(n, d, p) ? \quad (1)$$

No quantifiers are written. The source looks for an upper bound of order $(d/n)^{1/2}$ for the star discrepancy that is obtained with “less randomness” [Nov04, p. 697], and (1) is posed for general n , d and even p . We read it as the question whether (1) holds for all $n, d \geq 1$ and all even p ; for a negative answer one triple (n, d, p) suffices, and we also describe what happens for each fixed d and p . The source adds that an answer would need the two-dimensional integrals over $(z, \Delta) \in [0, 1]^2$ of $\max_i(\{j_i z + \Delta\})^\alpha$; these are the numbers $\varphi_\alpha(S)$ of Section 2, where $\{\cdot\}$ denotes the fractional part.

The corpus record. The question is record OWR-723-005 of the dataset [ula26]. Its statement asks whether the expected L_p discrepancy of the lattices $M_n(z, \Delta)$ is at most that of the corresponding random point set; it does not mention the p -th power or the parity of p . In the literature on random points the average L_p discrepancy is $(\mathbb{E} \text{disc}_p^p)^{1/p}$ [Ste10, NP25], and in this reading the record asks (1). Read literally as the expectation of disc_p^p itself, the record asks a different question, which is not answered here; in all cases that were computed it has the opposite answer (Remark 7.2). Everything below concerns $\mathbb{E} \text{disc}_p^p$.

Conventions. Closed instead of half-open boxes, coincident points (a null set of (z, Δ)) and the index range $j = 1, \dots, n$ (replace Δ by $\{\Delta + z\}$) change nothing.

1.2 Results

Theorem 1.1 (equality cases). *Let $d \geq 1$.*

- (i) *For every $n \geq 1$, $E_{\text{lat}}(n, d, 2) = E_{\text{iid}}(n, d, 2) = (2^{-d} - 3^{-d})/n$.*
- (ii) *For $n \in \{1, 2\}$ and every even p , $E_{\text{lat}}(n, d, p) = E_{\text{iid}}(n, d, p)$.*

Theorem 1.2 (three and four points). *Let $d \geq 1$. For every $n \geq 1$,*

$$E_{\text{iid}}(n, d, 4) = n^{-3}[(2^{-d} - 3^{-d}) + 3(n-2)(3^{-d} - 2 \cdot 4^{-d} + 5^{-d})],$$

and

$$\begin{aligned} E_{\text{lat}}(3, d, 4) - E_{\text{iid}}(3, d, 4) &= \frac{8}{9} 2^{-d} \left[\left(\frac{2}{5}\right)^d - \left(\frac{19}{48}\right)^d \right] > 0, \\ E_{\text{lat}}(4, d, 4) - E_{\text{iid}}(4, d, 4) &= \frac{3}{4} 2^{-d} \left[2 \left(\frac{2}{5}\right)^d - \left(\frac{19}{48}\right)^d - \left(\frac{517}{1296}\right)^d \right] + \frac{3}{32} \left[\left(\frac{11}{54}\right)^d - \left(\frac{1}{5}\right)^d \right] > 0. \end{aligned}$$

In particular $E_{\text{lat}}(3, 1, 4) = \frac{19}{1620} > \frac{16}{1620} = E_{\text{iid}}(3, 1, 4)$ and $E_{\text{lat}}(4, 1, 4) = \frac{139}{17280} > \frac{99}{17280} = E_{\text{iid}}(4, 1, 4)$, so that (1) fails for $n = 3$, $d = 1$, $p = 4$.

Theorem 1.3 (failure for all large n). *Let $d \geq 1$ and let $p \geq 4$ be even. For every $n \geq 3$,*

$$E_{\text{lat}}(n, d, p) \geq \frac{4}{(p+1)^d(p+2)(p+3)(n-1)} \quad \text{and} \quad E_{\text{iid}}(n, d, p) \leq T_p (2^{-d} - 3^{-d}) n^{-p/2}, \quad (2)$$

where T_p is the number of partitions of $\{1, \dots, p\}$ without singleton blocks ($T_4 = 4$, $T_6 = 41$, $T_8 = 715$, $T_{10} = 17722$; $T_p \leq (p/2)^p$). Put $K(d, p) = \frac{1}{4} T_p (p+2)(p+3)(p+1)^d (2^{-d} - 3^{-d})$, and let $N(d, p)$ be the least integer $N \geq 3$ with $N^{p/2-1} \geq K(d, p)$. Then $E_{\text{lat}}(n, d, p) > E_{\text{iid}}(n, d, p)$ for every $n \geq N(d, p)$, and

$$\frac{E_{\text{lat}}(n, d, p)}{E_{\text{iid}}(n, d, p)} \geq \frac{n^{p/2-1}}{K(d, p)} \quad \text{for every } n \geq 3. \quad (3)$$

In particular, for fixed d and p there is no constant C , independent of n , with $E_{\text{lat}}(n, d, p) \leq C E_{\text{iid}}(n, d, p)$ for all n .

Theorem 1.4 (complete cases; computer-assisted). *For each of the thirteen pairs*

$$(p, d) \in \{(4, 1), (4, 2), (4, 3), (4, 4), (6, 1), (6, 2), (6, 3), (6, 4), (8, 1), (8, 2), (8, 3), (10, 1), (10, 2)\}$$

one has $E_{\text{lat}}(n, d, p) > E_{\text{iid}}(n, d, p)$ for every $n \geq 3$. For $(4, 1)$ and $(6, 1)$ the proof uses no computer.

Conjecture 1.5. $E_{\text{lat}}(n, d, p) > E_{\text{iid}}(n, d, p)$ for all $n \geq 3$, $d \geq 1$ and even $p \geq 4$.

So the answer is negative (Theorem 1.2, $n = 3$, $d = 1$, $p = 4$), for every even $p \geq 4$ in every dimension (Theorem 1.3), and (1) holds, with equality, for $p = 2$ and for $n \leq 2$ (Theorem 1.1). Conjecture 1.5 is supported by exact values in 2,354 cases (Remark 7.1).

The mechanism. If z is close to 0 or to 1, an event of probability about $2/(n-1)$, the n points form a short arithmetic progression and disc_p^p is of order one; this gives the lower bound in (2). For independent points $\mathbb{E} \text{disc}_p^p$ is of order $n^{-p/2}$. For $p = 2$ the two orders agree, and pairwise independence gives equality; for $p \geq 4$ the progression event dominates when n is large. For $n = 3$ the effect shows up in a correlation of three points: $\varphi_2(\{0, 1, 2\}) = \frac{19}{48}$, against $\frac{2}{5}$ for three independent points (Proposition 4.1).

1.3 What the results do not say

The regime of the source. Theorems 1.3 and 1.4 concern fixed d and p . The lower bound in (2) decreases like $(p+1)^{-d}$ as d grows, and E_{iid} more slowly (for $p = 4$ its leading term is $3(3^{-d} - 2 \cdot 4^{-d} + 5^{-d}) n^{-2}$); the thresholds n_0 of Section 6 grow exponentially with d (for $p = 4$: 4, 20, 54, 121, 245, 469 for $d = 1, \dots, 6$). So our results do not exclude $E_{\text{lat}} \leq C_p E_{\text{iid}}$, or bounds of the i.i.d. type for these lattices, in the regime that motivates the source, n proportional to or polynomial in d with d large, where the computed ratios $E_{\text{lat}}/E_{\text{iid}}$ are close to 1 (for $p = 4$, $n = 12$: 1.0115 for $d = 10$, 1.000004 for $d = 20$). We do not claim that the averaging approach of the source fails in that regime.

Typical generators. For $d = 1$ and irrational z with bounded partial quotients, the star discrepancy of $M_n^{z, \Delta}$ is $O(\log n/n)$ for every Δ [KN74, Chapter 2], much smaller than for independent points, and $\text{disc}_p \leq \text{disc}_\infty$. The negative answer comes from the rare generators close to rationals with small denominators, which dominate the p -th moment; it does not say that the lattices are worse than independent points for typical z .

The other open problem of the source. The last sentence of [Nov04] asks for an upper bound for the star discrepancy of lattices like the bound $c(d/n)^{1/2}$ that holds for some point sets [HNWW01]. That problem is not addressed here.

