

LOW-DISCREPANCY QUASI-UNIFORM DIGITAL NETS IN EVERY DIMENSION

LEONHARD GRUENSCHLOSS

ABSTRACT. Dick, Goda and Suzuki asked for low-discrepancy digital nets that are quasi-uniform, with minimum distance δ and covering radius both of the optimal order $N^{-1/s}$, and stated the problem as open in dimension $s \geq 3$. We construct such nets in every dimension. For every $s \geq 3$, every base q whose prime factors are at least $s - 1$, and every $k \geq 1$, we give explicit digital $(0, sk, s)$ -nets over $\mathbb{Z}/q\mathbb{Z}$ with $N = q^{sk}$ points, covering radius at most $\sqrt{s} N^{-1/s}$, and $\delta N^{1/s} \geq 1 - a_s^*/q$ once $q \geq 5a_s^* + 4$. The constant $a_s^* \leq e^{s \log s + O(s)}$ is computed from s by a deterministic polynomial-time lattice algorithm. In dimension three every $N = p^m$, $m \geq 3$, is covered for each prime $p \geq 37$, and, with computer assistance, every $N = 2^m$ and $N = 3^m$. In prime bases these families are well separated in the sense of Dick, Goda and Suzuki, and they stay so under every digital shift. One mechanism underlies all constructions. For $N = q^{sk}$ it reads as follows. The first k base- q digits of a point's coordinates select a cube of side q^{-k} , and a $(0, sk, s)$ -net has exactly one point in each such cube. Digit $k + 1$ of each coordinate is a linear function of the first k digits of all coordinates, because the net is digital. We choose this linear function so that, between the planes where this digit wraps around modulo q or where a carry occurs among the first k digits, the points lie on a translate of one lattice; for the main theorem this lattice is a slightly distorted copy of $\mathbb{Z}^s$. All later digits move a point by less than $1/q$ of the cube side. Part II studies the constant K in $\delta N^{1/s} = 1 - K/q + O(q^{-2})$. We prove lower bounds on K when the linear maps have bounded coefficients. At $N = q^3$ we find the optimal K among nets whose points lie on lines parallel to the main diagonal. With the cube-tiling theorems of Hajós and Keller we show that idealized lattices with one point per cube, whose points sit independently inside their cubes, cannot exceed $\delta N^{1/s} = 1$. When the positions inside the cubes are coupled, the value 1 can be exceeded: $\delta N^{1/3} \rightarrow \sqrt{281}/16$ at $N = p^3$, $\delta N^{1/5} > 1$ for $(0, 5, 5)$ -nets from $p = 37$ on, and $\delta N^{1/s} \rightarrow \min(\sqrt{s}/2, \sqrt{2})$ at $N = p^{sk}$, which is the E_8 value at $s = 8$ (limits as $p \rightarrow \infty$). The results are formalized in Lean 4, apart from some finite computations, which are checked by scripts.

1. INTRODUCTION

A point set $P \subset [0, 1)^s$ of N points is *quasi-uniform* if its covering radius h_P and its minimum distance δ_P are both of the optimal order $N^{-1/s}$. Dick, Goda and Suzuki [11] asked for digital nets that are both low-discrepancy and quasi-uniform. Their example is the two-dimensional Larcher–Pillichshammer net [40]; for $s \geq 3$ they state the problem as open, and Suzuki [60] recently stated that no such family is known. Without the word *digital* there are answers in every dimension: Frolov point sets, Kronecker sequences, and rank-1 lattices with prime N [10, Thms. 3.1, 3.9, 3.7]. A rank-1 lattice with prime N is formally a digital $(0, 1, s)$ -net, but over $\mathbb{F}_N$, in a base that grows with N . We work in the setting of [11, 60]: digital nets in a fixed base q , along $N = q^m$ with $m \rightarrow \infty$, with their exact stratification by elementary boxes. In [11] the base is a prime b and a digital net is defined over $\mathbb{F}_b$ [11, Def. 2.1]. Our nets are digital over $\mathbb{F}_p$ for prime bases $q = p$, which is the case that answers their question, and over the ring $\mathbb{Z}/q\mathbb{Z}$ for

Date: Version 1, 2026-10-13. The Lean formalization of this version is release v1.0.0 of <https://github.com/lgruen/separated-nets-lean>.

ORCID iD: <https://orcid.org/0009-0004-6476-2191>.

composite q , in the sense of Niederreiter [46] (see also [39]). All of them are $(0, m, s)$ -nets, so they have low discrepancy (Remark 66), and the question is only about separation.

We answer the question for nets, that is, for families of nets indexed by m , in every dimension; the corresponding question for sequences, whose initial segments would form such a family, remains open (Remark 123(10)). Our nets start from a classical construction of Niederreiter [46, Sec. 6], in which coordinate c reads the base- q Taylor coefficients of one polynomial at a point a_c of the projective line. We call this a *frame* and the a_c its *places*. For the places $\infty, 0$ the frame is the Hammersley net [24], and for $\infty, 0, 1$ it is, up to lower-triangular scrambles, the Hammersley net of the two-dimensional Faure sequence [16] (Proposition 9); we call the frame of the places $\infty, 0, 1, \dots, s-2$ the *Faure-Hammersley frame* (Section 3). We scramble each coordinate by a lower-triangular matrix, chosen so that digit $k+1$ of each coordinate depends on the first k digits of all coordinates through small integer matrices. These matrices form the *design* U_s^* , which a lattice algorithm computes from s alone (Definition 23).

Theorem A (Every dimension). *Let $s \geq 3$, let $q \geq 2$ be an integer all of whose prime factors are at least $s-1$, and let $k \geq 1$. Let $\mathcal{P}_{k,q}^{U_s^*}$ be the digital net over $\mathbb{Z}/q\mathbb{Z}$ of Definition 14 for the places $\infty, 0, 1, \dots, s-2$ and the design U_s^* of Definition 23, with $N = q^{sk}$ points. Then:*

- (1) $\mathcal{P}_{k,q}^{U_s^*}$ is a digital $(0, sk, s)$ -net over $\mathbb{Z}/q\mathbb{Z}$, every cell $\prod_i [n_i q^{-k}, (n_i + 1)q^{-k})$ holds exactly one point, and $h \leq \sqrt{s} N^{-1/s}$;
- (2) if $q \geq 5a_s^* + 4$, its toroidal (hence also Euclidean) minimum distance satisfies $\delta \geq (1 - a_s^*/q) N^{-1/s}$, for every $k \geq 1$; for $k \geq 2$ the constant a_s^* is first-order sharp for this net: $\delta N^{1/s} = 1 - a_s^*/q + O(q^{-2})$ as $q \rightarrow \infty$.

Here $a_3^* = 2$, and $a_s^* \leq 2(s-1)^{3/2}(3/2)^{s-2}(s-2)! = e^{s \log s + O(s)}$ for $s \geq 4$.

The range of q in (1) is the largest possible for digital nets over $\mathbb{Z}/q\mathbb{Z}$ [39, Cor. 2], and for prime q the nets are digital in the sense of [11]. The exact values are $a_s^* = 2, 5, 16, 43, 170, 543, 2842, 13640$ for $s = 3, \dots, 10$ (Table 3), so for $s = 3, 4, 5$ the separation bound holds from $q = 14, 29$ and 84 on (for $s = 4, 5$ with the computed values $a_4^* = 5, a_5^* = 16$; $a_3^* = 2$ is proved in Section 4.3). The design U_s^* is computed from s by a deterministic algorithm in time polynomial in s (Section 4.3). A simpler, monomial design U_s (Remark 24) gives the same theorem, but with the constant $a_s = e^{\Theta(s^2)}$ ($a_5 = 17407$). Theorem A uses the same frame and the same diagonal-dominance argument (Proposition 19) as U_s ; it only replaces the entries of the design by short vectors of a lattice, which brings the constant down to $e^{s \log s + O(s)}$ (Section 4). The separation bound is proved by a lower bound that uses only digit $k+1$ and treats all deeper digits as worst case (Lemma 4); we call it the *one-digit relaxation*. It holds for every $k \geq 1$, including $k = 1$, i.e. $N = q^s$, which is the size at which the nets are practical. Whether the base threshold can be polynomial in s is open (Part II). Write $\delta N^{1/s} = 1 - K/q + O(q^{-2})$ and call K the *first-order deficit*. Smaller bases are certified for particular designs: for a given design the certified deficit is a finite maximum that an exact computation determines (Proposition 75), searched designs have the certified deficits 2, 5, 10 for $s = 4, 5, 6$, against $a_s^* = 5, 16, 43$ (Table 6), and at $k = 1$, where the matrix of digit $k+1$ need not come from a frame, searched integer matrices give, for instance, $\delta N^{1/5} \geq 0.8$ from $N = 13^5 \approx 3.7 \cdot 10^5$ points and $\delta N^{1/6} \geq 0.8$ from $N = 19^6 \approx 4.7 \cdot 10^7$ (Proposition 83, Table 7, computer-assisted).

Natural candidates. The base-2 $(0, m, 3)$ -net of Grünschloß and Keller [20, Sec. 2] was designed for large minimum distance at fixed m ; in our computation its normalized separation $\delta N^{1/3}$ falls, not monotonically, from 0.75 ($m = 3$) to 0.18 ($m = 13$) (Appendix G). The p -dimensional Faure sequence is not quasi-uniform [11, Thm. 4.3, Cor. 4.4], [18, Thm. 2(3)], and Goda, Hofer and Suzuki [18, Remark 3] extend this to the $(0, p)$ -sequences $(I, L_2 P, \dots, L_p P^{p-1})$ with nonsingular

lower-triangular L_i , along $N = p^m$, $m = (p-1)p^w$; for $p = 3$ these are three-dimensional. This does not conflict with our results: those nets are prefixes of one sequence whose first coordinate is unscrambled, whereas ours are Hammersley-type nets that depend on m (so they answer the question for nets, not for sequences) and scramble every coordinate.

Dimension three: every resolution. In dimension three the nets cover every N , not only $N = q^{3k}$:

- $m \equiv 0 \pmod{3}$, $m \geq 6$, every base $q \geq 4$: one integer lower-triangular scramble, the same for all three coordinates, of the frame of the places $\infty, 0, 1$ in its Möbius form (Section 3), with $\delta N^{1/3} \geq 1 - 1/q$ for $q \geq 8$ (Theorem 45);
- $m = 3$, every base $q \geq 5$ coprime to 6: column nets (points on lines parallel to $(1, 1, 1)$), whose minimum distance is known exactly, $\delta N^{1/3} = 1 - \frac{1}{3q} + O(q^{-2})$ or $1 - \frac{2}{3q} + O(q^{-2})$ according to $q \pmod{3}$, and $\delta N^{1/3} > 0.9059$ (Theorem 49);
- every $m \geq 3$ and every prime $p \geq 37$: $\delta N^{1/3} > 0.2715$, and > 0.4250 for $p \geq 83$, uniformly in m , with a bounded mesh ratio for each p (Corollary 57);
- every $m \geq 1$ in the bases 2 and 3: $\delta N^{1/3} \geq 0.4129$ resp. 0.3538 with an explicit digital shift, and ≥ 0.1718 resp. 0.0770 without a shift and under every digital shift (Theorem 64, computer-assisted);
- every prime $5 \leq p \leq 31$: every $m \geq 3$ except $m \in \{4, 7\}$, and except $m = 5$ for $p \leq 7$ (Theorems 49 and 45, and nets designed separately for each prime, Appendix C).

So in every prime base there are well-separated families of digital $(0, m, 3)$ -nets in the sense of [11, Def. 3.8] (no two points of $\mathcal{P}_m$ lie in a common shifted elementary box with $m/3 + O(1)$ digits in every coordinate), on all of $\mathbb{N}$ (Corollary 71, Remark 72). The prime-base families of Theorems A, 45, 33 and Corollary 57 stay well separated under every digital shift (Proposition 68, Corollaries 69 and 71), and so do the per-prime nets of Appendix C (Remark 132) and, in the bases two and three, the nets of Theorem 64 (part (3)). So in every prime base there are families that are well separated under every digital shift, on all of $\mathbb{N}$ (Remark 72).

When m is not a multiple of s , the boxes that hold one point each cannot all be cubes. We then give some coordinates, the *skeleton coordinates*, one cell digit fewer than the others. For such a coordinate the first digit after its cell digits, the *skeleton digit*, places the point in one of p thinner slices of its cell, so that every point lies in a cube of side p^{-k-1} , a *fine cell*. Inside each cube of side p^{-k} (a *coarse block*) the occupied fine cells form a lattice defined by congruences modulo p , for instance a Korobov lattice (Section 5). In every dimension this covers $m \equiv -1$ and $m \equiv -2 \pmod{s}$ for all large primes (Theorems 33 and 35).

One mechanism. All nets in this paper work the same way (Figure 1). We explain it for Theorem A, with $m = sk$, in the order in which it suggests itself: a frame, the trouble with its closest pair, and two fixes. Fixing the first k base- q digits of every coordinate selects a cube of side q^{-k} ; we call these N cubes the *cells*. In units of the cell side, cell $n = (n_1, \dots, n_s)$ is the unit cube $n + [0, 1)^s$, and n_c , the integer with the first k digits of coordinate c , is its *cell index* in coordinate c . A $(0, sk, s)$ -net has exactly one point in each cell. So the cells can serve as the index of the points, and the covering radius is at most the cell diameter $\sqrt{s} q^{-k}$. A net written in this way, as the graph of the map from the cell digits to the remaining (*offset*) digits, is a *graph form* (Section 2).

The frame and its closest pair. The Faure–Hammersley frame is a $(0, sk, s)$ -net for free: each of its box minors (the determinant that decides $t = 0$ for one shape of box, Section 2) is a product of differences $a_c - a_d$ of its places, hence ± 1 for the places $\infty, 0, 1$ and a unit modulo q whenever the prime factors of q are at least $s-1$ (Lemma 10). Its separation is another matter. Inside its cell a point is placed, up to $1/q$ of the cell side, by digit $k+1$ of each coordinate, the first offset digit; we call it the *geometric digit* r_c . In a digital net the vector $r = (r_1, \dots, r_s)$ is a

linear function, modulo q , of the cell digits. Suppose we move from a cell n to a neighbouring cell $n + e$, $e \in \{-1, 0, 1\}^s$, and only the last digit of each n_d changes, that is, no carry occurs. Then r changes by $\tilde{M}e \bmod q$ for one fixed integer $s \times s$ matrix $\tilde{M}$, the *geometric layer*; a step whose carry reaches further changes r by another matrix, which depends on how far the carry reaches. As long as no carry occurs and no coordinate of r leaves the range $0, \dots, q - 1$ (no *wrap*), the point of cell n therefore sits at $n + (r^{(0)} + \tilde{M}(n - n^{(0)}))/q$, up to the deeper digits, where $r^{(0)}$ is the geometric digit of a fixed cell $n^{(0)}$. On such a patch of cells the points lie on a translate of the lattice $(I + \tilde{M}/q)\mathbb{Z}^s$. So the closest pair is decided by $\tilde{M}$ and by the matrices of the steps with carries, and the frame does not control them: its geometric digit depends on the cell digits through coefficients that depend on k and on how far a carry reaches (Lemma 11), its geometric layer is, off the diagonal, a Cauchy matrix in the places up to row and column scalars (Proposition 12), and nothing in the frame keeps these residues modulo q small. The frame comes with no separation bound, and $t = 0$ does not supply one: the coding data of a $(0, m, s)$ -net do not determine its separation (Section 3), and families of $(0, m, s)$ -nets need not be quasi-uniform (the natural candidates above).

First fix: scrambles that keep $t = 0$. A lower-triangular scramble of a coordinate adds to each of its digits a combination of the earlier digits of the same coordinate. It maps every elementary box onto a box of the same shape, so every box still holds exactly one point. This is classical [43, 62, 14], and it holds as well for Owen's nested scrambles [47], which permute each digit depending on the earlier digits of its coordinate. In the frame these scrambles, like the gauge moves of Lemma 2, multiply every box minor by a unit (1), so $t = 0$ holds in the whole frame orbit (Section 3). They change the geometric digits, and that is all we use them for. The digits after the geometric digit are not designed: they are what the frame, after the scramble, supplies. We call this bounded, deterministic displacement the *jitter* (Figure 1(b)); it is not the random jitter of stochastic sampling in computer graphics [6]. The jitter does necessary work: a box that fixes more than $k + 1$ digits of some coordinate has a box minor that involves the deeper offset rows (Lemma 2), so the jitter is what keeps these thin boxes filled. And it is cheap: it moves each point by less than $1/q$ of a cell in each coordinate, which costs one unit of $1/q$ per coordinate in the separation bound (Lemma 4), the summand 1 of the first-order deficit K (Remark 5).

Second fix: move the lattice into each cell. Within this freedom we re-choose only the geometric digit. A design prescribes it on the last few levels of the cell indices, by small integer matrices: the geometric layer and the matrices of the steps whose carries reach these levels; the scramble removes its dependence on all more significant levels, for every k (Proposition 13). On each patch the points then lie on a translate of $(I + \tilde{M}/q)\mathbb{Z}^s$, and when the entries of $\tilde{M}$ are small compared with q , this lattice is a slightly rotated and contracted copy of $\mathbb{Z}^s$. Where some r_c wraps, the patch ends and the next patch starts about one cell further on. We call these boundaries *slip planes* (Figure 1(a)); they are what keeps one point in every cell. So the separation is at least the minimum of the local lattice minus a jitter cost of order $1/q$, and every separation proof in the paper is a version of this sentence (Lemma 4). This is the division of labour: the jitter can be borrowed from the frame, since whatever the frame supplies costs less than $1/q$ of a cell, whereas the lattice decides the separation and has to be moved into each cell, through the choice of its geometric digit.

The result. Theorem A carries this out in every dimension: its design U_s^* takes the entries of these matrices as short vectors of a lattice, small and independent of k (Section 4). In dimension three one scramble serves all three coordinates (Theorem 45). Faure–Hammersley frames also underlie the nets with one skeleton coordinate (Section 5) and, in dimension three, the nets for $m \equiv 0, 1, 2 \pmod{3}$, $m \geq 4$ (Section 6); frames with other places underlie the remaining

skeletons; and split frames (Section 13), which read each coordinate at two places, have unit box minors by the same confluent Vandermonde determinant (Lemma 111).

Other nets. Not every net here is a frame scramble. The column nets at $m = 3$ (Section 6.5), the nets $\mathcal{T}_p$ and $\mathcal{W}_p$ (Section 13), the nets $\mathcal{Q}_p^*$ (Proposition 118) and the nets at $k = 1$ whose geometric layer is chosen directly (Proposition 84) choose all their offset digits directly, and their $t = 0$ is proved by checking that their box minors are units (Lemmas 1 and 2). The nets in the bases two and three are built by a recursion $m \rightarrow m + 3$ (Section 7), in which copies of the old net play the role of the lattice and shifted lower digits are the jitter. The same pattern is visible already in dimension two (Remark 6, Figure 2): the points of the even- m permutation nets of Grünschloß and Keller [20, Sec. 3] lie on the lines of a lattice, and van der Corput slides along these lines are the jitter; since these nets are a nested scrambling of the Hammersley net, the frame of the places $\infty, 0$, the slides carry $t = 0$.

Separation constants. Part II asks how large the constant can be, that is, how small the first-order deficit K in $\delta N^{1/s} = 1 - K/q + O(q^{-2})$ can be. If the geometric layer $\tilde{M}$ is *bounded*, i.e. its entries are bounded independently of q , and has no zero on the diagonal, then K cannot be small: $K \geq 1$ in dimension three (Corollary 78), and $K \geq \sqrt{(s-3)/8}$ in general (Theorem 87). Geometric layers whose entries grow with q do better. The column nets at $m = 3$ (Section 6.5), whose points lie on lines parallel to the main diagonal, have $K = \frac{1}{3}$ and $\frac{2}{3}$, according to $q \bmod 3$, and these values are optimal among all column nets (Theorem 95). Part II explains them by a bookkeeping with two terms (Section 11). The first term, the *drift*, is forced by the torus: the column nets imitate the reflected cube $H\mathbb{Z}^3$ ($\mathbb{Z}^3$ reflected in the plane perpendicular to $(1, 1, 1)$), and when $3 \nmid q$, q steps of the reflected cube along an axis do not close up around the torus. The mismatch has to be spread over these q steps, and its share per step gives the deficits $\frac{1}{3}$ and $\frac{2}{3}$. The second term is the cost of the *jitter*, the displacement by the deeper digits. In dimension five the same bookkeeping gives digital $(0, 5, 5)$ -nets with $\delta N^{1/5} > 1$ for every prime $p \geq 37$ (Proposition 118). At the resolutions $m = sk$ the cells are cubes. By the theorems of Hajós and Keller, an idealized lattice with one point per cube cannot exceed the value 1 of $\mathbb{Z}^s$ (the *cubic value*) if the positions of its points inside their cubes vary independently (Proposition 100). Nets whose positions inside the cubes are coupled go beyond 1:

- At $m = 3$, a geometric layer of rank one makes all three coordinates wrap together. It gives $\delta N^{1/3} > 1$ for every prime $p \geq 17$ and $\delta N^{1/3} \rightarrow \sqrt{281/16} = 1.0476\dots$ (Proposition 104). The optimum of this family of layers is $\mu^* = \sqrt{(72 - 8\sqrt{31})/25} = 1.0480\dots$, reached as $p \rightarrow \infty$ (Proposition 106), and a union of two lattice cosets gives $\sqrt{66}/8$ (Proposition 103).
- A variant of the frame in which each coordinate reads its cell digits and its offset digits at two different places (a *split frame*) gives the packing D_s^+ locally, with $\delta N^{1/s} \rightarrow \min(\sqrt{s}/2, \sqrt{2})$ as $p \rightarrow \infty$ at every resolution $m = sk$; this is the E_8 value at $s = 8$ (Theorem 116).

Status and organization. Every result is proved in the text, by hand or, where stated, with an exact finite computation (*computer-assisted*). The theorems, propositions, lemmas and corollaries are also formalized in Lean 4, apart from some finite computations that are checked by scripts instead (Section 14). Part I (Existence) is organized by the resolutions it covers. Section 2 sets up graph forms, the one-digit relaxation and the lattice picture; Section 3 the frames, how one scramble works for every k , and why $t = 0$ comes for free. Section 4 proves Theorem A ($m \equiv 0 \pmod{s}$), Section 5 treats $m \not\equiv 0 \pmod{s}$ with lattice skeletons, Section 6 covers every resolution in dimension three, Section 7 the bases two and three, and Section 8 relates all this to the definitions of Dick, Goda and Suzuki, including digital shifts. Part II (Separation constants) treats the

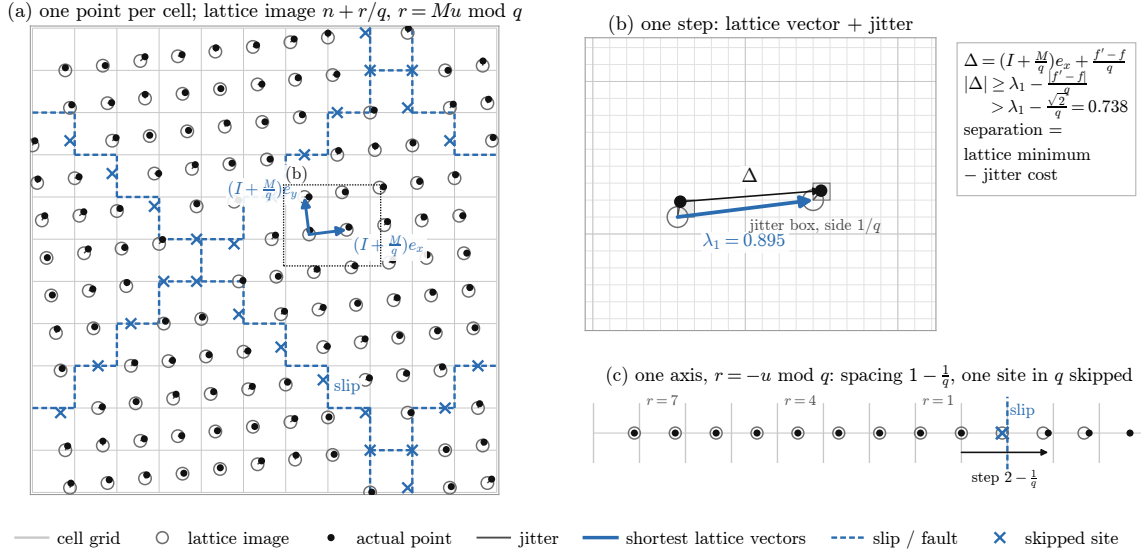


FIGURE 1. The mechanism of the nets of this paper, on a toy two-dimensional example ($q = 9$; schematic, not a net from the text). (a) A 11×11 window of cells (grey grid), one point per cell. The geometric digit $r = Mu \bmod q$ is linear in the last cell digits u , with $M = -I + R_{90^\circ}$ (the xy -block of the geometric layer of the three-dimensional nets, Proposition 43); it puts the point of cell n at the lattice image $n + r/q$ (open circles). On each patch this is a piece of $(I + \frac{M}{q})\mathbb{Z}^2$, which is $\mathbb{Z}^2$ rotated by $\arctan \frac{1}{q-1}$ and contracted, with shortest vectors $(I + \frac{M}{q})e_x, (I + \frac{M}{q})e_y$ (arrows). Where a coordinate of r wraps modulo q the patch ends at a slip (dashed), which keeps one point per cell. The deeper digits add a jitter f/q , $f \in [0, 1)^2$ (grey segments to the actual points, dots). Since $\det(I + \frac{M}{q}) = (1 - \frac{1}{q})^2 + \frac{1}{q^2} < 1$, the lattice image is about $2/q$ too dense: about every q cells one lattice site is skipped ($\times$) and the point jumps by about one cell at a slip; here 27 skipped sites against the density surplus $(\det^{-1} - 1) 11^2 = 29.7$, up to boundary effects. (b) The dotted box of (a): the jitter stays in a sub-cell of side $1/q$, so the separation is at least the lattice minimum $\lambda_1 = 0.895$ minus the jitter cost. (c) One axis, $r = -u \bmod q$ (the diagonal entry -1 of M): the points of cells $1, \dots, q$ sit on the sites $1 + i(1 - \frac{1}{q})$, $i \in \mathbb{Z}$; cell q receives a second site, which is skipped, and the next point steps $2 - \frac{1}{q}$ across the slip. Theorem 46 makes this exact ($1 - 1/q$ from the own-axis step); the other regimes (II and III, Section 2) change only the lattice and the cost. Interactive version: [explainers/anatomy.html](https://lgruen.github.io/separated-nets-lean/explainers/) (Section 1).

first-order deficit and lower bounds for it, why the column nets attain $\frac{1}{3}$ and $\frac{2}{3}$, why one point per cube caps idealized lattices at the cubic value 1, and constructions above 1. Section 15 lists open problems, and Section 16 discusses prior work. The appendices contain designs, deferred proofs, tables, pictures, the map of the formal verification and the list of reproducible computations. Interactive versions of several figures, which compute the nets in the browser from their generator matrices, are at <https://lgruen.github.io/separated-nets-lean/explainers/>.

s	resolution N	base	bound on $\delta N^{1/s}$	status	result
<i>Part I. Existence</i>					
s	$q^{sk}, k \geq 1$	$\text{lpf}(q) \geq s-1, q \geq 5a_s^* + 4$	$1 - a_s^*/q$	Lean	Thm. A
3	$q^{3k}, k \geq 2$	every $q \geq 4$	$1 - 1/q$ ($q \geq 8$)	Lean	Thm. 45
s	$p^{sk+s-1}, k \geq 0$	prime $p > 2^s$	$(\rho - 1)p^{-1/s} > \frac{1}{3}, \rightarrow 1$	Lean	Thm. 33
$s \geq 4$	$p^{sk+s-2}, k \geq 1$	prime $p \geq p_0(s)$	$(\rho - 4)p^{-1/2}; (B - F)p^{-2/s}$	Lean	Thm. 35
3	$p^{3k+1}, k \geq 1$	prime $p \geq 37$	$(\rho^2 - 4)p^{-2/3} \rightarrow 1$	Lean	Thm. 56
3	q^3	$\gcd(q, 6) = 1, q \geq 5$	exact; $> .9059, \rightarrow 1$	Lean	Thm. 49
3	p^m , every $m \geq 3$	prime $p \geq 37$	$> .2715; > .4250$ ($p \geq 83$)	Lean	Cor. 57
3	$p^{3k+r}, r \in \{1, 2\}$	primes $5 \leq p \leq 79^\ddagger$	.50–1.03 per prime	Lean	App. C
3	$2^m, 3^m$, every $m \geq 1$	$b = 2, 3$	.4129, .3538 (explicit shift) .1718, .0770 (every shift)	comp.-ass. Lean	Thm. 64
<i>Part II. Separation constants</i>					
4	$q^{4k}, k \geq 1$	odd $q \geq 17$	$1 - 2/q$, sharp for $k \geq 2$	Lean	Prop. 81
5, 6	q^s	Tab. 7	$\geq .8$ ($q \geq 13$ resp. 19)	comp.-ass.	Prop. 83
$s \geq 4$	$q^{sk}, k \geq 3$	bounded $\tilde{M}$	$< 1 - \sqrt{(s-3)/8}/q + O(q^{-2})$	Lean	Thm. 87
s	$p^{sk+s-1}, k \geq 0$	prime $p \geq s-1$	up to 1.238 ($s = 7$)	Lean	Prop. 102
3	q^3	$3 \nmid q$, column nets	$\leq 1 - \frac{1}{3q}$ resp. $1 - \frac{2}{3q}, +O(q^{-2})$	Lean	Thm. 95
3	p^3	prime $p \geq 41$	$\sqrt{\frac{33}{32} - \frac{41}{16p}} - \frac{\sqrt{3}}{p} \rightarrow \frac{\sqrt{66}}{8} = 1.0155$	Lean	Prop. 103
3	p^3	prime $p \geq 17$	$> 1, \rightarrow \frac{\sqrt{281}}{16} = 1.0476$	Lean	Prop. 104
3	p^3	rank-one family	$< \mu^* + \frac{\sqrt{3}}{p}; \mathcal{W}_p^* \rightarrow \mu^* = 1.0480$	Lean	Prop. 106
$s \geq 4$	$p^{sk}, k \geq 1$	prime $p \geq \max(2s, 2B_s + 2)$	$\rightarrow \min(\frac{\sqrt{s}}{2}, \sqrt{2})$	Lean	Thm. 116
5	p^5	prime $p \geq 37$	$> 1, \rightarrow \frac{\sqrt{5}}{2} = 1.118$	Lean	Prop. 118
5	$p^{5k}, k \geq 1$	prime $p \geq 1511$	$> 1.0265, \rightarrow \frac{\sqrt{5}}{2} = 1.118$	Lean	Prop. 122

TABLE 1. Overview of the separation results: Part I by the resolutions covered, Part II by the constant. Here q is an integer base, p a prime, b a prime base and $\text{lpf}(q)$ the least prime factor of q . All nets are explicit digital $(0, m, s)$ -nets (digitally shifted where stated) with one point in every cell (for $m = sk + r$, $0 < r < s$: every box with $k+1$ digits in r coordinates and k digits in the others), so their covering radius is $O(N^{-1/s})$ for a fixed base. The parameters ρ and $B = B(p)$ grow like powers of p (Definitions 34, 36 and 53), $F = 1 + \lceil (s-2)/2 \rceil$, and $\mathcal{W}_p^*$ is the net of the rank-one family whose parameter is tuned to the limit optimum μ^* (after Proposition 106). Status: *Lean*, the net property and the separation bound are also formalized in Lean (Section 14); *comp.-ass.* (computer-assisted), the bound rests on finite computations that are checked by scripts, not in Lean (the net property is formalized). All results are proved in the text. ‡ For $r = 2$ except $p = 67, 71, 73$ (where the nets $\mathcal{B}^2$ give .717–.738, Remark 55).

Part I. Existence

2. GRAPH FORMS AND THE ONE-DIGIT RELAXATION

Fix integers $q \geq 2$ and $m \geq 1$. The digits of a coordinate are indexed $0, \dots, m-1$, with digit 0 the most significant; so the first k digits are the digits $0, \dots, k-1$, and what the introduction calls digit $k+1$ is the digit with index k . The digits v_i of the index of a point are counted the other way, from the least significant, as the coefficients of t^i (Section 2.5). For $d \in \mathbb{Z}^m$ put $\phi_q(d) = \sum_{j < m} (d_j \bmod q) q^{-j-1}$. Integer matrices $C_1, \dots, C_s \in \mathbb{Z}^{m \times m}$ define the digital point set $\{(\phi_q(C_1 v), \dots, \phi_q(C_s v)) : v \in (\mathbb{Z}/q\mathbb{Z})^m\}$. For $d_1 + \dots + d_s = m$, the *box matrix* stacks the first d_i rows of each C_i , and its determinant is the corresponding *box minor*.

The same definitions apply over any finite commutative ring R with q elements, the digits being read through a fixed bijection $R \rightarrow \{0, \dots, q-1\}$.

Lemma 1 (Box criterion; Niederreiter [46, Thm. 6.1]). *For each d , every elementary box with d_i digits in coordinate i contains exactly one point if and only if the box minor for d is a unit of R . In particular the point set is a $(0, m, s)$ -net in base q if and only if every box minor is a unit of R , i.e., over a field, nonzero.*

Proof. The point with index v lies in a given box of shape d if and only if the box matrix maps v to the prescribed leading digits. So the boxes of shape d correspond bijectively to the values of the linear map $v \mapsto (\text{box matrix})v$ on R^m . There are q^m points and q^m boxes, so every box holds exactly one point if and only if this map is bijective, i.e. if and only if the box matrix is invertible, i.e. its determinant is a unit. This is [46, Thm. 6.1]. $\square$

In particular, integer matrices all of whose box minors are ± 1 give a $(0, m, s)$ -net in *every* base $q \geq 2$; conversely, for integer systems $t = 0$ over every $\mathbb{Z}/q$ is equivalent to $t = 0$ over every prime field [39, Lemmas 8–9], i.e. to all box minors being ± 1 . If L is lower-triangular, the first d rows of LC equal $L_{[d]}C_{[d]}$ ($L_{[d]}$ the leading $d \times d$ block), so

$$(1) \quad \det(\text{box of } (L_1C_1, \dots, L_sC_s)) = \prod_i \det L_{i,[d_i]} \cdot \det(\text{box of } (C_1, \dots, C_s)).$$

This is why linear [43] and generalized-Faure [62] scrambling preserve t . Throughout, a *scramble* is such a lower-triangular (linear) scramble of the digits of a coordinate. Owen's nested scrambles [47] form a much larger, nonlinear family: each digit of a coordinate is permuted by a permutation that may depend on the earlier digits of the same coordinate. They contain the lower-triangular scrambles and also preserve t , but they do not preserve digitality, and they are used here only in Remark 6.

2.1. Graph forms. Since a $(0, m, s)$ -net has exactly one point in each cell, the point is a function of its cell. A *graph form* writes the net as the graph of this function: the cell digits are the index, and the remaining digits are linear in them. Precisely, let $\mathbf{k} = (k_1, \dots, k_s)$ with $\sum_c K_c = m$ (the *depths*), let R be a commutative ring, and let $\Phi_{cd} \in R^{(m-k_c) \times k_d}$. The *graph form* Φ with depths $\mathbf{k}$ is the digital point set whose index is the vector of *cell indices* $n_c \in R^{k_c}$ and whose coordinate c has the digits n_c followed by its *offset* $\sum_d \Phi_{cd}n_d$; together the n_c select the *cell*, the box of all points whose coordinate c begins with the digits n_c . Its generator matrix C_c has the identity in the cell rows of column block c and $(\Phi_{c1} | \dots | \Phi_{cs})$ in the offset rows, so that the index digits are the cell digits (conventions in Section 2.5). Row r of Φ_{cd} belongs to digit $k_c + r$ of coordinate c , and column j to the *level* j of n_d , its digit with index j : level 0 is the most significant, and level $k_d - 1$ the last.

For $R = \mathbb{Z}/q\mathbb{Z}$ every cell of depths $\mathbf{k}$ holds exactly one point. The same holds for Φ with entries in $\mathbb{Z}$ or in $\mathbb{Z}[1/D]$, $\gcd(q, D) = 1$, reduced modulo q ; an integer Φ thus defines a point set over every $\mathbb{Z}/q\mathbb{Z}$. Conversely, if the box matrix of a digital point set for the depths $\mathbf{k}$ is invertible (for instance by $t = 0$, Lemma 1), the cells are coordinates on R^m , and in these coordinates the point set is a graph form: the same point set, re-indexed.

For $d = (d_1, \dots, d_s)$ with $\sum_c d_c = m$ call c *over* if $d_c > k_c$ and *under* if $d_c < k_c$: the box of shape d fixes more, resp. fewer, digits of c than the cell does.

Lemma 2 (Box condition and gauge moves). *The box minor of a graph form for d equals, up to sign, the determinant of the square matrix formed by the top $d_c - k_c$ offset rows of the over coordinates c , restricted to the last $k_e - d_e$ levels of the under coordinates e (it is 1 if $d = \mathbf{k}$). In particular the diagonal blocks Φ_{cc} never enter. Consequently the following gauge moves multiply every box minor by a unit of R , and so, by Lemma 1, map $(0, m, s)$ -nets over $\mathbb{Z}/q\mathbb{Z}$ or $\mathbb{F}_q$ to $(0, m, s)$ -nets: (a) replacing the diagonal blocks arbitrarily; (b) for $s = 3$ only:*

$\Phi_{cd} \mapsto \mu_{cd}\Phi_{cd}$ ($c \neq d$) with units μ_{cd} of R (block scalings); (c) $\Phi_{cd} \mapsto L_c\Phi_{cd}U_d$ ($c \neq d$) with L_c, U_d lower-triangular whose diagonal entries are units of R .