1.4 Related work and what is new

The question and the expansion of Lemma 2.1 are due to Novak [Nov04]; the average L_p discrepancy of independent points had been used by Heinrich, Novak, Wasilkowski and Woźniakowski [HNWW01] to bound the star discrepancy (see [Nov04, Ste10] and [NP25, Section 4]). Theorem 1.1(i) follows from the pairwise independence of the points $\{jz + \Delta\}$ (Lemma 2.2(a)). Pairwise independent samples of this kind are the basis of the random Weyl sampling of Sugita and Takanobu [ST00] and, in a discrete form, of Sugita [Sug02] (we know these papers through their zbMATH reviews); the case $p = 2$ of (1) is therefore known in substance, and we include its short proof. That generators close to rationals dominate Kronecker sequences with a random generator is also visible in another normalization: for z uniformly distributed on the d -dimensional torus, Dolgopyat and Fayad [DF20] show that the discrepancy of the visits of $(\{jz\})_{j \leq N}$ to a random box, divided by $(\ln N)^d$, converges in law to a Cauchy distribution (we read the abstract); they do not compare with independent points.

The works citing the report that we found concern independent points only: Gnewuch [Gne05] carried out the symmetrization approach sketched in [Nov04]; Steinerberger [Ste10] and Hinrichs and Weyhausen [HW12] determined the asymptotic behaviour of the average L_p discrepancies; Novak and Pillichshammer [NP25] cite the report in their footnote 3, which says that the version of the symmetrized bound for independent points stated in the report contains a minor error (Gnewuch [Gne05, Section 1] also suspects an error there); we do not use that bound. The survey [Hin13], which also cites the report, could not be read.

Randomized lattices with a finite generator are of a different kind. Wnuk, Gnewuch and Hebbinghaus [WGH20, Theorem 4.6 of the arXiv version] state that their randomly shifted and jittered rank-1 lattices, with a generator drawn from a finite grid and N prime, are pairwise negatively dependent, and remark that for $d \geq 2$ and $N \geq 3$ they are in general not $\mathcal{C}_0^d$ -negatively dependent. Dick and Pillichshammer [DP26] and Du and Dick [DD26] show that unions of randomly (digitally) shifted Korobov (polynomial) lattice point sets have a star discrepancy that depends polynomially on the dimension; (1) is not discussed there. Dick, Hinrichs and Pillichshammer [DHP20, Remark 2] relate their result on Korobov's p -sets to Open Problem 40 of [NW10, p. 57], which asks for a polynomial-time construction of point sets whose L_p discrepancy is below the average.

New, to our knowledge and relative to the literature we found, are the negative answer to (1) and the explicit results of Theorems 1.2 to 1.4; see the paragraph “Scope and priority” in Section 8.

2 The expansion, the law of the points, and the gap formula

Lemma 2.1 (Novak's expansion [Nov04, p. 697]). *Let p be even and $t_0, \dots, t_{n-1} \in [0, 1)^d$. Then*

$$\text{disc}_p^p(t_0, \dots, t_{n-1}) = \sum_{j=0}^p \binom{p}{j} \left(-\frac{1}{n}\right)^j (p-j+1)^{-d} \sum_{u \in \{0, \dots, n-1\}^j} \prod_{m=1}^d \left(1 - \max_{1 \leq k \leq j} t_{u_k, m}^{p-j+1}\right),$$

where the maximum over the empty set ($j = 0$) is 0.

Proof. Since p is even, $|D|^p = D^p = \sum_j \binom{p}{j} V^{p-j} (-A/n)^j$. For each j , with $a_m(u) = \max_k t_{u_k, m}$, the first identity below holds, and Fubini's theorem gives the second:

$$A(x)^j = \sum_{u \in \{0, \dots, n-1\}^j} \prod_{m=1}^d \mathbf{1}[x_m > a_m(u)], \quad \int_{[0, 1]^d} V^{p-j} \prod_m \mathbf{1}[x_m > a_m] dx = \prod_m \frac{1 - a_m^{p-j+1}}{p-j+1}. \quad \square$$

For a finite set $S \subset \mathbb{Z}$ and $\alpha > 0$ we put

$$\varphi_\alpha(S) = \mathbb{E} \left[1 - \max_{s \in S} \{sz + \Delta\}^\alpha \right], \quad \varphi_\alpha(\emptyset) = 1,$$

where z and Δ are independent and uniformly distributed in $[0, 1)$. These are, up to the term 1, the integrals named in the source.

Lemma 2.2 (the law of the lattice points). *Let z and Δ be independent and uniformly distributed in $[0, 1)^d$, and let $t_j = \{jz + \Delta\}$, coordinatewise.*

- (a) *For integers $j \neq j'$ the pair $(t_j, t_{j'})$ is uniformly distributed in $[0, 1)^{2d}$.*
- (b) *For every finite $S \subset \mathbb{Z}$ and $\alpha > 0$, $\mathbb{E} \prod_{m=1}^d (1 - \max_{s \in S} t_{s,m}^\alpha) = \varphi_\alpha(S)^d$.*
- (c) *$\varphi_\alpha(S + c) = \varphi_\alpha(S)$ for $c \in \mathbb{Z}$, and $\varphi_\alpha(cS) = \varphi_\alpha(S)$ for $c \in \mathbb{Z} \setminus \{0\}$.*
- (d) *If $U_1, \dots, U_k$ are independent and uniform in $[0, 1)$, then $\mathbb{E}[1 - \max_i U_i^\alpha] = \alpha/(\alpha + k)$. Hence $\varphi_\alpha(S) = \alpha/(\alpha + |S|)$ if $|S| \leq 2$.*

Proof. The pairs (z_m, Δ_m) , $m = 1, \dots, d$, are independent, and the m -th coordinate of every t_j depends only on (z_m, Δ_m) . This gives (b), and it reduces (a) to $d = 1$. Let $d = 1$. For fixed z the map $\Delta \mapsto \{jz + \Delta\}$ preserves Lebesgue measure on $[0, 1)$; hence $s = t_j$ is uniform and independent of z . Write $t_{j'} = \{s + w\}$ with $w = \{(j' - j)z\}$. For an integer $c \neq 0$ the map $z \mapsto \{cz\}$ preserves Lebesgue measure on $[0, 1)$, since the preimage of an interval of length ℓ consists of $|c|$ intervals of length $\ell/|c|$; so w is uniform, and it is independent of s because it is a function of z . Hence $(s, \{s + w\})$ is uniform in $[0, 1)^2$, which proves (a). For (c), $\{(s + c)z + \Delta\} = \{sz + \Delta'\}$ with $\Delta' = \{cz + \Delta\}$, and (z, Δ') has the same law as (z, Δ) ; and $\{csz + \Delta\} = \{sz' + \Delta\}$ with $z' = \{cz\}$, which is uniform and independent of Δ . For (d), $\max_i U_i$ has the density ky^{k-1} on $[0, 1]$, so $\mathbb{E} \max_i U_i^\alpha = k/(\alpha + k)$; if $|S| \leq 2$, the points $\{sz + \Delta\}$, $s \in S$, are independent and uniform by (a). $\square$

Lemma 2.3 (gap formula). *Let $P \subset [0, 1)$ be a set of $k \geq 1$ points, and let $g_1, \dots, g_k$ be the lengths of the k arcs into which P cuts the circle $\mathbb{R}/\mathbb{Z}$ (for $k = 1$ the single gap is 1). If Δ is uniform in $[0, 1)$ and $\alpha > 0$, then*

$$\mathbb{E} \max_{q \in P} \{q + \Delta\}^\alpha = \sum_{i=1}^k \frac{1 - (1 - g_i)^{\alpha+1}}{\alpha + 1}.$$

Consequently, for every set $S \subset \mathbb{Z}$ with $k \geq 1$ elements,

$$\varphi_\alpha(S) = 1 - \frac{1}{\alpha + 1} \int_0^1 \sum_{i=1}^k [1 - (1 - g_i(z))^{\alpha+1}] dz, \quad (4)$$

where $g_1(z), \dots, g_k(z)$ are the gaps of the points $\{sz\}$, $s \in S$, which are distinct for all but finitely many $z \in [0, 1)$. In particular

$$\varphi_1(S) = \frac{1}{2} \int_0^1 \sum_i g_i(z)^2 dz, \quad \varphi_2(S) = \int_0^1 \left[\sum_i g_i(z)^2 - \frac{1}{3} \sum_i g_i(z)^3 \right] dz. \quad (5)$$

Proof. Let $u = \{-\Delta\}$, which is uniform in $[0, 1)$. For $q \in P$, the number $\{q + \Delta\} = \{q - u\}$ is the length of the arc from u to q in the positive direction. With probability one $u \notin P$; let q_i be the last point of P before u , so that u lies in the gap of length g_i that starts at q_i , at a distance $y \in (0, g_i)$ from q_i . Every other point of P lies on the positive arc from u to q_i , so $\max_{q \in P} \{q - u\} = \{q_i - u\} = 1 - y$. The point u lies in the gap that starts at q_i with probability g_i , and then y is uniform in $(0, g_i)$; hence $\mathbb{E} \max_q \{q + \Delta\}^\alpha = \sum_i \int_0^{g_i} (1 - y)^\alpha dy$, which is the first formula. Two points $\{sz\}$ and $\{s'z\}$ coincide only if $(s - s')z \in \mathbb{Z}$; applying the first formula for fixed z and integrating over z gives (4). Formulas (5) follow from $\sum_i g_i = 1$, $\frac{1}{2}(1 - (1 - g)^2) = g - \frac{1}{2}g^2$ and $\frac{1}{3}(1 - (1 - g)^3) = g - g^2 + \frac{1}{3}g^3$. $\square$

Corollary 2.4 (the two expectations). *Let p be even, $n, d \geq 1$, and $\alpha_j = p - j + 1$. Then*

$$E_{\text{iid}}(n, d, p) = \sum_{j=0}^p \binom{p}{j} \left(-\frac{1}{n}\right)^j \alpha_j^{-d} \sum_{k=0}^{\min(j, n)} \binom{n}{k} \text{Surj}(j, k) \left(\frac{\alpha_j}{\alpha_j + k}\right)^d \quad (6)$$

and

$$E_{\text{lat}}(n, d, p) - E_{\text{iid}}(n, d, p) = \sum_{j=3}^p \binom{p}{j} \left(-\frac{1}{n}\right)^j \alpha_j^{-d} \sum_{k=3}^{\min(j, n)} \text{Surj}(j, k) \sum_S \left[\varphi_{\alpha_j}(S)^d - \left(\frac{\alpha_j}{\alpha_j + k}\right)^d \right], \quad (7)$$

where S runs over the k -element subsets of $\{0, \dots, n-1\}$ and $\text{Surj}(j, k) = \sum_{i=0}^k (-1)^i \binom{k}{i} (k-i)^j$ is the number of maps from a j -element set onto a k -element set.

Proof. Take expectations in Lemma 2.1. For a tuple u with $S = \{u_1, \dots, u_j\}$, the expectation of $\prod_m (1 - \max_k t_{u_k, m}^\alpha)$ is $(\alpha/(\alpha + |S|))^d$ for independent points, by independence of the coordinates and Lemma 2.2(d), and it is $\varphi_\alpha(S)^d$ for the lattice, by Lemma 2.2(b). For every k -element set S there are $\text{Surj}(j, k)$ tuples u with $\{u_1, \dots, u_j\} = S$. In the difference, the terms with $|S| \leq 2$ cancel by Lemma 2.2(d). $\square$

Proposition 2.5 (independent points). *Let p be even and $n, d \geq 1$. Then*

$$E_{\text{iid}}(n, d, p) = n^{-p} \sum_{\pi} \binom{n}{|\pi|} \int_{[0,1]^d} \prod_{B \in \pi} \mu_{|B|}(V(x)) dx, \quad (8)$$

where π runs over the partitions of $\{1, \dots, p\}$ into blocks of size at least 2, $|\pi|$ is the number of blocks, $(n)_m = n(n-1) \cdots (n-m+1)$, and $\mu_r(v) = v(1-v)^r + (1-v)(-v)^r$. In particular $n^p E_{\text{iid}}(n, d, p)$ is a polynomial in n of degree at most $p/2$ with rational coefficients, and

$$E_{\text{iid}}(n, d, 4) = n^{-3} [(2^{-d} - 3^{-d}) + 3(n-2)(3^{-d} - 2 \cdot 4^{-d} + 5^{-d})]. \quad (9)$$

Proof. Fix x and put $Y_i = \mathbf{1}[t_i \in [0, x]] - V(x)$. The Y_i are independent, $\mathbb{E}Y_i^r = \mu_r(V(x))$ (in particular $\mathbb{E}Y_i = 0$), and $nD(x) = -\sum_i Y_i$. Expand $(\sum_i Y_i)^p$ and group the index tuples $(i_1, \dots, i_p)$ according to the partition of $\{1, \dots, p\}$ into the classes of equal indices. A tuple whose partition has a block of size 1 has expectation 0; each other partition π is induced by $(n)_{|\pi|}$ tuples, each with expectation $\prod_{B \in \pi} \mu_{|B|}(V(x))$. Integration over x gives (8); since $\int V^r dx = (r+1)^{-d}$ the coefficients are rational, and $|\pi| \leq p/2$. For $p = 4$ the partition with one block contributes $n\mu_4(V) = nv(1-3v)$, where $v = V(1-V)$, and the three partitions into two pairs contribute $3n(n-1)v^2$; so $\mathbb{E}(\sum_i Y_i)^4 = nv + 3n(n-2)v^2$, and $\int v dx = 2^{-d} - 3^{-d}$, $\int v^2 dx = 3^{-d} - 2 \cdot 4^{-d} + 5^{-d}$. $\square$

3 The equality cases

Proof of Theorem 1.1. (i) For $p = 2$ the sum (7) is empty, so $E_{\text{lat}}(n, d, 2) = E_{\text{iid}}(n, d, 2)$, and (8) gives $E_{\text{iid}}(n, d, 2) = n^{-2} \cdot n \int \mu_2(V(x)) dx = (2^{-d} - 3^{-d})/n$. (ii) For $n = 1$ the only point $t_0 = \Delta$ is uniform, and for $n = 2$ the pair (t_0, t_1) is uniform in $[0, 1)^{2d}$ by Lemma 2.2(a); so $M_n^{z, \Delta}$ has the same law as n independent uniform points. $\square$

Remark 3.1. The proof uses only the pairwise independence of the lattice points (Lemma 2.2(a)), the principle of random Weyl sampling [ST00, Sug02]; so Theorem 1.1(i) is known in substance. The points are not independent in triples, since $t_2 = \{2t_1 - t_0\}$; for $p \geq 4$ the expansion contains sets S with at least three elements, and there the two models differ.

4 Three and four points

The map $z \mapsto 1 - z$ replaces the points $\{sz\}$ by $\{-sz\} = 1 - \{sz\}$ (for $sz \notin \mathbb{Z}$), a reflection of the circle, and does not change the gaps. In the computations below it therefore suffices to integrate over $z \in (0, \frac{1}{2})$ and to double.

Proposition 4.1. (a) For every $\alpha > 0$,

$$\varphi_\alpha(\{0, 1, 2\}) = \frac{\alpha^2 + 1 - 2^{-\alpha}}{(\alpha + 1)(\alpha + 2)}, \quad \frac{\alpha}{\alpha + 3} - \varphi_\alpha(\{0, 1, 2\}) = \frac{\alpha - 3 + (\alpha + 3)2^{-\alpha}}{(\alpha + 1)(\alpha + 2)(\alpha + 3)};$$

the last expression is 0 for $\alpha = 1$ and positive for every integer $\alpha \geq 2$. In particular $\varphi_1(\{0, 1, 2\}) = \frac{1}{4}$ and $\varphi_2(\{0, 1, 2\}) = \frac{19}{48}$.

(b) $\varphi_1(\{0, 1, 3\}) = \frac{1}{4}$ and $\varphi_2(\{0, 1, 3\}) = \frac{517}{1296}$.

(c) $\varphi_1(\{0, 1, 2, 3\}) = \frac{11}{54}$ and $\varphi_1(\{0, 1, 2, 4\}) = \frac{85}{432}$.