Proof. The first $\min(d_c, k_c)$ rows of C_c are unit rows selecting the first $\min(d_c, k_c)$ levels of n_c . Laplace expansion along all these unit rows removes the selected columns; what remains are the top $d_c - k_c$ offset rows of the over coordinates, on the unselected columns, which are the levels $\geq d_e$ of the under coordinates. A coordinate is not both over and under, so no diagonal block occurs. (c) Left multiplication by L_c preserves the span of the top rows of $\Phi_{c\cdot}$, and right multiplication by U_d the span of the last columns of $\Phi_{\cdot d}$; the determinant changes by the product of the corresponding diagonal entries. (b) For $d \neq \mathbf{k}$ both over and under coordinates exist; for $s = 3$ there is therefore a single over or a single under coordinate, so the matrix is $[\Phi_{cd} | \Phi_{cd'}]$ or $[\Phi_{cd}; \Phi_{c'd}]$ restricted in this way, and scaling one block multiplies its determinant by a power of μ_{cd} . For $s \geq 4$ a box can have two over and two under coordinates, for instance $(k+1, k+1, k-1, k-1)$, and single-block scalings are no longer gauge moves. $\square$

For instance, for the depths $(k, \dots, k)$ and $d = (k+1, k-1, k, \dots, k)$ the box minor is the single entry of Φ_{12} in the first offset row and on the last level of n_2 . We call the moves (a)–(c) *gauge moves* because they change the generator matrices but not the net property: they multiply every box minor by a unit, so they never change t .

Definition 3 (Geometric digit and geometric layer). Let a graph form have the depths $(k, \dots, k)$. The first offset digit of a coordinate c (its digit with index k) is its *geometric digit* r_c . The *geometric layer* is the integer matrix $\tilde{M}$ of the centred representatives $\tilde{M}_{cd} \in (-q/2, q/2]$ of the level- $(k-1)$ entries $(\Phi_{cd})_{0, k-1}$ of the first offset rows, diagonal included.

So $\tilde{M}_{cd}$ is the change, modulo q , of the geometric digit of coordinate c when the last digit of n_d increases by one without a carry. The geometric digits locate a point inside its cell up to $1/q$ of the cell side. A geometric layer is *bounded*, along a family of nets, if its entries are bounded independently of q .

2.2. Designs. Let the depths be $(k, \dots, k)$. A design prescribes how the geometric digits depend on the last L levels of the cell indices; the more significant levels are to have no influence on them. Since a design is read from the last level upwards, we say that level $k-1-n$ lies at *carry depth* n : the last level is at carry depth 0, and a step by ± 1 along an axis changes the level at carry depth $n \geq 1$ only if its carry (or borrow) reaches it. A *design* with L levels is a tuple $(F_0, \dots, F_{L-1})$ of $s \times s$ matrices (integer, except in Section 13); a graph form *realizes* it if row 0 of every block Φ_{cd} , the diagonal included, equals $F_n[c][d]$ at carry depth n (the level $k-1-n$) for $n < L$ and vanishes on the levels $0, \dots, k-1-L$. So F_0 is the geometric layer. We write $M^{(j)} = F_0 + \dots + F_j$ for the partial sums: a step by ± 1 along axis d whose carry has depth j , i.e. changes the levels at carry depths $0, \dots, j$ of n_d (the levels $k-1, \dots, k-1-j$), changes the geometric digit of coordinate c by $\pm M^{(j)}[c][d]$ modulo q . Which designs a frame can reach, for every k , is the subject of Section 3.

2.3. The one-digit relaxation. Two points in neighbouring cells n and $n+e$ differ in coordinate i by e_i cells plus the change of $(r_i + f_i)/q$, where r_i is the geometric digit and f_i the contribution of the deeper digits. The next lemma bounds each coordinate of this difference from below, using only the change σ of the geometric digits and the worst case for the deeper digits. It relaxes the exact distance by replacing the deeper digits with their worst case; hence its name, the *one-digit relaxation*.

Lemma 4 (One-digit relaxation). *Let $q \geq 3$, $k \geq 1$, and let a digital net over $\mathbb{Z}/q\mathbb{Z}$ be given in graph form with depths $(k, \dots, k)$ such that (H1) row 0 of every block Φ'_{cd} , diagonal included,*

equals a design $(F_0, \dots, F_{L-1})$, $1 \leq L \leq k$, on the levels $k-1, \dots, k-L$ and vanishes on the levels $0, \dots, k-1-L$; (H2) the rows ≥ 1 of the diagonal blocks vanish. In cell units write coordinate i of a point as $n_i + (r_i + f_i)/q$ with r_i its first offset digit and $f_i \in [0, 1)$. For a step $e \in \{-1, 0, 1\}^s \setminus \{0\}$ to a toroidally adjacent cell and carry depths j_d on the moving axes (j_d is the number of further levels that change, by a carry if $e_d = 1$ and by a borrow if $e_d = -1$), put

$$\sigma_i = \sum_d e_d M^{(\min(j_d, L-1))}[i][d], \quad \bar{\sigma}_i = \sigma_i \bmod q \in [0, q), \quad \text{jit}_i = \begin{cases} 0 & e = \pm e_i, \\ 1 & \text{otherwise,} \end{cases}$$

and $b_i = \min_t \max(0, |e_i q + t| - \text{jit}_i)$, the minimum over $t \in \{\bar{\sigma}_i, \bar{\sigma}_i - q\}$ if $\bar{\sigma}_i \neq 0$ and over $t = 0$ if $\bar{\sigma}_i = 0$. Then the two points in cells n and $n + e$ satisfy $q|\Delta_i| \geq b_i$ for every i , where Δ_i is coordinate i of the point in cell $n + e$ minus that of the point in cell n , in cell units ($n + e$ taken as the toroidal neighbour), and the toroidal minimum distance satisfies

$$\delta q^k \geq \text{LB} := \min\left(1, \min_{e,j} (\sum_i b_i^2)^{1/2}/q\right).$$

Proof. A carry of depth j on axis d changes the levels $k-1, \dots, k-1-j$ of n_d by e_d modulo q ; the torus wrap has $j = k-1$ (at $k=1$ every step has $j=0$). By (H1), r_i changes by σ_i modulo q , and capping the carry depth at $L-1$ is exact because row 0 vanishes on the levels $0, \dots, k-1-L$. Since $r'_i - r_i \in (-q, q)$ and $r'_i - r_i \equiv \sigma_i$, we have $r'_i - r_i \in \{\bar{\sigma}_i, \bar{\sigma}_i - q\}$, and $r'_i - r_i = 0$ if $\bar{\sigma}_i = 0$. Always $|f'_i - f_i| < 1$, and $f'_i = f_i$ if only axis i moves: by (H2) the deeper digits of i do not depend on n_i . So $q\Delta_i = e_i q + (r'_i - r_i) + (f'_i - f_i)$ gives $q|\Delta_i| \geq b_i$.

It remains to compare with the toroidal distance; this is the only place where the size of q^k enters. In cell units the torus has period $G = q^k \geq 3$. Let $n \neq n'$ be two cells, let $E \in \mathbb{Z}^s$ be the representative of $n' - n$ modulo G with $|E_c| \leq G/2$, and let $\theta_c \in (-1, 1)$ be coordinate c of $(r' - r + f' - f)/q$. The toroidal distance in coordinate c is $\text{tor}_c = \min_{z \in \mathbb{Z}} |E_c + zG + \theta_c|$. If some $|E_c| \geq 2$, then $|E_c + zG| \geq |E_c|$ for every z , so $\text{tor}_c \geq |E_c| - |\theta_c| > 1$. Otherwise $E = e \in \{-1, 0, 1\}^s \setminus \{0\}$ and $\Delta = e + \theta$ with $|\Delta_c| < 2$; if $|\Delta_c| \leq G/2$, then $\text{tor}_c = |\Delta_c| \geq b_c/q$, and otherwise $\text{tor}_c \geq G - |\Delta_c| > G - 2 \geq 1$. So either some coordinate has toroidal distance at least one cell, or the distance is at least $(\sum_i b_i^2)^{1/2}/q$ cells; as a cell has side q^{-k} , this is the claim. $\square$

Like Theorem 46, Lemma 4 uses only that the cells determine the point and the shape of the first offset rows, not $t = 0$. The lemma is formally verified for every $k \geq 1$. We call a step e together with carry depths $j = (j_d)$ on its moving axes a *configuration* (e, j) . At $k = 1$ there are no carries, and the configurations are those with all $j_d = 0$, a subset of the configurations for $k \geq 2$; so for a given design the value of LB at $k = 1$ is at least its value with more levels, and every lower bound proved below through Lemma 4 for $k \geq 2$ holds at $k = 1$ as well.

Remark 5 (First-order expansion). Call a moving coordinate *backward* if $e_i \sigma_i \leq 0$ and *forward* otherwise. For a fixed design and $q \rightarrow \infty$: if some configuration with at least two moving axes has no backward coordinate, or some diagonal partial sum $M^{(j)}[a][a]$ is positive, then $\text{LB} = O(1/q)$; otherwise $\text{LB} = 1 - K/q + O(q^{-2})$ with K the maximum of $|M^{(j)}[a][a]|$ and of $|\sigma_b| + 1$ over the configurations with at least two moving axes and a single backward coordinate b . (Two backward coordinates cost nothing at first order, and the jitter costs the +1.) In dimension three, $M = -I + S$ with S skew with entries ± 1 gives $K = 1$.

2.4. The lattice picture. The mechanism of the introduction underlies every net in this paper. Write the point of a graph form with depths $(k, \dots, k)$ in cell units as $n + (r + f)/q$, with n its cell, r its geometric digits and $f \in [0, 1)^s$ the contribution of the deeper digits (the *jitter*); we call $n + r/q$ its *lattice image*. For a step $n \rightarrow n + e$ that changes only the last cell digits, the geometric

digits change by $\tilde{M}e$ modulo q . So on a patch of cells where no geometric digit wraps, the lattice images form a piece of a translate of the lattice $(I + \tilde{M}/q)\mathbb{Z}^s$, and the points differ from them by f/q . Where a geometric digit wraps, the patch ends at a *slip plane*, and every cell keeps exactly one point. This picture is behind every separation proof here: the separation is the minimum of the lattice, or union of lattice cosets, that the geometric digit realizes locally, minus a jitter cost of less than $1/q$ of a cell per coordinate and, at unequal depths, a bounded cost from shifts of the lattice between neighbouring blocks of cells (*faults*, Section 5). Lemma 4 makes this exact for $m = sk$, and Lemma 25 for $m = sk + r$. Three regimes occur (Figure 1): (I) bounded centred entries give a slightly rotated and contracted copy of $\mathbb{Z}^s$, of minimum $1 - O(1/q)$ (Sections 4 and 6); (II) when $m \not\equiv 0 \pmod{s}$, some coordinates have one cell digit fewer, their first offset digit selects a thinner box (a *fine cell*, Section 5.1), and the occupied fine cells form lattices of index p^ℓ , with minimum at the scale of $p^{\ell/s}$ fine cells (Section 5); and (III) entries of size $\Theta(q)$, $\tilde{M} \approx qA$ with a rational A , put the point of cell n near $n + \{An\}$, a lattice or packing other than $\mathbb{Z}^s$ (the column nets of Section 6.5, and Section 13 in Part II).

Remark 6 (A two-dimensional example). The permutation $(0, m, 2)$ -nets of Grünschloß and Keller [20, Sec. 3] for even m show this mechanism in the smallest case, base 2 and dimension two (Figure 2). For even $m = 2r \geq 4$, $Q = 2^r$, $N = Q^2$ and $0 \leq i, j < Q$ they are the points $(X, Y)/N$ with $X = (Q\varrho(i) + \lfloor i/4 \rfloor + \frac{Q}{4}(j+1)) \bmod N$, $Y = i + Qj$, where ϱ reverses r bits; distances are taken modulo the lattice $\langle (N, 0), (N/4, N) \rangle$ of the row-shifted tiling for which they were designed [20, 53] (the tiling metric). (i) *Cells and geometric digit*. Since $\lfloor i/4 \rfloor < Q/4$, the binary digits of X are the fields $[c_x; (j+1) \bmod 4; \lfloor i/4 \rfloor]$ with $c_x = \varrho(i) + \lfloor (j+1)/4 \rfloor \bmod Q$, and those of Y are $[j; i]$. So the cells of depths (r, r) hold one point each, and the first two offset digits of X , one base-4 geometric digit, are $(j+1) \bmod 4$, a function of the last two cell digits of Y . The occupied cells of depths $(r+2, r)$ are exactly the coset $\{(a, b) : a \equiv b+1 \pmod{4}\}$ of an index-4 lattice. (ii) *Lattice and jitter*. With $e = (Q, 0)$, $v = (Q/4, Q)$ and $u = \varrho(i)$,

$$(X, Y) \equiv ue + \left(j + \frac{\varrho(u)}{Q}\right)v + \left(\frac{Q}{4} + \left\lfloor \frac{i}{4} \right\rfloor - \frac{i}{4}, 0\right) \pmod{N} :$$

the points lie on the lines of the lattice $\Lambda = \mathbb{Z}e + \mathbb{Z}v$ in direction v , exactly v apart along each line, and line u is slid along itself by $\varrho(u)/Q$ of one step (the *slide* of line u , a van der Corput value), up to less than one grid unit. The slides are the jitter. The tiling lattice is $Q\Lambda$, so the lines close up and there are no slips. (iii) *Separation*. The functional $X - Y/4$ separates distinct lines by at least $Q - \frac{3}{4}$, so $\delta\sqrt{N} \geq (4/\sqrt{17})(1 - 1/Q)$ for every choice of the slides; the van der Corput slides give exactly $\delta^2 N = 241/256$ in the tiling metric for every even $m \geq 8$ [53]. On these lines the slides that keep $t = 0$ are exactly the nested scramblings of the van der Corput slides, and all of them are equally far from lattice slides (both computed for $m \leq 8$), so only their arrangement is free. Flipping the third binary digit of the slide on the lines $u \equiv 2, 3 \pmod{4}$ is again a nested scrambling, so it gives a $(0, m, 2)$ -net, by (iv) and [47]. In the tiling metric it is worse at $m = 8$ ($\delta^2 N = 229/256$ against $241/256$), and for every even m with $10 \leq m \leq 20$ it has $\delta^2 N = 977/1024$ against $241/256 = 964/1024$, i.e. $\delta\sqrt{N} = 0.9767\dots$ against $0.9702\dots$ (computed). The jitter is not reduced, only moved off the direction across the lines, as in Section 11. (iv) *The net property*. The slides carry $t = 0$: the net is a nested (Owen) scrambling of the Hammersley net, the frame of the two places $\infty, 0$, and nested scramblings of a (t, m, s) -net are (t, m, s) -nets [47]; this gives a short proof of the net property proved in [53]. The net is not digital (it does not contain the origin [20, 53]), its scramblings are not linear, and its metric (the row-shifted torus) is adapted to its lattice of lines. The nets of this paper are digital: they use linear scrambles of frames with more places, keep the standard torus, and pay with a slip plane wherever a geometric digit wraps around modulo q ; a nonlinear permutation

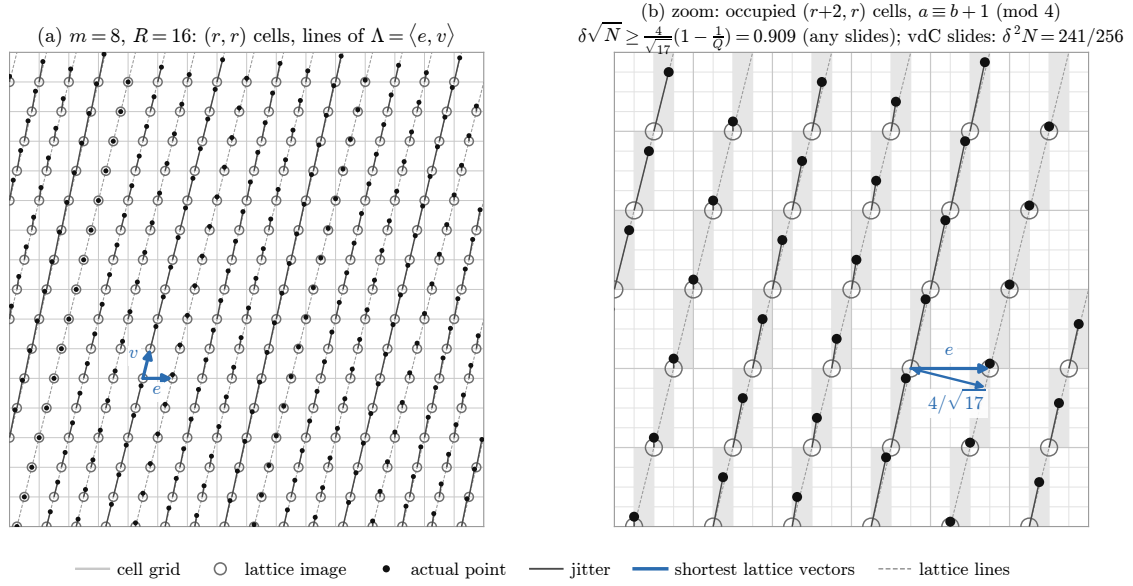


FIGURE 2. The mechanism in its simplest instance: the permutation $(0, m, 2)$ -net of Grünscloß and Keller [20, Sec. 3] for $m = 2r = 8$, $Q = 2^r = 16$, $N = Q^2 = 256$, in cell units (Remark 6). (a) The (r, r) cells (grey grid), one point each. Open circles: the lattice image $ue + jv + (\frac{1}{4}, 0)$, $e = (1, 0)$, $v = (\frac{1}{4}, 1)$, on the lines (dashed) of $\Lambda = \langle e, v \rangle$ in direction v ; the tiling lattice of the row-shifted torus is $Q\Lambda$, so the lines close up and there are no slips. Dots: the points $(X, Y) = ue + (j + \varrho(u)/Q)v + (d, 0)$, $|d| < 1$ grid unit: line u is slid along itself by its slide $\varrho(u)/Q$ of one step, a van der Corput value (grey segments, the jitter). Accent: the basis e (shortest, length 1) and v . (b) Zoom on 6×6 cells with the cells of depths $(r + 2, r)$ (light grid); the occupied ones (shaded) are exactly the coset $\{(a, b) : a \equiv b + 1 \pmod{4}\}$ of the index-4 lattice Λ . Since the slides move the points arbitrarily along the lines, only the line spacing $4/\sqrt{17}$ (double arrow) survives as a separation bound: $\delta\sqrt{N} \geq \frac{4}{\sqrt{17}}(1 - \frac{1}{Q}) = 0.909$ for every choice of slides; the van der Corput slides give exactly $\delta^2 N = 241/256$ (in the tiling metric; [53]).

can traverse a sub-cell (a box of side $1/q$ of a cell) without such a jump, and linear offsets cannot (Section 12).

2.5. Notation. Table 2 collects the notation used throughout. Symbols that are not in the table are defined where they are first used; a letter defined inside one statement, proof or remark is local to it and may have another meaning elsewhere. *Index conventions.* The index $i \in \{0, \dots, q^m - 1\}$ of a point has base- q digits $v_0, \dots, v_{m-1}$, v_0 *least* significant, and v is the coefficient vector of $V(t) = \sum_l v_l t^l$; coordinate c has the digits $d = C_c v \bmod q$, d_0 *most* significant, and the integer coordinate $\sum_j d_j q^{m-1-j} \in [0, q^m)$. Row j of a generator matrix belongs to output digit j , column l to t^l ; column l of Ψ is the coefficient vector of $(1-t)^{m-1-l}$. A graph form is indexed by its cells, $v = (n_{1,0}, \dots, n_{1,k_1-1}, n_{2,0}, \dots)$ with $n_{c,j}$ the level- j digit of n_c ; for any digital net the graph-form matrices are $C_c B_{\mathbf{k}}^{-1}$, $B_{\mathbf{k}}$ the box matrix of the depths $\mathbf{k}$ (the same point set, re-indexed by $v \mapsto B_{\mathbf{k}} v$). Decimals are truncated (not rounded) to the digits shown: certified lower bounds,

exact values and computed values alike; only upper bounds are rounded up, so that they stay upper bounds.

Digital shifts. Dick, Goda and Suzuki also consider digitally shifted nets, the digital analogue of the random shifts of Cranley and Patterson [8], and so do we (Sections 7 and 8).

Definition 7 (Digital shift [11, Def. 2.2]). For a point set given by digit vectors $x_c \in (\mathbb{Z}/q\mathbb{Z})^m$ and $\tau = (\tau_1, \dots, \tau_s) \in (\mathbb{Z}/q\mathbb{Z})^{s \times m}$, the *digitally shifted* point set $P \oplus \tau$ has the digit vectors $x_c + \tau_c$, added digit by digit modulo q without carries. For prime q this is [11, Def. 2.2]. A *digital net* is unshifted ($\tau = 0$) unless stated otherwise.

A digital shift maps every elementary box of shape d bijectively onto one of the same shape, so it preserves the $(0, m, s)$ -property; in graph form it only adds a constant to the offsets (Lemma 67).

3. FRAMES: $t = 0$ FOR FREE

A *frame* is a digital point set whose coordinate c reads the base- q Taylor coefficients (the *jets*) of one polynomial V at a point a_c of the projective line, its *place*; these are the points β_i of Niederreiter's construction [46, Sec. 6]. For the places $\infty, 0$ the frame is the Hammersley net [24]. For the places $\infty, 0, 1, \dots, s-2$ it is the Hammersley net of the $(s-1)$ -dimensional Faure sequence [16], whose generator matrices, the powers of the Pascal matrix, read the jets at $0, 1, \dots, s-2$; we call it the *Faure–Hammersley frame*. A frame gives one point per cell and $t = 0$ for free (Lemma 8), and $t = 0$ survives every scramble and gauge move. The nets obtained from a frame by lower-triangular scrambles and the gauge moves of Lemma 2 form its *frame orbit*. In the order of the introduction: the frame supplies $t = 0$ and the deeper digits (the jitter), and the moves are used to re-choose the geometric digit, which decides the separation (Section 2). What these moves cannot change is the shape of the geometric layer: it is a Cauchy matrix in the places, up to row and column scalars and a free diagonal (Proposition 12), and its Plücker relations (Lemma 18) are the obstructions specific to frames; the obstructions that hold for every digital net, or for every net, are those of Section 12.

For a commutative ring R and $V \in R[t]_{<m}$, the α -jet of V at $x \in R$ is $([(t-x)^j]V)_{j < \alpha}$, and the α -jet at ∞ is $([t^{m-1-j}]V)_{j < \alpha}$.

Lemma 8 (Hermite interpolation). *Let $x_1, \dots, x_n \in R$ and $\alpha_1, \dots, \alpha_n, \alpha_\infty \geq 0$ with $\sum_P \alpha_P + \alpha_\infty = m$, and let H be the matrix of the map that sends $V \in R[t]_{<m}$ to its α_P -jets at the x_P and its α_∞ -jet at ∞ . Then $\det H = \pm \prod_{P < Q} (x_Q - x_P)^{\alpha_P \alpha_Q}$. In particular, over a field, H is invertible if the x_P with $\alpha_P \geq 1$ are pairwise distinct, and H has two equal rows if two of them coincide.*

Proof. The value is the confluent Vandermonde determinant [46, Sec. 6]. The consequences used below also follow by counting zeros: if over a field the points are distinct and all jets of V vanish, the product $\prod_P (t - x_P)^{\alpha_P}$ of pairwise coprime factors, of degree $m - \alpha_\infty$, divides V , while $\deg V < m - \alpha_\infty$ because the jet at ∞ vanishes; so $V = 0$. If $x_P = x_Q$ and $\alpha_P, \alpha_Q \geq 1$, the rows $V(x_P)$ and $V(x_Q)$ coincide. Over a field this zero count is Skrikanov's proof that the hyperderivative (Rosenbloom–Tsfasman Reed–Solomon) codes [52] are MDS in that metric [56, Prop. 5.1, Thms. 5.1, 5.2]. $\square$

In coding language this is the complementary, classical half of the picture: q^m points form a $(0, m, s)$ -net if and only if their digit array is an MDS code in the Rosenbloom–Tsfasman metric [52], [56, Thm. 2.1]; the frames below are the Reed–Solomon codes of this metric, and the moves (a), (c) of Lemma 2 are isometries of it [56, Rem. 2.2]; the isometries of this metric that act on each coordinate separately are exactly the nested scrambles of the coordinates [50], which

s, q, p	dimension; base (any integer $q \geq 2$, the ring $\mathbb{Z}/q\mathbb{Z}$); a prime base; $b \in \{2, 3\}$ in Section 7
$m, N, k, \mathbf{k}$	number of digits, $N = q^m$ points; number of cell levels ($m = sk$, or $m = sk + r$); depths $\mathbf{k} = (k_1, \dots, k_s)$ of a graph form
n_c, r_c, f_c	cell index of coordinate c (levels $0, \dots, k - 1$, most significant first); geometric digit; jitter $\in [0, 1)$
ϖ, P_c, a	in Section 5: fine unit $\varpi = p^{m-k-1}$; fine cell of coordinate c ; centred fine difference (Section 5.1)
$\Phi_{cd}, \tilde{M}$	blocks of a graph form; geometric layer (Definition 3)
$F_n, M^{(j)}$	design (target at carry depth n , i.e. level $k - 1 - n$); its partial sums
e, j_d, σ, b_i	cell step; carry depths; change of the geometric digits; per-coordinate bounds of the relaxation
ω	wraps of a step: $\omega_c = 1$ if the digit in question of coordinate c wraps around modulo q on the step, else 0 (geometric digits in Lemma 98; last cell digits in the proof of Theorem 46; third digits in Lemma 93)
E, Δ	difference of two cells, or a step; difference of two points in cell units
$K, K(F), K_{\text{pair}}$	first-order deficit of a family of nets, $c = 1 - K/q + O(q^{-2})$; certified deficit of a design (Definition 74); lower bound from two-axis steps (Definition 86)
$\sigma_{\max}(F), q_{\text{tail}}$	largest digit change of a design; base from which Proposition 75 certifies $1 - K(F)/q$
Σn	coordinate sum $\sum_c n_c$ of a cell or a step
c	normalized separation $c = \delta N^{1/s}$; also a coordinate index (in Proposition 77 the coordinates are a, b, b')
$\mathcal{K}$	lower-triangular Toeplitz matrix of $(1 - t)^{-k}$ (used in Definition 41)
Ψ, T	Möbius map of the frame of the places $0, 1, \infty$, and $T = s_k \Psi$, $s_k = (-1)^{k+1}$, with $T^3 = 1$ (Section 3)
$\mathcal{P}_{k,q}, \mathcal{B}^1, \mathcal{B}^2$	the nets of Theorem 45 (Definition 41); the nets for $m \equiv 1, 2$ in dimension three (Definition 53)
δ, h	toroidal minimum distance (at most the Euclidean one, so lower bounds carry over); covering radius
$a_c; u_c, v_c$	places of a frame (numeric indices $a_1, a_2, \dots$ in Section 5); offset and cell points of a split frame (in Section 6.3: the last two cell digits)
α_c, a_s^*	diagonal magnitudes of a dominant design (Proposition 19; in Lemma 18 $[\alpha_c : \beta_c]$ are homogeneous coordinates of the places); $a_s^* = \max_c \alpha_c$ for U_s^* (Definition 23)
$\Lambda_j, \text{lc}_j, \gamma_j, \eta_j$	lattice of admissible design columns at carry depth j ; leading coefficient; generator of its values; projection length (Section 4.2)
λ_c, μ_d, D_{cd}	row and column scalars and place differences of a Cauchy layer $\lambda_c \mu_d / D_{cd}$
ℓ, ρ, Λ_A	number of skeleton coordinates; Korobov or congruence parameter; skeleton lattice
$S_z, \kappa, \Lambda_\kappa$	skeleton digit; its coefficients on the full coordinates; the skeleton lattice for $\ell = 1$
$\lambda_\infty, \lambda_2, \lambda_{\text{jit}}$	lattice minimum in the maximum norm; in the Euclidean norm; Euclidean minimum after one fine cell of jitter per coordinate (Proposition 102)
H, D_s^+, γ_s	reflection in $\mathbf{1}^\perp$ (reflected cube $H\mathbb{Z}^3$); the packing D_s^+ ; Hermite constant
$\mathbb{T}, \varphi, \mathcal{C}_q$	columns $(\mathbb{Z}/q\mathbb{Z})^3 / \langle \mathbf{1} \rangle$; heights of a column point set; column net (Section 6.5)
$a, b, w, \xi, \varepsilon_i, \eta$	shared row $a = \frac{1}{3}(q\mathbf{1} + w)$ of a column net and its third-digit row b (Definition 47); w gives its drift $\frac{1}{3}qw_i$ per step; excess of a step; excess of a step along $\mathbf{e}_i$ without a wrap; largest excess (Section 11)
$b = \beta/p$	glue of a step: change of the phase (in-cell position) in cell units, modulo 1 (Lemma 98)
dr, dj	drift and drift plus jitter of a half-integer layer at $s = 5$ (Section 13.7)
Y, ψ	phase group of a lattice (Section 12); phase subtorus of a layer at $m = 3$, and a point ψ of it (Section 13.3)
$\mathcal{T}_p, \mathcal{W}_p, \zeta, \varepsilon$	two-coset and rank-one nets; the digit read by z in $\mathcal{W}_p$; $\varepsilon = \rho/(2p)$ with $\rho = 2\lfloor p/48 \rfloor + 1$ (Sections 13.2, 13.3)
B_s, τ	constant of Theorem 116; a digital shift (Definition 7)

TABLE 2. Notation.

preserve t [47] but not the separation. All MDS codes of this metric with the same parameters have the same weight distribution [56, Thms. 3.1, 3.2], so the coding data do not determine the separation: $t = 0$ comes for free, and the separation is decided by the geometric digit, whose values form a single code (Remark 32 describes this code for the skeletons of Section 5).

The box matrices of a frame are Hermite matrices, so every box minor is a product of differences of places, and $t = 0$ holds as soon as the places are distinct modulo every prime factor of the base. We use three frames: the Möbius frame (the frame of the places $0, 1, \infty$, written with a Möbius map of order three that permutes them cyclically; Theorem 42, and, after a re-indexing, Proposition 9), the frame of s places (Lemma 10) and the split frame, which reads the cell digits of a coordinate at one place and its offset digits at another (Section 13, Lemma 111). Lower-triangular scrambles of the digits (1) and the gauge moves of Lemma 2 multiply every box minor by a unit, so $t = 0$ holds in the whole frame orbit.

3.1. The Möbius frame. Here $s = 3$ and $m = 3k$ (Section 6.6 uses the frame with $m = 3k + r$). Write $[W]_m \in \mathbb{Z}^m$ for the vector of the first m coefficients ($[t^0]W, \dots, [t^{m-1}]W$) of a power series $W \in \mathbb{Z}[[t]]$, and identify $V \in \mathbb{Z}[t]_{<m}$ with $[V]_m$.

Let Ψ act on $\mathbb{Z}[t]_{<m}$ by $(\Psi V)(t) = (1 - t)^{m-1}V(1/(1 - t))$, and put $T = s_k \Psi$ with $s_k = (-1)^{k+1}$. A direct computation gives $(\Psi^2 V)(t) = (-t)^{m-1}V((t - 1)/t)$ and $\Psi^3 = (-1)^{m-1}$, hence $T^3 = s_k^3(-1)^{3k-1} = 1$. On binary forms, Ψ is the $(m - 1)$ -st symmetric power of $g = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$, which satisfies $g^3 = -I$ and cycles $0 \rightarrow 1 \rightarrow \infty$: it is the 3-cycle of the anharmonic group $S_3 \subset PGL_2(\mathbb{Z})$ stabilizing $\{0, 1, \infty\}$.

The *frame* is the triple of readings (the digit sequences that the three coordinates read off V) $([T^2 V]_m, [V]_m, [TV]_m)$, that is, the generator matrices (T^2, I, T) . Replacing V by TV shifts the three coordinates of the point cyclically.

Proposition 9 (The frame is the Faure–Hammersley net). *Let $P_{ji} = \binom{i}{j}$ be the upper Pascal matrix, J the reversal, $D_{\pm} = \text{diag}((-1)^i)$, and $(\Lambda_m)_{ij} = (-1)^{i-j} \binom{m-1-j}{i-j}$ (lower-unitriangular). Then $\Psi = \Lambda_m P$ and $\Psi^2 = D_{\pm} J P$. Consequently, for each m , any net with generator matrices (LT^2, L, LT) , L lower-triangular, is (after re-indexing $v \mapsto D_{\pm} P v$) the net with generator matrices*

$$((-1)^{m-1} L J, (L D_{\pm}) P, (s_k L \Lambda_m D_{\pm}) I),$$

the Hammersley net of the two-dimensional generalized Faure sequence $(A_1, A_2 P)$ of Tezuka [62] with $A_1 = s_k L \Lambda_m D_{\pm}$, $A_2 = L D_{\pm}$, and its Hammersley coordinate scrambled by $\pm L$. Since A_1, A_2 depend on m , the family is not the set of prefixes of one sequence.

Proof. Expand $V = \sum_j w_j (t - 1)^j$ with $w = P v$. Then $\Psi V = \sum_j w_j t^j (1 - t)^{m-1-j}$, giving $\Psi = \Lambda_m P$, and $\Psi^2 V = \sum_j w_j (-t)^{m-1-j}$, giving $\Psi^2 = D_{\pm} J P$. Finally use $P^{-1} = D_{\pm} P D_{\pm}$ and $D_{\pm} J D_{\pm} = (-1)^{m-1} J$. $\square$

With $L = I$ this is, up to the lower-triangular scrambles $D_{\pm}$ and $s_k \Lambda_m D_{\pm}$ (which do not change t), Niederreiter's construction [46, Thm. 6.2] with $\beta = (0, 1)$ plus the reversal; in base 2 it is the Hammersley net of the first two Sobol' coordinates [57] with the van der Corput coordinate scrambled by $\Lambda_m \neq I$ (for $m = 3$, $(\Lambda_3)_{20} = 1$).

3.2. The frame of s places. In dimension three a single scramble works because a Möbius map of order three permutes the places $0, 1, \infty$. One scramble shared by all coordinates, as in dimension three (Definition 41), would need a Möbius map that permutes the s places cyclically, of order exactly s ; the finite orders in $PGL_2(\mathbb{Q})$ are $1, 2, 3, 4, 6$, so no rational frame admits one for $s = 5$ or $s \geq 7$. For $s \geq 4$ we therefore scramble each coordinate separately. We develop

the machinery for s places; Theorem A is the general case (Section 4), and dimension four is a worked example in Part II (Section 9.4).

Let $\mathcal{A} = \{a_0, \dots, a_{s-1}\} \subset \mathbb{Q} \cup \{\infty\}$ be s distinct places, one of them ∞ , the others rational numbers (integers in all our examples), and let $F = \mathcal{A} \setminus \{\infty\}$. Let $m = sk$ and $V \in R[t]_{<m}$ for a commutative ring R . The *reading* at a finite place a has digits $[(t-a)^j]V$, $j = 0, \dots, m-1$, and the reading at ∞ has digits $[t^{m-1-j}]V$. These are generator matrices over $\mathbb{Z}[1/v]$, v the common denominator of the finite places (Pascal matrices and the reversal; integer matrices for integer places). For $s = 3$ and $\mathcal{A} = \{\infty, 1, 0\}$ this is the Möbius frame above up to per-coordinate lower-triangular unimodular matrices and a re-indexing (Proposition 9).

Lemma 10 (Frame). *Every box minor of the frame is, up to sign, $\prod_{\{c,d\} \subset F} (a_c - a_d)^{d_c d_d}$. In particular, for $m \geq 2$ and q coprime to the denominators of the places, the frame is a $(0, m, s)$ -net over $\mathbb{Z}/q\mathbb{Z}$ if and only if the finite places are pairwise distinct modulo every prime factor of q .*

Proof. The box matrix for the depths (d_c) is the Hermite matrix of Lemma 8 for the places with multiplicities d_c , which gives the value, a unit modulo a prime p if the finite places are distinct modulo p . Conversely, if $a_c \equiv a_d \pmod{p}$, a box with $d_c = d_d = 1$ (it exists as $m \geq 2$) contains the two equal rows $V(a_c)$, $V(a_d)$ modulo p . The net statement then follows from Lemma 1. $\square$

For the places $\{\infty, 0, 1, \dots, s-2\}$ the condition is $\text{lpf}(q) \geq s-1$ (lpf the least prime factor), the largest possible range: a digital $(0, m, s)$ -net over $\mathbb{Z}/q\mathbb{Z}$ reduces to one over $\mathbb{F}_p$ for every $p \mid q$, which needs $s \leq p+1$ for $m \geq 2$ [46, Cor. 5.11], [39, Thm. 2, Cor. 2]. Let D be the product of the denominators of the finite places and of the numerators of their pairwise differences, and $R = \mathbb{Z}[1/D]$; Lemma 10 and the results below (Lemma 11, Propositions 12 and 13) hold verbatim over R . By Lemma 10 the $(k, \dots, k)$ box is invertible over R , so the frame has a graph form Φ^F with entries in R (Section 2). We write $Q_b = \prod_{b' \in F \setminus \{b\}} (b - b')$ for $b \in F$, $Q_\infty = 1$, $\Pi(t) = \prod_{b \in F} (t - b)^k$ and $\Pi_b = \Pi / (t - b)^k$. A row ρ indexed by levels has the generating function $\rho(x) = \sum_{j < k} \rho_j x^{k-1-j} \pmod{x^k}$ (so the power x^n marks carry depth n , the level $k-1-n$), and $\text{Toep}(u)$ is the lower-triangular Toeplitz matrix of a power series u , with $(\rho \text{Toep}(u))(x) = \rho(x)u(x)$.

Row 0 of Φ_{cd}^F is the dependence of the geometric digit of c on the cell digits of d ; the next lemma computes it for the frame.

Lemma 11 (First offset rows of the frame). *For every $k \geq 1$ and $c \neq d$, row 0 of Φ_{cd}^F has the generating function*

$$\frac{Q_c^k}{\Pi_d(d+x)(c-d-x)} \quad (c, d \in F), \quad \frac{Q_c^k \prod_{b \in F} (1-bx)^{-k}}{1-cx} \quad (c \in F, d = \infty),$$

and $1/\Pi_d(d+x)$ for $c = \infty$, $d \in F$.

Proof. The $(t-b)^k$, $b \in F$, are pairwise comaximal in $R[t]$, so partial fractions give $V/\Pi = H + \sum_{b \in F} N_b/(t-b)^k$ with $\deg H < k$ (as $\deg V < sk = \deg \Pi + k$) and $\deg N_b < k$; that is, $V = \Pi H + \sum_b \Pi_b N_b$.

Cells. For $b \in F$, $V \equiv \Pi_b N_b \pmod{(t-b)^k}$ with $\Pi_b(b) = Q_b^k$ a unit, so the cell of b and N_b determine each other. As $\deg \sum_b \Pi_b N_b < m-k$, the cell of ∞ (the top k coefficients of V) is that of ΠH , which determines H as Π is monic.