Proof. (a) For $z \in (0, \frac{1}{2})$ the points are $0 < z < 2z$, with gaps $z, z, 1 - 2z$. Hence, for $\beta > 0$,

$$\int_0^1 \sum_i (1 - g_i)^\beta dz = 2 \int_0^{1/2} [2(1 - z)^\beta + (2z)^\beta] dz = \frac{2[2(1 - 2^{-\beta-1}) + \frac{1}{2}]}{\beta + 1} = \frac{5 - 2^{1-\beta}}{\beta + 1},$$

and (4) with $\beta = \alpha + 1$ gives $\varphi_\alpha = 1 - (3 - \frac{5-2^{-\alpha}}{\alpha+2})/(\alpha+1)$, which is the stated formula. The difference has the numerator $\alpha(\alpha+1)(\alpha+2) - (\alpha^2 + 1 - 2^{-\alpha})(\alpha+3) = \alpha - 3 + (\alpha+3)2^{-\alpha}$; it is 0 for $\alpha = 1$, equal to $\frac{1}{4}$ for $\alpha = 2$, and positive for $\alpha \geq 3$ because both summands are then nonnegative and the second is positive.

(b) The gaps of $0, z, 3z$ are $z, 2z, 1 - 3z$ for $z \in (0, \frac{1}{3})$ and $3z - 1, 1 - 2z, 1 - z$ for $z \in (\frac{1}{3}, \frac{1}{2})$. Hence $\int \sum_i g_i^2 = 2(14/81 + 25/324) = 1/2$ and $\int \sum_i g_i^3 = 2(1/9 + 35/864) = 131/432$, and (5) gives $\varphi_1 = 1/4$ and $\varphi_2 = 1/2 - 131/1296 = 517/1296$.

(c) The gaps of $0, z, 2z, 3z$ are $z, z, z, 1 - 3z$ on $(0, \frac{1}{3})$ and $3z - 1, 1 - 2z, z, 1 - 2z$ on $(\frac{1}{3}, \frac{1}{2})$; so $\int \sum_i g_i^2 = 2(4/27 + 1/18) = 11/27$. The gaps of $0, z, 2z, 4z$ are $z, z, 2z, 1 - 4z$ on $(0, \frac{1}{4})$, then $4z - 1, 1 - 3z, z, 1 - 2z$ on $(\frac{1}{4}, \frac{1}{3})$, and $z, 3z - 1, 1 - 2z, 1 - 2z$ on $(\frac{1}{3}, \frac{1}{2})$; so $\int \sum_i g_i^2 = 2(11/96 + 23/864 + 1/18) = 85/216$. Now apply (5). $\square$

Remark 4.2 (all triples, and four points). (a) $\varphi_1(S) = \frac{1}{4}$ for every three-element set $S \subset \mathbb{Z}$. Indeed, for three points on the circle every pair of points is joined by one of the three gaps, and the positive arc from one point of the pair to the other has length g_i or $1 - g_i$. The Bernoulli polynomial $B_2(x) = x^2 - x + \frac{1}{6}$ satisfies $B_2(1 - x) = B_2(x)$, so that $\sum_{s < s'} B_2(\{(s' - s)z\}) = \sum_i (g_i^2 - g_i + \frac{1}{6}) = \sum_i g_i^2 - \frac{1}{2}$, the sum on the left running over the three pairs in S . Each $\{(s' - s)z\}$ is uniform in $[0, 1)$ (proof of Lemma 2.2), and $\int_0^1 B_2 = 0$; hence $\int \sum_i g_i^2 dz = \frac{1}{2}$, and (5) gives the claim.

(b) For triples, the formula $\varphi_2(\{0, a, b\}) = \frac{2}{5} - \frac{a'^2 + b'^2 + (b' - a')^2}{360(a'b'(b' - a'))^2}$, where $a' = a/g$, $b' = b/g$ and $g = \gcd(a, b)$, holds in exact arithmetic for all 7021 triples with $0 < a < b \leq 119$, but we have not proved it in general. It would show that $\varphi_2(S) < \frac{2}{5}$ for every triple. It is not used below.

(c) For four points there is no such sign: $\varphi_1(\{0, 1, 2, 3\}) - \frac{1}{5} = \frac{1}{270} > 0$, whereas $\varphi_1(\{0, 1, 2, 4\}) - \frac{1}{5} = -\frac{7}{2160} < 0$; among the 41664 sets $\{0 < a < b < c\}$ with $c \leq 64$, exactly 21630 have $\varphi_1 < \frac{1}{5}$. For larger n we therefore use the bound of Section 5 rather than a term-by-term argument.

Proof of Theorem 1.2. The formula for $E_{\text{iid}}(n, d, 4)$ is (9). For $p = 4$ we have $\alpha_3 = 2$, $\alpha_4 = 1$, $\text{Surj}(3, 3) = 6$, $\text{Surj}(4, 3) = 36$ and $\text{Surj}(4, 4) = 24$, so (7) reads

$$\begin{aligned} E_{\text{lat}}(n, d, 4) - E_{\text{iid}}(n, d, 4) &= \frac{24}{n^3 2^d} \sum_{|S|=3} \left[\left(\frac{2}{5}\right)^d - \varphi_2(S)^d \right] + \frac{36}{n^4} \sum_{|S|=3} \left[\varphi_1(S)^d - \left(\frac{1}{4}\right)^d \right] \\ &\quad + \frac{24}{n^4} \sum_{|S|=4} \left[\varphi_1(S)^d - \left(\frac{1}{5}\right)^d \right], \end{aligned} \quad (10)$$

with $S \subseteq \{0, \dots, n-1\}$. The middle sum vanishes by Remark 4.2(a) (for $n \leq 4$ also by Proposition 4.1(a),(b)). For $n = 3$ the only three-element set is $\{0, 1, 2\}$ and there is no four-element set, so the difference is $\frac{24}{27} 2^{-d} \left[\left(\frac{2}{5}\right)^d - \left(\frac{19}{48}\right)^d \right]$, which is positive because $\frac{2}{5} = \frac{96}{240} > \frac{95}{240} = \frac{19}{48}$. For $n = 4$ the three-element sets are $\{0, 1, 2\}$, $\{1, 2, 3\} = \{0, 1, 2\} + 1$, $\{0, 1, 3\}$ and $\{0, 2, 3\} = 3 - \{0, 1, 3\}$, so by Lemma 2.2(c) and Proposition 4.1 the first sum equals $2 \left[2 \left(\frac{2}{5}\right)^d - \left(\frac{19}{48}\right)^d - \left(\frac{517}{1296}\right)^d \right]$; the only four-element set is $\{0, 1, 2, 3\}$. With $\frac{24}{64} = \frac{3}{8}$ and $\frac{24}{256} = \frac{3}{32}$ this gives the stated formula, and it is positive because $\frac{19}{48} < \frac{2}{5}$, $\frac{517}{1296} < \frac{2}{5}$ (as $2585 < 2592$) and $\frac{11}{54} > \frac{1}{5}$ (as $55 > 54$). For $d = 1$: $E_{\text{iid}}(3, 1, 4) = (1/27)(1/6 + 1/10) = 4/405 = 16/1620$ and the difference is $(4/9)(2/5 - 19/48) = 1/540 = 3/1620$; $E_{\text{iid}}(4, 1, 4) = (1/64)(1/6 + 1/5) = 11/1920 = 99/17280$ and the difference is $(3/8)(4/5 - 19/48 - 517/1296) + (3/32)(1/270) = 1/432 = 40/17280$. $\square$

5 Failure for all large n

Theorem 5.1 (the progression event). *For $d \geq 1$, $n \geq 3$ and even $p \geq 2$,*

$$E_{\text{lat}}(n, d, p) \geq \frac{4}{(p+1)^d (p+2)(p+3)(n-1)}.$$

Proof. Step 1: reduction to $d = 1$. Fix $x \in [0, 1]^d$ and (z_1, Δ_1) , and let $\mathbb{E}'$ denote the expectation over (z_m, Δ_m) , $m \geq 2$, which are independent of (z_1, Δ_1) . For each j the coordinates $t_{j,m} = \{jz_m + \Delta_m\}$, $m \geq 2$, are independent and uniform, so $\mathbb{E}' \mathbf{1}[t_j \in [0, x]] = \mathbf{1}[t_{j,1} < x_1] \prod_{m \geq 2} x_m$ and

$$\mathbb{E}' D(x) = \left(\prod_{m \geq 2} x_m \right) \left(x_1 - \frac{N(x_1)}{n} \right), \quad N(x_1) = \#\{j : t_{j,1} < x_1\}.$$

By Jensen's inequality for the convex function $y \mapsto y^p$, $\mathbb{E}' D(x)^p \geq \prod_{m \geq 2} x_m^p (x_1 - N(x_1)/n)^p$. Integrating over x and over (z_1, Δ_1) gives $E_{\text{lat}}(n, d, p) \geq (p+1)^{1-d} E_{\text{lat}}(n, 1, p)$.