Digit k at $c \in F$. $V = \Pi_c N_c + (t-c)^k \Pi_c G_c$ with $G_c = H + \sum_{b \neq c} N_b/(t-b)^k$, regular at c . So digit k is a term depending on N_c only (the own cell) plus $Q_c^k G_c(c) = Q_c^k (H(c) + \sum_{b \neq c} \text{pp}_b(c))$, where $\text{pp}_b = N_b/(t-b)^k$ is the principal part at b .

Digit k at ∞ , the coefficient of t^{m-1-k} , is a term from ΠH (the own cell) plus, from each $\Pi_b N_b$, the top coefficient of N_b , i.e. $\text{Res}_b(V dt/\Pi)$.

Column (d, j) , $d \in F$. All other cells vanish, so $H = 0$, $N_b = 0$ for $b \neq d$, and pp_d is the principal part at d of $(t - d)^{j-k}/\Pi_d$. For a function f whose only pole near d has principal part pp , $\text{pp}(c) = \text{Res}_{t=d} f(t)/(c - t)$; hence $\text{pp}_d(c) = [u^{k-1-j}] 1/(\Pi_d(d + u)(c - d - u))$ and $\text{Res}_d(V/\Pi) = [u^{k-1-j}] 1/\Pi_d(d + u)$. Summing over j with weights x^{k-1-j} gives the first and the third entry.

Column (∞, j) . The finite cells vanish, so $V = \Pi H \equiv t^{m-1-j}$ modulo degree $< m - k$, and H is the polynomial part of $t^{k-1-j} \prod_b (1 - b/t)^{-k}$, and $\sum_j x^{k-1-j} H_j(c) = \prod_b (1 - bx)^{-k}/(1 - cx) \bmod x^k$; multiply by Q_c^k . $\square$

Proposition 12 (Normal form). *Apply the move of Lemma 2(c) with $L_c = \text{diag}(Q_c^{-k}, 1, \dots, 1)$, $U_d = \text{Toep}(\Pi_d(d + x))$ for $d \in F$ and $U_\infty = \text{Toep}(\prod_{b \in F} (1 - bx)^k)$; their diagonal entries are units of R . Then row 0 of every off-diagonal block becomes*

$$N_{cd}(x) = \frac{w_{cd}}{1 - y_{cd}x}, \quad \text{i.e. the entry at carry depth } n \text{ is } w_{cd} y_{cd}^n,$$

independently of k , where $w_{cd} = y_{cd} = 1/(a_c - a_d)$ for $c, d \in F$; $w = 1$, $y = 0$ for $c = \infty$; and $w = 1$, $y = a_c$ for $d = \infty$.

Proof. Substitute into Lemma 11: for instance $Q_c^{-k} \cdot Q_c^k/(\Pi_d(d + x)(c - d - x)) \cdot \Pi_d(d + x) = 1/(c - d - x)$. $\square$

We call the y_{cd} the *nodes* and the w_{cd} the *weights*. So the k -dependence of Lemma 11 sits in the scalars Q^k and in a local unit, the Taylor expansion of the other places' factor around d , which a Toeplitz column move absorbs exactly as $\mathcal{K} = \text{Toep}((1 - t)^{-k})$ does in dimension three. What remains is the Cauchy kernel $1/(c - d - x)$: the polar part at d , evaluated at the place c . In particular the geometric layer (Section 2) of any net obtained from the frame by per-coordinate lower-triangular scrambles is a Cauchy matrix

$$\tilde{M}_{cd} = \lambda_c \mu_d w_{cd} \quad (c \neq d),$$

with arbitrary units λ_c , μ_d and a free diagonal. In residue language, the geometric digit of a finite place c is Q_c^k times the value at c of the other places' polar parts of $V dt/\Pi$ (plus $H(c)$), and that of ∞ is the sum of the finite residues; for $s = 3$ this is the residue description after Proposition 43.

3.3. Designs that work for every k . For the frame of s places we use designs $(F_0, \dots, F_{s-2})$ with $L = s - 1$ levels (Section 2): $F_n[c][d]$ is the target at carry depth n (level $k - 1 - n$) of row 0 of block (c, d) , the diagonal being the own blocks, all other levels are to be 0, and $M^{(j)} = F_0 + \dots + F_j$. After the normal form of Proposition 12, what remains to be chosen no longer involves k ; we call it the *residual problem*. It asks for units $\lambda'_c \in R^\times$ and, for each d , an upper-triangular $(s - 1) \times (s - 1)$ matrix U'_d over R indexed by the carry depths, with diagonal in $R^\times$, such that

$$F_n[c][d] = \lambda'_c \sum_{n' \leq n} w_{cd} y_{cd}^{n'} (U'_d)_{n'n} \quad (c \neq d, n \leq s - 2).$$

It does not involve k . For each d let $v_n = (w_{cd} y_{cd}^n)_{c \neq d} \in R^{s-1}$.

In words: a scramble that realizes the design at the carry depths $0, \dots, s - 2$ extends to every k , by clearing all deeper levels column by column.

Proposition 13 (Scrambles for every k). *Suppose the residual problem is solvable. For $k \geq 1$ put $\lambda_c = \lambda'_c Q_c^{-k}$ and $U_d = U_d^0 U_d'^{(k)}$, where U_d^0 is the Toeplitz column move of Proposition 12, and $U_d'^{(k)}$ agrees with U'_d at the carry depths $< \min(s - 1, k)$ and has, for $s - 1 \leq n < k$, the column $e_n - \sum_{i \leq s-2} \beta_{n,i} \cdot (\text{column } i \text{ of } U'_d)$, where $\beta_n \in R^{s-1}$ solves $\lambda' \odot v_n = \sum_i \beta_{n,i} F_i[\cdot][d]$*

(rows $c \neq d$). Then row 0 of $L_c \Phi_{cd}^F U_d$ equals the design at the carry depths $< s - 1$ (truncated if $k < s - 1$) and vanishes at the larger carry depths; all unit factors and all entries lie in R .

Proof. For $n < s - 1$ this is the residual problem (Proposition 12). The y_{cd} , $c \neq d$, are pairwise distinct with unit differences $(1/(a_c - a_d) - 1/(a_{c'} - a_d) = (a_{c'} - a_c)/((a_c - a_d)(a_{c'} - a_d))$, and 0 resp. the a_c in the other cases), and the w_{cd} are units, so the matrix $(v_0, \dots, v_{s-2})$ is invertible over R , and so is $(F_i[\cdot][d])_{i \leq s-2} = \Lambda'(v_0, \dots, v_{s-2})U'_d$. Hence β_n exists over R , and the new column n has row-0 entries $\lambda'_c v_n[c] - \sum_i \beta_{n,i} F_i[c][d] = 0$ and diagonal entry 1. $\square$

Equivalently, v_n satisfies the linear recurrence with characteristic polynomial $\prod_{c \neq d} (X - y_{cd})$, of order $s - 2$ for $n \geq s - 1$ when some $y_{cd} = 0$; for $s = 4$ it gives $v_n = \alpha_n v_1 + \beta_n v_2$ (Section 9.4).

Definition 14. Let (F_n) be a design whose residual problem is solvable over $R' = R[1/D']$, where D' collects the primes in the units and denominators of λ' and U' , and let $\gcd(q, DD') = 1$. The digital net $\mathcal{P}_{k,q}^F$ over $\mathbb{Z}/q\mathbb{Z}$ is the graph form with depths $(k, \dots, k)$ and blocks $\Phi'_{cd} = L_c \Phi_{cd}^F U_d$ ($c \neq d$; Proposition 13), Φ'_{cc} with row 0 equal to $(F_{s-2}[c][c], \dots, F_0[c][c])$ on the levels $(k - s + 1, \dots, k - 1)$ (truncated if $k < s - 1$) and all other entries 0, all entries reduced modulo q .

Corollary 15. Every box minor of $\mathcal{P}_{k,q}^F$ over R' is a unit of R' ; so $\mathcal{P}_{k,q}^F$ is a digital $(0, sk, s)$ -net over $\mathbb{Z}/q\mathbb{Z}$ for every $k \geq 1$, with one point in every cell.

Proof. The box minors of Φ^F are those of the frame divided by its $(k, \dots, k)$ minor, units of R (Lemma 10); Lemma 2 and Proposition 13 multiply them by units of R' ; then Lemma 1. $\square$

So $\mathcal{P}_{k,q}^F$ consists of lower-triangular scrambles of the s readings of the frame: with the new cells $n'_c = U_c^{-1} n_c$, Φ' is the graph form of $(\hat{L}_c C_c^F)_c$ with $\hat{L}_c = \begin{pmatrix} U_c^{-1} & 0 \\ B_c & L_c \end{pmatrix}$ and $B_c = \Phi'_{cc} U_c^{-1} - L_c \Phi_{cc}^F$. The s scrambles differ (in dimension three one scramble serves all coordinates, Definition 41).

Remark 16 (Two-dimensional projections). Let $m = sk$ be odd with $(s, k) \neq (3, 1)$, and $r^* = (m - 1)/2$. For any two coordinates of $\mathcal{P}_{k,q}^F$ (Definition 14), and of $\mathcal{P}_{k,q}$ (Definition 41), the digits with index r^* agree up to a sign and a linear combination of more significant digits; for $\mathcal{P}_{k,q}^F$ the sign is $+1$ if one of the two places is ∞ , and $(-1)^{r^*}$ otherwise. For the places ∞ and 0 this is the reversal symmetry of the two-dimensional Hammersley set, which reads digit r^* as $[t^{m-1-r^*}]V = [t^{r^*}]V$; a Möbius change of variable transports it to every pair of places, and the lower-triangular scrambles of Corollary 15 keep it, since $r^* \geq k + 1$ and their diagonal entries in the rows below the first offset row are 1. This digit relation is proved. Its visible effect is computed, not proved: in the computed cases every two-dimensional projection lies on parallel lines, at a dual frequency of length about $\sqrt{2/q} \sqrt{N}$ (Figure 3), which the t -parameter does not see. The phenomenon is akin to the known diagonal and rank-1-lattice clustering of generalized Faure sequences whose generator matrices coincide up to a scalar [38, 37]; there the coincidence is in the top digits, here in the middle one. The remedy is of the classical kind: a t -preserving left multiplication by a nonsingular lower-triangular, here diagonal, matrix, as in Tezuka's generalized Faure sequences [61, 62] and Matoušek's linear scrambling [43], with per-coordinate multipliers chosen on two-dimensional projections as in [17, 38]. What is specific here is that only row r^* is rescaled, by units ρ_c . This keeps $t = 0$, as it multiplies every box minor by a unit, and, since Lemma 4 and Theorem 46 use that row only through (H2), it keeps the proved separation bounds (of Lemma 4, Proposition 19, Theorems A(2) and 46); both facts are proved. For a two-dimensional projection with points x let $S(\mathbf{h}) = N^{-1} \sum_x e^{2\pi i \mathbf{h} \cdot x}$, $\mathbf{h} \in \mathbb{Z}^2$, and call the least $|\mathbf{h}|/\sqrt{N}$ over the frequencies with $|S(\mathbf{h})| \geq \frac{1}{2}$ its *spectral value* (about 1 for a good two-dimensional lattice; lines at spacing $N^{-1/2}$ divided by this value appear when it is

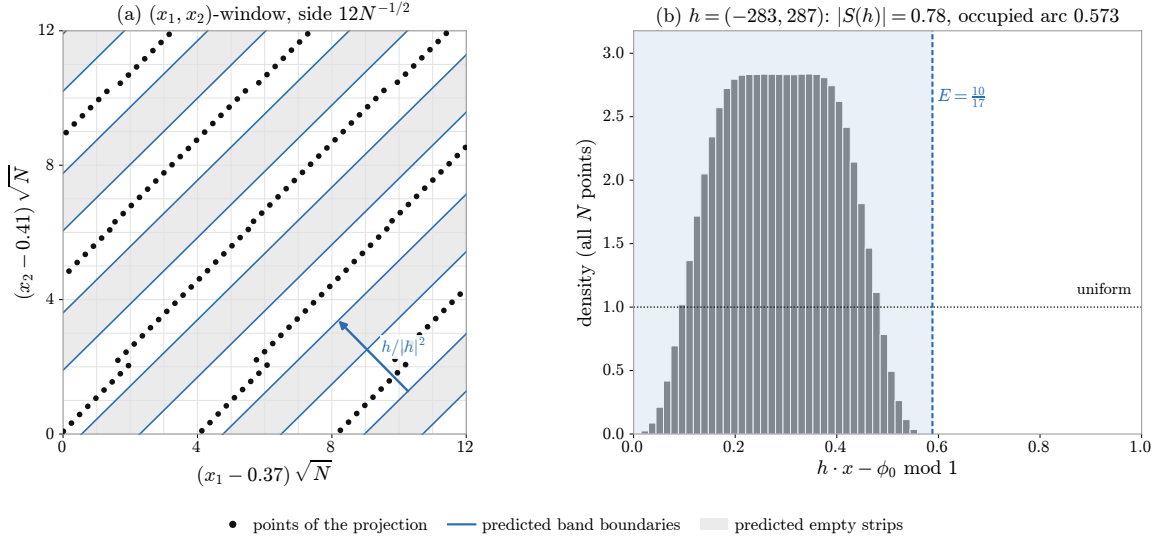


FIGURE 3. Lines in a two-dimensional projection (Remark 16). For odd $m = sk$, $(s, k) \neq (3, 1)$, the middle digit $r^* = (m - 1)/2$ of every pair of coordinates of $\mathcal{P}_{k,q}^F$ satisfies $y_{r^*}(x_b) \equiv \pm y_{r^*}(x_a)$ modulo more significant digits; the sign is $+1$ when one place is ∞ , and $(-1)^{r^*}$ otherwise (checked by computation on all pairs of the net shown, and of U_7^* at $q = 29$, $k = 1$, where $r^* = 3$). This is the reversal symmetry of the two-dimensional Hammersley set (Proposition 9), transported by Möbius maps; $t = 0$ does not see it. Shown: the frame net with the design U_5^* , $q = 17$, $k = 1$, $N = q^5$, coordinates (x_1, x_2) at the places $(\infty, 0)$, $r^* = 2$. The relation, with balanced digits, gives the dual frequency $h = (-283, 287)$, $|h| = 0.338\sqrt{N}$, and puts $h \cdot x \bmod 1$ for all N points in an interval of length at most $E = 10/17$: the points lie in bands around parallel lines with normal h and spacing $1/|h| = 2.95 N^{-1/2}$. (a) A window of side $12N^{-1/2}$ (light grid: $N^{-1/2}$); accent: the predicted band boundaries $h \cdot x \in \phi_0 + \{0, E\} + \mathbb{Z}$ (ϕ_0 : start of the occupied arc); shaded: the predicted empty strips. (b) The distribution of $h \cdot x - \phi_0 \bmod 1$ over all N points (computed): it occupies an arc of length 0.572, and $|S(h)| = 0.78$. A per- q scaling of the middle generator row can break the lines without changing t or the separation bounds (Remark 16).

small). With ρ found per q by an exhaustive search that keeps an estimate of $|S(\mathbf{h})|$ small for $|\mathbf{h}| < 0.8\sqrt{N}$ in every pair of coordinates, the least spectral value over the pairs of coordinates at $s = 5$, $q = 13$ – 23 rises from 0.22–0.30 to about 0.80 (computed).

3.4. Reachable designs.

Proposition 17 (Reachable designs). *The off-diagonal part of a design is reachable from the frame by the gauge moves of Lemma 2(c) with row scalars λ' (that is, the residual problem is solvable with these λ') if and only if, for every column d and every $j \leq s - 2$,*

$$M^{(j)}[c][d] = \lambda'_c w_{cd} g_{d,j}(y_{cd}) \quad (c \neq d)$$

for a polynomial $g_{d,j} \in R[X]$ of degree j whose leading coefficient is a unit. For finite c, d this says $M^{(j)}[c][d] = \lambda'_c \tilde{g}_{d,j}(z_{cd})$ with $z_{cd} = 1/(a_c - a_d)$ and $\tilde{g}_{d,j}(z) = z g_{d,j}(z)$ of degree $j + 1$ without constant term.

Proof. A lower-triangular column move with unit diagonal is a Toeplitz move times an upper-triangular matrix in the carry depths, so the residual problem captures all of Lemma 2(c) on row 0. Column n of $\lambda'^{-1} \odot F_{\cdot d}$ must be $\sum_{n' \leq n} v_{n'}(U'_d)_{n'n}$, i.e. $(w_{cd}f_n(y_{cd}))_c$ with $\deg f_n \leq n$ and the coefficient of X^n a unit; as the y_{cd} are distinct with unit differences, interpolation is unique over R , and this is exactly the condition. Partial sums of such polynomials have the same form, and conversely. $\square$

At carry depth 0 the design is the Cauchy layer $\lambda'_c \mu_d w_{cd}$; at carry depth $s - 2$ any column whose interpolating polynomial has a unit leading coefficient is allowed (for instance a unit vector). Columns are coupled only through the shared row scalars λ'_c .

3.5. Cauchy identities. By Proposition 12 the geometric layer stays a Cauchy matrix with free diagonal under the moves of Lemma 2(a), (c). In homogeneous coordinates $a_c = [\alpha_c : \beta_c]$, with $\infty = [1 : 0]$, put $D_{cd} = \alpha_c \beta_d - \alpha_d \beta_c$; then $D_{cd} = a_c - a_d$ for finite places, $D_{c\infty} = 1$ and $D_{\infty c} = -1$, and the layer is $\tilde{M}_{cd} = \lambda_c \mu_d / D_{cd}$ ($c \neq d$) with units λ_c, μ_d (the sign of $D_{c\infty}$ is absorbed into μ_∞). The same holds over $\mathbb{F}_p$ for places in $\mathbb{P}^1(\mathbb{F}_p)$, and for the skeleton rows of Section 5 at carry depth 0 (Proposition 27(i)). Put $\nu_c = \lambda_c \mu_c$ and $\pi_{cd} = \tilde{M}_{cd} \tilde{M}_{dc} = -\nu_c \nu_d / D_{cd}^2$.

Lemma 18 (Cauchy identities). *Let R be a commutative ring, $\alpha, \beta \in R^s$, $D_{cd} = \alpha_c \beta_d - \alpha_d \beta_c$, and $W_{cd} = \lambda_c \mu_d / D_{cd}$ for $c \neq d$, where all λ_c, μ_d and D_{cd} are units of R ; let $\nu_c = \lambda_c \mu_c$ and $\pi_{cd} = W_{cd} W_{dc}$.*

- (C) *For distinct c, d, e : $W_{cd} W_{de} W_{ec} = -W_{dc} W_{ed} W_{ce}$. Hence, if R is an ordered field, $\pi_{cd} \pi_{de} \pi_{ec} < 0$, and “ $c \sim d$ iff $\pi_{cd} < 0$ ” is an equivalence relation with at most two classes.*
- (P) *For distinct a, b, c, d let $\chi = D_{ac} D_{bd} / (D_{ab} D_{cd})$ and $\psi = D_{ad} D_{bc} / (D_{ab} D_{cd})$. Then $\chi - \psi = 1$, $\chi^2 = \pi_{ab} \pi_{cd} / (\pi_{ac} \pi_{bd})$ and $\psi^2 = \pi_{ab} \pi_{cd} / (\pi_{ad} \pi_{bc})$; consequently $(\chi^2 - \psi^2 - 1)^2 = 4\psi^2$.*
- (H) *If $R \subset \mathbb{R}$: for distinct i, j, k, l , the largest of $|\pi_{ij} \pi_{kl}|^{-1/2}$, $|\pi_{ik} \pi_{jl}|^{-1/2}$, $|\pi_{il} \pi_{jk}|^{-1/2}$ is the sum of the other two.*
- (X) *For distinct i, j, l, d :*

$$\frac{W_{ji} W_{ld}}{W_{jd} W_{li}} + \frac{W_{ij} W_{ld}}{W_{id} W_{lj}} = 1.$$

Proof. Everything follows from $D_{dc} = -D_{cd}$ and the Plücker relation $D_{ab} D_{cd} - D_{ac} D_{bd} + D_{ad} D_{bc} = 0$. (C) The λ, μ cancel, and the D cancel up to $(-1)^3$; then $\pi_{cd} \pi_{de} \pi_{ec} = -(W_{dc} W_{ed} W_{ce})^2$. If $c \sim d$ and $d \sim e$, two of the three factors are negative, so the third is too; if $c \not\sim d$ and $d \not\sim e$, then $c \sim e$. (P) Dividing the Plücker relation by $D_{ab} D_{cd}$ gives $\chi - \psi = 1$. Since $\pi_{xy} = -\nu_x \nu_y / D_{xy}^2$, we have $\pi_{ab} \pi_{cd} = \nu_a \nu_b \nu_c \nu_d / (D_{ab} D_{cd})^2$ and similarly for the other pairings, which gives χ^2 and ψ^2 ; and $\chi = 1 + \psi$ gives $2\psi = \chi^2 - \psi^2 - 1$. (H) By the same formula $|D_{ij} D_{kl}|, |D_{ik} D_{jl}|, |D_{il} D_{jk}|$ are proportional to the three numbers, and by the Plücker relation the products sum to zero with signs. (X) The λ and μ cancel, the two terms are $D_{jd} D_{il} / (D_{ij} D_{ld})$ and $-D_{id} D_{jl} / (D_{ij} D_{ld})$, and $D_{il} D_{jd} - D_{id} D_{jl} = D_{ij} D_{ld}$ is the Plücker relation for (i, j, l, d) . $\square$

Each regime meets one of these identities as its frame-orbit obstruction: (X), or (P), modulo q excludes ± 1 layers in dimension four (Remark 82); (C) and (H) exclude the deficit $K = 1$ in dimension $s \geq 5$ for the designs of Theorem 88; (X) rules out, for $\ell \geq 3$ skeleton coordinates (Section 5), the Korobov skeleton digits that the nets $\mathcal{B}^1$ of Section 6.6 use in dimension three, when the faults are small (Lemma 38, Corollary 39); and (P), read 2-adically, excludes half-integer layers (Proposition 109). The identities need the row and the column of a layer entry to carry the *same* places; there are three ways out. The block scalings of Lemma 2(b), only for $s = 3$, break the Cauchy form (the nets $\mathcal{B}^1$ of Definition 53 use them); graph forms at $m = s$ that are written down directly, not obtained from a frame, are not subject to it (Section 13);

on split frames the layer $\lambda_c \mu_d / (u_c - v_d)$ has different row and column points and satisfies no Plücker relation (Proposition 113).

4. CUBIC CELLS, $m \equiv 0 \pmod{s}$: DESIGNS FROM SHORT LATTICE VECTORS

At the resolutions $m = sk$ the cells are cubes. A geometric layer $\tilde{M}$ with bounded centred entries puts the points locally on $(I + \tilde{M}/q)\mathbb{Z}^s$, a slightly rotated and contracted $\mathbb{Z}^s$ broken along slip planes, at separation $1 - K/q + O(q^{-2})$ (Remark 5). This section proves Theorem A: a lower bound by diagonal dominance (Proposition 19) reduces the separation to the size of the entries of a reachable design, and the reachable design columns form a lattice whose short vectors make the entries small (Sections 4.2 and 4.3). Dimension three, where one integer scramble works in every base, follows in Section 6.

4.1. Diagonal dominance. We keep the notation of Section 3 and use the relaxation LB of Lemma 4 with $L = \min(k, s - 1)$ levels; for $k < s - 1$ the frame realizes the truncated design $(F_0, \dots, F_{k-1})$ (Proposition 13).

Proposition 19 (Diagonal dominance). *Let F be a reachable design whose diagonal vanishes at every carry depth $n \geq 1$, with $F_0[c][c] = -\alpha_c$ and*

$$\alpha_c \geq \sum_{d \neq c} \max_{0 \leq j \leq s-2} |M^{(j)}[c][d]|, \quad a = \max_c \alpha_c.$$

Then $\text{LB} \geq 1 - a/q$ for every $q \geq 5a + 4$ (and every $k \geq 1$).

Proof. Since the diagonal vanishes at every carry depth $n \geq 1$, the own term of every moving coordinate i is $-\alpha_i$ for every carry depth j_i , and dominance gives $e_i \sigma_i \leq -\alpha_i + \alpha_i = 0$ and $|\sigma_i| \leq 2a < q$: every moving coordinate is backward, so $b_i \geq q - |\sigma_i| - \text{jit}_i$. An own-axis step along c has $b_c = q - \alpha_c \geq q - a$ (no jitter). A step with at least two moving axes has $\sum b_i^2 \geq 2(q - 2a - 1)^2$, and $\sqrt{2}(q - 2a - 1) \geq q - a$ holds for $q \geq (2\sqrt{2} - 1)a/(\sqrt{2} - 1) + \sqrt{2}/(\sqrt{2} - 1)$, in particular for $q \geq 5a + 4$. A truncated design is dominant with the same a , and at $k = 1$ the configurations are a subset of those for $k \geq 2$ (after Lemma 4). $\square$

So the base threshold is $5a + 4$, where a measures the largest entries of the partial sums of a reachable design. By Proposition 17 a design is reachable with row scalars λ' if and only if each column of its partial sums interpolates a polynomial with a unit leading coefficient at the nodes y_{cd} ; the question is how small such columns can be. The answer is a lattice problem.

4.2. Admissible design columns form a lattice. Fix $s \geq 3$, the places $\infty, 0, 1, \dots, \nu$ with $\nu = s - 2$, and the row scalars $\lambda' \equiv 1$. Let S be the set of primes $p \leq \nu$ and $R_S = \mathbb{Z}[1/\nu!]$, so that the units of R_S are $\pm$ the products of powers of primes in S (the S -units); for these places the ring R of Section 3 is R_S . Fix a column d . For the $s - 1$ rows $c \neq d$ let $w_c = w_{cd}$ and $y_c = y_{cd}$ be as in Proposition 12: $w_c = y_c = 1/(c - d)$ if c and d are finite, $w_c = 1$, $y_c = 0$ for $c = \infty$, and $w_c = 1$, $y_c = c$ for $d = \infty$. The weights w_c and the differences $y_c - y_{c'}$, $c \neq c'$, are S -units: they are $1/(c - d)$, $(c' - c)/((c - d)(c' - d))$ or $c - c'$, with integers of absolute value at most ν . For $0 \leq j \leq \nu$ put

$$V_j = \{(w_c g(y_c))_{c \neq d} : g \in \mathbb{Q}[X], \deg g \leq j\} \subset \mathbb{Q}^{s-1}, \quad \Lambda_j = V_j \cap \mathbb{Z}^{s-1},$$

and let $\text{lc}_j : V_j \rightarrow \mathbb{Q}$ map a vector to the coefficient of X^j in its polynomial g . As the $s - 1$ nodes are distinct and $j \leq s - 2$, g is determined by the vector, $\dim V_j = j + 1$, $V_{j-1} \subset V_j$ is the kernel of lc_j ($V_{-1} = 0$), and $V_\nu = \mathbb{Q}^{s-1}$. By Proposition 17 (with $\lambda' \equiv 1$, over R_S) an integer column $(M^{(j)}[c][d])_{c \neq d}$ is an *admissible* design column at carry depth j if it is a vector of V_j whose polynomial has coefficients in R_S and degree j with an S -unit leading coefficient.

- Lemma 20** (The lattice of admissible design columns). (i) For $E \in \Lambda_j$ the polynomial of E has coefficients in R_S .
(ii) $\text{lc}_j(\Lambda_j) = \gamma_j \mathbb{Z}$ for a positive S -unit γ_j .
(iii) An integer column is admissible at carry depth j if and only if it lies in Λ_j and $\text{lc}_j(E)$ is an S -unit; in particular every $E \in \Lambda_j$ with $\text{lc}_j(E) = \gamma_j$ is admissible.
(iv) If $E_i \in \Lambda_i$ and $\text{lc}_i(E_i) = \gamma_i$ for $i = 0, \dots, j$, then $E_0, \dots, E_j$ is a basis of Λ_j , and $\{E \in \Lambda_j : \text{lc}_j(E) = \gamma_j\} = E_j + \Lambda_{j-1}$.

Proof. (i) Lagrange interpolation at any $j+1$ rows J recovers $g = \sum_{b \in J} (E_b/w_b) \prod_{b' \in J \setminus b} (X - y_{b'})/(y_b - y_{b'})$, and all denominators are S -units. (ii) $\text{lc}_j(\Lambda_j)$ is a finitely generated subgroup of $\mathbb{Q}$, nonzero because Λ_j spans V_j , so it is $\gamma_j \mathbb{Z}$ with $\gamma_j > 0$; by (i), $\gamma_j \in R_S$. The vector $(w_c y_c^j)_c$ of $g = X^j$ has S -unit or zero entries, so some product P of primes in S makes $P(w_c y_c^j)_c$ integral, with $\text{lc}_j = P$; hence $P \in \gamma_j \mathbb{Z}$, and γ_j has no prime factor outside S in its numerator either. (iii) is (i) together with the definition. (iv) If $v \in \Lambda_j$ has $\text{lc}_j(v) = t\gamma_j$, then $v - tE_j \in \Lambda_j \cap \ker \text{lc}_j = \Lambda_{j-1}$; induction on j . $\square$

So the admissible design columns at carry depth j are the lattice vectors on the affine hyperplanes $\text{lc}_j = \pm \gamma_j \cdot (S\text{-unit})$ of Λ_j , and the smallest ones are governed by the distance between consecutive hyperplanes. That distance is a product of local Chebyshev constants, one for each place of $\mathbb{Q}$ that matters (in the sense of number theory: the archimedean absolute value and the p -adic ones; not the places of a frame). For the archimedean absolute value and each $p \in S$ let

$$A_{j,\mathbb{R}} = \min\{\|E\|_2 : E \in V_j \otimes \mathbb{R}, \text{lc}_j(E) = 1\}, \quad A_{j,p} = \min_c \{\max |E_c|_p : E \in V_j, \text{lc}_j(E) = 1\},$$

the least size, at that place, of the vectors $(w_c g(y_c))_c$ of monic polynomials g of degree j (the minimum at p exists because these sizes are powers of p and are bounded below by Lagrange interpolation).

Lemma 21 (Adelic Chebyshev identity). Let π_j be the orthogonal projection of $\mathbb{R}^{s-1}$ onto the line $V_j \cap V_{j-1}^\perp$. Then $\pi_j(\Lambda_j)$ is generated by a vector of length

$$\eta_j = A_{j,\mathbb{R}} \prod_{p \in S} A_{j,p}, \quad \text{and} \quad \gamma_j = \prod_{p \in S} A_{j,p}.$$

Every $E \in \Lambda_j \setminus V_{j-1}$ has $\|E\|_2 \geq \eta_j$.

Proof. The p -adic places, $p \in S$. If $E \in V_j$ has $\text{lc}_j(E) = 1$ and $\max_c |E_c|_p = p^e$, then $p^e E$ is p -integral, and $D'p^e E \in \Lambda_j$ for an integer D' prime to p ; so $D'p^e \in \gamma_j \mathbb{Z}$ and $v_p(\gamma_j) \leq e$. Conversely, for $v \in \Lambda_j$ with $\text{lc}_j(v) = \gamma_j$ the vector v/γ_j has $\text{lc}_j = 1$ and $\max_c |v_c/\gamma_j|_p \leq p^{v_p(\gamma_j)}$. So $A_{j,p} = p^{v_p(\gamma_j)}$, and as $\gamma_j > 0$ is an S -unit, $\gamma_j = \prod_{p \in S} A_{j,p}$. The archimedean place. On V_j , $\text{lc}_j(E) = \langle \theta, E \rangle$ for a unique $\theta \in V_j$, and $\theta \perp V_{j-1}$. Hence $\|\pi_j(E)\| = |\text{lc}_j(E)|/\|\theta\|$, and the least norm with $\text{lc}_j = 1$ is $A_{j,\mathbb{R}} = 1/\|\theta\|$, attained at $\theta/\|\theta\|^2$. So $\pi_j(\Lambda_j) = \gamma_j \mathbb{Z} \theta/\|\theta\|^2$, generated by a vector of length $\gamma_j A_{j,\mathbb{R}} = \eta_j$, and $\|E\| \geq \|\pi_j(E)\| \geq \eta_j$ if $\text{lc}_j(E) \neq 0$. $\square$

This is the product formula at work: an S -unit scalar can move the p -adic cost of a collision of nodes (Proposition 12) to the archimedean place, but never remove it. For the upper bounds below it suffices to exhibit, *independently at each place*, one monic polynomial that is small there. At the place p a monic polynomial is small on the nodes if its roots sit p -adically near the nodes that collide modulo p (two finite rows c, c' collide if $p \mid c - c'$, and then y_c is p -adically large); different primes want the roots in different places, so no single closed-form basis serves all primes, and the lattice reduction chooses the roots for each prime automatically.

s	3	4	5	6	7	8	9	10
a_s^*	2	5	16	43	170	543	2842	13640
largest entry of U_s^*	1	2	6	14	86	198	1446	5364
$5a_s^* + 4$	14	29	84	219	854	2719	14214	68204
bound of Theorem A	–	46.7	324	2716	$2.67 \cdot 10^4$	$3.03 \cdot 10^5$	$3.89 \cdot 10^6$	$5.58 \cdot 10^7$
a_s of U_s (Remark 24)	4	63	17407	$5.67 \cdot 10^6$	$1.86 \cdot 10^{12}$	$2.05 \cdot 10^{14}$	$1.34 \cdot 10^{23}$	$5.57 \cdot 10^{28}$

TABLE 3. The constant a_s^* of Theorem A (exact values of Definition 23, computed), the largest entry $\max |M^{(j)}|$ of U_s^* , the base threshold $5a_s^* + 4$, the bound $2(s-1)^{3/2}(3/2)^{s-2}(s-2)!$ of Theorem A (truncated), and, for comparison, the constant a_s of the monomial design U_s .

Lemma 22 (Babai rounding along the flag). *Let $E_i \in \Lambda_i$ with $\text{lc}_i(E_i) = \gamma_i$ for $i < j$, and let $v \in \Lambda_j$ with $\text{lc}_j(v) = \gamma_j$. Write the orthogonal projection of v onto V_{j-1} as $\sum_{i < j} c_i E_i$ and put $E_j = v - \sum_{i < j} \lfloor c_i + \frac{1}{2} \rfloor E_i$. Then $E_j \in \Lambda_j$, $\text{lc}_j(E_j) = \gamma_j$, and*

$$\|E_j\|_2 \leq \eta_j + \frac{1}{2} \sum_{i < j} \|E_i\|_2.$$

Consequently, if $E_0, \dots, E_j$ are all obtained in this way and $\eta_i \leq H$ for every $i \leq j$, then $\|E_i\|_2 \leq (3/2)^i H$ for every $i \leq j$.

Proof. $E_j - v \in \Lambda_{j-1} = \ker \text{lc}_j \cap \Lambda_j$, and $E_j = \pi_j(v) + \sum_{i < j} (c_i - \lfloor c_i + \frac{1}{2} \rfloor) E_i$ with $\|\pi_j(v)\| = \eta_j$ (Lemma 21) and every coefficient in $[-\frac{1}{2}, \frac{1}{2}]$. For the consequence let $T_i = \sum_{i' \leq i} \|E_{i'}\|$. Then $T_0 = \eta_0 \leq H$ and $T_i \leq \frac{3}{2}T_{i-1} + H$, so $T_i \leq 2H((3/2)^{i+1} - 1)$ by induction, and $\|E_i\| \leq H + \frac{1}{2}T_{i-1} \leq (3/2)^i H$. $\square$

4.3. The design U_s^* and the proof of Theorem A.

Definition 23 (The design U_s^*). Let $s \geq 3$, $\nu = s - 2$, and take the places $\infty, 0, 1, \dots, \nu$ and $\lambda' \equiv 1$. For each column d let $E_{d,0}$ be the generator of Λ_0 with $\text{lc}_0 > 0$, and for $1 \leq j \leq \nu$ let $E_{d,j}$ be the unique $E \in \Lambda_j$ with $\text{lc}_j(E) = +\gamma_j$ whose orthogonal projection onto V_{j-1} has all its coefficients in the basis $E_{d,0}, \dots, E_{d,j-1}$ in $[-\frac{1}{2}, \frac{1}{2}]$. The design $U_s^* = (F_0, \dots, F_\nu)$ has the partial sums $M^{(j)}[c][d] = E_{d,j}[c]$ ($c \neq d$, $j \leq \nu$), the diagonal $F_0[c][c] = -\alpha_c$ at carry depth 0 with $\alpha_c = \sum_{d \neq c} \max_j |E_{d,j}[c]|$, and zero diagonal at the carry depths $n \geq 1$. Let $a_s^* = \max_c \alpha_c$.

By Lemma 20(iv) the set $\{E \in \Lambda_j : \text{lc}_j(E) = \gamma_j\}$ is a coset of $\Lambda_{j-1} = \bigoplus_{i < j} \mathbb{Z}E_{d,i}$, so $E_{d,j}$ exists, is unique, and is the vector of Lemma 22 for any v in that coset (with ties rounded up). Only the two conventions $\text{lc}_j = +\gamma_j$ and “ties up” matter: the result does not depend on the choice of v , of a basis of Λ_j or of the order of the rows. The construction is deterministic and runs in time polynomial in s : there are $s(s-1)$ pairs (d, j) , each needs an integer kernel and a Hermite normal form of a lattice of dimension at most $s-1$ with entries of $O(s^2 \log s)$ bits [31], an extended Euclid step for v , and one rational Gram solve, and the output entries have $O(s \log s)$ bits by the proof below; it is not a closed formula. For $s = 3$ (places $\infty, 0, 1$, $S = \emptyset$) the definition gives, in the coordinate order $\infty, 0, 1$,

$$F_0 = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & -1 \\ 1 & 1 & -2 \end{pmatrix}, \quad F_1 = \begin{pmatrix} 0 & -2 & -1 \\ -2 & 0 & 2 \\ -1 & -1 & 0 \end{pmatrix},$$

so $a_3^* = 2$. Table 3 lists a_s^* for $s \leq 10$ (computed exactly by two independent implementations of Definition 23).

Proof of Theorem A. Reachability. By Lemma 20(iii) every column $E_{d,j}$ is admissible at carry depth j , with polynomial $g_{d,j} \in R_S[X]$ of degree j and leading coefficient γ_j , an S -unit; so by Proposition 17 the off-diagonal part of U_s^* is reachable with $\lambda' \equiv 1$ over $R' = R_S$, and the diagonal is free (Lemma 2(a)).

(1) Every prime factor of q is at least $s-1 > \nu$, so $\gcd(q, \nu!) = 1$, and Corollary 15 gives a digital $(0, sk, s)$ -net with one point in every cell, for every $k \geq 1$. A cell has diameter $\sqrt{s} q^{-k} = \sqrt{s} N^{-1/s}$, which bounds h .