Step 2: $d = 1$. Let $0 \leq z < \frac{1}{n-1}$, $s = (n-1)z$ and $0 \leq \Delta < 1 - s$. Then the points $\Delta + jz$, $0 \leq j \leq n-1$, lie in $[\Delta, \Delta + s] \subset [0, 1)$, so no reduction modulo 1 occurs, and $N(x) = 0$ for $x \leq \Delta$, $N(x) = n$ for $x > \Delta + s$. Hence

$$\text{disc}_p^p \geq \int_0^\Delta x^p dx + \int_{\Delta+s}^1 (1-x)^p dx = \frac{\Delta^{p+1} + (1-s-\Delta)^{p+1}}{p+1}.$$

Integration over $\Delta \in [0, 1-s)$ gives $2(1-s)^{p+2}/((p+1)(p+2))$, and integration over $z \in [0, \frac{1}{n-1})$, with $dz = ds/(n-1)$, gives $2/((p+1)(p+2)(p+3)(n-1))$. The range $1 - \frac{1}{n-1} < z < 1$ gives the same amount: with $w = 1 - z$ and $\Delta \in ((n-1)w, 1)$ the points are $\{jz + \Delta\} = \Delta - jw \in [\Delta - (n-1)w, \Delta] \subset (0, 1)$, and the same computation applies with the lowest point $\Delta - (n-1)w$ in place of Δ . The two ranges of z are disjoint because $n \geq 3$. Hence $E_{\text{lat}}(n, 1, p) \geq 4/((p+1)(p+2)(p+3)(n-1))$, and Step 1 completes the proof. $\square$

Proposition 5.2 (an upper bound for independent points). *For even p and $n, d \geq 1$, $E_{\text{iid}}(n, d, p) \leq T_p(2^{-d} - 3^{-d})n^{-p/2}$, where T_p is the number of partitions of $\{1, \dots, p\}$ without blocks of size 1. Moreover $T_p \leq (p/2)^p$.*

Proof. In (8), $\mu_r(V)$ is the r -th moment of a random variable Y with $|Y| \leq 1$ and $\mathbb{E}Y^2 = \mu_2(V) = V(1 - V) \leq \frac{1}{4}$. So $|\mu_r(V)| \leq \mu_2(V)$ for $r \geq 2$, and $|\prod_{B \in \pi} \mu_{|B|}(V)| \leq \mu_2(V)^{|\pi|} \leq \mu_2(V)$. Moreover $(n)_{|\pi|} \leq n^{|\pi|} \leq n^{p/2}$. Hence $E_{\text{iid}}(n, d, p) \leq n^{-p} T_p n^{p/2} \int V(1 - V) dx = T_p(2^{-d} - 3^{-d})n^{-p/2}$. Label the blocks of a partition by $1, \dots, |\pi|$ in the order of their smallest elements; then the sequence of the labels of $1, \dots, p$ determines the partition, and $|\pi| \leq p/2$; so $T_p \leq (p/2)^p$. $\square$

The numbers T_p form the sequence A000296 of the OEIS; $T_2 = 1$, $T_4 = 4$, $T_6 = 41$, $T_8 = 715$, $T_{10} = 17722$.

Proof of Theorem 1.3. The two bounds (2) are Theorem 5.1 and Proposition 5.2. Dividing them, for $n \geq 3$,

$$\frac{E_{\text{lat}}(n, d, p)}{E_{\text{iid}}(n, d, p)} \geq \frac{4n^{p/2}}{T_p(p+2)(p+3)(p+1)^d(2^{-d} - 3^{-d})(n-1)} = \frac{n^{p/2}}{K(d, p)(n-1)} > \frac{n^{p/2-1}}{K(d, p)},$$

which is (3). Since $p \geq 4$, the right-hand side is nondecreasing in n , and it is at least 1 for $n \geq N(d, p)$; then $E_{\text{lat}}(n, d, p) > E_{\text{iid}}(n, d, p)$. The ratio tends to infinity with n , so no constant C independent of n can work. $\square$

Remark 5.3. For $d = 1, 2, 3, 5, 10$ the numbers $N(d, p)$ are 35, 146, 462, 3562, 393598 for $p = 4$; 30, 71, 150, 581, 14144 for $p = 6$; 31, 61, 109, 316, 4037 for $p = 8$; and 34, 59, 95, 235, 2037 for $p = 10$. They are crude, because Proposition 5.2 is; with the exact E_{iid} , the bound of Theorem 5.1 alone decides all $n \geq n_0(d, p)$, with much smaller n_0 (Table 1). Theorem 5.1 is nearly sharp for $n = 3$ and large p : for $d = 1$ the ratio of $E_{\text{lat}}(3, 1, p)$ to the bound is 1.2315, 1.0895, 1.0371, 1.0160 for $p = 4, 6, 8, 10$ and 1.000005 for $p = 30$. The exact values suggest that E_{lat} is of order $1/n$: $n E_{\text{lat}}(n, 1, 4) = 0.02875, 0.02813, 0.02796, 0.02791, 0.02790$ for $n = 10, 20, 40, 80, 120$, while the bound gives $4n/(210(n-1)) \approx 0.019$; we have no proof of an upper bound of order $1/n$.

6 The complete cases

Let (p, d) be one of the thirteen pairs of Theorem 1.4, let $L(n) = 4/((p+1)^d(p+2)(p+3)(n-1))$ be the bound of Theorem 5.1, and put $c = 4/((p+1)^d(p+2)(p+3))$. By Proposition 2.5, $Q(n) = n^p E_{\text{iid}}(n, d, p)$ is a polynomial in n of degree at most $p/2$ with rational coefficients, and so is

$$P(n) = n^p(n-1)(L(n) - E_{\text{iid}}(n, d, p)) = cn^p - (n-1)Q(n),$$

a polynomial of degree p with leading coefficient $c > 0$ (since $p/2 + 1 < p$), whose coefficients follow from (6).

Proof of Theorem 1.4. Step 1: $n \geq n_0$. For the value $n_0 = n_0(d, p)$ in Table 1, all coefficients of the polynomial $t \mapsto P(n_0 + t)$ are nonnegative, and its constant term $P(n_0)$ is positive. Hence $P(n) > 0$ for all real $n \geq n_0$, so that $L(n) > E_{\text{iid}}(n, d, p)$, and $E_{\text{lat}}(n, d, p) > E_{\text{iid}}(n, d, p)$ for every integer $n \geq n_0$ by Theorem 5.1. (If $n_0 > 3$ then $P(n_0 - 1) \leq 0$, so that the bound of Theorem 5.1 alone does not decide $n_0 - 1$.)