(2) *Lower bound.* (H1) and (H2) of Lemma 4 hold by Proposition 13 and Definition 14, with $L = \min(k, s-1)$. U_s^* is diagonally dominant by construction, with the maximum over all carry depths, so Proposition 19 gives $\delta q^k \geq 1 - a_s^*/q$ for $q \geq 5a_s^* + 4$ and every $k \geq 1$.

Sharpness ($k \geq 2$). Let i attain $a_s^* = \alpha_i$. For $q > 2a_s^*$ the entries of F_0 are centred, so $\tilde{M} = F_0$. By (H2) the own-axis step e_i from a cell whose last digit of n_i is not $q-1$ changes coordinate i by exactly $1 - a_s^*/q$ cells if its first offset digit is at least a_s^* (no wrap, no jitter), and every other coordinate u by less than $(|\tilde{M}_{ui}| + 1)/q$ if r_u avoids the $|\tilde{M}_{ui}|$ values from which adding $\tilde{M}_{ui}$ wraps. For each $u \neq i$ the $t=0$ box with depths $k+1$ on i and u and 0 elsewhere (total $2k+2 \leq sk$) makes (n_i, r_i, n_u, r_u) jointly uniform (that box fixes exactly these $2k+2$ digits, so every value of them occurs equally often), so among the cells satisfying the conditions on n_i and r_i the fraction with a wrapping r_u is $|\tilde{M}_{ui}|/q$; for $q > \sum_{u \neq i} |\tilde{M}_{ui}|$ a union bound leaves a cell. Its pair of points lies inside the unit cube, so

$$\delta N^{1/s} < \left(\left(1 - \frac{a_s^*}{q}\right)^2 + \sum_{u \neq i} \frac{(|F_0[u][i]| + 1)^2}{q^2} \right)^{1/2} = 1 - \frac{a_s^*}{q} + O(q^{-2}).$$

The bound on a_s^ .* Let $s \geq 4$. By Lemma 22 it suffices to show $\eta_{d,j} \leq \Xi_s := 2\sqrt{s-1}(s-2)!$ for every column d and carry depth j ; then every entry of U_s^* is at most $\max_{d,j} \|E_{d,j}\|_2 \leq (3/2)^{s-2} \Xi_s$, and $a_s^* \leq (s-1)(3/2)^{s-2} \Xi_s = 2(s-1)^{3/2} (3/2)^{s-2} (s-2)!$. By Lemma 21 it suffices to give, at each place of $\mathbb{Q}$, one monic g of degree j .

Finite column d . Archimedean place: all nodes y_c lie in $[-1, 1]$ and $|w_c| \leq 1$, so the monic Chebyshev polynomial $2^{1-j}T_j$ ($j \geq 1$; $g = 1$ for $j = 0$) gives $A_{j,\mathbb{R}} \leq 2\sqrt{s-1}$. At $p \in S$: let $\mathcal{R}_p$ be the finite rows $c \neq d$ with $p \mid c-d$, $e_c = v_p(c-d) \geq 1$ for $c \in \mathcal{R}_p$, let $\mathcal{R}' \subset \mathcal{R}_p$ consist of $\min(j, |\mathcal{R}_p|)$ rows with the largest e_c , and $g_p = \prod_{r \in \mathcal{R}'} (X - y_r) \cdot X^{j-|\mathcal{R}'|}$. For $c \in \mathcal{R}'$ the entry vanishes. For $c, r \in \mathcal{R}_p$, $|y_c - y_r|_p = |(r-c)/((c-d)(r-d))|_p \leq p^{\max(e_c, e_r)}$; so for $c \in \mathcal{R}_p \setminus \mathcal{R}'$ (then $|\mathcal{R}'| = j$ and $e_c \leq e_r$ for $r \in \mathcal{R}'$) the entry has p -adic size at most $p^{e_c + \sum_{r \in \mathcal{R}'} e_r} \leq p^{\sum_{r \in \mathcal{R}_p} e_r}$. For a finite row $c \notin \mathcal{R}_p$, and for the row ∞ ($y = 0, w = 1$), $|w_c|_p = 1$, $|y_c|_p \leq 1$ and $|y_c - y_r|_p \leq p^{e_r}$, so the size is at most $p^{\sum_{r \in \mathcal{R}'} e_r}$. Hence $A_{j,p} \leq p^{\sum_{r \in \mathcal{R}_p} e_r} = p^{v_p(d!(\nu-d)!)}$, and $\prod_{p \in S} A_{j,p} \leq d!(\nu-d)! \leq \nu!$, since every prime factor of $d!(\nu-d)!$ lies in S . So $\eta_{d,j} \leq 2\sqrt{s-1}\nu!$.

Column ∞ . The nodes are $y_c = c \in \{0, \dots, \nu\}$ with $w_c = 1$. At the archimedean place the monic Chebyshev polynomial of $[0, \nu]$ gives $A_{j,\mathbb{R}} \leq 2\sqrt{s-1}(\nu/4)^j$. At $p \in S$ the falling factorial $X(X-1)\cdots(X-j+1)$ takes the values $j! \binom{c}{j}$, so $A_{j,p} \leq |j!|_p$ and $\prod_p A_{j,p} \leq 1/j!$. So $\eta_{\infty,j} \leq 2\sqrt{s-1}(\nu/4)^j/j! \leq 2\sqrt{s-1}e^{\nu/4} \leq 2\sqrt{s-1}\nu!$ for $\nu \geq 2$.

Finally, with $\nu = s-2$ the elementary bounds $\nu^\nu e^{-\nu} \leq \nu! \leq \nu^\nu$ give $|\log(2(s-1)^{3/2}(3/2)^{s-2}(s-2)! - s \log s)| \leq 3s$ for $s \geq 4$, so the bound is $e^{s \log s + O(s)}$; and $a_3^* = 2$ is the display before Table 3. (At the archimedean place the Chebyshev polynomial even gives $A_{j,\mathbb{R}} \leq \sqrt{s-1}$ for a finite column, since $|2^{1-j}T_j| \leq 1$ on $[-1, 1]$ for $j \geq 1$; the factor 2 in Ξ_s is slack.) $\square$

The bound is far from the computed values: $5.58 \cdot 10^7$ against $a_{10}^* = 13640$ (Table 3). The proof shows where the size comes from: the archimedean Chebyshev constants are harmless, and the cost sits at the primes $p \leq s-2$, through the factorials $d!(s-2-d)!$ of the place differences.

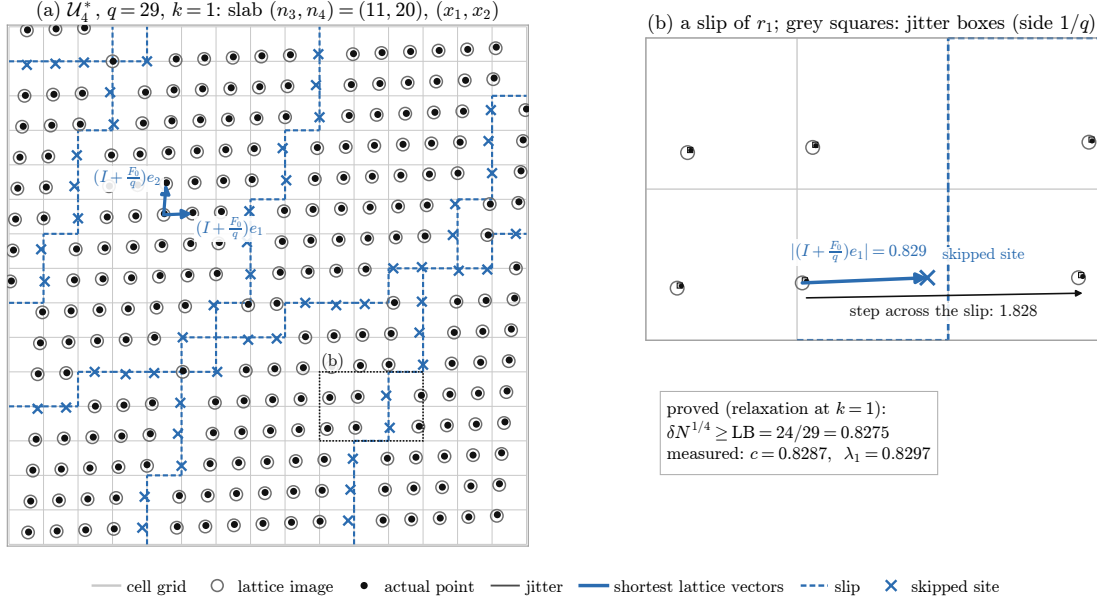


FIGURE 4. Theorem A at its threshold: the net $\mathcal{P}_{1,q}^{U_4^*}$ of the lattice design U_4^* ($a_4^* = 5$) at $q = 5a_4^* + 4 = 29$, $k = 1$, $N = q^4$; in cell units (side $N^{-1/4}$). (a) The elementary slab of the cells $(n_3, n_4) = (11, 20)$, a 15×15 window of cells (n_1, n_2) , projected to (x_1, x_2) ; one point per cell. Open circles: the lattice image $n + r/q$, $r = F_0 n \bmod q$ ((H1) of Lemma 4); dots: the points; grey segments: the jitter of the two deeper digits, inside $[0, 1/q]^4$. Accent arrows: the projections of $(I + F_0/q)e_1$ and $(I + F_0/q)e_2$; dashed: slips, where r_1 or r_2 wraps; crosses: lattice sites the net skips there. (b) Zoom on one slip of r_1 (dotted box in (a)), with the jitter boxes of side $1/q$: across the slip the step is 1.828 instead of $|(I + F_0/q)e_1|$. Proved: $\delta N^{1/4} \geq \text{LB} = 24/29 = 0.8275$, the relaxation of Lemma 4 at $k = 1$ (here equal to the bound $1 - a_4^*/q$ of Theorem A). Measured (computed, exact): $c = 0.8287$; the lattice minimum is $\lambda_1(I + F_0/q) = 0.8297$.

Whether other row scalars λ' , other places or another lower-bound argument bring the base threshold down to a polynomial in s is open.

Remark 24 (The monomial design U_s). The every-dimension theorem also holds with the monomial design U_s : put $L_s = \text{lcm}(1, \dots, s-2)^{s-1}$, $\lambda'_c = L_s$ for finite c , $\lambda'_\infty = 1$, and $F_n[c][d] = L_s/(c-d)^{n+1}$ for finite c, d , $F_n[\infty][d] = [n=0]$, $F_n[c][\infty] = L_s \binom{c}{n}$, with a diagonal that is dominant in the sense of Proposition 19. Its increments are monomials in the nodes, and the proof of Theorem A applies verbatim with its constant $a_s = \max_c \alpha_c$ in place of a_s^* (for $k \geq 2$ the net property, the separation bound for $q \geq 5a_s + 4$ and the sharpness are formally verified for this design). But $\log a_s = (1 + o(1))s^2$: for finite c , $\alpha_c \geq |F_0[c][\infty]| = L_s$, and $\log L_s = (s-1)\psi(s-2)$ with Chebyshev's function ψ , while $a_s \leq L_s(s^2 + 2^{s-2})$; so $a_s = e^{\Theta(s^2)}$ already by Chebyshev's bounds $\psi(x) \asymp x$, and the constant 1 uses the prime number theorem [21, 12]. In the language above the reason is p -adic: a monomial has all its roots at 0, so at a collision of nodes it is as large as possible, $|y^j|_p = p^j v_p(c-d)$, at every carry depth and in every column, and the single row scalar λ' must clear all of it. Theorem A puts the roots near the colliding nodes, separately for

each prime, and so replaces $e^{\Theta(s^2)}$ by the upper bound $e^{s \log s + O(s)}$ (Table 3: $a_5 = 17407$ against $a_5^* = 16$).

5. LATTICE SKELETONS: $m = sk + r$

For $N = p^m$, $m = sk + r$ with $1 \leq r \leq s - 1$, the boxes with one point each cannot all be cubes (regime II of Section 2, Figure 8). We give r coordinates $k + 1$ cell digits (the *full* coordinates) and the other $\ell = s - r$ coordinates only k (the *skeleton* coordinates). The first offset digit of a skeleton coordinate, its *skeleton digit*, places the point, along that coordinate, in one of the p sub-intervals of side $p^{-(k+1)}$ of its cell. So we measure positions in *fine cells*, the cubes of side $p^{-(k+1)}$: a cell (with the depths above) consists of p^ℓ fine cells, and each point lies in one of them. A *coarse block* is a cube of side p^{-k} , fixed by the first k digits of every coordinate; it consists of p^s fine cells and holds p^r points. The skeleton digits build the lattice (the ‘skeleton’) on which the occupied fine cells lie: inside each coarse block they form a coset of a lattice of index p^ℓ , a Construction A lattice of an MDS code (Remark 32). From one block to the next this coset is shifted by a small vector, a *fault*; the faults come from the coefficients g_{ij} of Lemma 26(N2). So the separation, in fine cells, is at least the lattice minimum minus the largest fault minus one fine cell for the deeper digits (Lemma 25). One skeleton coordinate needs no faults (Theorem 33); two force them (Theorems 35 and 56). For three or more, a Plücker identity satisfied by every net in the frame orbit (Section 3) rules out the Korobov skeleton digits of the nets $\mathcal{B}^1$ when the faults are small (Corollary 39); these residues are open for all large primes.

Conventions. Here p is a prime, $s \geq 3$ and $\ell = s - r$. The r *full* coordinates $x_1, \dots, x_r$ have depth $k + 1$, the ℓ skeleton coordinates $z_1, \dots, z_\ell$ depth k , and S_z denotes the skeleton digit of z . Level l of the cells is $x_{d,l}, z_{j,l}$ (level 0 is the most significant; the letter x has nothing to do with the variable x of Lemma 11). As in Section 2, the depth of a coordinate is its number of cell digits, and the last level of a coordinate of depth k_c is at carry depth 0, the level $k_c - 1 - n$ at carry depth n . In dimension three ($m = 3k + r$) the coordinates are (x, y, z) , with depths $\mathbf{k} = (k + 1, k, k)$ for $r = 1$ ($\ell = 2$) and $\mathbf{k} = (k + 1, k + 1, k)$ for $r = 2$ ($\ell = 1$), and cell levels x_l, y_l, z_l .

5.1. Fine cells and the separation reduction. Fine cells have side $p^{-(k+1)}$ in every coordinate, and the fine unit is $\varpi = p^{m-k-1}$ integer units. Put $P_c = n_c$ for a full and $P_c = p n_c + S_c$ for a skeleton coordinate, where n_c is the cell index as an integer. So P_c is the position of the point along axis c measured in fine cells: for a full coordinate its $k + 1$ cell digits, for a skeleton coordinate its k cell digits followed by the skeleton digit. Then $P_c \in [0, p^{k+1})$ is the *fine cell* of coordinate c , and the integer coordinate is $X_c = P_c \varpi + \theta_c$ with $0 \leq \theta_c < \varpi$. Since $n_c = \lfloor P_c/p \rfloor$ for skeleton coordinates, P determines all cell digits, hence the index: distinct points have distinct P . For a full coordinate, level $k - j$ is $\lfloor P_c/p^j \rfloor \bmod p$; for a skeleton coordinate, level $k - 1 - j$ is $\lfloor P_c/p^{j+1} \rfloor \bmod p$, and $P_c \equiv S_c \pmod{p}$.

Lemma 25 (Separation reduction). *Let $v \neq w$ be two points, and let a_c be the centred residue $(-p^{k+1}/2 < a_c \leq p^{k+1}/2)$ of $P_c(w) - P_c(v)$ modulo p^{k+1} ; we call a the fine difference of v and w .*

- (i) *The toroidal distance of $X_c(w)$ and $X_c(v)$ modulo N is at least $(|a_c| - 1)\varpi$. Hence, if $|a|_\infty \geq M$ for every pair of distinct points, the toroidal minimum distance satisfies $\delta N^{1/s} \geq (M - 1)p^{-\ell/s}$.*
- (ii) *If $|a_c| < p$ and $1 \leq j \leq k$, then $\lfloor P_c(w)/p^j \rfloor - \lfloor P_c(v)/p^j \rfloor \equiv \xi_{c,j} \pmod{p^{k+1-j}}$ with $\xi_{c,j} \in \{0, \text{sgn } a_c\}$, and $\xi_{c,j} \neq 0$ implies $\xi_{c,j-1} \neq 0$ for $j \geq 2$.*

Proof. (i) $N = p^{k+1}\varpi$, so $X_c(w) - X_c(v) \equiv x := a_c\varpi + (\theta' - \theta) \pmod{N}$ with $|\theta' - \theta| < \varpi$. If $|x| \leq N/2$, the distance is $|x| \geq |a_c|\varpi - (\varpi - 1)$. Otherwise it is $N - |x| \geq N - (|a_c| +$

1) $\varpi + 1 > (p^{k+1} - |a_c| - 1)\varpi \geq (|a_c| - 1)\varpi$, as $|a_c| \leq p^{k+1}/2$. So $\delta N \geq (M - 1)\varpi$, and $\varpi N^{1/s}/N = p^{m/s-k-1} = p^{-\ell/s}$. (ii) Write $P_c(w) = P_c(v) + a_c + \varepsilon p^{k+1}$ with $\varepsilon \in \{-1, 0, 1\}$. The difference of the floors is $\lfloor (P_c(v) + a_c)/p^j \rfloor - \lfloor P_c(v)/p^j \rfloor + \varepsilon p^{k+1-j}$. As $|a_c| < p \leq p^j$, the first part lies in $\{0, \text{sgn } a_c\}$, and it is nonzero only if a multiple of p^j , hence of p^{j-1} , lies between $P_c(v)$ and $P_c(v) + a_c$. Neither part uses that p is odd or prime; $p \geq 2$ suffices. $\square$

Part (ii) says: if two points are less than p fine cells apart along axis c , the cell digits above the fine one change only by one carry or borrow in the direction of a_c , and a change at a level implies a change at every less significant level. So along each coordinate the changed levels are the last j levels for some j , all changed with the same sign $\text{sgn } a_c$ (a *sign-consistent prefix*). Every lattice $\Lambda \subset \mathbb{Z}^s$ of index p^ℓ has a nonzero vector with $|\cdot|_\infty \leq \lfloor p^{\ell/s} \rfloor$ (pigeonhole: the cube $\{0, \dots, \lfloor p^{\ell/s} \rfloor\}^s$ has more than p^ℓ points, so two of them are congruent modulo Λ). So when all fine differences lie in one lattice of index p^ℓ , as for $\ell = 1$ (Theorem 33), the bound of (i) is less than 1. For $\ell \geq 2$ only differences within one coarse block are lattice vectors, so there this ceiling is a heuristic, not a theorem.

5.2. Necessary conditions, forced faults and completion.

Lemma 26 (Necessary conditions on the skeleton digits). *Let a graph form with the depths above be a $(0, m, s)$ -net over $\mathbb{F}_p$. Let $A \in \mathbb{F}_p^{\ell \times r}$ hold the coefficients of the skeleton digits on the last levels $x_{d,k}$, and, for $k \geq 1$ and $i \neq j$, let g_{ij} be the coefficient of S_{z_i} on $z_{j,k-1}$.*

- (N1) *Every square submatrix of A is invertible.*
- (N2) *(Forced faults.) If $\ell \geq 2$ and $k \geq 1$, then $g_{ij} \neq 0$ for all $i \neq j$.*
- (N3) *For every full coordinate x_d and every set I of j skeleton coordinates, the coefficients of the S_{z_i} , $i \in I$, on the levels $x_{d,k}, \dots, x_{d,k-j+1}$ form an invertible matrix; for a skeleton coordinate $z_e \notin I$ the same holds on the levels $z_{e,k-1}, \dots, z_{e,k-j}$ (whenever these levels exist).*

Proof. All three follow from Lemma 2 for suitable boxes. For (N1) take depth $k + 1$ on the skeleton coordinates of a set I , depth k on the full coordinates of a set J with $|J| = |I|$, and k_c elsewhere: the over coordinates are those of I , by one digit (their skeleton digits), the under coordinates those of J , by one level (the level k), and the minor is $\det A[I, J]$. (N2) is the box with depth $k + 1$ on z_i and $k - 1$ on z_j ; (N3) the box with depth $k + 1$ on I and $k_e - j$ on the coordinate e . $\square$

In words, (N3) says that any j of the skeleton digits together depend invertibly on the last j cell levels of each other coordinate. We call the coefficients g_{ij} the *faults*. By (N2), for $\ell \geq 2$ every skeleton digit depends, with a nonzero coefficient, on the last cell digit of every other skeleton coordinate: when the last cell digit of z_j changes, the skeleton digit of z_i shifts by g_{ij} , and with it the lattice coset of the occupied fine cells. So the occupied fine cells form a lattice coset only inside each coarse block, shifted by the faults between neighbouring blocks (as for $\mathcal{B}^1$, Section 6.6). In our constructions the faults are bounded integers (centred), so at the lattice scale $p^{\ell/s}$ they cost a bounded number of fine cells.

Fix s distinct places in $\mathbb{P}^1(\mathbb{F}_p)$ (so $p \geq s - 1$) and assign them to the coordinates. Lemmas 10, 11 and Proposition 12 hold verbatim over $\mathbb{F}_p$, since their proofs use only that the differences of the finite places are units. By Lemma 10 the frame has a graph form Φ^F with depths $\mathbf{k}$, all of whose box minors are units.

The key observation behind the next proposition: the points of the frame with $s(k + 1)$ digits whose skeleton coordinates start with the digit 0 form, after these coordinates are rescaled by p , the frame with m digits, and a skeleton digit is the old first offset digit.

Proposition 27 (Completion). *Let the frame and Φ^F be as above.*

- (i) (Normal form.) After the moves of Proposition 12, applied to the restricted frame as described in the proof below, row 0 of every block (z_i, d) , $d \neq z_i$, of Φ^F has the generating function $w_{id}/(1 - y_{id}x)$ of Proposition 12, where x^n marks carry depth n , the level $k_d - 1 - n$; this holds for every k . For a column block d let ℓ_d be the number of skeleton coordinates other than d ($\ell_d = \ell$ if d is full, $\ell_d = \ell - 1$ if d is a skeleton coordinate). Then Propositions 17 and 13 hold for the skeleton rows, with the ℓ_d skeleton rows $z_i \neq d$ of block d in place of the rows $c \neq d$, and $\ell_d - 1$, ℓ_d in place of $s - 2$, $s - 1$ (the carry depths $n \leq \ell_d - 1$).
- (ii) ($\ell = 1$.) For every $k \geq 0$ and all units $\kappa_1, \dots, \kappa_r$, the moves of Lemma 2 turn Φ^F into a graph form whose skeleton digit is $S_z = \sum_d \kappa_d x_{d,k}$ (all other entries of row 0 of z , own block included, are 0). It is a $(0, m, s)$ -net over $\mathbb{F}_p$.
- (iii) ($\ell = 2$.) Let $k \geq 1$ and prescribe skeleton digits

$$S_{z_i} = \sum_d A_{id} x_{d,k} + \sum_d \beta_{id} x_{d,k-1} + g_{ij} z_{j,k-1} + o_i z_{i,k-1} \quad (\{i, j\} = \{1, 2\})$$

satisfying (N1)–(N3), with arbitrary own coefficients o_i . For a suitable choice of the places they are reachable for every $k \geq 1$, and they complete to a $(0, m, s)$ -net over $\mathbb{F}_p$.

Proof. (i) *Restriction.* Let $m' = s(k + 1)$ and $V \in \mathbb{F}_p[t]_{<m'}$. The first digit of the reading at a finite skeleton place a_z vanishes iff $(t - a_z) \mid V$, and at ∞ iff $\deg V < m' - 1$. So the points of the m' -frame whose skeleton coordinates have first digit 0 are given by $V = \prod_{z \text{ finite}} (t - a_z) V'$ with $\deg V' < m$, and their readings are those of V' times a unit power series, shifted by one digit at a skeleton place. Hence this point set, with the skeleton coordinates rescaled by p , is the m -frame up to per-coordinate lower-triangular scrambles, i.e. up to the moves of Lemma 2; each new elementary box is an old one with one more leading digit on each skeleton coordinate. In the graph form of the m' -frame with depths $(k + 1, \dots, k + 1)$ the restriction is the vanishing of level 0 of the skeleton cells, and the old first offset row of z becomes its skeleton digit. The move of Proposition 12 is lower-triangular in the levels and only scales level 0, so it commutes with deleting the level-0 columns of the skeleton blocks; this gives the normal form, with carry depth n at level $k_d - 1 - n$. The proofs of Propositions 17 and 13 use only this normal form and the distinctness, with unit differences, of the y_{cd} on the rows involved, so they apply to the ℓ_d skeleton rows of a column.

(ii) For each full x_d , the entry of S_z on $x_{d,k}$ is the box minor with depth $k + 1$ on z and k on x_d , hence a unit. Subtract multiples of level k from the levels $l < k$ (move (c) with U_{x_d} lower-triangular) so that S_z vanishes there, scale level k to κ_d , and set all diagonal blocks to 0 (move (a)). By Lemma 2 every box minor stays a unit, and Lemma 1 applies. This is the recipe of Definition 53($\mathcal{B}^2$) in s dimensions; it needs no normal form.

(iii) By (i), the only constraints are these. On a full column d ($\ell_d = 2$): at carry depth 0, $A_{id} = \lambda_i \mu_d w_{id}$ (a generalized Cauchy column); at carry depth 1 Proposition 17 only asks that the interpolating polynomial have a unit leading coefficient, and for two rows this is the determinant $\det[A_{\cdot d}, \beta_{\cdot d}]$, which is (N3). On a skeleton column ($\ell_d = 1$): $g_{ij} \neq 0$, which is (N2). Larger carry depths are set to 0 by Proposition 13, for every k , and the own terms by move (a). It remains to realize the ratios A_{2d}/A_{1d} . Put z_1 at ∞ and z_2 at a finite place a_2 ; then $w_{1d} = 1$ and $w_{2d} = 1/(a_2 - b_d)$, with b_d the place of x_d , and the condition is $b_d = a_2 - \Lambda A_{1d}/A_{2d}$ with $\Lambda = \lambda_2/\lambda_1$. Take $\Lambda = 1$, $\lambda_1 = 1$ and $\mu_d = A_{1d}$. The b_d are finite, differ from a_2 because $A_{1d} \neq 0$, and are pairwise distinct because the 2×2 minors of A are nonzero (N1). The net property follows as in (ii). $\square$

With Lemma 26, part (iii) is sharp. Here a graph form is *reachable from the frame* if the moves of Lemma 2 produce it from Φ^F .

Corollary 28 (Reachable skeletons with two skeleton coordinates). *Let $\ell = 2$, and fix skeleton digits of the form in Proposition 27(iii), with coefficients that do not depend on k . For a suitable choice of the places they are reachable from the frame for every $k \geq 1$ if and only if they satisfy (N1)–(N3). The necessity holds for each single $k \geq 1$: every graph form with these skeleton digits that is a $(0, m, s)$ -net over $\mathbb{F}_p$ satisfies (N1)–(N3).*

Proof. For skeleton digits of this form, (N1)–(N3) say: every entry and every 2×2 minor of A is nonzero (N1, which contains (N3) for $j = 1$ on a full coordinate); $g_{12} \neq 0$ and $g_{21} \neq 0$ (N2, which is also (N3) for $j = 1$ on a skeleton coordinate); and $\det[A_{\cdot d}, \beta_{\cdot d}] \neq 0$ for every full coordinate x_d ((N3) for $j = 2$; for $\ell = 2$ no skeleton coordinate lies outside a set I of size 2). These conditions involve only the coefficients, not k . *If:* Proposition 27(iii). *Only if:* let $k \geq 1$, and let a graph form with the given skeleton digits be reachable from the frame for some choice of the places. All box minors of Φ^F are units (Lemma 10, over $\mathbb{F}_p$), and the moves multiply every box minor by a unit (Lemma 2), so the graph form is a $(0, m, s)$ -net over $\mathbb{F}_p$ (Lemma 1). Lemma 26 applies to every such net and gives (N1)–(N3). $\square$

For $\ell \geq 3$ the carry depths $j \leq \ell - 2$ of the full columns are constrained, and a three-term identity holds at carry depth 0 (Lemma 38); for $\ell \geq 3$ it is open whether every skeleton satisfying (N1)–(N3) completes to a net for every k by some construction not based on a frame.

5.3. Lattices. For $A \in \mathbb{Z}^{\ell \times r}$ let $\Lambda_A = \{(x, z) \in \mathbb{Z}^r \times \mathbb{Z}^\ell : z \equiv Ax \pmod{p}\}$, a lattice of index p^ℓ , and $\lambda_\infty(\Lambda_A)$ its minimum in the maximum norm. By the pigeonhole argument above, $\lambda_\infty(\Lambda_A) \leq \lfloor p^{\ell/s} \rfloor$.

Lemma 29 (Short vectors). *Let Λ_A be as above.*

- (L) ($\ell = 1$.) *If $\rho \geq 2$, $\rho^s < p$ and $A = (\rho, \rho^2, \dots, \rho^{s-1})$, then $\lambda_\infty(\Lambda_A) = \rho$. For $\rho = \lfloor p^{1/s} \rfloor$ this is the largest minimum of any lattice of index p .*
- (L1) ($r = 1$.) *If $\rho \geq 2$, $\rho^\ell(\rho + 1) \leq p$ and $A = (\rho, \rho^2, \dots, \rho^\ell)^\top$, then $\lambda_\infty(\Lambda_A) = \rho^\ell$.*
- (T) ($\ell = r = 2$.) *If $\rho \geq 2$, $\rho^2 - 4 < p$ and $A = \begin{pmatrix} \rho & 1 \\ 1 & \rho \end{pmatrix}$, then $\lambda_\infty(\Lambda_A) \geq \rho - 1$.*
- (G) ($\ell = 2, r \geq 3$.) *Let $B \geq 1$ and let $\nu_1 > \sqrt{2}B$ and $\nu_2, \dots, \nu_{r-1}$ be integers with $\nu_1^2 + 1 > B$. Put $\zeta_i = \nu_i + i$ and $\Omega_i = \zeta_1 \cdots \zeta_i \in \mathbb{Z}[i]$, and define $A \in \mathbb{Z}^{2 \times r}$ by*

$$A_1 x + i A_2 x = \sum_{l=1}^{r-2} x_l \Omega_l + (x_{r-1} + i x_r) \Omega_{r-1}.$$

If $B(1 + \|A_j\|_1) < p$ for $j = 1, 2$, then $\lambda_\infty(\Lambda_A) \geq B + 1$.

Proof. (L) If $0 < |u|_\infty \leq \rho - 1$, then $|z - \sum_d \rho^d x_d| \leq (\rho - 1)(1 + \rho + \dots + \rho^{s-1}) = \rho^s - 1 < p$, so $z = \rho(x_1 + \rho x_2 + \dots)$ exactly. Then $\rho \mid z$ and $|z| < \rho$ give $z = 0$, then $|x_1| < \rho$ and $\rho \mid x_1$ give $x_1 = 0$, and so on: $u = 0$. The vector $x = e_1$, $z = \rho$ shows equality, and $\rho = \lfloor p^{1/s} \rfloor$ attains the pigeonhole bound. (L1) Let $u = (x, z_1, \dots, z_\ell) \neq 0$ and $B = |u|_\infty$. If $B(\rho + 1) \geq p$, then $B \geq p/(\rho + 1) \geq \rho^\ell$. Otherwise $|z_1 - \rho x| \leq B(1 + \rho) < p$ gives $z_1 = \rho x$, and for $i < \ell$, $z_{i+1} - \rho z_i \equiv \rho^{i+1} x - \rho^{i+1} x = 0$ with $|z_{i+1} - \rho z_i| < p$ gives $z_{i+1} = \rho z_i$; so $z_\ell = \rho^\ell x$. As $u \neq 0$, $x \neq 0$, so $B \geq |z_\ell| \geq \rho^\ell$; the vector $(1, \rho, \dots, \rho^\ell)$ shows equality. (T) If $0 < |u|_\infty \leq \rho - 2$, then $|z_1 - \rho x_1 - x_2| \leq (\rho - 2)(\rho + 2) < p$, so $z_1 = \rho x_1 + x_2$, and likewise $z_2 = x_1 + \rho x_2$. If $x = 0$ then $z = 0$. Otherwise, say $|x_1| \geq |x_2|$, and $|z_1| \geq (\rho - 1)|x_1| \geq \rho - 1$, a contradiction. (G) Let $0 < |u|_\infty \leq B$. Since $|z_j - A_j x| \leq B(1 + \|A_j\|_1) < p$, the relations are exact. Then $Z = z_1 + i z_2$ is divisible by ζ_1 in $\mathbb{Z}[i]$, and $|Z| \leq \sqrt{2}B < |\zeta_1|$, so $Z = 0$. Dividing by ζ_1 shows that ζ_2 divides the rational integer x_1 . For a rational integer n , $n/\zeta_2 = n(\nu_2 - i)/(\nu_2^2 + 1)$, so $\zeta_2 \mid n$ iff $\nu_2^2 + 1 \mid n$; as $|x_1| \leq B < \nu_2^2 + 1$, $x_1 = 0$. Continuing with $\zeta_3, \dots, \zeta_{r-1}$ gives $x_1 = \dots = x_{r-2} = 0$ and then $x_{r-1} + i x_r = 0$, so $u = 0$. $\square$

For $s = 3$, (L) and (L1) are the lattices $\Lambda_{\mathcal{B}^2} = \{a : a_z \equiv \rho a_x + \rho^2 a_y\}$ of $\mathcal{B}^2$ and $\Lambda_{\mathcal{B}^1} = \{u : u_y \equiv \rho u_x, u_z \equiv \rho^2 u_x\}$ of $\mathcal{B}^1$ (Definition 53); with $\rho \approx p^{1/s}$ both are sharp to first order. (L1) keeps the optimal order $p^{\ell/s}$ by comparing z_{i+1} with ρz_i rather than with $\rho^{i+1}x$; inside the frame orbit it is not reachable with small faults once $\ell \geq 3$ (Corollary 39). In (G) the row sums are of order $\sqrt{2}B \cdot B^{(r-2)/2}$, so the largest allowed B is of order $(p/\sqrt{2})^{2/s}$, again the optimal exponent: the last factor Ω_{r-1} multiplies $x_{r-1} + ix_r$, so one Gaussian ‘digit’ carries two coordinates, whereas the naive choice $A_2 = \rho A_1$ plus a small correction is capped at $B^r < p$, and splitting the x ’s into two groups, one per row, reaches the optimal exponent only for even r . For $3 \leq \ell \leq s-2$ we have no explicit family, but such lattices exist by counting. If $0 < |u|_\infty < p$ then $x \neq 0$ (otherwise $z \equiv 0$ forces $z = 0$), so for A uniform in $\mathbb{F}_p^{\ell \times r}$ the vector u lies in Λ_A with probability $p^{-\ell}$. The expected number of nonzero $u \in \Lambda_A$ with $|u|_\infty \leq L$ is thus below $(2L+1)^s p^{-\ell}$, at most 1 if $2L+1 \leq p^{\ell/s}$, so some A has $\lambda_\infty(\Lambda_A) > (p^{\ell/s} - 1)/2$; this says nothing about (N1)–(N3) or reachability.

Definition 30. Let $s \geq 5$, $r = s-2$ and $B \geq 1$. Let $A(B)$ be the matrix of Lemma 29(G) with $\nu_1 = \lfloor \sqrt{2}B \rfloor + 1$ and $\nu_l = \lfloor \sqrt{B} \rfloor + 1$ for $2 \leq l \leq r-1$, and, for a prime p , let $B(p)$ be the largest integer $\beta \geq 1$ with $\beta(1 + \max_j \|A_j(\beta)\|_1) < p$. This $B(p)$ is nondecreasing in p .

Lemma 31 ((N1) for the Gaussian matrix). *Let $s \geq 5$, $B \geq 1$, $A = A(B)$ and $B(1 + \max_j \|A_j\|_1) < p$. Then:*

- (a) $\nu_j^2 + 1 < p$ for every j ;
- (b) if $\sum_{j=1}^{r-1} \arctan(1/\nu_j) < \pi/2$, every entry and every 2×2 minor of A is nonzero modulo p , i.e. A satisfies (N1);
- (c) the hypothesis of (b) holds if $s \leq 8$ and $B \geq g^* + 1$, where $g^* = 1 + \lceil r/2 \rceil$, and, for every B , if $B > (2(r-1)/\pi)^2$.

Proof. (a) Columns $r-1$ and r of A are $(\operatorname{Re} \Omega_{r-1}, \operatorname{Im} \Omega_{r-1})$ and $(-\operatorname{Im} \Omega_{r-1}, \operatorname{Re} \Omega_{r-1})$, so $\|A_j\|_1 \geq |\Omega_{r-1}| = \prod_j (\nu_j^2 + 1)^{1/2} \geq \sqrt{5}(\nu_1^2 + 1)^{1/2}$, as $r \geq 3$ and $\nu_l \geq 2$. Hence $p > B\sqrt{5}(\nu_1^2 + 1)^{1/2}$. Since $\nu_1 \leq \sqrt{2}B + 1$, we have $\nu_1^2 + 1 \leq 2B^2 + 2\sqrt{2}B + 2 \leq 5B^2$ for $B \geq 2$, and $\nu_1^2 + 1 = 5 = 5B^2$ for $B = 1$. So $p > \nu_1^2 + 1 \geq \nu_j^2 + 1$. (b) The arguments of all Ω_l lie in $(0, \pi/2)$, so the entries are nonzero integers, of absolute value $< p$ by the hypothesis. The 2×2 minor of the columns $l < l' \leq r-1$ is $\operatorname{Im}(\overline{\Omega_l} \Omega_{l'}) = |\Omega_l|^2 \operatorname{Im}(\zeta_{l+1} \cdots \zeta_{l'})$, and that of the columns $l \leq r-1$ and r is $|\Omega_l|^2 \operatorname{Re}(\zeta_{l+1} \cdots \zeta_{r-1})$. Here $|\Omega_l|^2$ is a product of the factors $\nu_j^2 + 1 < p$, so it is prime to p . The second factor is a nonzero integer of absolute value at most $|\zeta_2 \cdots \zeta_{r-1}| < |\Omega_{r-1}| < p$. (c) The ν_j are nondecreasing in B . At $B = g^* + 1$ they are $(6, 3)$, $(6, 3, 3)$, $(8, 3, 3, 3)$, $(8, 3, 3, 3, 3)$ for $s = 5, 6, 7, 8$, with arctangent sums below 0.487, 0.809, 1.090, 1.412, all $< \pi/2$. For every B , $\nu_j > \sqrt{B}$ (Definition 30), so the sum is $< (r-1)/\sqrt{B}$. $\square$

For $s \geq 9$ part (c) gives no threshold of the form $B \geq g^* + 1$: at $B = g^* + 1$ the sum is $1.7194 \dots > \pi/2$ for $s = 9$, and larger for $s \geq 10$.

Remark 32 (Codes). The lattices of this section are Construction A lattices [9, Ch. 5] (stated there for binary codes; the p -ary version is the same): with the systematic $[s, r]$ code $C_A = \{(x, Ax) : x \in \mathbb{F}_p^r\} \subset \mathbb{F}_p^s$ of the skeleton digits, $\Lambda_A = C_A + p\mathbb{Z}^s$. For every prime p the nonzero vectors of $p\mathbb{Z}^s$ have maximum and Euclidean norm at least p , and the centred lift of a codeword is a shortest lift in every coordinate. So $\lambda_\infty(\Lambda_A)$ is the least largest centred entry of a nonzero codeword, and $\lambda_2(\Lambda_A)^2 = \min(p^2, w_E(C_A))$, with w_E the least Euclidean (squared Lee) weight. We call skeleton digits *pure* if they depend only on the last levels $x_{d,k}$ of the full coordinates (as in Definition 34). For pure skeleton digits, $P_{x_d} \equiv x_{d,k}$ and $P_z \equiv S_z \pmod{p}$ constrain only the

lowest fine digit, so the occupied fine cells lie in Λ_A (for $\ell = 1$ they fill it, Theorem 33(2)); the faults shift C_A to cosets that vary between coarse blocks. In this language:

(a) Condition (N1) of Lemma 26 says that C_A is MDS [45, Ch. 11, Thm. 8], which says nothing about the Lee or Euclidean minimum: $A = (1, \dots, 1)$ is MDS with $\lambda_\infty(\Lambda_A) = 1$.

(b) Inside the frame orbit the layer at carry depth 0 is a generalized Cauchy matrix in the places (Proposition 27(i)), so C_A is a generalized Reed–Solomon code [51] (doubly extended if $s = p + 1$). This restricts the code only if $r \geq 3$ and $\ell \geq 3$, since every MDS code of dimension or codimension at most two is generalized Reed–Solomon; for $r \leq 2$ or $\ell \leq 2$ the restriction comes instead from the faults: the code and the faults must be realized with the same row scalars λ' (Proposition 17), which ties their values together. Lemma 38 is the Plücker relation (Lemma 18(X)) applied jointly to the code and the faults; Corollary 39 concerns the Korobov column with bounded faults, not other codes.

(c) For $\ell = 1$, $\Lambda_A = \{a \in \mathbb{Z}^s : h \cdot a \equiv 0 \pmod{p}\}$ with the (parity-)check vector $\mathbf{h} = (\kappa_1, \dots, \kappa_r, -1)$ is the dual of the rank-1 lattice $\mathbb{Z}^s + \mathbb{Z}\mathbf{h}/p$ [55], and $\lambda_2(\Lambda_A)$ is its spectral test [5], [32, Sec. 3.3.4]; for $\kappa_d = \rho^d$ (Definition 34) it is Knuth's spectral-test lattice of the multiplier ρ in dimension s , after $a_z \mapsto -a_z$. For $\rho = \lfloor p^{1/s} \rfloor$ the normalized minimum $\lambda_2(\Lambda_A)p^{-1/s}$ lies between $\rho p^{-1/s}$ and $\sqrt{\rho^2 + 1} p^{-1/s}$ and tends to 1, against the upper bound $\sqrt{\gamma_s}$ valid for every $\mathbf{h}$ (Remark 124). So $\kappa_d = \rho^d$ is optimal in the maximum norm but not for the spectral test, which Proposition 102 (Part II) exploits.

5.4. One skeleton coordinate.

Theorem 33 (One skeleton coordinate). *Let $s \geq 3$, let p be a prime, let $\rho \geq 2$ be an integer with $\rho^s < p$ (one exists iff $p > 2^s$), and let $k \geq 0$. The net $\mathcal{S}_{k,p,\rho}^1$ of Definition 34, whose skeleton digit is $S_z = \sum_d \rho^d x_{d,k}$, with $N = p^{sk+s-1}$ points, is a digital $(0, sk + s - 1, s)$ -net over $\mathbb{F}_p$, and:*

- (1) *its toroidal (hence also Euclidean) minimum distance satisfies $\delta N^{1/s} \geq (\rho - 1)p^{-1/s}$; for $\rho = \lfloor p^{1/s} \rfloor$ the bound exceeds $(\rho - 1)/(\rho + 1)$, so it is $> 1/3$ for every prime $p > 2^s$, $> 1/2$ for $p > 3^s$, and tends to 1;*
- (2) *its occupied fine cells are exactly the cells of a lattice of index p with minimum $\lambda_\infty = \rho$, which for $\rho = \lfloor p^{1/s} \rfloor$ is the largest minimum of any lattice of index p ;*
- (3) *for $\rho = \lfloor p^{1/s} \rfloor$ its covering radius satisfies $hN^{1/s} \leq \sqrt{s}(\mu + 1)p^{-1/s}$ with $\mu = \lceil p/\rho^{s-1} \rceil < \rho(1 + 1/\rho)^s + 1$, so the mesh ratio $h/\delta \leq \sqrt{s}(\mu + 1)/(\rho - 1)$ is bounded uniformly in p and k , and is at most $\sqrt{s}(1 + o(1))$ as $p \rightarrow \infty$.*

Definition 34. Let $s \geq 3$, $\rho \geq 2$ with $\rho^s < p$, $k \geq 0$ and $m = sk + s - 1$. Take the frame that assigns the places $\infty, 0, 1, \dots, s - 2$ to the coordinates $x_1, \dots, x_{s-1}, z$, respectively, the depths $(k + 1, \dots, k + 1, k)$ with the skeleton coordinate z last, and the recipe of Proposition 27(ii) with $\kappa_d = \rho^d$. The result is the digital net $\mathcal{S}_{k,p,\rho}^1$ over $\mathbb{F}_p$. Its skeleton digit is

$$S_z = \sum_{d=1}^{s-1} \rho^d x_{d,k}.$$

Proof of Theorem 33. Net. Proposition 27(ii): $p > 2^s \geq s - 1$, and the prescribed coefficients ρ^d are units since $\rho^{s-1} < p$.

(1) Since $x_{d,k} \equiv P_{x_d}$ and $P_z \equiv S_z \pmod{p}$, every point satisfies $P_z \equiv \sum_d \rho^d P_{x_d} \pmod{p}$. This congruence passes to the differences modulo p^{k+1} , so every difference $a \neq 0$ lies in Λ_A of Lemma 29(L), and $|a|_\infty \geq \rho$. Lemma 25(i) gives $\delta N^{1/s} \geq (\rho - 1)p^{-1/s}$. There are no faults. With $\rho = \lfloor p^{1/s} \rfloor$ we have $p < (\rho + 1)^s$, so the bound exceeds $(\rho - 1)/(\rho + 1)$, which is $\geq 1/3$ for $\rho \geq 2$ ($p > 2^s$) and $\geq 1/2$ for $\rho \geq 3$ ($p > 3^s$).

s	p_0	Theorem 33 ($r = s - 1$)					p_0	Theorem 35 ($r = s - 2$)				
		37	101	1009	10007	10^6+3		101	1009	10007	10^5+3	10^6+3
3	11	.600	.644	.897	.928	.989						
4	17	.405	.630	.709	.899	.948	23	.597	.849	.959	.986	.995
5	37	.485	.397	.501	.792	.883	137	0	.440	.652	.759	.796
6	67	–	.463	.631	.646	.899	443	0	.299	.556	.689	.769
7	131	–	–	.372	.536	.833	2179	0	0	.287	.484	.617
8	257	–	–	.421	.632	.711	6101	0	0	.199	.449	.632

TABLE 4. The lower bounds of Theorems 33 and 35 for $\delta N^{1/s}$, with ρ maximal (Theorem 33: $\rho = \lfloor p^{1/s} \rfloor$; Theorem 35: ρ resp. $B(p)$ maximal), at the primes shown, and the least prime p_0 from which on they are positive; truncated (not rounded) to three digits. Both bounds are sawtooth functions of p . For $s \geq 5$ the bound of Theorem 35 tends to $2^{-1/s}$ by a heuristic estimate (Remark 125).

(2) There are $N = p^{s(k+1)-1}$ points with distinct P , all in Λ_A , and Λ_A has $p^{s(k+1)}/p = N$ classes modulo $p^{k+1}\mathbb{Z}^s$. So the occupied fine cells are exactly the cells of Λ_A . Optimality is Lemma 29(L).

(3) Let $Q \in \{0, \dots, p^{k+1} - 1\}^s$ be the fine cell of a point $y \in [0, 1)^s$. We look for a cell $a = Q - v \in \Lambda_A$ in the same range with $|v|_\infty \leq \mu := \lceil p/\rho^{s-1} \rceil$. Prescribe the sign ϵ_c of v_c : -1 if $Q_c < p^{k+1}/2$, else $+1$. Since $\mu \leq p/4 + 1 \leq p^{k+1}/2$, any v with these signs and $|v|_\infty \leq \mu$ keeps a in range. With $T \equiv Q_z - \sum_d \rho^d Q_{x_d} \pmod{p}$, the vector a lies in Λ_A iff $v_z - \sum_d \rho^d v_{x_d} \equiv T$. Choose the representative T' of T in $[0, p)$ or in $(-p, 0]$, and expand $T' = \sum_{i=0}^{s-1} t_i \rho^i$ in base ρ with signed digits: $t_0, \dots, t_{s-2}$ are taken one at a time from the window $[0, \rho - 1]$ or $[-(\rho - 1), 0]$, according to the sign of T' , and t_{s-1} is the rest. Put $v_z = t_0$ and $v_{x_i} = -t_i$; the windows give the required signs of $v_z, v_{x_1}, \dots, v_{x_{s-2}}$. The lower digits contribute less than ρ^{s-1} in absolute value, so t_{s-1} has the sign of T' (which we choose) and $|t_{s-1}| < p/\rho^{s-1} + 1$. So $|v|_\infty \leq \mu$, since also $\rho - 1 < p/\rho^{s-1}$. The point in the cell a differs from y by less than $(\mu + 1)p^{-(k+1)}$ in every coordinate, so

$$hN^{1/s} \leq \sqrt{s}(\mu + 1)p^{-1/s}, \quad \frac{h}{\delta} \leq \frac{\sqrt{s}(\mu + 1)}{\rho - 1}.$$

For $\rho = \lfloor p^{1/s} \rfloor$, $\mu < \rho(1 + 1/\rho)^s + 1$, so both bounds are bounded in p for fixed s , and $h/\delta \leq \sqrt{s}(1 + o(1))$ as $p \rightarrow \infty$. $\square$

For the toroidal covering radius, balanced digits $|t_i| \leq \lfloor \rho/2 \rfloor$ and $|T'| < p/2$ give $\mu \leq \lceil p/(2\rho^{s-1}) \rceil$, and the resulting bound on the toroidal mesh ratio tends to $\sqrt{s}/2$.

The bounds of Table 4 hold for every net with the given skeleton digits, and for Theorem 33 the lattice bound is attained: some two points have a fine difference with $|a|_\infty = \rho$ (Theorem 33(2) and Lemma 29(L)).

5.5. Two skeleton coordinates.

Theorem 35 (Two skeleton coordinates). *Let $s \geq 4$, let p be a prime and $k \geq 1$, and let $\mathcal{S}_{k,p}^2$ be the net of Definition 36, with $N = p^{sk+s-2}$ points.*

- (1) ($s = 4$.) *For every prime $p \geq 5$, $\mathcal{S}_{k,p}^2$ is a digital $(0, 4k + 2, 4)$ -net over $\mathbb{F}_p$ with $\delta N^{1/4} \geq (\rho - 4)p^{-1/2}$, where $\rho = \max\{\rho : \rho^2 < p + 4\}$; the bound is positive for every prime $p \geq 23$ and tends to 1.*

- (2) ($5 \leq s \leq 8$.) For every prime $p \geq 137, 443, 2179, 6101$ ($s = 5, 6, 7, 8$), $\mathcal{S}_{k,p}^2$ is a digital $(0, sk+s-2, s)$ -net over $\mathbb{F}_p$ with $\delta N^{1/s} \geq (B(p) - g^*) p^{-2/s} > 0$, where $g^* = 1 + \lceil (s-2)/2 \rceil$ and $B(p) \asymp p^{2/s}$ is defined in Definition 30.
- (3) ($s \geq 9$.) The same holds for every prime p with $B(p) > g^*$ and $\sum_{j=1}^{s-3} \arctan(1/\nu_j) < \pi/2$ for the ν_j of Definition 30 at $B = B(p)$; this holds if $B(p) > \max\{g^*, (2(s-3)/\pi)^2\}$, in particular for all sufficiently large p .

Definition 36. Let $s \geq 4$, $r = s - 2$, $k \geq 1$, $m = sk + s - 2$. For $s = 4$ let A be the matrix of Lemma 29(T) with ρ maximal such that $\rho^2 - 4 < p$, and put $I_1 = \{2\}$, $I_2 = \{1\}$. For $s \geq 5$ let $A = A(B(p))$ (Definition 30), and let $I_1 \sqcup I_2 = \{1, \dots, r\}$ with $|I_1| = \lfloor r/2 \rfloor$. The net $\mathcal{S}_{k,p}^2$ is the completion (Proposition 27(iii)) of the skeleton digits

$$S_{z_1} = A_1 x_{\cdot,k} + \sum_{d \in I_1} x_{d,k-1} + z_{2,k-1}, \quad S_{z_2} = A_2 x_{\cdot,k} + \sum_{d \in I_2} x_{d,k-1} - z_{1,k-1},$$

with no dependence of S_{z_i} on the cell of z_i itself (own coefficients 0), and $x_{\cdot,k} = (x_{1,k}, \dots, x_{r,k})$.

The faults $g_{12} = +1$ and $g_{21} = -1$ have opposite signs (they are *skew*); this excludes the case $u = 0$ in the proof below. (N3) holds: $\det[A_{\cdot d}, e_1] = -A_{2d}$ and $\det[A_{\cdot d}, e_2] = A_{1d}$ are nonzero by (N1).

Proof of Theorem 35. (N1). For $s = 4$ the entries $\rho, 1$ are units, and $\det A = \rho^2 - 1 = (\rho - 1)(\rho + 1)$ with $0 < \rho - 1 < \rho + 1 < p$, since $\rho^2 < p + 4$ and $p \geq 5$. For $s \geq 5$ use Lemma 31: in (2), $B(p) \geq g^* + 1$ exactly for $p > 132, 440, 2170, 6095$ ($s = 5, \dots, 8$), which gives the primes 137, 443, 2179, 6101. These four numbers are $\Gamma(g^* + 1)$ for $\Gamma(B) = B(1 + \max_j \|A_j(B)\|_1)$, and Γ is increasing on $B \geq g^* + 1$ (below), so some $B \geq g^* + 1$ has $\Gamma(B) < p$ iff $\Gamma(g^* + 1) < p$. In (3) the hypothesis is that of Lemma 31(b), and the closed-form sufficient condition is that of Lemma 31(c). *Net.* Proposition 27(iii).

Monotonicity of Γ . Let $5 \leq s \leq 8$ and $g^* + 1 \leq B < B'$. The ν_j do not decrease from B to B' , and $\sum_j \arctan(1/\nu_j) < \pi/2$ at B by Lemma 31(c). The absolute values of the entries of $A(B)$ are the real and imaginary parts of $\Omega_1, \dots, \Omega_{r-1}$ (proof of Lemma 31(a)). Raise the ν_j one at a time from their values at B to those at B' . If ν_j is a factor of $\Omega_l = P(\nu_j + i)$, the other factors have arctangents no larger than at B , so $P = a + ib$ with $\arg P \in [0, \pi/2)$, i.e. $a > 0$, $b \geq 0$; and $P(\nu_j + i) = (a\nu_j - b) + i(b\nu_j + a)$, so raising ν_j by $\Delta \geq 0$ raises the real part by $a\Delta$ and the imaginary part by $b\Delta$. All parts stay positive, so every $|A_{jd}|$ is nondecreasing, $\|A_j(B')\|_1 \geq \|A_j(B)\|_1$, and $\Gamma(B') > \Gamma(B)$. (The thresholds are also verified in Lean, by a different route: Γ is evaluated exactly for $g^* + 1 \leq B < B_1$, $B_1 = 7, 7, 9, 9$, and $(B \max_j \|A_j(B)\|_1)^2 \geq 2B^s$, from $\|A_j\|_1 \geq |\Omega_{r-1}|$, covers $B \geq B_1$.)

Separation. Let $a \neq 0$ be a difference and $M = |a|_\infty$. If $M \geq p - 1$, then $M \geq \lambda_\infty(\Lambda_A) - g^*$ below holds, since $\lambda_\infty(\Lambda_A) \leq \lfloor p^{2/s} \rfloor \leq p - 1$. Otherwise let $\xi_c = \xi_{c,1}$ be the floor changes of Lemma 25(ii); they give the changes of the level- $(k-1)$ digits modulo p . Put

$$u = \left(a_x, a_{z_1} - \sum_{d \in I_1} \xi_{x_d} - \xi_{z_2}, a_{z_2} - \sum_{d \in I_2} \xi_{x_d} + \xi_{z_1} \right).$$

By the skeleton digits, the change of S_{z_i} is $A_i a_x$ plus the contributions of the level- $(k-1)$ changes ξ ; subtracting these, as in u , leaves a vector of Λ_A . So $u \in \Lambda_A$, and $|u|_\infty \leq M + g^*$ with $g^* = 1 + \lceil r/2 \rceil$. If $u \neq 0$, then $M \geq \lambda_\infty(\Lambda_A) - g^*$. If $u = 0$, then $a_x = 0$, so every $\xi_{x_d} = 0$, and $a_{z_1} = \xi_{z_2}$, $a_{z_2} = -\xi_{z_1}$. If $\xi_{z_2} = 1$ then $a_{z_2} > 0$ and $a_{z_1} = 1$, so $\xi_{z_1} \in \{0, 1\}$ and $a_{z_2} = -\xi_{z_1} \leq 0$, a contradiction. The case $\xi_{z_2} = -1$ is symmetric, and $\xi_{z_2} = 0$ gives $a_{z_1} = 0$, $\xi_{z_1} = 0$, $a_{z_2} = 0$, contradicting $a \neq 0$. Here the opposite signs of g_{12} and g_{21} give the contradiction, so no dependence of S_{z_i} on its own cell is needed. So $M \geq \lambda_\infty(\Lambda_A) - g^*$, and

Lemma 25(i) gives $\delta N^{1/s} \geq (\lambda_\infty(\Lambda_A) - g^* - 1)p^{-2/s}$. With $\lambda_\infty \geq \rho - 1$ and $g^* = 2$ ($s = 4$), resp. $\lambda_\infty \geq B + 1$ (Lemma 29), this is the claim. For $s = 4$, $\rho \geq 5$ iff $p \geq 23$, and $(\rho - 4)/\sqrt{p} \rightarrow 1$. $\square$

Since $B(p)$ and $\rho(p)$ are nondecreasing, the bounds are positive for every $p \geq p_0$ (Table 4); their limits and the growth of $p_0(s)$ are discussed in Remark 125.

Remark 37 (Comparison with $m \equiv 0$). Seen one digit deeper, the case $m = sk$ fits this picture as the case $\ell = s$: every coordinate is a skeleton coordinate whose skeleton digit is its geometric digit, the occupied fine cells are a translate of all of $p\mathbb{Z}^s$, and the geometric layer $\tilde{M}$ plays the role of the faults; so $1 - K/q$ is the analogue of “ λ_∞ minus faults” (up to the one fine cell more that Lemma 25 loses). Since $p\mathbb{Z}^s$ attains the pigeonhole bound, only the scale of the faults differs: K/q at $r = 0$ against $g^* p^{-\ell/s}$ for $r \neq 0$. This is why the thresholds ($p > 2^s$ for $r = s - 1$; $p \geq 23, 137, 443, 2179, 6101$ for $r = s - 2, s = 4, \dots, 8$) are far below the threshold $5a_s^* + 4 \leq e^{s \log s + O(s)}$ of Theorem A, while at a fixed large p the constants for $r = 0$ are larger: the skeletons gain in the range of p , not in the constant (heuristic comparison).

5.6. Three or more skeleton coordinates. For $\ell = 2$ the frame orbit imposes nothing beyond (N1)–(N3) on skeleton digits of the form in Proposition 27(iii) (Corollary 28). For $\ell \geq 3$ it constrains the skeleton beyond (N1)–(N3).

Lemma 38 (A Plücker identity for skeleton digits). *Let $\ell \geq 3$, let a graph form be obtained from a frame over $\mathbb{F}_p$ by the moves of Lemma 2, and let d be a full coordinate. Let κ_i be the coefficient of S_{z_i} on $x_{d,k}$, g_{ij} that on $z_{j,k-1}$, and $\psi_i = 1/\kappa_i$. Then, for distinct i, j, l ,*

$$g_{ji} g_{lj} \psi_j + g_{ij} g_{li} \psi_i = g_{li} g_{lj} \psi_l.$$

Proof. The moves only scale the entries of the first offset rows on the last cell level, so by Proposition 27(i) these entries form a Cauchy layer $W_{ce} = \lambda_c \mu_e / D_{ce}$ in the places (Section 3), with $W_{z_i z_j} = g_{ij}$ and $W_{z_i x_d} = \kappa_i$. Lemma 18(X) for the coordinates z_i, z_j, z_l, x_d reads $g_{ji} \kappa_l / (\kappa_j g_{li}) + g_{ij} \kappa_l / (\kappa_i g_{lj}) = 1$; multiplying by $g_{li} g_{lj} / \kappa_l$ gives the identity. $\square$

Corollary 39 (Korobov skeleton digits need large faults). *Let $\ell \geq 3$, $k \geq 1$, let d be a full coordinate, and let $\rho, G \geq 1$ be integers with $G^2 < \rho$ and $p > G^2(2\rho^2 + 1)$. Then no graph form obtained from a frame over $\mathbb{F}_p$ by the moves of Lemma 2 has, in the notation of Lemma 38, $\kappa_1, \kappa_2, \kappa_3 \equiv \rho, \rho^2, \rho^3$ and centred g_{ij} with $|g_{ij}| \leq G$ for $i \neq j \leq 3$.*

Proof. Suppose such a graph form exists. The moves multiply every box minor by a unit, so it is a $(0, m, s)$ -net, and $g_{ij} \neq 0$ by (N2). Multiply the identity for $(i, j, l) = (1, 2, 3)$ by ρ^3 : $g_{21} g_{32} \rho + g_{12} g_{31} \rho^2 \equiv g_{31} g_{32} \pmod{p}$. The difference of the two sides is at most $G^2(\rho^2 + \rho + 1) < p$ in absolute value, so the congruence is an equality of integers. Hence $\rho \mid g_{31} g_{32}$. But $0 < |g_{31} g_{32}| \leq G^2 < \rho$, a contradiction. $\square$

The corollary is about nets in the frame orbit, about the coefficients on the last cell level (carry depth 0), about faults bounded by G , and about the Korobov vector (ρ, ρ^2, ρ^3) , the analogue of the skeleton digits of $\mathcal{B}^1$, or any unit multiple of it (the identity of Lemma 38 is homogeneous in ψ). Other Korobov vectors, faults growing with p (harmless while $o(p^{\ell/s})$), and nets outside the frame orbit are not excluded. Lemma 38 and Corollary 39, with the same proofs, hold for every depth vector with all depths at least 1 and any four distinct coordinates in the roles of z_1, z_2, z_3 and x_d , with κ_i and g_{ij} the entries of the first offset rows on the last cell level; this is the form verified in Lean (Appendix F).

For individual primes, other Korobov vectors with faults ± 1 do give nets. Proposition 40 works out one instance in dimension four. Designs of the same kind, found by a finite search, give such nets in dimension four for $m \equiv 1 \pmod{4}$ at every prime $7 \leq p \leq 83$, and in dimension

five for $m \equiv 2 \pmod{5}$ at seven primes $31 \leq p \leq 199$ (computed; these designs are not printed here; they are included in the software deposit, Appendix G, whose scripts do not rerun these checks). So the obstruction of Corollary 39 is specific to the Korobov vector (ρ, ρ^2, ρ^3) ; a family for all large primes with $\ell \geq 3$ skeleton coordinates is open.

Proposition 40 (A Korobov skeleton with faults ± 1 ; computer-assisted). *Let $p = 13$, $s = 4$ and $m = 4k + 1$ with $k \geq 1$, with one full coordinate x of depth $k + 1$ (we write x_l for its level l) and three skeleton coordinates z_1, z_2, z_3 of depth k , and take the frame with the place ∞ for x and the places $0, 1, 3$ for z_1, z_2, z_3 . The skeleton digits*

$$\begin{aligned} S_{z_1} &= 4x_k - 2x_{k-1} + x_{k-2} - z_{1,k-1} - z_{2,k-1} + z_{2,k-2} - z_{3,k-1} + z_{3,k-2}, \\ S_{z_2} &= 7x_k - x_{k-1} - z_{1,k-1} + z_{1,k-2} - z_{3,k-1}, \\ S_{z_3} &= 8x_k - x_{k-1} - z_{1,k-1} + z_{2,k-1} \end{aligned}$$

(terms with nonexistent levels omitted) are reachable from the frame for every $k \geq 1$, so they complete to digital $(0, 4k + 1, 4)$ -nets over $\mathbb{F}_{13}$. Every graph form over $\mathbb{F}_{13}$ with the depths $(k + 1, k, k, k)$ and these skeleton digits, net or not, satisfies $\delta N^{1/4} \geq 3 \cdot 13^{-3/4} > 0.438$ (toroidal).

Proof. Write $\kappa = (4, 7, 8)$, $\beta = (-2, -1, -1)$ and $\eta = (1, 0, 0)$ for the coefficients of the S_{z_i} on $x_k, x_{k-1}, x_{k-2}, g_{ij}$ and H_{ij} for those of S_{z_i} on $z_{j,k-1}$ and $z_{j,k-2}$ ($i \neq j$), and $\alpha = (0, 1, 3)$ for the places of z_1, z_2, z_3 ; all faults g_{ij} are ± 1 .

Reachability. By Proposition 27(i), Propositions 17 and 13 hold for the skeleton rows: column x carries the three rows S_{z_i} and the levels $k, k - 1, k - 2$ (the carry depths $0, 1, 2$), and column z_j carries the two rows S_{z_i} , $i \neq j$, and the levels $k - 1, k - 2$; one vector λ' of row scalars is shared by all columns. The coefficients of S_{z_i} on its own cell are diagonal entries, free by move (a). By Proposition 17 (with $w = 1, y = \alpha_i$ on the column at ∞ , and $w = y = 1/(\alpha_i - \alpha_j)$ on the column z_j), the digits are reachable, with all deeper levels 0, if there are units $\lambda'_i, \mu_x, \mu_{z_j}$ such that, modulo 13: (R1) $\kappa_i = \lambda'_i \mu_x$; $\kappa_i + \beta_i = \lambda'_i(c_0 + c_1 \alpha_i)$ with $c_1 \neq 0$; and $\kappa_i + \beta_i + \eta_i = \lambda'_i G(\alpha_i)$ with $\deg G = 2$; (R2) $g_{ij} = \lambda'_i \mu_{z_j} / (\alpha_i - \alpha_j)$, and $g_{ij} + H_{ij} = \lambda'_i (\alpha_i - \alpha_j)^{-1} (c'_0 + c'_1 / (\alpha_i - \alpha_j))$ with $c'_1 \neq 0$, for each j and the two $i \neq j$. Take $\lambda' = \kappa$ and $\mu_x = 1$. For (R2) at level $k - 1$ each column must give one value of $\mu_{z_j} = g_{ij}(\alpha_i - \alpha_j) / \kappa_i$ for both $i \neq j$: column z_1 needs $7\mu = -1$ and $8\mu = -3$, column z_2 needs $4\mu = 1$ and $8\mu = 2$, column z_3 needs $4\mu = 3$ and $7\mu = 2$, and indeed $(\mu_{z_1}, \mu_{z_2}, \mu_{z_3}) = (-2, -3, 4)$ solves all six. For (R1), $(\kappa_i + \beta_i) / \kappa_i = (2/4, 6/7, 7/8) = (7, 12, 9) = c_0 + c_1 \alpha_i$ with $(c_0, c_1) = (7, 5)$. The remaining conditions say that leading coefficients of interpolation polynomials are nonzero: three values $\lambda'_i G(\alpha_i)$ at distinct α_i always come from a G of degree at most 2, and since $\det[\lambda', \lambda' \odot (c_0 + c_1 \alpha), \lambda' \odot G(\alpha)]$ is $\lambda'_1 \lambda'_2 \lambda'_3 c_1$ times the leading coefficient of G times a Vandermonde determinant, $\deg G = 2$ is equivalent to $\det[\kappa, \beta, \eta] \neq 0$; here $\det[\kappa, \beta, \eta] = 7 \cdot (-1) - 8 \cdot (-1) = 1$. Likewise $c'_1 \neq 0$ in column z_j is equivalent to $g_{ij} H_{lj} - H_{ij} g_{lj} \neq 0$ for $\{i, l\} = \{1, 2, 3\} \setminus \{j\}$, and these are $1, -1, 1$ for $j = 1, 2, 3$. The places $\infty, 0, 1, 3$ are distinct modulo 13. So Proposition 13 gives, for every $k \geq 1$, moves of Lemma 2 that turn the graph form Φ^F of the frame into one with these skeleton digits (truncated for $k = 1$). The box minors of Φ^F are units (Lemma 10), the moves multiply them by units, and Lemma 1 gives the net property.

Separation. Let a be the centred difference of the fine positions of two distinct points (Lemma 25). If some $|a_c| \geq 13/2$, then $|a|_\infty \geq 7$. Otherwise, as $P_x \equiv x_k$ and $P_{z_i} \equiv S_{z_i} \pmod{13}$, Lemma 25(ii) gives

$$a_{z_i} \equiv \kappa_i a_x + \beta_i \xi_{x,1} + \eta_i \xi_{x,2} + \sum_{j \neq i} (g_{ij} \xi_{z_j,1} + H_{ij} \xi_{z_j,2}) - [i = 1] \xi_{z_1,1} \pmod{13},$$

with sign-consistent prefix patterns $(\xi_{c,1}, \xi_{c,2}) \in \{(0, 0), (\text{sgn } a_c, 0), (\text{sgn } a_c, \text{sgn } a_c)\}$ (and $\xi = 0$ for missing levels). We enumerate $|a_x| \leq 6$ and all patterns (4625 combinations, with both signs

for the patterns of the z_i before the sign check; rerun by the scripts of Appendix G), take the centred a_{z_i} and keep the sign-consistent solutions: the least $|a|_\infty$ of a nonzero solution is $M_{13} = 4$. Lemma 25(i) gives $\delta N^{1/4} \geq (M_{13} - 1) 13^{-3/4} = 0.4381 \dots$ $\square$

Without the faults the occupied fine cells of a coarse block would lie on the Korobov lattice $\{u : u_{z_i} \equiv \kappa_i u_x \pmod{13}\}$, whose minimum is $\lambda_\infty = 5$, against the pigeonhole bound $\lfloor 13^{3/4} \rfloor = 6$; the faults ± 1 cost one fine cell. The vector κ is not a unit multiple of (ρ, ρ^2, ρ^3) (as $\kappa_2/\kappa_1 = 5 \neq 3 = \kappa_3/\kappa_2$ modulo 13), in accordance with Corollary 39.

6. DIMENSION THREE, EVERY RESOLUTION

In dimension three the cells can be cubes only for $m \equiv 0 \pmod{3}$, and a frame needs only three places, 0, 1 and ∞ . For $m \equiv 0$ one lower-triangular scramble, applied to all three coordinates of this frame, gives $t = 0$ in every base $q \geq 2$ and the separation $1 - 1/q$ for every $q \geq 8$ (Theorem 45). The scramble is the Toeplitz matrix of $(1 - t)^{-k}$, followed by a matrix that differs from the identity in three rows. It is one integer matrix whose box minors are all ± 1 (Theorem 42), so $t = 0$ holds in every base at once. The other resolutions use the other two regimes of the lattice picture (Section 2): at $m = 3$ one geometric digit shared by all three coordinates (regime III, the column nets, Theorem 49), and for $m \equiv 1, 2 \pmod{3}$ skeleton digits on cells of unequal depths (regime II, Theorem 56, Remark 55). Corollary 57 puts them together.

6.1. $m \equiv 0$: the scramble. Here $s = 3$, $k \geq 2$, $m = 3k$, and Ψ, T are the maps of the Möbius frame. Let $\mathcal{K}$ be the lower-triangular Toeplitz matrix of $(1 - t)^{-k}$: $\mathcal{K}_{ij} = \binom{i-j+k-1}{k-1}$ ($i \geq j$), so $\mathcal{K}[W]_m = [W(1 - t)^{-k}]_m$. The three rows of the second matrix are chosen so that the digit with index k , the first offset digit, depends only on the last two cell digits of each coordinate, through two small matrices (Proposition 43 and the paragraph after its proof). Let $\mathcal{E}$ be the identity except in three rows: for a digit vector d ,

$$(\mathcal{E}d)_{k-2} = d_0 + d_1 + \dots + d_{k-2}, \quad (\mathcal{E}d)_{k-1} = -d_{k-1}, \quad (\mathcal{E}d)_k = d_{k-1} + d_k,$$

and put $L = \mathcal{E}\mathcal{K}$, lower-triangular with diagonal $(1, \dots, 1, -1, 1, \dots, 1)$ (-1 at position $k - 1$).

Definition 41. $\mathcal{P}_{k,q}$ is the digital net over $\mathbb{Z}/q\mathbb{Z}$ with generator matrices (LT^2, L, LT) . For $V \in (\mathbb{Z}/q\mathbb{Z})[t]_{<3k}$ the point has coordinates $\phi_q(d(W))$ for $W = T^2V, V, TV$, where $d(W) = L[W]_m$:

$$\begin{aligned} d_j &= [t^j] W(1 - t)^{-k} \quad (j \notin \{k-2, k-1, k\}), & d_{k-2} &= [t^{k-2}] W(1 - t)^{-k-1}, \\ d_{k-1} &= -[t^{k-1}] W(1 - t)^{-k}, & d_k &= [t^k] (1 + t) W(1 - t)^{-k}. \end{aligned}$$

The same L is applied to all three readings, so $\mathcal{P}_{k,q}$ inherits the cyclic symmetry of the frame. Definition 41 also makes sense for $k = 1$ (row $k - 2$ of $\mathcal{E}$ is absent); then $k = 1$ is covered by Theorem 42 but not by the separation bound, and Figure 16 shows it.

6.2. The net property.

Theorem 42. For every $k \geq 1$, every box minor of (LT^2, L, LT) equals ± 1 . Hence $\mathcal{P}_{k,q}$ is a $(0, 3k, 3)$ -net in base q for every $q \geq 2$.

In words: a box with all its prescribed digits zero asks one binary form of degree $m - 1$ to vanish to total order m at 0, 1 and ∞ , which forces it to be zero. After the re-indexing of Proposition 9 this is Lemma 8 [46, Thm. 6.2]; we give the direct proof, which is also the one formalized.

Proof. From $(\Psi V)(t) = \sum_i v_i(1-t)^{m-1-i}$ one reads off, over any commutative ring: (F1) if $t^j \mid V$ then $\deg \Psi V < m-j$; (F2) if $\deg V < m-j$ then $(1-t)^j \mid \Psi V$. Let $d_1 + d_2 + d_3 = m$ and suppose that, over a field, the first d_1, d_2, d_3 digits of T^2V , V , TV vanish: $t^{d_1} \mid \Psi^2V$, $t^{d_2} \mid V$, $t^{d_3} \mid \Psi V$. Since $V = \pm \Psi(\Psi^2V)$, (F1) gives $\deg V < m - d_1 = d_2 + d_3$; and (F1) applied to ΨV gives $\deg \Psi^2V < m - d_3$, whence $(1-t)^{d_3} \mid V$ by (F2). As $1 = t + (1-t)$, the factors t^{d_2} and $(1-t)^{d_3}$ are coprime, so their product, of degree $d_2 + d_3$, divides V ; hence $V = 0$. So every box minor of the frame is nonzero modulo every prime, i.e. ± 1 ; the scramble multiplies it by ± 1 (1), and Lemma 1 concludes. $\square$

What is specific here is L : it does not change t , but it decides the geometry.

6.3. Cells and the geometric digit. By Theorem 42 with $(d_1, d_2, d_3) = (k, k, k)$ (or directly by the proof of Proposition 43), the first k digits of the three coordinates determine the point. Let $n_c \in \{0, \dots, q^k - 1\}$ be the integer with base- q digits $d_0^c \cdots d_{k-1}^c$ (the *cell index* of coordinate c ; the cell is the box with the indices (n_x, n_y, n_z)), $u_c \equiv d_{k-1}^c$ and $v_c \equiv d_{k-2}^c$ its last two digits, and $r_c \equiv d_k^c$ the *geometric digit*. In cell units (the cell side q^{-k} as unit), coordinate c of the point is

$$n_c + \frac{r_c + f_c}{q}, \quad f_c = \sum_{j>k} (d_j^c \bmod q) q^{k-j} \in [0, 1).$$

Proposition 43. *The geometric digit of each coordinate depends only on the last two cell digits of the three coordinates, and the deeper digits of a coordinate do not depend on its own cell. Precisely, for every V , writing d^x, d^y, d^z for the digit vectors of the three coordinates: (a) $d_k^x = -d_{k-1}^x - d_{k-1}^y + d_{k-1}^z - d_{k-2}^z$; (b) for $j > k$, d_j^x is a function of the cells (n_y, n_z) alone; (c) the same holds after the cyclic shift $(x, y, z) \mapsto (y, z, x)$. Consequently $r \equiv Mu + Jv \pmod{q}$ with*

$$M = \begin{pmatrix} -1 & -1 & 1 \\ 1 & -1 & -1 \\ -1 & 1 & -1 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix},$$

and f_c does not depend on n_c .