Step 2: $3 \leq n < n_0$. For these n the right-hand side of (7) was evaluated exactly, in rational arithmetic, and is positive. The numbers $\varphi_\alpha(S)$ are computed from (4). After a translation (Lemma 2.2(c)) we may assume that 0 is the smallest element of S . On each open interval between consecutive points

(p, d)	n_0	exact	(p, d)	n_0	exact	(p, d)	n_0	exact
(4, 1)	4	65	(6, 1)	3	25	(8, 1)	3	10
(4, 2)	20	65	(6, 2)	8	25	(8, 2)	6	10
(4, 3)	54	65	(6, 3)	16	25	(8, 3)	11	10
(4, 4)	121	120	(6, 4)	26	25	(10, 1)	3	6
						(10, 2)	5	6

Table 1: The thresholds $n_0 = n_0(d, p)$ of Step 1, and the largest n up to which all four exact computations of $E_{\text{lat}} - E_{\text{iid}}$ went (Step 2). The three verification runs went further for $p = 4$, $d \leq 3$ (up to $n = 120$), and two of them also covered $(8, 4)$ for $n \leq 10$ and $(10, 3)$ for $n \leq 6$.

of the finite set $\{m/D : D = s - s' > 0 \text{ with } s, s' \in S, 0 \leq m \leq D\}$ the integer parts $\lfloor sz \rfloor$ and the circular order of the points $\{sz\}$ are constant, so every gap has the form $A + Bz$ with integers A and B , and (4) is a finite sum of integrals of polynomials with rational coefficients. By Lemma 2.2(c) one representative suffices for each class of sets under translation, reflection $S \mapsto -S$ and scaling $S \mapsto cS$. $\square$

Five programs computed the thresholds: by root isolation, by the coefficient certificate with a Sturm count, by root counting up to a Cauchy bound, by the exact program of this note, and by the program of the verification run of this text (the coefficient certificate, the sign of $P(n_0 - 1)$ and root isolation, with E_{iid} from the moment-cumulant recursion); all give Table 1. Step 2 was carried out four times, by independent programs (Section 8). For $(p, d) = (4, 5)$ and $(4, 6)$ the certificate gives $n_0 = 245$ and 469 , beyond the exact computations.

Two cases without computer. For $(p, d) = (4, 1)$, (9) gives $E_{\text{iid}}(n, 1, 4) = (3n - 1)/(30n^3)$, and $L(n) = 2/(105(n - 1))$; hence

$$L(n) - E_{\text{iid}}(n, 1, 4) = \frac{f(n)}{210n^3(n - 1)}, \quad f(n) = 4n^3 - 21n^2 + 28n - 7 = (n - 4)(4n^2 - 5n + 8) + 25.$$

Since $4n^2 - 5n + 8 > 0$, $f(n) \geq 25$ for $n \geq 4$, and Theorem 5.1 gives $E_{\text{lat}} > E_{\text{iid}}$ for all $n \geq 4$; the case $n = 3$ is Theorem 1.2. (Here $n_0 = 4$, and $f(3) = -4$.) For $(p, d) = (6, 1)$ we use (8) with $p = 6$: there is one partition with one block, 15 of type $(4, 2)$, 10 of type $(3, 3)$ and 15 of type $(2, 2, 2)$. With $v = x(1 - x)$ one has $\mu_2 = v$, $\mu_3^2 = v^2(1 - 4v)$, $\mu_4 = v(1 - 3v)$, $\mu_6 = v(1 - 5v + 5v^2)$, and $\int_0^1 v = \frac{1}{6}$, $\int_0^1 v^2 = \frac{1}{30}$, $\int_0^1 v^3 = \frac{1}{140}$. Hence

$$E_{\text{iid}}(n, 1, 6) = n^{-6} \left[\frac{n}{28} + \frac{19n(n - 1)}{84} + \frac{3n(n - 1)(n - 2)}{28} \right] = \frac{9n^2 - 8n + 2}{84n^5},$$

and with $L(n) = 1/(126(n - 1))$,

$$L(n) - E_{\text{iid}}(n, 1, 6) = \frac{g(n)}{252n^5(n - 1)}, \quad g(n) = 2n^5 - 27n^3 + 51n^2 - 30n + 6.$$

Now $g(3) = 132 > 0$, and for $n \geq 4$ both $2n^5 - 27n^3 = n^3(2n^2 - 27)$ and $51n^2 - 30n + 6$ are positive. So $E_{\text{lat}}(n, 1, 6) > E_{\text{iid}}(n, 1, 6)$ for every $n \geq 3$. This proves the last sentence of Theorem 1.4.

7 Remarks and open questions

Remark 7.1 (evidence for Conjecture 1.5). Every exact computation made for this note with $n \geq 3$ and $p \geq 4$ gave $E_{\text{lat}} > E_{\text{iid}}$. Together they cover 2,354 distinct triples (n, d, p) : besides the ranges of

Table 1 (for $p = 4$, $d \leq 4$ up to $n = 120$, and $(8, 4)$, $(10, 3)$ as in its caption), $p = 4$ with $n \leq 65$ for $d \in \{6, 10\}$, and in verification run B $p = 4$ with $d, n \leq 40$, $p = 6$ with $n \leq 25$ and ten values of d up to 20, $p = 8$ with $n \leq 10$ and seven values of d up to 16, $p = 10$ with $n \leq 6$ and six values of d up to 12, and $d = 1$, $n \leq 5$ for $p \in \{12, 14, 16, 20, 24, 30\}$. For fixed n the ratio $E_{\text{lat}}/E_{\text{iid}}$ decreases to 1 as d grows; for fixed d it grows with n (for $p = 4$, $d = 1$: 18.24 at $n = 65$, 33.57 at $n = 120$).

Remark 7.2 (the expectation of disc_p itself). For the expectation of disc_p , without the p -th power, the verification runs found the opposite inequality in every case they computed; these are numerical results, not proofs. Pairs of values (lattices, independent points) for $d = 1$, by quadrature on the cells of the (z, Δ) -square on which the sorted points are affine (the same code reproduces the exact values of $\mathbb{E} \text{disc}_p^p$): (0.2601443, 0.2681902) for $n = 3$, $p = 4$; (0.288563, 0.297889) for $n = 3$, $p = 6$; (0.308520, 0.318620) for $n = 3$, $p = 8$; (0.215452, 0.221410) for $n = 3$, $p = 2$. By Monte Carlo for $p = 4$ (standard errors below $2 \cdot 10^{-4}$): (0.1211, 0.1465) for $d = 1$, $n = 10$; (0.0101, 0.0267) for $d = 1$, $n = 300$; (0.26730, 0.26882) for $d = 2$, $n = 3$; (0.13880, 0.14790) for $d = 2$, $n = 10$; (0.18200, 0.18330) for $d = 3$, $n = 5$. The progression event of Theorem 5.1 dominates $\mathbb{E} \text{disc}_p^p$, but after the p -th root inside the expectation the typical generators dominate. The comparison of $\mathbb{E} \text{disc}_p$ is not settled here.

Remark 7.3 (other readings). The question is about z uniform in the cube, not about Korobov vectors $z = g/n$ or lattice rules with a fixed generator and a random shift. For $z = g/n$ with g uniform in $\{0, 1, 2\}$ ($n = 3$, $d = 1$, $p = 4$), the generator $g = 0$ alone, for which all points coincide with Δ , contributes $\frac{1}{3} \int_0^1 \frac{1}{5} (\Delta^5 + (1 - \Delta)^5) d\Delta = \frac{1}{45} > \frac{16}{1620} = E_{\text{iid}}(3, 1, 4)$.

Open questions. (1) Conjecture 1.5: does (1) fail for every $n \geq 3$ and every even $p \geq 4$, in every dimension? A proof might combine Theorem 5.1 with a lower bound for the contribution of three or four points in (7); the closed form of Remark 4.2(b) would settle the three-point part for $p = 4$. (2) Is $E_{\text{lat}}(n, d, p) = O(1/n)$ for fixed d and p (Remark 5.3)? (3) The comparison of $\mathbb{E} \text{disc}_p$ (Remark 7.2). (4) In the regime $n \leq d^C$ that motivates the source, does $E_{\text{lat}}(n, d, p) \leq C_p E_{\text{iid}}(n, d, p)$ hold, or at least an upper bound of the i.i.d. type for E_{lat} (Section 1.3)? (5) Does a comparison hold when z is restricted to a set of good generators?

8 Computations and reproducibility

The proofs in Sections 2 to 5 use no computation; Theorem 1.4 is computer-assisted (exact arithmetic in both steps), except for the cases $(4, 1)$ and $(6, 1)$. The reproducibility package has four parts.