Proof. For $\deg F \leq N$ put $\Psi_N F = (1-t)^N F(1/(1-t))$, so $\Psi = \Psi_{m-1}$, and $\Psi_{a+b}(FG) = \Psi_a F \cdot \Psi_b G$ whenever $\deg F \leq a$, $\deg G \leq b$ (on binary forms, Ψ_N is the N -th symmetric power of the matrix g of Section 3). Moreover $\Psi_k t^k = 1$, $\Psi_k(t-1)^k = t^k$, $\Psi_k(1-t)^k = (-t)^k$, $\Psi_k 1 = (1-t)^k$, and for $\deg F < k$, with $\Psi' = \Psi_{k-1}$: $(\Psi'^2 F)(0) = F_{k-1} = (\Psi' F)(1)$. Partial fractions of $V/(t^k(t-1)^k)$ (over $\mathbb{Z}$: divide by the monic $t^k(t-1)^k$, then use a Bézout identity $1 = \alpha t^k + \beta(t-1)^k$ in $\mathbb{Z}[t]$, obtained by expanding $1 = (t - (t-1))^{2k-1}$) give

$$V = A(t-1)^k + B t^k + Q t^k(t-1)^k, \quad \deg A, \deg B, \deg Q < k,$$

and multiplicativity gives

$$\begin{aligned} \Psi V &= \Psi' A \cdot t^k(1-t)^k + \Psi' B \cdot (1-t)^k + \Psi' Q \cdot t^k, \\ \Psi^2 V &= (-t)^k \Psi'^2 A + (-t)^k(1-t)^k \Psi'^2 B + (1-t)^k \Psi'^2 Q. \end{aligned}$$

Write $\psi_j(W) = (\mathcal{K}[W]_m)_j = [t^j] W(1-t)^{-k}$, so that $d(W) = \mathcal{E}(\psi_j(W))_j$.

Cells and (b). Modulo t^k , $V \equiv A(t-1)^k$ and $\Psi V \equiv \Psi' B(1-t)^k$, so the y -cell determines A and the z -cell B (L is lower-triangular with diagonal ± 1 , $(t \mp 1)^k$ are units modulo t^k , and Ψ' is invertible). For $j < k$, $\psi_j(\Psi^2 V) = [t^j] \Psi'^2 Q$, so the x -cell determines Q , and the three cells determine V . For $j \geq k$, $\psi_j(\Psi^2 V) = [t^j] (-t)^k (\Psi'^2 A(1-t)^{-k} + \Psi'^2 B)$ depends on A, B only; as $\mathcal{E}$ changes only rows $k-2, k-1, k$, this is (b).

(a). From the displays, $\psi_k(\Psi^2 V) = (-1)^k(A_{k-1} + B_{k-1})$, $\psi_{k-1}(V) = (-1)^k A_{k-1}$ and, as $\Psi V(1-t)^{-k} \equiv \Psi' B \pmod{t^k}$, $\sum_{j<k} \psi_j(\Psi V) = (\Psi' B)(1) = B_{k-1}$. By the definition of $\mathcal{E}$ (and

$T^2 = \Psi^2$, $T = s_k \Psi$, $d_k^x = -d_{k-1}^x + (-1)^k(A_{k-1} + B_{k-1})$, $d_{k-1}^y = -(-1)^k A_{k-1}$ and $d_{k-2}^z - d_{k-1}^z = s_k B_{k-1}$; with $(-1)^k s_k = -1$ this is (a). Part (c) follows from $T^3 = 1$. $\square$

Among the q^3 cells that agree in all but their last cell digit (so that v is fixed), the points sit at $n + ((Mu + Jv) \bmod q)/q$ up to a jitter f/q : this is the lattice picture of Section 2 with the geometric layer $\tilde{M} = M$, the matrix by which the geometric digits change when the last cell digits move by one step without a carry (Remark 44). The coefficients A_{k-1} and B_{k-1} are the residues at 0 and 1 of the differential $V dt/(t^k(t-1)^k)$, so by (a) the geometric digit is, up to the sign $(-1)^k$ and the own term $-d_{k-1}^x$, the sum of the two finite residues of this differential. $\mathcal{K}$ absorbs the partial-fraction coefficients of $1/(t^k(t-1)^k)$, rows $k-2$, $k-1$ of $\mathcal{E}$ express the two residues in the last two cell digits, and row k installs the diagonal -1 of M .

Figures 5(a) and 16 show slabs of cells with n_z fixed. Up to the jitter, and up to a shift by $\pm 1/q$ where a last cell digit wraps (the carry term ω in (2) below), the points form patches of the square lattice spanned by the (x, y) parts of $(I + M/q)e_x$, $(I + M/q)e_y$. The patches are separated by staircase-shaped slip lines, the traces of the slip planes where a geometric digit wraps (more views in Appendix E).

Remark 44 (Lattice reading). Figure 5 shows the lattice picture for $\mathcal{P}_{k,q}$. On a patch where no geometric digit wraps, the points form, up to the jitter, a piece of a translate of the lattice $\Lambda_q = (I + M/q)\mathbb{Z}^3$ (in cell units). Since $M = -I + [\mathbf{1}]_\times$, where $[\mathbf{1}]_\times E = \mathbf{1} \times E$ is the cross product with $\mathbf{1} = (1, 1, 1)$, Λ_q is $\mathbb{Z}^3$ rotated by $\arctan(\sqrt{3}/(q-1))$ about $\mathbf{1}$, scaled by $1 - 1/q$ along $\mathbf{1}$ and by $((1 - 1/q)^2 + 3/q^2)^{1/2}$ across it; $\det(I + M/q) < 1$. Its shortest vectors are $\pm(I + M/q)e_i$, e.g. $(I + M/q)e_x = (1 - \frac{1}{q}, \frac{1}{q}, -\frac{1}{q})$, of length $\lambda_1(\Lambda_q) = (1 - 2/q + 3/q^2)^{1/2} = 1 - 1/q + O(q^{-2})$: for $E \in \mathbb{Z}^3$, $|(I + M/q)E|^2 = (1 - 1/q)^2|E|^2 + (3/q^2)|E_\perp|^2$ with $E_\perp$ the component orthogonal to $\mathbf{1}$, which is at least $2(1 - 1/q)^2 > 1 - 2/q + 3/q^2$ when $|E|^2 \geq 2$ and $q \geq 3$. The own-axis term $1 - 1/q$ of $c(q)$ is its component along the moving axis. The proof of Theorem 46 uses only this component: the transverse parts $\pm 1/q$ are of the size of the jitter, which may cancel them, so the certified $c(q)$ is below $\lambda_1(\Lambda_q)$. Λ_q has covolume $\det(I + M/q) < 1$, so it has slightly more than one site per cell; reducing Mu modulo q skips the extra sites at the slip planes, so that each cell keeps exactly one point. Theorem 46 bounds the steps coordinatewise and does not use $\lambda_1(\Lambda_q)$.

6.4. The separation bound.

Theorem 45 (Dimension three, $m \equiv 0$). *Let $q \geq 4$ and $k \geq 2$, and let $\mathcal{P}_{k,q}$ be the digital net of Definition 41, with $N = q^{3k}$ points. Then:*

- (1) $\mathcal{P}_{k,q}$ is a $(0, 3k, 3)$ -net in base q (Theorem 42; this holds for every $q \geq 2$);
- (2) every cell $\prod_i [n_i q^{-k}, (n_i + 1)q^{-k})$ contains exactly one point, so $h_{\mathcal{P}} \leq \sqrt{3} N^{-1/3}$;
- (3) the toroidal (hence also the Euclidean) minimum distance satisfies $\delta_{\mathcal{P}} \geq c(q) N^{-1/3}$, where

$$c(q)^2 = \min \left\{ \left(1 - \frac{1}{q}\right)^2, \left(1 - \frac{2}{q}\right)^2 + \left(1 - \frac{4}{q}\right)^2, 3\left(1 - \frac{3}{q}\right)^2 \right\}.$$

In particular $c(q) = 1 - 1/q$ for all $q \geq 8$ (Theorem 46).

The constant is close to sharp for this net: for $q = 8, \dots, 13$ and 16 the exact minimum distance at $m = 6$ exceeds $c(q)$ by less than $4 \cdot 10^{-4}$ (Table 12), and for odd prime q the first-order term $1 - 1/q$ cannot be improved by any digital $(0, 3k, 3)$ -net over $\mathbb{F}_q$, $k \geq 3$, whose geometric layer has bounded entries and a negative diagonal entry (the first-order ceiling, Corollary 78). Compared with Theorem A at $s = 3$ ($a_3^* = 2$), the net $\mathcal{P}_{k,q}$ has $\delta N^{1/3} \geq 1 - 1/q$ against the $1 - 2/q$ of Theorem A, half the loss, and needs no threshold beyond $q \geq 4$. Part (3) is the following theorem, which we state on its own (it is also a separate formal statement) and prove now.

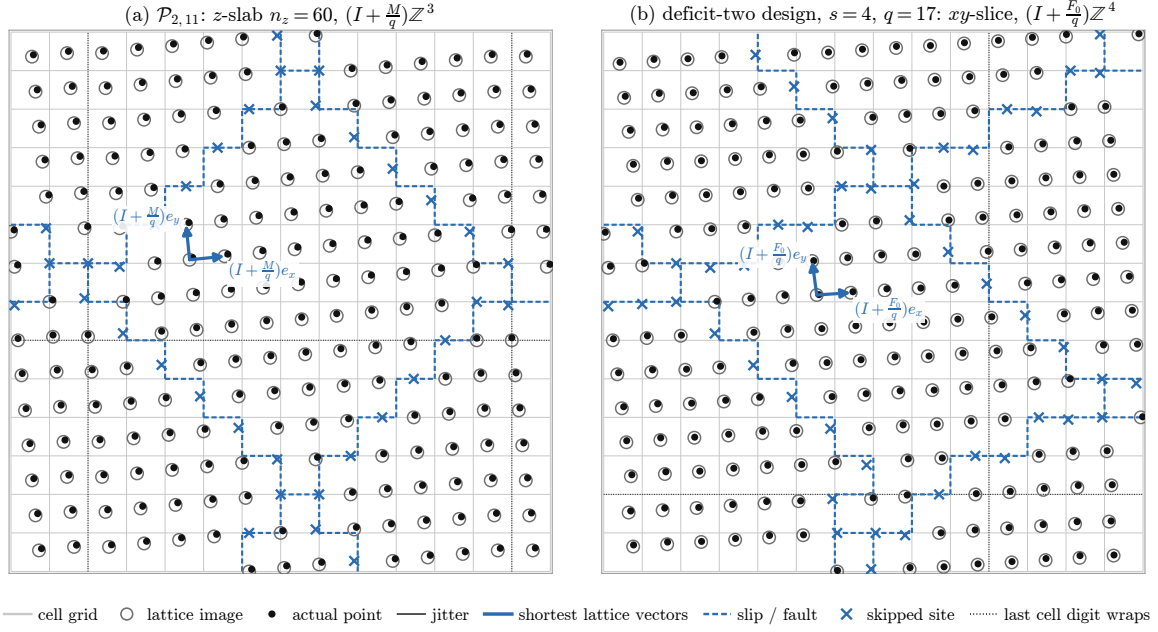


FIGURE 5. Regime I, small-entry layers ($m = sk$). (a) $\mathcal{P}_{2,11}$ ($q = 11$, $k = 2$, $N = 11^6$; Theorem 45): the 196 points with z -cell $n_z = 60$ and (x, y) -cells in a 14×14 window, projected to the xy -plane in cell units. Open circles: the lattice image $n + r/q$, with $r = Mu + Jv \bmod q$ the geometric digit of Proposition 43; dots: the points; grey segments: the jitter ($< 1/q$ per coordinate). Arrows: the (x, y) parts of the shortest vectors $(I + \frac{M}{q})e_x$, $(I + \frac{M}{q})e_y$ of $\Lambda_q = (I + \frac{M}{q})\mathbb{Z}^3$, $\lambda_1(\Lambda_q) = 0.918$ (Remark 44). Dashed: slip edges, where a geometric digit wraps; dotted: cell boundaries where the last cell digit wraps (the term Jv enters); $\times$: skipped sites. As in Figure 1, Λ_q is too dense, $\det(I + \frac{M}{q}) = 0.773 \approx 1 - \frac{3}{q}$: 35 skipped sites against the density surplus 38.8, up to boundary effects. (b) Dimension four: a $(0, 8, 4)$ -net over $\mathbb{F}_{17}$ ($k = 2$, $N = 17^8$) whose row 0 is the deficit-two design over $\mathbb{Z}[1/2]$ (places $\infty, 0, 1, 2$; Section 9.4), xy -slice with $n_z = 144$, $n_w = 96$ fixed; arrows: two of the eight shortest vectors $\pm(I + \frac{F_0}{q})e_c$ of $(I + \frac{F_0}{q})\mathbb{Z}^4$ ($\lambda_1 = 0.888$). Despite the larger base, the entries of size two of F_0 (Remark 82) make the patches smaller and the slips denser than in (a): 68 against 58 slip edges in the same window, and 46 $\times$ against a planar density surplus of 53.5, up to boundary effects. The separation bound of Section 9.4 uses only row 0.

Theorem 46. For $q \geq 4$ and $k \geq 2$, the toroidal minimum distance of $\mathcal{P}_{k,q}$ is at least $c(q)q^{-k}$, with $c(q)$ as in Theorem 45.

Proof. Work in cell units, with two points in cells n and $n + e$ (toroidally). If some $|e_i| \geq 2$, the i -th coordinates differ by at least $1 \geq c(q)$; $e = 0$ is impossible. So let $e \in \{-1, 0, 1\}^3 \setminus \{0\}$, and let ν be the number of moving axes.

The step. For a moving axis d , u_d changes by e_d modulo q , and v_d changes by e_d if u_d wraps ($\omega_d = 1$; this includes the step across the torus boundary, n_d from $q^k - 1$ to 0 or back, where all cell digits wrap; since $k \geq 2$, v_d then still changes by exactly e_d) and is unchanged otherwise

($\omega_d = 0$). Hence $r' - r \equiv \sigma \pmod{q}$ with

$$(2) \quad \sigma_i = -e_i - e_{i+1} + (1 - \omega_{i+2})e_{i+2} \quad (\text{indices mod } 3, x \rightarrow y \rightarrow z),$$

$|\sigma_i| \leq 3$, and $\Delta_i = e_i + ((r'_i - r_i) + (f'_i - f_i))/q$, where $r'_i - r_i \in \{\sigma_i, \sigma_i - q \operatorname{sgn} \sigma_i\}$ ($\{0\}$ if $\sigma_i = 0$), $|f'_i - f_i| < 1$, and $f'_i = f_i$ if only axis i moves (Proposition 43(b)).

Per-coordinate bound. Call a moving coordinate *backward* if $e_i \sigma_i \leq 0$ and *forward* otherwise. For a backward coordinate, $r'_i - r_i = \sigma_i$ gives $|\Delta_i| \geq 1 - (|\sigma_i| + 1)/q$ and $r'_i - r_i = \sigma_i + qe_i$ gives $|\Delta_i| \geq 2 - (|\sigma_i| + 1)/q$; as $q \geq 4 > |\sigma_i|$, both give $|\Delta_i| \geq c_{|\sigma_i|+1}$ with $c_j := 1 - j/q \geq 0$. Forward coordinates, and coordinates that do not move, are only bounded by 0.

Signs. From (2): (i) If $e = \pm e_i$ then $\sigma_i = -e_i$ and there is no jitter, so $\Delta_i \in \{e_i(1 - 1/q), e_i(2 - 1/q)\}$ and $|\Delta| \geq c_1$. (ii) $e_i \sigma_i = -1 - e_i e_{i+1} + (1 - \omega_{i+2})e_i e_{i+2}$ is positive iff $e_{i+1} = -e_i$, $e_{i+2} = e_i$ and $\omega_{i+2} = 0$. So a forward coordinate exists only if $\nu = 3$, and it is unique; then $\sigma_{i+1} = (1 - \omega_i)e_i$ (backward, $|\sigma| \leq 1$) and $\sigma_{i+2} = -(3 - \omega_{i+1})e_i$ (backward, $|\sigma| \leq 3$). (iii) $|\sigma_i| = 3$ forces $e_{i+1} = e_i$, $e_{i+2} = -e_i$, $\omega_{i+2} = 0$, and then $\sigma_{i+2} = (1 - \omega_{i+1})e_i$: backward with $|\sigma| \leq 1$. (iv) If $\nu = 2$ with moving axes $\{i, i+1\}$, both are backward by (ii); either $e_{i+1} = e_i$ and $|\sigma_{i+1}| \leq 1$, or $e_{i+1} = -e_i$ and $\sigma_i = 0$; the other value is at most 2 in absolute value.

Cases. $\nu = 1$: $|\Delta| \geq c_1$ by (i). $\nu = 2$: $|\Delta|^2 \geq c_2^2 + c_3^2$ by (iv). $\nu = 3$ with some backward $|\sigma_i| = 3$: $|\Delta|^2 \geq c_4^2 + c_2^2$ by (iii). $\nu = 3$ with a forward coordinate and all backward $|\sigma| \leq 2$: $|\Delta|^2 \geq c_2^2 + c_3^2$ by (ii). Otherwise three backward coordinates with $|\sigma| \leq 2$: $|\Delta|^2 \geq 3c_3^2$. As $c_3 \geq c_4$, the minimum is $c(q)^2$. For $q \geq 8$, $c_2^2 + c_4^2 \geq c_1^2$ (as $1 - 10x + 19x^2 \geq 0$ for $x = 1/q \leq 1/8$) and $3c_3^2 \geq c_1^2$, so $c(q) = 1 - 1/q$. $\square$

For $s = 3$ and the layer (M, J) of $\mathcal{P}_{k,q}$, the quantity σ of (2) is the σ of Lemma 4, and the proof above is that lemma together with the sign analysis (i)–(iv).

The three terms of $c(q)$ come from an own-axis step, a twisted diagonal $e = \pm(1, 1, -1)$ and the body diagonal; for $q \geq 8$ the own-axis step binds. Dimension three is the largest in which one integer family has $t = 0$ in every base (Remark 59).

6.5. Resolution $m = 3$: column nets. At $m = 3$ a cell is a cube of side q^{-1} , and each coordinate has one cell digit and two offset digits. The nets of this section give all three coordinates the same two offset digits. Then every point is the corner of its cell moved along the body diagonal of the cell, and the net is a union of q^2 lines of points parallel to $\mathbf{1} = (1, 1, 1)$, its *columns* (Figure 6). For such nets the minimum distance can be computed exactly.

Throughout this subsection $q \geq 2$ is an integer, $\mathbf{1} = (1, 1, 1)$, $\Sigma n = n_x + n_y + n_z$ (the coordinate sum, also for steps: $\Sigma E = \sum_c E_c$), and we work on the torus $(\mathbb{Z}/q^3\mathbb{Z})^3$, the integer scale at which a cell has side q^2 ; so $\delta N^{1/3}$ is the toroidal distance divided by q^2 . Let $\mathbb{T} = (\mathbb{Z}/q\mathbb{Z})^3 / \langle \mathbf{1} \rangle$, a group with q^2 elements; the class $[n] \in \mathbb{T}$ of a cell $n \in \{0, \dots, q-1\}^3$ is its *column*. A *column point set* is a set of q^3 points of the torus, one for each cell, at

$$X(n) = q^2 n + \varphi([n]) \mathbf{1}, \quad \varphi : \mathbb{T} \rightarrow \{0, \dots, q^2 - 1\}$$

(the *heights*). The first base- q digits of $X(n)$ are n , so every cell holds exactly one point, whatever the heights. The q points of a column $[n]$ are $q^2(n + t\mathbf{1}) + \varphi([n])\mathbf{1}$, $t = 0, \dots, q-1$: they lie on a closed line of the torus parallel to $\mathbf{1}$, $q^2\sqrt{3}$ apart, and projected along $\mathbf{1}$ the columns stand over the triangular lattice $q^2\Pi_\perp\mathbb{Z}^3$, $\Pi_\perp = I - \frac{1}{3}\mathbf{1}\mathbf{1}^\top$ (the projection along $\mathbf{1}$).

Definition 47 (Column nets). Let $q \geq 5$ with $\gcd(q, 6) = 1$, let $w = (-2, 1, 1)$ if $q \equiv 2 \pmod{3}$ and $w = (-1, -1, 2)$ if $q \equiv 1 \pmod{3}$, and let $a = \frac{1}{3}(q\mathbf{1} + w)$, an integer vector with $a_x + a_y + a_z = q$ (w is forced modulo 3, $w \equiv -q\mathbf{1}$, by the integrality of a , and $w \cdot \mathbf{1} = 0$). The *column net* $\mathcal{C}_q$ is the digital net over $\mathbb{Z}/q\mathbb{Z}$ whose point with index $n \in (\mathbb{Z}/q\mathbb{Z})^3$ has, in every

coordinate c , the three digits

$$n_c, \quad r(n) = a \cdot n, \quad j(n) = n_y - n_x,$$

i.e. the generator matrices with the rows $\mathbf{e}_c$, a and $b := (-1, 1, 0)$.

So $a = (\frac{q-2}{3}, \frac{q+1}{3}, \frac{q+1}{3})$ for $q \equiv 2$ and $a = (\frac{q-1}{3}, \frac{q-1}{3}, \frac{q+2}{3})$ for $q \equiv 1 \pmod{3}$, and the geometric layer is $\tilde{M} = \mathbf{1}a^\top$: one geometric digit, shared by all three coordinates, with entries between $\frac{q-2}{3}$ and $\frac{q+2}{3}$. Because all three coordinates read the same two offset digits, each point lies on the main diagonal of its cell, and the distance between two points depends only on their cells and the difference of these shared digits (Theorem 48). Since $a \cdot \mathbf{1} = q \equiv 0$ and $b \cdot \mathbf{1} = 0$, both shared digits are functions of the column, and the integer coordinates are $X(n) = q^2 n + \varphi([n])\mathbf{1}$ with $\varphi = qr + j$: $\mathcal{C}_q$ is a column point set. The first theorem computes the minimum distance of every column point set.

Theorem 48 (Minimum distance of column point sets). *Let $q \geq 2$, let X be a column point set, and for a direction $i \in \{x, y, z\}$ and a cell n let $\Delta_i([n]) = \varphi([n + \mathbf{e}_i]) - \varphi([n])$. Then the toroidal minimum distance d of X at integer scale q^3 satisfies*

$$d^2 = \frac{2}{3}q^4 + 3g^2, \quad g = \min_{i, [n]} \text{dist}\left(\Delta_i([n]), \frac{2}{3}q^2 + q^2\mathbb{Z}\right),$$

and it is attained by two points in neighbouring columns $[n]$, $[n + \mathbf{e}_i]$. In particular $\delta N^{1/3} \geq \sqrt{2/3}$.

Here $\frac{2}{3}q^2$ is the worst height step: two neighbouring columns whose heights differ by $\frac{2}{3}q^2$ modulo q^2 hold points only $\sqrt{2/3}$ cells apart, and g measures how far every step stays from it.

Proof. Let $n \neq n'$ be cells and D a representative of $X(n') - X(n)$ modulo q^3 . Then $D = q^2 E + \Delta \mathbf{1}$ with an integer vector $E \equiv n' - n \pmod{q}$ and $\Delta = \varphi([n']) - \varphi([n])$; every such E occurs, and the toroidal distance of the pair is the least $|D|$. With $\Sigma E = E_x + E_y + E_z$,

$$|q^2 E + \Delta \mathbf{1}|^2 = q^4 |PE|^2 + \frac{1}{3}(q^2 \Sigma E + 3\Delta)^2, \quad |PE|^2 = \frac{1}{3}((E_x - E_y)^2 + (E_y - E_z)^2 + (E_z - E_x)^2).$$

The three differences $E_x - E_y$, $E_y - E_z$, $E_z - E_x$ are integers with sum 0. If they all vanish, $E = t\mathbf{1}$ with $t \in \mathbb{Z}$; then $n' \equiv n + t\mathbf{1}$ lies in the column of n , $\Delta = 0$, $t \not\equiv 0 \pmod{q}$, and $|D|^2 = 3t^2 q^4 \geq 3q^4$. If one of them has absolute value at least 2, the other two sum to its negative, so the three squares sum to at least 6 and $|D|^2 \geq 2q^4$. Otherwise they are $\pm(1, -1, 0)$ up to order, i.e. $E = \pm \mathbf{e}_i + t\mathbf{1}$ for some i and $t \in \mathbb{Z}$. For $E = \mathbf{e}_i + t\mathbf{1}$ we get $D = q^2 \mathbf{e}_i + U\mathbf{1}$ with $U = \Delta + tq^2$, and

$$|q^2 \mathbf{e}_i + U\mathbf{1}|^2 = (q^2 + U)^2 + 2U^2 = \frac{2}{3}q^4 + 3(U + \frac{1}{3}q^2)^2.$$

As t runs over $\mathbb{Z}$, U runs over $\Delta + q^2\mathbb{Z}$, so the least such value is $\frac{2}{3}q^4 + 3 \text{dist}(\Delta, -\frac{1}{3}q^2 + q^2\mathbb{Z})^2$, and $-\frac{1}{3}q^2 \equiv \frac{2}{3}q^2 \pmod{q^2}$; it is at most $\frac{2}{3}q^4 + 3(\frac{1}{2}q^2)^2 < 2q^4$. A pair with $E = -\mathbf{e}_i + t\mathbf{1}$ is, read backwards, a pair with $E = \mathbf{e}_i - t\mathbf{1}$. Every pair of neighbouring columns occurs (take any cell n and $n' = n + \mathbf{e}_i$), so the minimum over all pairs is $\frac{2}{3}q^4 + 3g^2$. $\square$

Theorem 49 (Resolution $m = 3$). *Let $q \geq 5$ with $\gcd(q, 6) = 1$, and let $\mathcal{C}_q$ be the column net of Definition 47, with $N = q^3$ points.*

- (1) $\mathcal{C}_q$ is a digital $(0, 3, 3)$ -net over $\mathbb{Z}/q\mathbb{Z}$; up to sign, its box minors are 1, a_x , a_y , a_z and $a_x + a_y$ (the last two modulo q ; as integers the minors of the boxes with depth 3 on x , y and z are, up to sign, a_z , a_z and $a_x + a_y$). Every cell of side q^{-1} holds one point, so $h \leq \sqrt{3} N^{-1/3}$.

(2) Its toroidal minimum distance d at integer scale q^3 , and also its Euclidean one, is

$$d^2 = \frac{2}{3}q^4 + 3g^2, \quad 3g = \begin{cases} q^2 - q - 3 & \text{if } q \equiv 2 \pmod{3}, \\ q^2 - 2q & \text{if } q \equiv 1 \pmod{3}, \end{cases}$$

with g as in Theorem 48, that is, $d^2 = q^4 - \frac{2}{3}q^3 - \frac{5}{3}q^2 + 2q + 3$ resp. $q^4 - \frac{4}{3}q^3 + \frac{4}{3}q^2$, and

$$\delta N^{1/3} = 1 - \frac{1}{3q} - \frac{8}{9q^2} + O(q^{-3}) \quad \text{resp.} \quad \delta N^{1/3} = 1 - \frac{2}{3q} + \frac{4}{9q^2} + O(q^{-3}).$$

Two points are closest on the torus if and only if they differ by $\pm D$ modulo q^3 , where $D = \frac{1}{3}(-(2q^2 - q - 3), q^2 + q + 3, -(2q^2 - q - 3))$ for $q \equiv 2$ and $D = \frac{1}{3}(-(2q^2 - 2q), q^2 + 2q)$ for $q \equiv 1 \pmod{3}$.

(3) Within each residue class of q modulo 3, $\delta N^{1/3}$ increases with q . It is 0.9059... at $q = 5$ and 0.9147... at $q = 7$, so $\delta N^{1/3} > 0.9059$ for every such q , and $\delta N^{1/3} > 0.9823$ for every such $q \geq 37$.

Proof. (1) The first rows are $\mathbf{e}_x, \mathbf{e}_y, \mathbf{e}_z$, so $\mathcal{C}_q$ is a graph form with the depths $(1, 1, 1)$, and we use Lemma 2. The box of shape $(1, 1, 1)$ has determinant 1 and puts one point in every cell. A box with depth 2 on c , 1 on c' and 0 on c'' has, up to sign, the determinant $a_{c''}$; as $3a_{c''} = q + w_{c''} \equiv w_{c''} \in \{\pm 1, \pm 2\}$ and $\gcd(q, 6) = 1$, it is a unit. A box with depth 3 on c has, up to sign, the 2×2 minor of the rows a and b on the two columns other than c . Both rows sum to 0 modulo q , so in each of them column c is minus the sum of the other two modulo q , and modulo q all three such minors equal $\pm\mu$ with $\mu = a_x b_y - a_y b_x = a_x + a_y$ (as integers they are $a_x + a_y$ and $\pm a_z$); and $3\mu = 2q + w_x + w_y \equiv -w_z \in \{-1, -2\} \pmod{q}$, a unit. Lemma 1 concludes.

(2) We apply Theorem 48. Let $\bar{b}_i \in \{0, \dots, q-1\}$ be the residue of $b \cdot \mathbf{e}_i$, so $\bar{b} = (q-1, 1, 0)$. A step from the cell n to $n + \mathbf{e}_i$ changes r by a_i and j by $\bar{b}_i$ modulo q , so

$$\Delta_i([n]) = q(a_i - q[r(n) + a_i \geq q]) + (\bar{b}_i - q[j(n) + \bar{b}_i \geq q]).$$

The map $[n] \mapsto (r(n), j(n))$ is a bijection from $\mathbb{T}$ onto $(\mathbb{Z}/q\mathbb{Z})^2$, because μ is a unit; so the two wraps occur independently, in all four combinations (two if $\bar{b}_i = 0$). Modulo q^2 the values of Δ_i are therefore s_i and, if $\bar{b}_i \neq 0$, $s_i - q$, where $s_i = qa_i + \bar{b}_i$, and $3 \operatorname{dist}(\Delta_i, -\frac{1}{3}q^2 + q^2\mathbb{Z})$ is the least value of $|3U + q^2|$ over $U \in s_i + \{0, -q\} + q^2\mathbb{Z}$. Here $3s_i + q^2$ lies between $2q^2 - q + 3$ and $2q^2 + 2q$, so the least value is attained at $U = s_i - q^2$ or $U = s_i - q^2 - q$, where $3U + q^2 = -(2q^2 - 3s_i)$ resp. $-(2q^2 - 3s_i + 3q)$; every other U gives at least $2q^2 - 4q + 3 > q^2 + q$. The values $2q^2 - 3s_i$ for $i = x, y, z$ are

$$q^2 - q + 3, \quad q^2 - q - 3, \quad q^2 - q \quad (q \equiv 2), \quad q^2 - 2q + 3, \quad q^2 + q - 3, \quad q^2 - 2q \quad (q \equiv 1),$$

all positive, and adding $3q$ only increases them. So $3g$ is the least of them, $q^2 - q - 3$ resp. $q^2 - 2q$, attained only at $i = y$ (resp. $i = z$) with $U = s_i - q^2$, and Theorem 48 gives $d^2 = \frac{2}{3}q^4 + 3g^2$. The closest differences are then $\pm(q^2\mathbf{e}_i + U\mathbf{1}) = \pm D$ modulo q^3 . The Euclidean minimum distance is at least d , and it is attained without a wrap: $\varphi([\mathbf{1}]) = 0$ and $\varphi([\mathbf{e}_i]) = qa_i + \bar{b}_i = s_i$, so the points of the cells $\mathbf{1}$ and $\mathbf{e}_i$ differ by $q^2(\mathbf{e}_i - \mathbf{1}) + s_i\mathbf{1} = q^2\mathbf{e}_i + (s_i - q^2)\mathbf{1} = D$ exactly. The expansions follow from $(\delta N^{1/3})^2 = \frac{2}{3} + \frac{1}{3}(3g/q^2)^2$.

(3) $3g/q^2 = 1 - \frac{1}{q} - \frac{3}{q^2}$ resp. $1 - \frac{2}{q}$ is positive and increases with q . The values at $q = 5$ and 7 are $\sqrt{513}/25$ and $\sqrt{2009}/49$, and at $q = 37$ (the least $q \geq 37$ coprime to 6, in the class $q \equiv 1$; the least in the other class is 41, with 0.9913...) it is 0.9823... $\square$

Locally a reflected cube. In cell units the point of cell n is $n + \frac{\varphi([n])}{q^2}\mathbf{1}$: it lies on the body diagonal of its cell. As $a/q = \frac{1}{3}\mathbf{1} + \frac{1}{3q}w$, two points whose cells differ by a bounded E differ, in

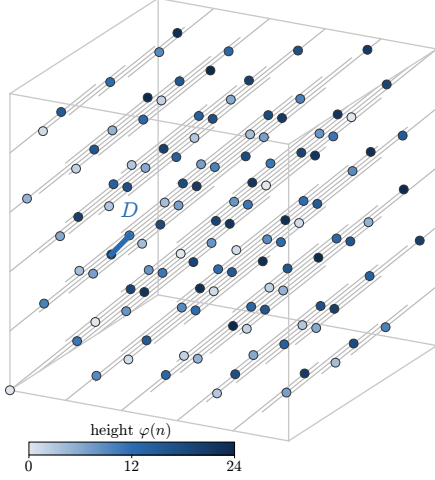
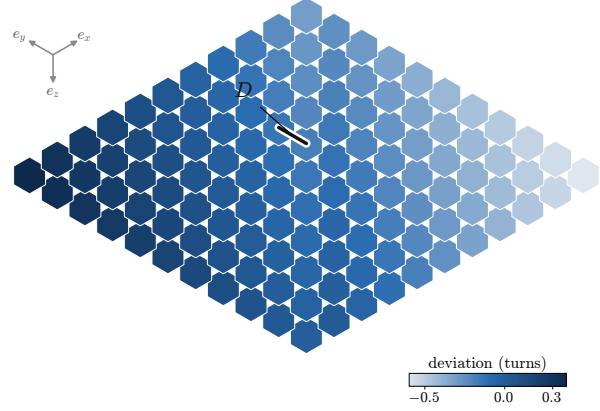
(a) $\mathcal{C}_5$: 125 points on 25 columns parallel to $(1, 1, 1)$ (b) $\mathcal{C}_{11}$ along $(1, 1, 1)$: deviation from $H\mathbb{Z}^3$ 

FIGURE 6. Column nets (Definition 47), in cell units. (a) The 125 points of $\mathcal{C}_5$ on the torus $[0, 5)^3$. Each lies on the body diagonal of its cell, and the points of one column lie on a closed line parallel to $(1, 1, 1)$ (grey; the 25 columns wrap around the torus). Shade: the height $\varphi(n) = qr(n) + j(n)$. Accent: a closest pair; every closest pair differs by $\pm D$, $D = (-14, 11, -14)$ at integer scale q^3 , $|D|^2 = 513$, $\delta N^{1/3} = 0.9059\dots$ (Theorem 49; checked against all pairs). (b) $\mathcal{C}_{11}$ viewed along $(1, 1, 1)$, one period: every column projects to one site of the triangular lattice $P\mathbb{Z}^3$ (a hexagon each). The points of a column are $\sqrt{3}$ apart, and their common height modulo $\sqrt{3}$ is, in turns, $\frac{2}{3}\Sigma n$ for the reflected cube $H\mathbb{Z}^3$ plus the deviation shown, $\frac{w \cdot n}{3q} + \frac{j(n)}{q^2}$ for the cell $n = (x, y, 0)$ of the column, a linear ramp (the drift) with a small ripple (the jitter of the third digit; checked for every column). Across one period the ramp gains $\frac{1}{3}w_c$ of a turn along e_c , which is not an integer, since $3 \nmid q$: an ideal reflected cube cannot close up on the torus, and the drift spreads the mismatch (Section 11). Black: a closest pair of $\mathcal{C}_{11}$, $|D|^2 = 13577$, between neighbouring columns. Interactive version: [explainers/anatomy.html](#) (Section 1).

cell units, by

$$E + \left(\frac{\Sigma E}{3} + z + \frac{w \cdot E}{3q} \right) \mathbf{1} + \frac{\Delta j}{q^2} \mathbf{1}$$

for an integer z (the wrap of r) and the change $\Delta j \in (-q, q)$ of the third digit. This is an $O(1/q)$ perturbation, *along* $\mathbf{1}$, of the point $E + \frac{z'}{3} \mathbf{1}$, $z' = \Sigma E + 3z$, of the set $\{E + \frac{z'}{3} \mathbf{1} : z' \equiv \Sigma E \pmod{3}\} = H\mathbb{Z}^3$, where $H = I - \frac{2}{3} \mathbf{1} \mathbf{1}^\top$ (for $v = E - \frac{z' + 2\Sigma E}{3} \mathbf{1}$ one checks $Hv = E + \frac{z'}{3} \mathbf{1}$). Here $-H$ is the rotation by 180° about the main diagonal, so $H\mathbb{Z}^3 = -H\mathbb{Z}^3$ is the cubic lattice turned half a turn about $\mathbf{1}$; we call it the *reflected cube*. It has covolume 1, minimum 1 and minimal vectors $\pm H\mathbf{e}_c = \pm(\mathbf{e}_c - \frac{2}{3}\mathbf{1})$.

Stacking. Seen along $\mathbf{1}$, both $\mathbb{Z}^3$ and $H\mathbb{Z}^3$ are the triangular lattice $\Pi_\perp \mathbb{Z}^3$ (a copy of A_2) with lines of points of period $\sqrt{3}$ over each site. In $\mathbb{Z}^3$ the line over the neighbour $\Pi_\perp \mathbf{e}_i$ is raised by $\frac{1}{3}$ of the period, in $H\mathbb{Z}^3$ by $\frac{2}{3}$, i.e. lowered by $\frac{1}{3}$ (in crystallographic terms, the stackings ABC and ACB of triangular planes). If neighbouring columns had equal heights (the stacking AA),

points would be only $\sqrt{2/3}$ apart. In the notation of Theorem 48, the height steps of $\mathbb{Z}^3$ and of $H\mathbb{Z}^3$ are $\Delta \equiv 0$ and $\Delta \equiv \frac{1}{3}q^2 \pmod{q^2}$, both at distance $\frac{1}{3}q^2$ from this worst step $\frac{2}{3}q^2$; the theorem measures every step by its distance from it.

Drift and jitter. The two perturbations are a *drift* $\frac{w \cdot E}{3q}$, linear in E and zero on $\mathbf{1}$, and a *jitter* $\Delta j/q^2$ of the third digit. Both are along $\mathbf{1}$, so the columns are exact and only the heights deviate from the ideal, by $O(1/q)$. Section 11 shows that the losses $\frac{1}{3q}$ and $\frac{2}{3q}$ of Theorem 49(2) are forced, and that $\mathcal{C}_q$ is optimal among all column nets: going once around the torus along an axis takes q steps, the ideal step of $H\mathbb{Z}^3$ is a third of the period, and $q/3$ is not an integer when $3 \nmid q$, so the heights must deviate somewhere. Globally the set is not a lattice, since $qH\mathbf{e}_c \notin \mathbb{Z}^3$: at the wraps of r the points jump back into their cells, and these are the slip planes of the column nets (Figure 7). The drift vanishes on $\mathbf{1}$ because $a \cdot \mathbf{1} = q$, the condition that q steps along $\mathbf{1}$ close up; this is what makes r a function of the column.

The column structure is special to $m = 3$. The following box count, which holds for every net, digital or not, shows that at every other resolution not even two coordinates can share the first offset digit (the geometric digit).

Lemma 50 (Shared digits). *Let P be a $(0, m, s)$ -net in base q , digital or not, $j \geq 0$, and $a \neq b$ two coordinates. If $2(j+1) \leq m$, then the pair of the digits with index j of a and of b takes every value in $\{0, \dots, q-1\}^2$ at exactly q^{m-2} points of P . In particular, if f is a map of digits such that for every point of P the digit with index j of coordinate b equals f of the digit with index j of coordinate a , then $2(j+1) > m$.*

Proof. Let $2(j+1) \leq m$ and choose the depths $d_a = j+1$, $d_b = m-j-1 \geq j+1$ and $d_c = 0$ for the other coordinates. Prescribing the digits $0, \dots, j$ of a and of b fixes the coordinate a of an elementary box of this shape and the first $j+1$ digits of its coordinate b , and leaves $q^{m-2(j+1)}$ choices for the other digits of b ; by $t = 0$ each such box holds exactly one point. So each prescription is met by q^{m-2j-2} points, and each value of the pair of digits with index j by $q^{2j} \cdot q^{m-2j-2} = q^{m-2}$ points. A map f as stated would leave the values (α, β) , $\beta \neq f(\alpha)$, unmet. $\square$

For $s = 3$ and $m = 3k$ the geometric digit has the index k , and $2(k+1) > 3k$ only for $k = 1$; so for $k \geq 2$ no two coordinates of a $(0, 3k, 3)$ -net can read the same geometric digit, let alone all three, and column nets exist only at $m = 3$. At the other resolutions $m \geq 4$ the lemma likewise excludes two coordinates that agree at the digit with index $\lfloor m/3 \rfloor$, since $2(\lfloor m/3 \rfloor + 1) \leq m$. So once $2(j+1) \leq m$ the lemma excludes every relation between the digits with index j of two coordinates, functional or not; it says nothing about relations among three coordinates, such as the rank-one layers of Section 13.3 (Remark 123(7)).

At $m = 3$ the third digit does not matter at first order: with the shared second digit of a reflected-cube layer and an arbitrary third digit in each coordinate, $\delta N^{1/3} = 1 - O(1/q)$.

Proposition 51 (Arbitrary third digits). *Let $q \geq 2$, let $w \in \mathbb{Z}^3$ with $w_x + w_y + w_z = 0$ and $w_c \equiv -q \pmod{3}$, $a = \frac{1}{3}(q\mathbf{1} + w)$, and $\beta \in \mathbb{Z}$. Let P be a set of q^3 points of the torus $(\mathbb{Z}/q^3\mathbb{Z})^3$, one for each cell $n \in \{0, \dots, q-1\}^3$, at*

$$X(n) = q^2 n + q r(n) \mathbf{1} + j(n), \quad r(n) \in [0, q), \quad r(n) \equiv a \cdot n + \beta \pmod{q}, \quad j(n) \in [0, q)^3$$

(integers; j arbitrary). Then any two distinct points of P have toroidal distance at least $q^2 - ((\|w\|_1 + 3)q - 3)/\sqrt{3}$.

Proof. Let $n \neq n'$ and let $D = q^2 E + q \Delta r \mathbf{1} + \Delta j$ be a representative of $X(n') - X(n)$ modulo q^3 , with an integer vector $E \equiv n' - n \pmod{q}$, $\Delta r \in (-q, q)$ and $\Delta j \in (-q, q)^3$. If some $|E_c| \geq 2$, then $|D_c| \geq 2q^2 - q(q-1) - (q-1) > q^2$. So let $E \in \{-1, 0, 1\}^3 \setminus \{0\}$ and $\Sigma E = E_x + E_y + E_z$.

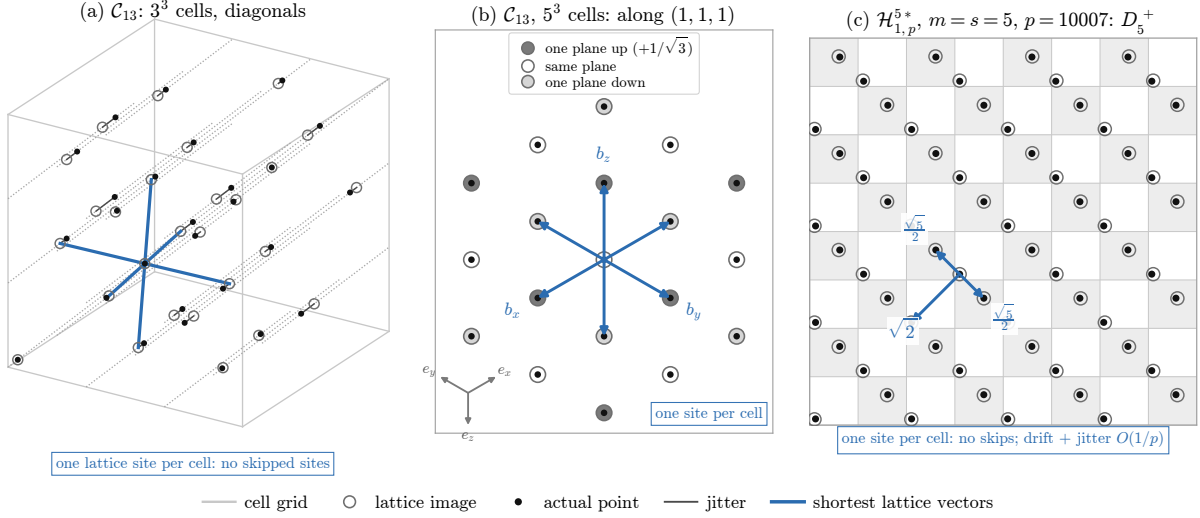


FIGURE 7. Regime III, large-entry layers ($m = s$). (a) The column net $\mathcal{C}_{13}$ (Theorem 49, $a = (4, 4, 5)$, $w = (-1, -1, 2)$): the 3^3 cells around $n = (8, 8, 3)$. All three coordinates read the same two offset digits, so each point lies exactly on the body diagonal of its cell (dotted), at the fraction $\varphi(n)/p^2$ of it, which changes by $\frac{1}{3} + \frac{w \cdot E}{3p}$ from cell to cell, up to the jitter $\Delta j/p^2$. Open circles: the reflected cube $H\mathbb{Z}^3$, $H = I - \frac{2}{3}\mathbf{1}\mathbf{1}^\top$, anchored at the central point; accent: its six minimal vectors $\pm H e_c$; grey segments: drift and jitter, both along $(1, 1, 1)$. (b) The same net, the 5^3 cells around n , viewed along $(1, 1, 1)$: the lattice points within one plane spacing $1/\sqrt{3}$ of the centre along $(1, 1, 1)$ (fill: the plane $x + y + z = \text{const}$). The three neighbours one plane up, $-H e_c$, project opposite to the cell axes e_c (grey), whereas in $\mathbb{Z}^3$ they are the e_c themselves: $H\mathbb{Z}^3$ is $\mathbb{Z}^3$ turned half a turn about $(1, 1, 1)$. Drift and jitter run along $(1, 1, 1)$ and are invisible here: every drawn point projects exactly onto its site, and differs from its site of the anchored lattice by less than 0.15 of a cell in each coordinate. (c) Dimension five: the net $\mathcal{H}_{1,p}^{5*}$ of Proposition 122 with $k = 1$ ($m = s = 5$), $p = 10007$, a $(0, 5, 5)$ -net over $\mathbb{F}_p$: the xy -slice of an 8×8 window of cells, the other three cells fixed. Its layer F_0 lies in $\frac{1}{2} + \mathbb{Z}$, so by the parity of Σn the point sits at $n + c_0$ or, in the shaded cells, at $n + c_0 + \frac{1}{2}\mathbf{1}$, for one fixed $c_0 \in [0, 1)^5$ (here $c_0 \approx 0.10$ in x and y), up to drift and jitter below 0.04 of a cell: locally the packing D_5^+ , whose minimum $\sqrt{5}/2 > 1$ (a step to a cell of the other parity) exceeds the cubic value 1; a diagonal step within one parity has length $\sqrt{2}$ (Proposition 115 with $k = 1$). In all three panels the limit lattice has covolume 1 and one site in each drawn cell: no site is skipped, and the net departs from the lattice only by the $O(1/p)$ drift and jitter.

The constant β cancels: $\Delta r \equiv a \cdot E \pmod{q}$, and $3a \cdot E = q\Sigma E + w \cdot E$, so $3\Delta r = w \cdot E + zq$ with an integer $z \equiv \Sigma E \pmod{3}$. Hence $v = E - \frac{z+2\Sigma E}{3}\mathbf{1}$ is an integer vector with $Hv = E + \frac{z}{3}\mathbf{1}$, and

$$3D = 3q^2E + q(w \cdot E + zq)\mathbf{1} + 3\Delta j = 3q^2Hv + R, \quad R = q(w \cdot E)\mathbf{1} + 3\Delta j,$$

with $|R_c| \leq q\|w\|_1 + 3(q-1)$, since $|w \cdot E| \leq \|w\|_1$. If $v \neq 0$, then $|D| \geq q^2|Hv| - |R|/3 \geq q^2 - ((\|w\|_1 + 3)q - 3)/\sqrt{3}$, as H is orthogonal. If $v = 0$, then $E = t\mathbf{1}$ with $3t = z + 2\Sigma E = z + 6t$, so $z = -3t$ and, as $w \cdot \mathbf{1} = 0$, $\Delta r = -tq$; then $|\Delta r| < q$ forces $t = 0$, i.e. $E = 0$, a contradiction. $\square$

For $\mathcal{C}_q$, $\|w\|_1 = 4$, and the bound is $\delta N^{1/3} \geq 1 - (7q - 3)/(\sqrt{3}q^2)$ whatever the third digits. The constant β is what a digital shift with equal second digits in the three coordinates adds to the shared digit; since β is arbitrary, the proposition also covers these shifts. Shifts whose second digits differ change the picture:

Proposition 52 (Every digital shift at $m = 3$). *Let $q \geq 5$ with $\gcd(q, 6) = 1$, let τ be a digital shift of $\mathcal{C}_q$ (Definition 7) with the digits $\tau_{c,1}, \tau_{c,2}, \tau_{c,3}$ in coordinate c (the first, second and third digit), and put $W = 2$ if $q \equiv 2 \pmod{3}$ and $W = 4$ if $q \equiv 1 \pmod{3}$ ($W/(3q)$ is the largest distance of a_i/q or $2a_i/q$ from $\frac{1}{3}$ or $\frac{2}{3}$ that occurs; see the proof), and $a_{\max} = \max_c a_c$. The toroidal minimum distance of $\mathcal{C}_q \oplus \tau$ satisfies:*

- (1) if $\tau_{x,2} = \tau_{y,2} = \tau_{z,2}$ and $\tau_{x,3} = \tau_{y,3} = \tau_{z,3}$, it equals that of $\mathcal{C}_q$ (Theorem 49(2));
- (2) if $\tau_{x,2} = \tau_{y,2} = \tau_{z,2}$, then $\delta N^{1/3} \geq 1 - (7q - 3)/(\sqrt{3}q^2)$;
- (3) for every τ ,

$$\delta N^{1/3} \geq \frac{1}{\sqrt{3}} \left(1 - \frac{W+3}{q} + \frac{3}{q^2} \right),$$

which exceeds 0.4693 for every $q \geq 37$; and if $\tau_{x,2}, \tau_{y,2}, \tau_{z,2}$ are not all equal, then $\delta N^{1/3} \leq \sqrt{3}(q a_{\max} + q - 1)/q^2 = \frac{1}{\sqrt{3}} \left(1 + \frac{3+w_{\max}}{q} - \frac{3}{q^2} \right)$, $w_{\max} = \max_c w_c$.

The lower bounds of (2) and (3), and the value of (1) as a lower bound, hold for the Euclidean minimum distance too, which is at least the toroidal one; so does the upper bound of (3), which is witnessed by a pair that does not wrap.

Proof. Shifted digits. By Lemma 67, after re-indexing by the cells, the point of cell n of $\mathcal{C}_q \oplus \tau$ has, in coordinate c , the digits $n_c, r_c(n) \equiv a \cdot n + \beta_c$ and $j_c(n) \equiv b \cdot n + \beta'_c$ with $\beta_c = \tau_{c,2} - a \cdot \tau_1$ and $\beta'_c = \tau_{c,3} - b \cdot \tau_1$, $\tau_1 = (\tau_{x,1}, \tau_{y,1}, \tau_{z,1})$. So the β_c are congruent if and only if the $\tau_{c,2}$ are equal, and likewise for β'_c and $\tau_{c,3}$.

(1) Then $X(n) = q^2n + \varphi'([n])\mathbf{1}$ with $\varphi' = qr + j$, $r = (a \cdot n + \beta) \bmod q$, $j = (b \cdot n + \beta') \bmod q$: a column point set. The map $[n] \mapsto (r, j)$ is still a bijection onto $(\mathbb{Z}/q\mathbb{Z})^2$, so in the proof of Theorem 49(2) the same values Δ_i occur, and Theorem 48 gives the same d .

(2) Proposition 51 with $\|w\|_1 = 4$.

(3) *Lower bound.* Let $n \neq n'$ and $D = q^2E + q\Delta r + \Delta j$ a representative, now with $\Delta r = (\Delta r_c)_c \in (-q, q)^3$. If some $|E_c| \geq 2$, then $|D_c| > q^2$. So let $E \in \{-1, 0, 1\}^3 \setminus \{0\}$, and let $\vartheta \in [0, q)$ be the residue of $a \cdot E$. The constants β_c cancel: $\Delta r_c \equiv a \cdot E$ and $|\Delta r_c| < q$, so $\Delta r_c = \vartheta - q\omega_c$ with $\omega_c \in \{0, 1\}$ ($\omega = 0$ if $\vartheta = 0$). Hence $D = q^2u + \Delta j$ with $u = E - \omega + \theta\mathbf{1}$, $\theta = \vartheta/q$, and $|D| \geq q^2|u| - \sqrt{3}(q-1)$. Every u_c lies in $\theta + \mathbb{Z}$, so $|u_c| \geq \|\theta\|$, the distance from θ to the nearest integer, and $\theta \equiv (a \cdot E)/q \pmod{1}$. If $\Sigma E = 0$, then $E = \pm(\mathbf{e}_c - \mathbf{e}_d)$, the two moving coordinates of u are $\pm(\theta + \{0, 1\})$ and $\pm(\theta - \{1, 2\})$, and $|u|^2 \geq \theta^2 + (1 - \theta)^2 \geq \frac{1}{2}$. If $E = \pm\mathbf{1}$, then $\vartheta = 0$ and $|u| = \sqrt{3}$. Otherwise, up to sign, $E = \mathbf{e}_i$ or $E = \mathbf{1} - 2\mathbf{e}_i$ or $E = \mathbf{1} - \mathbf{e}_i$, with $a \cdot E \equiv a_i, -2a_i, -a_i$ respectively. As $3a_i = q + w_i$ with $0 < a_i < \frac{q}{2}$, $\|a_i/q\| = \frac{q+w_i}{3q}$ and $\|2a_i/q\| = \min(\frac{q-2w_i}{3q}, \frac{2q+2w_i}{3q})$; over the entries $w_i \in \{-2, 1\}$ resp. $\{-1, 2\}$ the least of these is $\frac{q-W}{3q}$. So $|u| \geq \sqrt{3}\|\theta\| \geq (q - W)/(\sqrt{3}q)$ in these cases, which is also less than $\frac{1}{\sqrt{2}}$ and $\sqrt{3}$. Therefore $|D| \geq q(q - W)/\sqrt{3} - \sqrt{3}(q - 1) = (q^2 - (W + 3)q + 3)/\sqrt{3}$ for every pair, which is the bound. It increases with q within each residue class; for $q \geq 37$ its least value is 0.4693... at $q = 37$ ($W = 4$), and 0.5079... at $q = 41$ in the class $W = 2$.

Upper bound. Put $b_c \equiv -\beta_c \pmod{q}$; they are not all equal. Along $\mathbf{e}_c$ the shared digit changes by a_c , and r_d wraps if and only if $\vartheta = a \cdot n \pmod{q}$ lies in the cyclic interval $J_d^{(c)} = \{b_d - a_c, \dots, b_d - 1\}$ of a_c consecutive residues of $\mathbb{Z}/q\mathbb{Z}$. We find c and a residue ϑ that lies in $J_c^{(c)}$ and in no $J_d^{(c)}$, $d \neq c$. If the b_d are distinct, let $g_c \geq 1$ be the distance from b_c forward around $\mathbb{Z}/q\mathbb{Z}$ to the next of them. The gaps sum to $q = a_x + a_y + a_z$, so $g_c \geq a_c$ for some c ; then $\vartheta = b_c - 1$ lies in $J_c^{(c)}$, and it lies in $J_d^{(c)}$ only if b_d is at forward distance at most $a_c - 1$ from b_c , which no b_d is. If exactly two of them are equal, $b_d = b_{d'} \neq b_c$, then $J_c^{(c)}$ and $J_{d'}^{(c)} = J_d^{(c)}$ are two different cyclic intervals of the same length $a_c < q$, so neither contains the other. Take a cell n with $n_c = 0$ and $a \cdot n \equiv \vartheta$ (possible, as the entries a_d , $d \neq c$, are units) and $n' = n + \mathbf{e}_c$, so that the pair does not wrap in the cell digits. Then $\Delta r_c = a_c - q$ and $\Delta r_d = a_c$ for $d \neq c$, so the representative with $E = \mathbf{e}_c$ is $D = q^2 \mathbf{e}_c + q(a_c \mathbf{1} - q \mathbf{e}_c) + \Delta j = q a_c \mathbf{1} + \Delta j$, and $|D| \leq \sqrt{3}(q a_{\max} + q - 1)$. $\square$

So the exact minimum distance of $\mathcal{C}_q$ survives exactly the digital shifts whose digits agree in the three coordinates on the two shared digits, the first-order value 1 survives those that agree on the geometric digit, and the others give $1/\sqrt{3}$ at first order. Unequal second shift digits make the three coordinates wrap at different cells, so the shared digit no longer moves all three coordinates together, and a step across a wrap of one coordinate alone is short; Remark 99 explains why the value then drops to $1/\sqrt{3}$. The constants of Corollary 57 below survive every shift (Section 8).

6.6. $m \equiv 1, 2$: lattice skeletons. For $s = 3$ the residue $m \equiv 2$ ($\ell = 1$ skeleton coordinate) is the case $s = 3$ of Theorem 33. The residue $m \equiv 1$ ($\ell = 2$ skeleton coordinates, $r = 1$) needs a different lattice, since Theorem 35 needs $s \geq 4$: here the occupied fine cells form, in each coarse block, a coset of the Korobov lattice with generating vector $(1, \rho, \rho^2)$ modulo p . We realize both on the Möbius frame (Ψ^2, I, Ψ) of Section 3 (Definition 41 used $T = \pm\Psi$; the sign does not matter here). It is defined for every m , and the proof of Theorem 42 does not use $3 \mid m$ (only (F1), (F2) and $\Psi^3 = \pm 1$), so all its box minors are ± 1 and it has an integer graph form Φ^F with depths $\mathbf{k}$.

Notation. The *column block* x consists of the blocks Φ_{cx} , $c \in \{x, y, z\}$, which multiply the cell index n_x ; its columns are the levels x_l , $0 \leq l < k_x$, of n_x (level l of n_x). We write $Y0|x_l$ for the entry of the first offset row of y on the level l of n_x , and so on, and “box (d_x, d_y, d_z) ” for the elementary box with these depths. We modify Φ^F modulo p by the moves of Lemma 2: inside a column block, adding multiples of less significant levels to a level or scaling a level by a unit (move (c)); scaling single off-diagonal blocks (move (b)); and setting diagonal blocks (move (a)). Every pivot used below is a nonzero entry or 2×2 minor, because by Lemma 2 it is the box minor of the frame for the box indicated, which is ± 1 .

Definition 53. Let ρ be an integer with $\rho \not\equiv 0 \pmod{p}$.

($\mathcal{B}^2$) $\mathbf{k} = (k+1, k+1, k)$; the recipe of Proposition 27(ii) with $\kappa = (\rho, \rho^2)$. In column block x : $Z0|x_k \neq 0$ (box $(k, k+1, k+1)$); subtract multiples of level x_k from every level x_l , $l < k$, so that $Z0|x_l = 0$, then scale level x_k so that $Z0|x_k = \rho$. In column block y the same, with pivot $Z0|y_k$ (box $(k+1, k, k+1)$) and target ρ^2 . Set all diagonal blocks to 0. The result is the digital net $\mathcal{B}_{k,p,\rho}^2$ over $\mathbb{F}_p$; its skeleton digit is

$$S_z \equiv \rho x_k + \rho^2 y_k \pmod{p}.$$

($\mathcal{B}^1$) $\mathbf{k} = (k+1, k, k)$. The goal is a graph form whose skeleton digits are $S_y \equiv \rho x_k + z_{k-1}$ and $S_z \equiv \rho^2 x_k + x_{k-1} + y_{k-1} - z_{k-1} \pmod{p}$, with every box minor a unit; the steps are as follows. Column block x : the matrix $\begin{pmatrix} Y0|x_k & Y0|x_{k-1} \\ Z0|x_k & Z0|x_{k-1} \end{pmatrix}$ is invertible (box $(k-1, k+1, k+1)$);

call its determinant Δ ; use the levels x_k, x_{k-1} to make $Y0$ and $Z0$ vanish on the levels $l < k-1$; then add a multiple of x_k to x_{k-1} so that $Y0|x_{k-1} = 0$. Now $Y0|x_k \neq 0$ (box $(k, k+1, k)$), $Z0|x_k \neq 0$ (box $(k, k, k+1)$) and $Z0|x_{k-1} = \Delta/Y0|x_k \neq 0$. Scale the block Φ_{zx} so that $Z0|x_{k-1} = 1$, the level x_k so that $Z0|x_k = \rho^2$, and the block Φ_{yx} so that $Y0|x_k = \rho$. Column block y : with the pivot $Z0|y_{k-1} \neq 0$ (box $(k+1, k-1, k+1)$) make $Z0|y_l = 0$ for $l < k-1$ and scale Φ_{zy} so that $Z0|y_{k-1} = 1$. Column block z : the same for $Y0|z$ (box $(k+1, k+1, k-1)$). Diagonal blocks: $Z0|z_{k-1} = -1$ and all other entries 0. The result is $\mathcal{B}_{k,p,\rho}^1$; its skeleton digits are

$$S_y \equiv \rho x_k + z_{k-1}, \quad S_z \equiv \rho^2 x_k + x_{k-1} + y_{k-1} - z_{k-1} \pmod{p}.$$

The levels and blocks not mentioned keep the values of Φ^F modulo p . Each net is obtained by finitely many explicit elementary operations on the explicit integer matrix Φ^F , and only the skeleton digits matter for the separation proofs below.

Proposition 54. *For every prime p , every $k \geq 1$ and every $\rho \not\equiv 0 \pmod{p}$, $\mathcal{B}_{k,p,\rho}^2$ is a $(0, 3k+2, 3)$ -net and $\mathcal{B}_{k,p,\rho}^1$ is a $(0, 3k+1, 3)$ -net over $\mathbb{F}_p$.*

Proof. Every box minor of Φ^F is ± 1 , and each move multiplies every box minor by a unit of $\mathbb{F}_p$ (Lemma 2; the targets $\rho, \rho^2, 1$ and the pivots are units). Lemma 1 completes the proof. $\square$

Remark 55 (Dimension three, $m \equiv 2 \pmod{3}$). For $s = 3$ the recipes of Definitions 34 and 53($\mathcal{B}^2$) coincide (Proposition 27(ii) with $\kappa = (\rho, \rho^2)$, skeleton digit $S_z = \rho x_k + \rho^2 y_k$), and Theorem 33 uses only the skeleton digit. So for every prime p , every $k \geq 1$ and every $\rho \geq 1$ with $\rho^3 < p$, $\mathcal{B}_{k,p,\rho}^2$ is a $(0, 3k+2, 3)$ -net over $\mathbb{F}_p$ (Proposition 54) with toroidal $\delta N^{1/3} \geq (\rho-1)p^{-1/3}$ (Theorem 33(1) for $\rho \geq 2$; the bound is 0 for $\rho = 1$); its occupied fine cells are exactly the cells of the index- p lattice $\Lambda_{\mathcal{B}^2} = \{a : a_z \equiv \rho a_x + \rho^2 a_y \pmod{p}\}$, of minimum ρ (Theorem 33(2), Figure 8(a), (b)); and for $\rho = \lfloor p^{1/3} \rfloor$ its mesh ratio is bounded uniformly in p (Theorem 33(3)). With ρ maximal, $p < (\rho+1)^3$, so the bound exceeds $(\rho-1)/(\rho+1)$ and tends to 1. It is a sawtooth in p (it drops each time $\lfloor p^{1/3} \rfloor$ increases), first exceeds 0.9 at $p = 1361$, and stays above 0.9 for every prime $p \geq 6863$ ($\rho \geq 19$). The bound is sharp for the method: the bound of Lemma 25(i), which allows a jitter of one fine cell in every coordinate, equals $(\rho-1)p^{-1/3}$ exactly, attained at the step $(-\rho, 1, 0)$.

Theorem 56 (Dimension three, $m \equiv 1 \pmod{3}$). *Let p be a prime, $k \geq 1$, and let $\rho \geq 2$ with $\rho^2(\rho+1) \leq p$. The digital net $\mathcal{B}_{k,p,\rho}^1$ of Definition 53 is a $(0, 3k+1, 3)$ -net over $\mathbb{F}_p$ whose toroidal minimum distance satisfies $\delta N^{1/3} \geq (\rho^2-4)p^{-2/3}$. With ρ the largest integer such that $\rho^2(\rho+1) \leq p$, the bound tends to 1 as $p \rightarrow \infty$; it exceeds 0.9 once $\rho \geq 27$, i.e. $p \geq 27^2 \cdot 28 = 20412$, so for every prime $p \geq 20431$.*

Proof of Theorem 56. The net property is Proposition 54; the hypotheses give $2 \leq \rho < p$, so $\rho \not\equiv 0$. Let $v \neq w$ be two points, $a \neq 0$ the centred difference of their fine positions, and $M = |a|_\infty$. If $M \geq p-1$ we are done, since $p-1 \geq \rho^2-3$. Otherwise let $\xi_c = \xi_{c,1}$ be the floor changes of Lemma 25(ii) and $u = (a_x, a_y - \xi_z, a_z - \xi_x - \xi_y + \xi_z)$. By the displayed relations, $u \in \Lambda_{\mathcal{B}^1}$, and $|u|_\infty \leq M+3$. If $u \neq 0$, Lemma 29(L1) gives $M+3 \geq \rho^2$. If $u = 0$, then $a_x = 0$, hence $\xi_x = 0$, $a_y = \xi_z$ and $a_z = \xi_y - \xi_z$. If $\xi_z = 1$ then $a_z > 0$, so $\xi_y \geq 2$, impossible; if $\xi_z = -1$ then $a_z < 0$ and $\xi_y \leq -2$, impossible. So $\xi_z = 0$, $a_y = 0$, $\xi_y = 0$ and $a_z = 0$, contradicting $a \neq 0$. Hence $M \geq \rho^2-3$, and Lemma 25(i) with $\ell = 2$ gives $\delta N^{1/3} \geq (\rho^2-4)p^{-2/3}$.

Constants. Let $c_1(p) = (\rho^2-4)p^{-2/3}$ be the bound with ρ maximal. Then $p < (\rho+1)^2(\rho+2)$, hence

$$c_1(p)^3 > G(\rho) = \frac{(\rho-2)^3(\rho+2)}{(\rho+1)^4}.$$

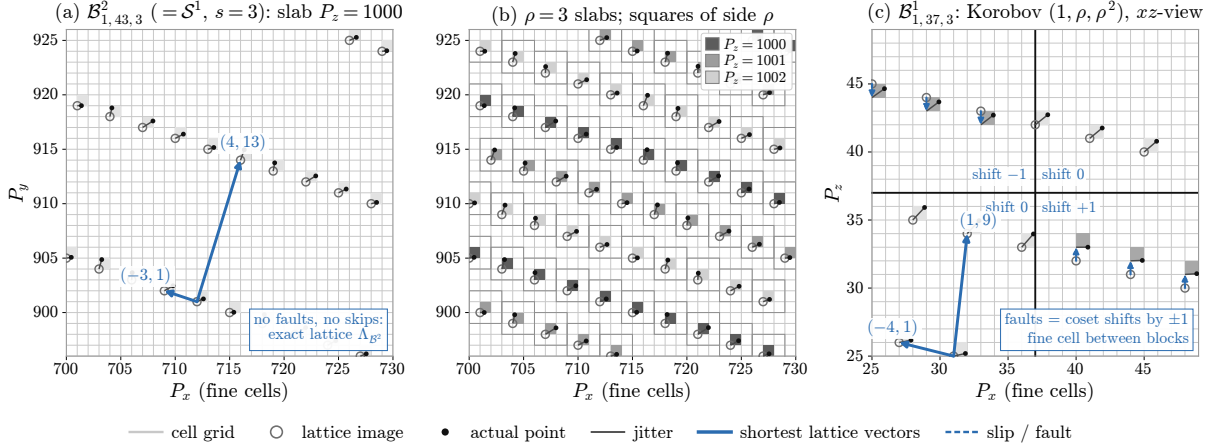


FIGURE 8. Regime II, lattice skeletons ($m = sk + r$), in fine-cell units. (a) $\mathcal{B}^2_{1,43,3}$ ($p = 43, \rho = 3, m = 5$; Remark 55): the slab of fine cells $P_z = 1000$ over a 30×30 window. Shaded: the occupied fine cells, which are exactly the cells of the index- p lattice $\Lambda_{\mathcal{B}^2} = \{a : a_z \equiv \rho a_x + \rho^2 a_y \pmod{p}\}$: no faults, no skipped sites. Open circles: their corners (the lattice image); dots: the points, displaced by up to one fine cell of jitter; arrows: a reduced basis $(-3, 1), (4, 13)$ of the lattice section. (b) The three slabs $P_z = 1000, 1001, 1002$ (shades): the squares of side ρ about the occupied cells have disjoint interiors, so two points of these slabs differ by at least ρ fine cells in x or y (Lemma 29(L)), and $\delta N^{1/3} \geq (\rho - 1)p^{-1/3}$ after one fine cell of jitter. (c) $\mathcal{B}^1_{1,37,3}$ ($m = 4$; Theorem 56): xz -view of the points with y -cell index 5 over the four coarse blocks around $(37, 37)$ (black lines). Open circles: the coset of the Korobov lattice $\Lambda_{\mathcal{B}^1}$ (generating vector $(1, \rho, \rho^2)$ modulo p), continued from the lower-left block (projected basis $(-4, 1), (1, 9)$); dashed arrows: the faults. In each coarse block the occupied cells are exactly a Korobov coset, shifted by ± 1 fine cell from block to block (dark where shifted): the faults are coset shifts, like stacking faults, not skips. The separation is the shortest vector minus faults and jitter (Lemma 25).

G increases for $\rho \geq 3$, since $(\log G)' = 9/((\rho - 2)(\rho + 1)) - 1/((\rho + 1)(\rho + 2))$ is positive, and tends to 1. Since $\rho \geq 27$ iff $p \geq 20412$, and $G(27)^{1/3} = 0.9033\dots$, the bound exceeds 0.9 from this prime on. $\square$

The case $u = 0$ uses the own-coordinate term $-z_{k-1}$ of S_z : with $+z_{k-1}$ or 0 there and equal signs of the faults this argument does not apply. Like that of Remark 55, the bound is a sawtooth in p .

Lattice reading. For $\mathcal{B}^1$ the skeleton digits give, with P_c the fine cell of coordinate c (Section 5.1),

$$P_y \equiv \rho P_x + \lfloor P_z/p \rfloor, \quad P_z \equiv \rho^2 P_x + \lfloor P_x/p \rfloor + \lfloor P_y/p \rfloor - \lfloor P_z/p \rfloor \pmod{p},$$

so inside each coarse block the occupied fine cells (one in p^2) form a coset of $\Lambda_{\mathcal{B}^1}$, the Korobov lattice with generating vector $(1, \rho, \rho^2)$ and modulus p [34, 55], shifted by unit *faults* between neighbouring coarse blocks (Figure 8(c)). The choice $\rho \approx p^{1/3}$ makes the shortest (primal) vector as long as possible for a lattice of index p^2 , up to a constant (the pigeonhole bound after Lemma 25). For integration it would be a poor Korobov generator: $(\rho, -1, 0)$ lies in the dual

lattice, so its Zaremba index is at most ρ . Separation (primal) and integration (dual) favour different generators.

6.7. Every resolution. Together, the nets of this section cover every resolution $m \geq 3$ for every large prime.

Corollary 57 (Every prime $p \geq 37$, every $m \geq 3$). *For every prime $p \geq 37$ and every $m \geq 3$ the nets of Theorems 49 ($m = 3$), 45 ($m \equiv 0$, $m \geq 6$), 56 ($m \equiv 1$) and 33 with $s = 3$ ($m \equiv 2$; the nets $\mathcal{B}^2$ of Remark 55), with ρ maximal, are explicit digital $(0, m, 3)$ -nets over $\mathbb{F}_p$ with*

$$\delta N^{1/3} > 0.2715, \quad \text{and} \quad \delta N^{1/3} > 0.4250 \text{ if } p \geq 83,$$

uniformly in m , and the lower bound tends to 1 as $p \rightarrow \infty$. Their covering radius satisfies $hN^{1/3} \leq \sqrt{3}$ for $m \equiv 0$, $hN^{1/3} \leq p^{1/3}\sqrt{2+p^{-2}}$ for $m \equiv 1$, and $hN^{1/3} \leq \min\{p^{2/3}\sqrt{1+2p^{-2}}, 4.264\}$ for $m \equiv 2 \pmod{3}$. So for each such p the mesh ratio h/δ is bounded uniformly in m : the nets are quasi-uniform along every $N = p^m$, $m \geq 3$. For $m \equiv 2$ the mesh ratio is moreover at most $7\sqrt{3} < 12.2$ for every prime $p \geq 11$ and every $m \geq 5$ (Theorem 33(3)).

Proof of Corollary 57. Take $\mathcal{C}_p$ for $m = 3$ (Theorem 49; for $p \geq 37$, $\delta N^{1/3} > 0.9823$, and its covering radius is at most $\sqrt{3}N^{-1/3}$ because every cell holds a point), $\mathcal{P}_{k,p}$ for $m = 3k \geq 6$, $\mathcal{B}_{k,p,\rho}^1$ for $m = 3k+1 \geq 4$ and $\mathcal{B}_{k,p,\rho}^2$ for $m = 3k+2 \geq 5$, with ρ maximal: ρ_1 and ρ_2 , the largest integers with $\rho_1^2(\rho_1+1) \leq p$ and $\rho_2^3 < p$. For $p \geq 37$, $\rho_1 \geq 3$ and $\rho_2 \geq 3$. If $37 \leq p \leq 79$ then $\rho_1 = 3$ and the bound of $\mathcal{B}^1$ is $5p^{-2/3} \geq 5 \cdot 79^{-2/3} = 0.27157\dots$, the bound of $\mathcal{B}^2$ is $\geq 2 \cdot 61^{-1/3} > 0.508$, and $1 - 1/p > 0.97$. If $p \geq 83$ then $\rho_1 \geq 4$ and $\rho_2 \geq 4$, and the bounds exceed $G(4)^{1/3} = (48/625)^{1/3} > 0.4250$ and $(\rho-1)/(\rho+1) = 3/5$ at $\rho = 4$ (Remark 55). All bounds tend to 1. For the covering radius: by $t = 0$ the elementary box with depths $\mathbf{k}$ (resp. (k, k, k)) around any point of the torus contains a net point, and its diagonal is $p^{-k}\sqrt{2+p^{-2}} = p^{1/3}\sqrt{2+p^{-2}}N^{-1/3}$ for $m \equiv 1$ and $p^{-k}\sqrt{1+2p^{-2}} = p^{2/3}\sqrt{1+2p^{-2}}N^{-1/3}$ for $m \equiv 2$. For $m \equiv 2$, Theorem 33(3) with $s = 3$ gives $hN^{1/3} \leq \sqrt{3}(\mu+1)p^{-1/3}$ and $h/\delta \leq \sqrt{3}(\mu+1)/(\rho-1)$, $\mu = \lceil p/\rho^2 \rceil$; over all primes $p \geq 11$ the maxima are $4.2633\dots < 4.264$ and $7\sqrt{3}$, both at $p = 23$ (for $\rho \geq 4$ use $\mu < \rho(1+1/\rho)^3 + 1$). $\square$

For $m \equiv 1$ the mesh ratio obtained in this way grows like $p^{1/3}$. Whether a bound uniform in p holds is open (Remark 123(5); for $m \equiv 2$ it is Theorem 33(3)). (Heuristic for one: the cosets of $\Lambda_{\mathcal{B}^1}$ have reduced bases of about ρ^2 fine cells, i.e. $O(N^{-1/3})$; a proof has to handle the faults between coarse blocks, and we have not given one.) The separation bounds and the lattice reading use only the skeleton digits: the bounds of Theorem 56 hold for every graph form over $\mathbb{F}_p$ with the depths $\mathbf{k}$ and the skeleton digits of Definition 53, net or not.