The exact program of this note (`writing_stage/check_note.py`, Python standard library, about fifteen seconds). It computes $\varphi_\alpha(S)$ from the definition and compares with Lemma 2.3, Lemma 2.2(c),(d), Proposition 4.1 and Remark 4.2(a); it checks Lemma 2.1 on random rational point sets; it computes $E_{\text{lat}}(n, 1, p)$ ($p = 4$, $n \leq 8$; $p \in \{2, 6, 8, 10\}$, $n \leq 3$) and $E_{\text{lat}}(n, 2, 4)$ ($n \leq 4$) by a direct integration over the (z, Δ) -square that uses none of Lemmas 2.1 to 2.3, and compares with the expansion; it checks Theorem 1.1, the closed forms of Theorem 1.2 for $d \leq 12$, Table 2, the bounds of Section 5 on exact values, the numbers in Remark 5.3 (the values of $N(d, p)$, the ratios for $n = 3$, and $n E_{\text{lat}}(n, 1, 4)$ for $n = 10, 20$), Step 1 of the proof of Theorem 1.4 for all thirteen pairs and the two cases done without a computer; and it rejects seven deliberately wrong inputs (negative controls), for instance $\varphi_2(\{0, 1, 2\})$ replaced by $\frac{2}{5}$ or the threshold $n_0 - 1$. All checks pass.

The programs with which the results were first obtained (`original/`, Python with `sympy` and `numpy`): $\varphi_\alpha(S)$ by exact piecewise integration; E_{lat} and E_{iid} by the expansion (rational and integer codes); a direct symbolic integration in $d = 1$ without Lemmas 2.1 and 2.3 ($p = 4$, $n \leq 6$; $p = 6$, $n \leq 5$); the thresholds by exact root isolation; a Monte Carlo test in $d = 2$ (for $p = 4$, $n = 3$, two runs with $2 \cdot 10^6$ samples gave 0.0087898 and 0.0087777, standard error $1.1 \cdot 10^{-5}$, against $6829/777600 = 0.0087822$). They found $378 + 118$, 92, 24 and 8 positive differences for $p = 4, 6, 8, 10$ (Step 2 and Remark 7.1).

n	$E_{\text{lat}}(n, 1, 4)$	$E_{\text{iid}}(n, 1, 4)$	ratio
3	19/1620	4/405 = 16/1620	1.1875
4	139/17280	11/1920	1.4040
5	31/5000	7/1875	1.6607
6	647/129600	17/6480	1.9029
7	274313/64827000	2/1029	2.1771
8	29399/8064000	23/15360	2.4347
14	1700176573/839091052800	41/82320	4.0682
65	$\approx 4.29527 \cdot 10^{-4}$	97/4119375	18.2411

Table 2: Exact values for $d = 1$, $p = 4$, where $E_{\text{iid}}(n, 1, 4) = (3n - 1)/(30n^3)$. For $n = 3$, $d = 1$: 353/81648 against 59/20412 ($p = 6$), 4399/2099520 against 37/32805 ($p = 8$), 196897/166281984 against 689/1299078 ($p = 10$). For $d = 2$, $p = 4$: 6829/777600 against 391/48600 ($n = 3$) and 620539/111974400 against 133/28800 ($n = 4$).

Two independent verification runs of the first written version. Their programs and outputs are in the folders `verification_run_A/` and `verification_run_B/`. All their Monte Carlo estimates of $\mathbb{E} \text{disc}_p^p$ ($d = 1, 2, 3$) agree with the exact values within about 2.3 standard errors.

The verification run of this text (`independent_run_2/`, Python with sympy and numpy): its own exact programs for $\varphi_\alpha(S)$ (the integrals $\int_0^1 \sum_i g_i(z)^r dz$ by a sweep over the breakpoints m/D), for E_{iid} (by the binomial law and by the moment-cumulant recursion) and for $E_{\text{lat}}(n, 1, p)$ (by direct integration), the checks of Sections 2 to 4, both steps of the proof of Theorem 1.4, a comparison of its exact values with those of run B, and the numerical values of Remark 7.2; see the paragraph “Verification”.

Verification. The results were first obtained, with proofs and with the programs in `original/`. Two independent verification runs (A and B), both AI-assisted, followed; each wrote its own programs from the definitions, and neither saw the report of the other.

The first run (A) compared the statement with the source, which it read in full, and re-derived all lemmas and the proofs of Theorems 1.1 to 1.3 and 5.1 and Proposition 5.2 line by line. Its programs computed $\varphi_\alpha(S)$ from the definition; $E_{\text{lat}}(n, 1, p)$ by a direct integration ($p = 4$, $n \leq 7$; $p = 6$, $n \leq 5$; $p = 8$, $n \leq 4$; $p = 10$, $n = 3$; $p = 2$, $n \leq 5$); $E_{\text{lat}} - E_{\text{iid}}$ with all index tuples enumerated (52 cases); Step 2 of Theorem 1.4 for $p = 4$, $d \leq 4$, $n \leq 120$, for $p = 6$, $d \leq 4$, $n \leq 25$, for $p = 8$, $d \leq 3$, $n \leq 10$, and for $p = 10$, $d \leq 2$, $n \leq 6$; and the thresholds with the certificate of Step 1 and a Sturm count. It also made the Monte Carlo tests in $d = 2, 3$ and the computations of $\mathbb{E} \text{disc}_p$ of Remark 7.2, after noticing that the wording of the corpus record differs from the source.

The second run (B) computed $E_{\text{lat}}(n, 1, p)$ by exact integration over the polygons of the (z, Δ) -square on which the sorted points are affine, without any lemma ($n \leq 14$ for $p = 4$, $n \leq 10$ for $p = 6$, $n \leq 8$ for $p = 8$, $n \leq 7$ for $p = 10$), and in $d = 2, 3$ by a product decomposition (15 cases); it checked the closed forms of Theorem 1.2 for $d \in \{1, 2, 3, 5, 8, 13, 20, 30\}$, computed E_{iid} in three ways, Step 2 of Theorem 1.4 (472, 92, 32 and 12 cases with $n \geq 3$ for $p = 4, 6, 8, 10$, all positive), the thresholds by root isolation and root counting, and 1,830 further cases (Remark 7.1); its 22 negative controls (deliberately wrong inputs) were all rejected; and it re-ran all programs of `original/` from a copy and obtained every recorded output again. It also found the work on random Weyl sampling and the paper of Dolgopyat and Fayad.

Both runs A and B confirmed the answer and all proofs, and required corrections of the first written version, which were made: the answer is stated for $\mathbb{E} \text{disc}_p^p$ only, with Remark 7.2; the scope

of Theorem 1.3 is qualified (fixed d and p ; nothing is claimed for n polynomial in d); the remark on badly approximable generators is restricted to $d = 1$; the case $p = 2$ is credited to random Weyl sampling; the descriptions of [NP25] and [WGH20] were made precise; journal versions and the works citing the source were added. This text was written after the two runs; its proofs are those of the first written version with these corrections, in the present numbering; the proofs of the cases $(4, 1)$ and $(6, 1)$ of Theorem 1.4 and the derivation of $\varphi_1(\{0, 1, 2, 4\})$ in Proposition 4.1(c) were added. The exact program of this note checks the statements as printed.

After the note was written, a further independent verification run, also AI-assisted, examined its text. It read the source again in full, the cited passages of [NP25, Gne05, Ste10, WGH20, DHP20], the abstracts of [DF20, DP26, DD26] and the zbMATH reviews of [ST00, Sug02], re-derived all proofs line by line, and wrote its own programs (`independent_run_2/`). It tested the gap formula against a brute-force double integral and Lemma 2.1 against a direct integration on random point sets; computed $E_{\text{lat}}(n, 1, p)$ directly, without any lemma ($p = 4, n \leq 8$; $p = 6, n \leq 5$; $p = 8, n \leq 4$; $p = 10, n = 3$; $p = 2, n \leq 5$); recomputed Step 2 of Theorem 1.4 with the full expansion (472, 92, 32 and 12 cases with $n \geq 3$ for $p = 4, 6, 8, 10$, all positive), with E_{iid} from the moment-cumulant recursion, and Step 1 by the coefficient certificate, the sign of $P(n_0 - 1)$ and root isolation; and found its exact values identical, as fractions, to all 638 values recorded by run B. It checked Table 2, the numbers of Remarks 4.2, 5.3 and 7.1 and of Section 1.3, reproduced the quadrature values of Remark 7.2 with its own code, ran the programs of the package again from the archive, reproducing all recorded outputs up to running times, and repeated the literature search. It found no error in a proof and required four corrections, which were made: the count of distinct cases in Remark 7.1, the attribution of two Monte Carlo runs to the programs of `original/`, a precise statement on the access to [HW12], and the record of this run.

Scope and priority. The note answers Novak’s question (1) in the negative, for the quantity of the source, the expectation of disc_p^p with even p ; the answer applies to the reading of the corpus record as the average L_p discrepancy $(\mathbb{E} \text{disc}_p^p)^{1/p}$, but not to the expectation of disc_p , for which nothing is proved here (Remark 7.2). The question and the expansion of Lemma 2.1 are Novak’s [Nov04]. The equality for $p = 2$ is known in substance: it rests on the pairwise independence of the points $jz + \Delta$ modulo 1, which underlies random Weyl sampling [ST00, Sug02]. New, to our knowledge and relative to the literature we found, are the negative answer and the explicit results: Theorem 1.2, Theorem 1.3 with the explicit $N(d, p)$, and Theorem 1.4. Not settled are Conjecture 1.5, the order of E_{lat} , the comparison of $\mathbb{E} \text{disc}_p$, and the regime in which n is polynomial in d . No answer to the question was found in the literature accessible to us; a search that finds nothing is not a proof of novelty, and no priority is claimed.

What was read: the source [Nov04], pp. 696–699, completely, in the open file of the publisher; [Gne05], [Ste10], and the passages cited here of [NP25] (arXiv v1), [WGH20] (arXiv v3) and [DHP20] (arXiv v1); the abstracts of [DF20, DP26, DD26]; and the zbMATH reviews of [ST00, Sug02]. The statement on badly approximable generators in Section 1.3 is quoted from [KN74] without re-checking. Not read: the survey [Hin13] (closed access), which cites the source and may contain a remark on the question; Chapter 9 (“Discrepancy and Integration”, pp. 1–70) and Appendix D (the list of open problems) of [NW10], which are not openly accessible, so that we know Open Problem 40 only through [DHP20]; and [HNWW01], cited after the source. A reader with access to [Hin13] or [NW10] should check them. The paper [HW12], in the open archive of the publisher, was read on 14 October 2026, after the verification runs, whose automated access the site had refused: it treats independent points only and contains no statement on lattices or shifted point sets. The searches (14 October 2026: when the results were first obtained, by the verification runs A and B, in part again when this note was written, and by the verification run of this text) used the arXiv API (Kronecker, lattice, random

shift, random generator, average or expected L_p discrepancy, pairwise independence, random Weyl sampling, the authors Novak and Hinrichs), zbMATH, Crossref, the lists of citing works in OpenAlex and Semantic Scholar, and nine general web searches. The works citing the source that we found are [Gne05, Ste10, HW12, Hin13, NP25]; none of the sources found answers the question.

AI-assisted tools were used to search the problem corpus and the literature, to find the arguments, to write and run the verification programs, and to help prepare this manuscript. The author has reviewed the proofs, the computations and the sources and is responsible for all claims. The note has not been peer reviewed.

References

- [DD26] Jiarui Du and Josef Dick. The star discrepancy of a union of randomly shifted Korobov lattice point sets depends polynomially on the dimension. *Journal of Complexity*, 95:102043, 2026. The title of arXiv version 1 differs. [arXiv:2601.16571](#), [doi:10.1016/j.jco.2026.102043](#).
- [DF20] Dmitry Dolgopyat and Bassam Fayad. Deviations of ergodic sums for toral translations II. Boxes. *Publications Mathématiques de l’IHÉS*, 132:293–352, 2020. [arXiv:1211.4323](#), [doi:10.1007/s10240-020-00120-2](#).
- [DHP20] Josef Dick, Aicke Hinrichs, and Friedrich Pillichshammer. A note on the periodic L_2 -discrepancy of Korobov’s p -sets. *Archiv der Mathematik*, 115(1):67–78, 2020. [arXiv:2001.01973](#), [doi:10.1007/s00013-020-01460-5](#).
- [DP26] Josef Dick and Friedrich Pillichshammer. The star discrepancy of a union of randomly digitally shifted Korobov polynomial lattice point sets depends polynomially on the dimension. *Journal of Complexity*, 95:102032, 2026. [arXiv:2509.15877](#), [doi:10.1016/j.jco.2026.102032](#).
- [Gne05] Michael Gnewuch. Bounds for the average L^p -extreme and the L^∞ -extreme discrepancy. *The Electronic Journal of Combinatorics*, 12:Research Paper R54, 2005. [doi:10.37236/1951](#).
- [Hin13] Aicke Hinrichs. Discrepancy, integration and tractability. In Josef Dick, Frances Y. Kuo, Gareth W. Peters, and Ian H. Sloan, editors, *Monte Carlo and Quasi-Monte Carlo Methods 2012*, volume 65 of *Springer Proceedings in Mathematics & Statistics*, pages 129–172. Springer, 2013. [doi:10.1007/978-3-642-41095-6_6](#).
- [HNWW01] Stefan Heinrich, Erich Novak, Grzegorz W. Wasilkowski, and Henryk Woźniakowski. The inverse of the star-discrepancy depends linearly on the dimension. *Acta Arithmetica*, 96(3):279–302, 2001. [doi:10.4064/aa96-3-7](#).
- [HW12] Aicke Hinrichs and Heidi Weyhausen. Asymptotic behavior of average L_p -discrepancies. *Journal of Complexity*, 28(4):425–439, 2012. [doi:10.1016/j.jco.2012.04.003](#).
- [KN74] Lauwerens Kuipers and Harald Niederreiter. *Uniform Distribution of Sequences*. Wiley, New York, 1974.
- [Nov04] Erich Novak. New bounds for the star discrepancy (joint work with Aicke Hinrichs). *Oberwolfach Reports*, 1(1):696–699, 2004. Extended abstract in Report 13/2004, *Discrepancy Theory and Its Applications*, organised by B. Chazelle, W. Chen and A. Srivastav, pp. 673–722. [doi:10.4171/OWR/2004/13](#).

- [NP25] Erich Novak and Friedrich Pillichshammer. Generalized discrepancy of random points, 2025. arXiv version 1. A journal article of the same authors with the same references, *Upper bounds for generalized L_p -discrepancy of random points*, J. Complexity 95 (2026), 102028, was not read. `arXiv:2512.08364`.
- [NW10] Erich Novak and Henryk Woźniakowski. *Tractability of Multivariate Problems. Volume II: Standard Information for Functionals*, volume 12 of *EMS Tracts in Mathematics*. European Mathematical Society, Zürich, 2010. `doi:10.4171/084`.
- [ST00] Hiroshi Sugita and Satoshi Takanobu. Random Weyl sampling for robust numerical integration of complicated functions. *Monte Carlo Methods and Applications*, 6(1):27–48, 2000. `doi:10.1515/mcma.2000.6.1.27`.
- [Ste10] Stefan Steinerberger. The asymptotic behavior of the average L^p -discrepancies and a randomized discrepancy. *The Electronic Journal of Combinatorics*, 17:Research Paper R106, 2010. `doi:10.37236/378`.
- [Sug02] Hiroshi Sugita. Robust numerical integration and pairwise independent random variables. *Journal of Computational and Applied Mathematics*, 139(1):1–8, 2002. `doi:10.1016/S0377-0427(01)00394-6`.
- [ula26] ulamai. UnsolvedMath. Hugging Face dataset, <https://huggingface.co/datasets/ulamai/UnsolvedMath>, 2026. Version 1.6.0; record OWR-723-005.
- [WGH20] Marcin Wnuk, Michael Gnewuch, and Nils Hebbinghaus. On negatively dependent sampling schemes, variance reduction, and probabilistic upper discrepancy bounds. In Dmitriy Bilyk, Josef Dick, and Friedrich Pillichshammer, editors, *Discrepancy Theory*, volume 26 of *Radon Series on Computational and Applied Mathematics*, pages 43–68. De Gruyter, Berlin, 2020. `arXiv:1904.10796`, `doi:10.1515/9783110652581-003`.