At $m = 3$ the constant can exceed 1 (Part II). If two coordinates share the geometric digit and the third reads it with the factor $\frac{1}{2}$ modulo p , the points lie locally on two cosets of a lattice, with the limit $\sqrt{66}/8 = 1.0155\dots$ (Proposition 103). If all three geometric digits are multiples of one digit, the three coordinates wrap together, and $\delta N^{1/3} > 1$ for every prime $p \geq 17$, with the limit $\sqrt{281}/16 = 1.0476\dots$ (Proposition 104). For small primes, the per-prime nets of Remark 58 give larger constants and close most of the remaining gaps:

Remark 58 (Per-prime designs). For small primes, computer-found designs give larger constants. They are graph forms with the depths $\mathbf{k}$, built by the same moves from the frame, in which the skeleton digits and the next offset digit of each coordinate (which controls the jitter) are prescribed on the last three or four levels; their skeletons are index- p^2 Korobov-type ($m \equiv 1$) and index- p congruence lattices ($m \equiv 2$). A finite computation analogous to Lemma 4 (it enumerates the steps between nearby fine cells, all carry patterns and both representatives

of each digit difference) certifies the constants of Table 10 for every $m = 3k + 1 \geq 10$ resp. $m = 3k + 2 \geq 8$, since the prescribed rows do not depend on k ; they exceed 1 for $p = 47, 53, 59, 61, 71, 73, 79$ ($m \equiv 1$) and $p = 41, 43, 59, 61, 79$ ($m \equiv 2$). This separation bound is Proposition 131, and it holds for every digital shift as well (Remark 132). The existence of such a $(0, m, 3)$ -net for every k (Propositions 128 and 129, Appendix C) rests on quantities that the moves of Lemma 2 do not change and that do not depend on k (Lemma 127: five for $m \equiv 1$, two for $m \equiv 2$), and on finitely many exact checks per design (proofs in Appendix C; formalization status in Section 14).

Together these results give, for every prime $p \geq 5$, explicit digital $(0, m, 3)$ -nets over $\mathbb{F}_p$ at the following resolutions. At $m = 3$, Theorem 49 gives $\delta N^{1/3} > 0.9059$, and Theorem 45 covers every $m \equiv 0, m \geq 6$. For $m \equiv 1, m \geq 10$, $\delta N^{1/3} > 0.4250$ (Theorem 56, and for $p \leq 79$ the per-prime certificates of Remark 58). For $m \equiv 2, m \geq 8$, $\delta N^{1/3} > 0.5$ (Remark 55, and for $p \leq 79$ the per-prime certificates); for $p \geq 11$ the nets $\mathcal{B}^2$ of Remark 55 also cover $m = 5$. Not covered are $m \in \{4, 7\}$ for $5 \leq p \leq 31$ and $m = 5$ for $p \leq 7$; finitely many resolutions do not matter for the question of Dick, Goda and Suzuki (Remark 72). In the bases 2 and 3 every m is covered (Theorem 64).

7. BASES TWO AND THREE: THE DEEP-SHIFT LIFT

The constructions so far need large bases. The net of Theorem 45 is a $(0, 3k, 3)$ -net in every base, but its separation bound needs $q \geq 4$; the other residues need large primes (Corollary 57). The bases two and three, the most common ones in practice, need another idea.

Remark 59 (Why $s = 3$, and base two). A $(0, m, s)$ -net in base 2 with $m \geq 2$ requires $s \leq 3$ [46, Cor. 5.11]; for digital nets over rings see [39, Thm. 2]. So $s = 3$ is the largest dimension in which one set of integer generator matrices can give $t = 0$ in every base (for dimension s see the text after Lemma 10). In the frame language of Section 3: $t = 0$ in every base needs places whose pairwise differences are ± 1 ; $\{0, 1\}$ is the largest set of integers with this property (in the language of exceptional units [36]), and the place ∞ gives the third coordinate.

In base $b \in \{2, 3\}$ we therefore build the nets recursively, $m \rightarrow m + 3$, from a finite seed. Each step adds one digit at the top of every coordinate and two at the bottom. The three new top digits form a $(0, 3, 3)$ -net in base b , so they split the cube into b^3 *top boxes* of side $1/b$. Every top box receives a copy of the old net, and the two new bottom digits are jitter. Neighbouring copies differ by digital shifts that change only the lower half of the old digits. The upper half of every old point therefore never changes (it is *frozen*), and the separation that the old net has at the scale of its upper half survives every later step. This is the mechanism of the introduction again, with the old net in the role of the lattice and the shifted lower digits as jitter (Figure 9).

Setting. Let b be a prime and $m_0 \geq 1$. A digitally shifted digital $(0, m_0, 3)$ -net over $\mathbb{F}_b$ is a set $P = \{\xi(n) = Cn + \tau : n \in \mathbb{F}_b^{m_0}\}$ with $C = (C_x, C_y, C_z)$, $C_c \in \mathbb{F}_b^{m_0 \times m_0}$, and a shift $\tau \in \mathbb{F}_b^{3m_0}$; a point has the three digit vectors $\xi_c(n) \in \mathbb{F}_b^{m_0}$, most significant digit first. For a pair of coordinates $(c, c') \in \{(y, z), (x, y), (x, z)\}$ let $P_{cc'} = \{(C_c n, C_{c'} n) : n \in \mathbb{F}_b^{m_0}\} \subset \mathbb{F}_b^{m_0} \times \mathbb{F}_b^{m_0}$, an m_0 -dimensional subspace (a digital $(0, m_0, 2)$ -net). For $1 \leq e \leq m_0$ let $Z_e \subset \mathbb{F}_b^{m_0} \times \mathbb{F}_b^{m_0}$ be the vectors that vanish on the first e digits of c and on the first $m_0 + 1 - e$ digits of c' . Since the map from $P_{cc'}$ to the first e digits of c and the first $m_0 - e$ digits of c' (the box of shape $(e, m_0 - e)$) is injective, $P_{cc'} \cap Z_e = 0$, so $H_e = P_{cc'} \oplus Z_e$ is a hyperplane; let $\lambda_e^{cc'}$ be a nonzero linear functional with kernel H_e . A point of $P_{cc'} + t s$, $t \neq 0$, and a point of $P_{cc'}$ fall into the same elementary box of shape $(e, m_0 + 1 - e)$ only if $s \in H_e$; so $\lambda_e^{cc'}(s) \neq 0$ says that adding multiples of s to the pair (c, c') creates no collision in boxes of that shape.

Definition 60 (Deep-shift lift). Let P be as above, $0 \leq D$, and let $s_A, s_B \in \mathbb{F}_b^{3m_0}$ vanish on the first D digits of each coordinate, i.e. change only the *deep* digits, those of index $> D$. They are *separating* if, for every $1 \leq e \leq m_0$,

$$\lambda_e^{yz}(s_A^{yz}) \neq 0, \quad \lambda_e^{xy}(s_B^{xy}) \neq 0, \quad \lambda_e^{xz}((s_B - s_A)^{xz}) \neq 0,$$

where $s^{cc'}$ is the restriction of s to the coordinates c, c' . The *lift* $L_D(P)$ is the set of b^{m_0+3} points with index $(n, \alpha, \beta_1, \beta_2) \in \mathbb{F}_b^{m_0+3}$ whose coordinates have the $m_0 + 3$ digits

$$\begin{aligned} x : \alpha & \mid (\xi(n) + s_\beta)_x & \mid \beta_2, \beta_1, \\ y : \alpha + \beta_1 & \mid (\xi(n) + s_\beta)_y & \mid \beta_1 + \beta_2, \beta_1, \quad s_\beta = \beta_1 s_A + \beta_2 s_B, \\ z : \alpha + \beta_1 + \beta_2 & \mid (\xi(n) + s_\beta)_z & \mid \beta_1, \beta_2, \end{aligned}$$

one *top* digit, m_0 *block* digits and two *jitter* digits. The shift τ of P stays in the block digits, so $L_D(P)$ is again a digitally shifted digital net over $\mathbb{F}_b$.

Lemma 61 (Lift). *Let P be a digitally shifted digital $(0, m_0, 3)$ -net over $\mathbb{F}_b$.*

- (A) *If s_A, s_B are separating, then $L_D(P)$ is a digitally shifted digital $(0, m_0 + 3, 3)$ -net over $\mathbb{F}_b$.*
- (B) *If $2D \leq m_0$, separating s_A, s_B exist.*

There are m_0 conditions for each pair of coordinates, one for each e . Each λ_e involves a deep digit, and $2D \leq m_0$ makes these deep digits distinct, so the conditions can be met independently.

Proof. (A) Let (d_x, d_y, d_z) be a box shape with $\sum_c d_c = m_0 + 3$; by Lemma 1 it suffices that the box map, from the index to the prescribed digits, is injective. All $d_c \geq 1$. The top digits $(\alpha, \alpha + \beta_1, \alpha + \beta_1 + \beta_2)$ determine (α, β) . The remaining depths $d_c - 1$ sum to m_0 and are at most m_0 each, so no jitter digit is prescribed, and what remains is an m_0 -box of the shifted net $P + s_\beta$, which is injective. *Exactly one* $d_c = 0$, say $d_x = 0$ (the cases $d_y = 0, d_z = 0$ are the same with the pairs xz and xy). The top digits of y and z fix $\alpha + \beta_1$ and β_2 , and the remaining index is (n, t) with $t = \beta_1$; the block digits of (y, z) are those of $P_{yz} + \text{const} + t s_A^{yz}$. If $d_y - 1 = e$ and $d_z - 1 = m_0 + 1 - e$ with $1 \leq e \leq m_0$, injectivity on (n, t) is injectivity of the projection to the first e resp. $m_0 + 1 - e$ digits on $P_{yz} + \mathbb{F}_b s_A^{yz}$; it holds on P_{yz} by the $(e, m_0 - e)$ box, and for $t \neq 0$ a collision would put s_A^{yz} in $H_e = \ker \lambda_e^{yz}$, which the separating condition excludes. If $d_y = 1$ or $d_z = 1$, the other coordinate reads all of its block and one jitter digit, β_1 for z and $\beta_1 + \beta_2$ for y , which determines t , and then the block determines n . For $d_y = 0$ the pair is (x, z) with the line $s_B - s_A$ and the jitter digits β_2, β_1 ; for $d_z = 0$ it is (x, y) with s_B and $\beta_2, \beta_1 + \beta_2$. Two $d_c = 0$. One coordinate carries all $m_0 + 3$ digits: its top digit, its block (a bijection in n for fixed $\beta = (\beta_1, \beta_2)$) and its two jitter digits, which are a bijection of $\mathbb{F}_b^2$ onto (β_1, β_2) in every coordinate.

(B) The functional $\lambda_e = \lambda_e^{cc'}$ vanishes on Z_e , so it is supported on the first e digits of c and the first $m_0 + 1 - e$ digits of c' . Its coefficient on digit e of c is nonzero: otherwise λ_e would live on a window of $e - 1$ plus $m_0 + 1 - e$ digits, onto which $P_{cc'}$ projects bijectively (the $(e - 1, m_0 + 1 - e)$ box), and vanish on $P_{cc'}$, hence be 0. Likewise its coefficient on digit $m_0 + 1 - e$ of c' is nonzero. If $e > D$, digit e of c is *deep* (index $> D$); if $e \leq D$, digit $m_0 + 1 - e \geq m_0 + 1 - D > D$ of c' is *deep*. So each λ_e has a nonzero coefficient on a deep digit, its own: digit e of c if $e > D$, digit $m_0 + 1 - e$ of c' if $e \leq D$. In any vanishing linear combination, the term with the largest $e > D$ (or, if there is none, the smallest e) is the only one that sees its own digit, so its coefficient is 0; by induction all coefficients are 0. Hence the restrictions of $\lambda_1, \dots, \lambda_{m_0}$ to the deep digits are linearly independent, and the deep parts of s_A^{yz} can be chosen with $\lambda_e^{yz}(s_A^{yz}) = 1$ for all e , those of s_B^{xy} with $\lambda_e^{xy}(s_B^{xy}) = 1$; the conditions on $(s_B - s_A)^{xz}$ involve the still free deep digits of $(s_A)_x$ and $(s_B)_z$, and are solved in the same way. $\square$

A *deep-shift chain* is a sequence $P_{m_0} \rightarrow P_{m_0+3} \rightarrow \cdots$ of lifts $P_{\ell+3} = L_{D_\ell}(P_\ell)$ with $2D_\ell \leq \ell$, where P_ℓ has b^ℓ points (the resolution ℓ); its *canonical continuation* from a resolution ℓ_0 on uses $D_\ell = \lfloor \ell/2 \rfloor$. For a resolution L write $A = b^{\lfloor L/2 \rfloor}$ (the number of values of the top $\lfloor L/2 \rfloor$ digits) and $W = b^{L-\lfloor L/2 \rfloor}$, read the coordinates of a point of P_L as integers $X_c \in [0, b^L)$, and let $t_c = \lfloor X_c/W \rfloor$ be the integer of its top $\lfloor L/2 \rfloor$ digits. Put

$$v_L^* = \min_{p \neq p' \in P_L} \sum_c \max(0, |t_c(p) - t_c(p')|_A - 1)^2, \quad g_L = W \sqrt{v_L^*} b^{-2L/3},$$

with $|\cdot|_A$ the distance to the nearest multiple of A ; v_L^* is an integer, computable from P_L alone. It is the smallest squared toroidal distance between the top halves of two points of P_L , in units of W , after one unit per coordinate is subtracted for the unknown lower half; g_L is the same quantity normalized like $\delta N^{1/3}$.

Lemma 62 (Freezing and separation). *Let $P_L \rightarrow P_{L+3} \rightarrow \cdots$ be lifts whose depth parameters satisfy $D_{L+3j'} \geq \lfloor L/2 \rfloor + j'$ for every $j' \geq 0$ (for instance the canonical continuation). Then for every $j \geq 0$ the toroidal (hence also Euclidean) minimum distance of P_{L+3j} satisfies*

$$\delta N^{1/3} \geq \min(g_L, b^{L/3} - W b^{-2L/3}).$$

Each lift prepends one digit, so the old top half moves one digit down; this is why the depth must grow by one per step. In the bound, the first term covers two points that come from different points of P_L , and the second two copies of the same point, which differ in a top digit.

Proof. Freezing. By induction on j , P_{L+3j} is the set of points whose coordinate c has the digits $\pi_c(u) \mid (p + \eta(u))_c \mid \text{low}_c(u)$, where $u \in \mathbb{F}_b^{3j}$ collects the new index digits, $u \mapsto \pi(u) = (\pi_c(u))_c \in \mathbb{F}_b^{3j}$ is a bijection (j top digits per coordinate), p runs over P_L , $\eta(u)$ is a digitwise shift of the L block digits, and $\text{low}(u)$ has $2j$ digits per coordinate. The lift at resolution $\ell = L + 3j'$ shifts only digits of index $> D_\ell$ of its own block, in which the block of P_L occupies the indices $j' + 1, \dots, j' + L$; so it touches block digits of index $> D_\ell - j' \geq \lfloor L/2 \rfloor$ only, and never the j' top digits before them. Hence $\eta(u)$ vanishes on the top $\lfloor L/2 \rfloor$ digits of every coordinate: these are *frozen*, equal to those of p .

Separation. Measure in units of $b^{-(L+3j)}b^{2j}$, so that the torus has period b^{L+j} and a point has coordinates $\pi_c(u)b^L + t_c(p)W + \varepsilon_c$ with $\varepsilon_c \in [0, W)$. Two points with different $p \neq p'$: reducing modulo b^L , which divides the period, does not increase toroidal distances, and modulo $b^L = AW$ the difference in coordinate c is $(t_c(p) - t_c(p'))W + (\varepsilon_c - \varepsilon'_c)$, of toroidal size more than $W(|t_c(p) - t_c(p')|_A - 1)$; so their distance is at least $W\sqrt{v_L^*}$. Two points with the same p and different u : some π_c differ, while t_c agree, so coordinate c differs by $(\pi_c - \pi'_c)b^L + (\varepsilon_c - \varepsilon'_c)$ with $\pi_c \not\equiv \pi'_c \pmod{b^j}$, of toroidal size more than $b^L - W$. A distance of x units is $x b^{-L-j}$ in $[0, 1)^3$, and $N^{1/3} = b^{L/3+j}$, so $\delta N^{1/3}$ is the distance in units times $b^{-2L/3}$. $\square$

The bound does not depend on j , nor on the shifts chosen after resolution L : one exact computation at the resolution L certifies every larger $m \equiv L \pmod{3}$, and finitely many exact computations certify the resolutions between the seed and L .

For the every-shift part of Theorem 64 below we need the same certificate for every digital shift. A digital shift adds digits without carries, so it can change the integer difference of two digit vectors; the following lemma computes the worst case exactly.

Lemma 63 (Every digital shift). *For $\mathbf{d} \in \mathbb{F}_b^n$ let $\mu_n(\mathbf{d})$ be the least toroidal distance $|X' - X|_{b^n}$ (the distance to the nearest multiple of b^n) over the integers $X \in [0, b^n)$, where X' has the digits of X plus $\mathbf{d}$, digit by digit modulo b . Let $H = \lfloor L/2 \rfloor$.*

- (a) Under the hypothesis of Lemma 62, for every $j \geq 0$ and every digital shift τ of P_{L+3j} (Definition 7),

$$\delta(P_{L+3j} \oplus \tau) N^{1/3} \geq \min(W\sqrt{v_L^\circ} b^{-2L/3}, b^{L/3} - W b^{-2L/3}),$$

where $v_L^\circ = \min_\Delta \sum_c \max(0, \mu_H(\Delta_c) - 1)^2$, the minimum over the differences $\Delta = (\Delta_x, \Delta_y, \Delta_z)$ of the top H digits of two distinct points of P_L ($\Delta = 0$ allowed, with weight 0).

- (b) For every digitally shifted digital $(0, m, 3)$ -net P over $\mathbb{F}_b$,

$$\min_\tau \delta(P \oplus \tau)^2 = b^{-2m} \min_\Delta \sum_c \mu_m(\Delta_c)^2,$$

the minimum over the digital shifts τ and over the nonzero digit differences Δ of two points of P (toroidal distances).

Proof. For a pair of points with digit difference Δ , coordinate c of the shifted pair has the digits X_c and $X_c + \Delta_c$, where X_c is coordinate c of the first point plus τ_c . As τ varies, (X_x, X_y, X_z) runs over all triples of digit vectors, independently in the three coordinates, so the minimum over τ of the squared distance of the pair is $\sum_c \min_{X_c} |X'_c - X_c|^2$. This gives (b). Since $t \mapsto \max(0, t-1)^2$ is nondecreasing, the same argument gives $v_L^\circ = \min_{\tau'} v_L^*(P_L \oplus \tau')$ over the digital shifts τ' of P_L . For (a), write the points of P_{L+3j} as in the proof of Lemma 62. A digital shift τ keeps $u \mapsto \pi(u) + \tau_\pi$ a bijection, where τ_π are its digits on the top j digits, and adds the same vector τ_{blk} to the block digits of every point. So $P_{L+3j} \oplus \tau$ has the structure used in that proof, with P_L replaced by the digitally shifted copy $P_L \oplus \tau_{\text{blk}}$: the top H block digits of every point are those of a point of $P_L \oplus \tau_{\text{blk}}$, and the proof applies verbatim. The first term is then $W\sqrt{v_L^*(P_L \oplus \tau_{\text{blk}})} b^{-2L/3} \geq W\sqrt{v_L^\circ} b^{-2L/3}$, and the second term does not involve the shift. $\square$

The quantity μ_n has a simple description. Write d_k for the digit of $\mathbf{d}$ of weight b^k . Each nonzero d_k contributes $d_k b^k$ or $(d_k - b)b^k$ to $X' - X$, according to whether digit k of X is below $b - d_k$ or not, and both occur. So $\mu_n(\mathbf{d})$ is the distance, modulo b^n , from the integer with the digits $\mathbf{d}$ to the nearest number $\sum_{k \in S} b^{k+1}$, $S \subseteq \text{supp } \mathbf{d}$; the numbers b^{k+1} , $k \in \text{supp } \mathbf{d}$, are super-increasing, so the nearest such sum is found greedily. Thus v_L° is the minimum weight, under an additive weight, of a linear code of length $3H$: the top H digits of the differences of points of P_L , of dimension L when the top-digit map is injective (as at all resolutions used below). It is computed exactly by enumerating the code words of small weight, in milliseconds even at 2^{30} points. It vanishes if and only if two distinct points of P_L share their top H digits or the code contains a nonzero vector whose coordinates are each 0 or $\pm(0, \dots, 0, 1, \dots, 1)$. The reason is the mechanism of Remark 70 in another guise: without a shift, two points whose digits differ by $0 \dots 01 \dots 1$ are close only if they happen to sit on a carry chain, as $d(b-1) \dots (b-1)$ and $(d+1)0 \dots 0$ do; a digital shift can put any such difference on a carry chain, and then the two coordinates differ by one unit.

Theorem 64 (Bases two and three; computer-assisted). *Let $b \in \{2, 3\}$. For every $m \geq 1$ there is an explicit digital $(0, m, 3)$ -net P_m over $\mathbb{F}_b$ and a digital shift $\tau_m \in (\mathbb{F}_b^m)^3$ (Definition 7) such that the toroidal (hence also Euclidean) minimum distances satisfy*

- (1) $\delta(P_m \oplus \tau_m) N^{1/3} \geq 0.4129$ for $b = 2$ and ≥ 0.3538 for $b = 3$;
- (2) $\delta(P_m) N^{1/3} \geq 0.1718$ for $b = 2$ and ≥ 0.0770 for $b = 3$;
- (3) $\delta(P_m \oplus \tau) N^{1/3} \geq 0.1718$ for $b = 2$ and ≥ 0.0770 for $b = 3$, for every digital shift $\tau \in (\mathbb{F}_b^m)^3$.

Per residue $m \equiv 0, 1, 2 \pmod{3}$ the constants are those of Table 5. For $m \geq 9$ ($b = 2$) resp. $m \geq 6$ ($b = 3$) the nets come from a finite seed by deep-shift lifts: along a fixed chain up to the

b	$m \bmod 3$	seed resolution	certificate resolution L	(1) shifted	(2) unshifted	(3) every shift
2	0	9	30	.4250	.4050	.4050
2	1	10	28	.4129	.4129	.4129
2	2	11	20	.4209	.1718	.1718
3	0	6	18	.4699	.4699	.1047
3	1	7	22	.3538	.2586	.1651
3	2	8	20	.3676	.0770	.0770

TABLE 5. Theorem 64: lower bounds for $\delta N^{1/3}$ per residue class, for all m in the class (including the explicit nets below the seed resolution, whose values are larger), truncated. One certificate resolution L serves all three columns. The certificates of (1) and (2) were reproduced exactly by two independent implementations, one of which the scripts of the software deposit (Appendix G) rerun, and so were the integers v_L° of (3). Columns (2) and (3), apart from the entries .4699 and .2586, are also checked in the Lean kernel, with the nets and the certificates v_L° ; column (1) is checked by these programs only (Section 14). The nets at the certificate resolutions have up to 2^{30} points; v_L^* is computed by grouping the points by their top digits, using that the groups are digit translates of one linear set (the structure in the proof of Lemma 62), and v_L° as a minimum code weight (after Lemma 63).

certificate resolution of Table 5, then by any continuation with $D_\ell = \lfloor \ell/2 \rfloor$. For smaller m they are explicit nets with exactly computed minimum distances.

Proof. For the lifted resolutions: Lemma 61(A) gives the net property at every resolution, Lemma 61(B) the existence of the continuation, and Lemma 62 the bound $\delta N^{1/3} \geq g_L$ for every $m \geq L$ in the residue class of a certificate resolution L , once the finite certificate v_L^* is known and the proviso $g_L \leq b^{L/3} - Wb^{-2L/3}$ holds. The finite part is an exact computation on explicitly given nets: the $t = 0$ property of the seeds and of the nets at the certificate resolutions, the integers v_L^* (with the proviso, which holds by a wide margin), the exact minimum distances at the finitely many resolutions between the seed and L , and, for m below the seed resolutions, explicit digital $(0, m, 3)$ -nets with their exact minimum distances (all above the stated constants). The constants are the minima of these exact values, truncated. Without the shift the same matrices are used: Lemmas 61 and 62 never use the shift, and only the certificates change. For (3), Lemma 63(a) gives the bound for every digital shift and every $m \geq L$ from one integer v_L° , computed at the same certificate resolution L (the proviso holds again); at the finitely many resolutions below L , and for the explicit nets below the seed, the exact minimum of $\delta(P_m \oplus \tau)N^{1/3}$ over all τ is computed by Lemma 63(b). $\square$

The shifts in (1) are explicit, one per m : the shift of the seed, carried into the block digits by each lift. The definitions of [11] need only a family indexed by m , so the shifted nets are well-separated families of digitally shifted digital nets in their sense (Corollary 71). Part (3) holds for every digital shift (Lemma 63). Its constants are those of (2) in base two and, for $m \equiv 0, 1$, lower in base three, where a shift can place a digit difference $0 \cdots 01 \cdots 1$ of two points on a carry chain. Digital $(0, m, 3)$ -nets in base 2 were classified by Hofer and Suzuki [30]; here we need only explicit seeds and the lift. Propagation rules for digital nets [14, Sec. 4.2, 4.4] control the quality parameter t , not distances; the lift is a propagation rule $m \rightarrow m + 3$ at $t = 0$ that also carries a separation certificate.

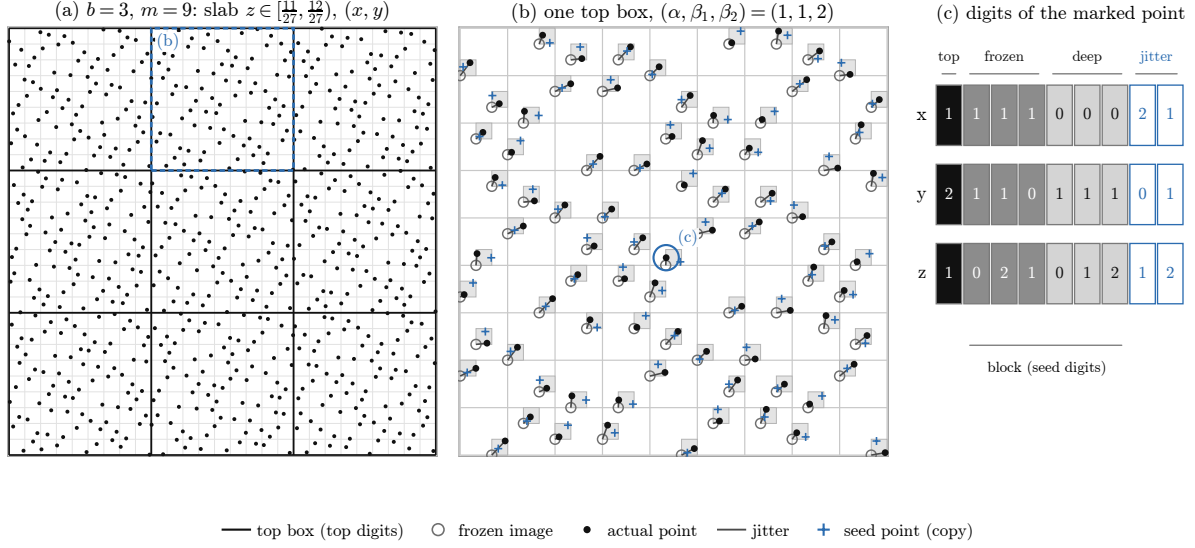


FIGURE 9. The deep-shift lift (Definition 60) in base $b = 3$: the digitally shifted (Definition 7) $(0, 9, 3)$ -net of Theorem 64(1) for $m \equiv 0 \pmod{3}$, one lift of the $m = 6$ seed. A point has one top digit per coordinate, 6 block digits (a copy of a seed point shifted below block depth $\lfloor 6/2 \rfloor = 3$) and two jitter digits; the top digits $(\alpha, \alpha + \beta_1, \alpha + \beta_1 + \beta_2)$ select one of 27 top boxes (side $\frac{1}{3}$). (a) The slab $z \in [\frac{11}{27}, \frac{12}{27})$ projected to (x, y) : 729 points, one in each box of side 3^{-3} ; the nine top boxes (thick) carry the same frozen pattern. (b) The top box $(\alpha, \beta_1, \beta_2) = (1, 1, 2)$ (dashed in (a)): each point (dot) lies in the frozen box of side 3^{-4} (shaded; open circle at its corner) of exactly one point of the seed copy (plus signs), i.e. the box fixed by the top digits of that point, which later lifts never change; grey segments: the jitter, i.e. the deep block digits and the two jitter digits. (c) The nine digits of the marked point of (b). Computed, exact: the net is a $(0, 9, 3)$ -net over $\mathbb{F}_3$, and its toroidal $\delta N^{1/3}$ is 0.5291, above the floor 0.4699 of Theorem 64(1) for $m \equiv 0 \pmod{3}$ (0.3538 for all m ; the seed has 0.5562).

Remark 65 (Why every-shift certificates vanish at some resolutions). Along the chains the every-shift certificate v_L° vanishes at many resolutions (for $b = 3, m \equiv 0$, at every resolution below 18; computed), and it is positive at the six certificate resolutions of Table 5, all of them even. Two facts explain the pattern. (i) *Parity*. If L is even and $v_L^\circ = 0$, then $v_{L+3}^\circ = 0$ for every lift P_{L+3} of P_L . Indeed, the indices $(n, 0, 0, 0)$ of the lift (Definition 60) give points with top digit 0, block digits those of P_L and jitter digits 0, so the top $\lfloor (L+3)/2 \rfloor = H+1$ digits of their differences are 0 followed by the top H digits of the differences of P_L . For such differences the toroidal μ_{H+1} of the extended vector is at most the plain (non-toroidal) value of the original one, and a vector $\pm(0, \dots, 0, 1, \dots, 1)$ has plain value 1; so a vanishing certificate at L gives one at $L+3$. For odd L the window of P_{L+3} gains one more block digit, so a certificate can first become positive only at an even resolution. (ii) *Dichotomy*. If $v_L^\circ = 0$, then along every lift chain from P_L every $m \geq L$ in the class has $\min_\tau \delta(P_m \oplus \tau) N^{1/3} < 2\sqrt{3} b^{\lfloor L/2 \rfloor - 2L/3}$. Indeed, the indices whose new digits are all 0 embed P_L into P_m with top and jitter digits 0, and a difference whose top window is 0 or $\pm(0, \dots, 0, 1, \dots, 1)$ in each coordinate can be shifted to have each coordinate

below $2W$ in the units $b^{-(L+j)}$ of the proof of Lemma 62, $m = L + 3j$. So, for a chain frozen from every resolution, a floor $\kappa N^{-1/3}$, $\kappa > 0$, that holds for every shift from some resolution on exists if and only if $v_L^\circ > 0$ for some L ; if the certificate vanished at infinitely many L , the every-shift separation would tend to 0. For the nets of Theorem 64 the certificate is positive at every certificate resolution (Table 5), so no shift makes their separation decay.

The six seeds are printed in Table 14 (Appendix D); the chains, shifts and small- m nets are data of the deposit, whose scripts rerun the certificates of Table 5 (Appendix G).

8. THE QUESTION OF DICK, GODA AND SUZUKI

This section relates the results of Part I to the definitions of [11]: low discrepancy, separation in their sense, digital shifts, and the maximum norm.

Remark 66 (Low discrepancy). All nets in this paper are $(0, m, s)$ -nets in base q : every elementary box of volume q^{-m} contains exactly one point (Lemma 1). This is a property of the point set alone, whatever ring the net is digital over, so Niederreiter's discrepancy bound for (t, m, s) -nets in an integer base [46] applies: $D_N^* \leq C_{s,q}(\log N)^{s-1}/N + O_{s,q}((\log N)^{s-2}/N)$ for $N = q^m$, with $C_{s,q}$ independent of m . So all our nets have low discrepancy in the sense of [11, 10], and the question of Dick, Goda and Suzuki reduces, for these nets, to separation. The same holds for digitally shifted nets, which are again $(0, m, s)$ -nets (Lemma 67).

8.1. Digital shifts.

Lemma 67 (Shifted graph forms). *Let P be a graph form over $\mathbb{Z}/q\mathbb{Z}$ with depths $\mathbf{k}$ and blocks Φ , and $\tau = (\tau_c^{\text{cell}}, \tau_c^{\text{off}})_c$ a digital shift (Definition 7), split into its digits on the cell digits and on the offset digits of each coordinate. Then $P \oplus \tau$ is the set of points whose coordinate c has the digits n_c followed by $\sum_d \Phi_{cd} n_d + \gamma_c$, $n \in \prod_c (\mathbb{Z}/q\mathbb{Z})^{k_c}$, where $\gamma_c = \tau_c^{\text{off}} - \sum_d \Phi_{cd} \tau_d^{\text{cell}}$. In particular n is the cell of the point, every cell holds one point, $P \oplus \tau$ is a $(0, m, s)$ -net if P is, and for two points in the cells n, n' every offset digit difference is congruent to the corresponding entry of $\Phi(n' - n)$ modulo q , as for P .*

Proof. Substitute $n = \tilde{n} - \tau^{\text{cell}}$ and index the shifted point by $\tilde{n}$. The shift maps every elementary box of shape d bijectively onto one of the same shape, since it shifts the first d_c digits of coordinate c . $\square$

So a shifted net is an *affine* graph form: offsets $\Phi n + \gamma$ with a constant γ . Lemma 4, Proposition 115 and the skeleton lemmas of Section 5 hold for affine graph forms with the same proofs, since they use only differences of digits.

Proposition 68 (Every digital shift). *Lemma 4 holds verbatim, with the same bound, for every digital shift of a graph form that satisfies (H1) and (H2). Consequently the lower bounds on the separation in Theorems A, 45, 33, 35, 56 and 116 and in Propositions 19 and 115 hold for every digital shift of the respective nets (in Theorem 33(2) the occupied fine cells form a coset of the lattice), and so does the first-order sharpness in Theorem A(2).*

Proof. By Lemma 67 the shift only adds the constant γ to the offsets. The proofs use the cells (the step and its carries), the residues of digit differences, the facts that a digit difference lies in $(-q, q)$ and vanishes if its residue does, and $|f' - f| < 1$; the constant cancels in every residue, and in Lemma 4 the deeper digits of a coordinate whose own axis alone moves are still equal, by (H2). Theorem 35 does not even need the re-indexing by the shifted cells: its proof uses only differences of the skeleton digits. The sharpness argument prescribes the cell digits and the first offset digits of a pair; in the shifted net these are digits of the unshifted net prescribed in

translated sets of the same size, so the joint uniformity of the digits of the unshifted net, given by its $t = 0$, suffices. $\square$

The nets of Theorem 64(1) carry one explicit shift by construction. Proposition 68 does not apply to them, because their bounds come from the lift certificates (Lemma 62), not from Lemma 4; Theorem 64(3) covers every digital shift instead. The per-prime nets of Remark 58 keep their constants under every digital shift as well (Remark 132). In dimension three, Proposition 68 gives every resolution under every digital shift:

Corollary 69 (Corollary 57 under digital shifts). *Let $p \geq 37$ be prime. For every $m \geq 3$ and every digital shift, the shifted nets of Corollary 57 satisfy its separation bounds, with the same constants 0.2715 and 0.4250, and its covering bounds; so they are quasi-uniform along every $N = p^m$, $m \geq 3$, as the Larcher–Pillichshammer nets in [11, Thm. 3.11]. For $m \geq 4$ the lower bound still tends to 1 as $p \rightarrow \infty$. At $m = 3$ the nets are the column nets $\mathcal{C}_p$, whose three coordinates share the second and third digits, and the bound depends on whether the shift keeps them shared:*

- (a) *for every shift, $\delta N^{1/3} > 0.4693$;*
- (b) *if the shift digits of the three coordinates agree at the second and at the third digit, the exact value of Theorem 49(2) holds;*
- (c) *if they agree at the second digit, $\delta N^{1/3} \geq 1 - (7p - 3)/(\sqrt{3}p^2)$;*
- (d) *otherwise $1/\sqrt{3} - 7/(\sqrt{3}p) \leq \delta N^{1/3} \leq 1/\sqrt{3} + 5/(\sqrt{3}p)$.*

Proof. A digital shift keeps one point in every cell and keeps $t = 0$ (Lemma 67), which is all the covering bounds use, except for the mesh-ratio constant 4.264 of Corollary 57, which comes from Theorem 33(3); at $m = 3$ this gives $h \leq \sqrt{3}N^{-1/3}$. In the shifted net the occupied fine cells form a coset $g + \Lambda_A$ (Proposition 68), and the proof of Theorem 33(3) runs with its target residue moved by $g_z - \sum_d \rho^d g_{x_d}$; this is not a translation of the unshifted construction, since the target cell must stay in range. For $m \geq 4$ the separation bounds of Theorems 45, 56 and 33 used in Corollary 57 hold for every shift by Proposition 68. For $m = 3$ Proposition 52 gives the lower bound $0.4693 > 0.4250$, the exact value and the bound for agreeing shift digits, and otherwise the two bounds $\frac{1}{\sqrt{3}}(1 - \frac{W+3}{p} + \frac{3}{p^2})$ and $\frac{1}{\sqrt{3}}(1 + \frac{3+w_{\max}}{p} - \frac{3}{p^2})$ with $W \leq 4$ and $w_{\max} \leq 2$, which lie in the stated interval. $\square$

So only the limit changes, and only at $m = 3$: with unequal shift digits at the geometric digit $\delta N^{1/3}$ lies within $7/(\sqrt{3}p)$ of $1/\sqrt{3}$. The reason: a digital shift adds a different constant to the shared digit in each coordinate, so the three coordinates no longer wrap at the same cells, and a step across a wrap of one coordinate alone has length about $1/\sqrt{3}$ (Remark 99).

Remark 70 (Shared digits under shifts). So the exact value of Theorem 49 does not extend to all shifted nets: if the shift digits of the three coordinates of $\mathcal{C}_q$ at the second digit are not all equal, then for every $q \geq 11$, prime or not, the shifted net has $\delta N^{1/3} \leq \frac{1}{\sqrt{3}}(1 + \frac{3+w_{\max}}{q} - \frac{3}{q^2})$, below the value of Theorem 49 (Proposition 52(3)). For each coordinate, the set of values of the shared digit at which a step wraps (its *wrap window*) is translated by that coordinate's shift digit; unequal shift digits give distinct windows, so some cell wraps in exactly one coordinate, and its step along that axis gives the pair $qa_c \mathbf{1} + \Delta j$ at integer scale. In general a digital shift translates the wrap windows independently in each coordinate. Bounds certified with arbitrary wraps (Remark 99) therefore survive every shift; bounds that use locked wraps, wraps that are correlated across coordinates, need not. The nets $\mathcal{T}_p$ and $\mathcal{W}_p$ of Part II are of the second kind (Remark 108).

8.2. Well-separated families. In [11] a point set is κ -separated (κ as in [11]) if no (toroidal) shifted elementary interval with κ digits in every coordinate contains two of its points [11, Defs. 3.1–3.3], and a family $(\mathcal{P}_m)_{m \in I}$ on an infinite set I of resolutions is *well separated* if $\mathcal{P}_m$ is κ_m -separated with $\kappa_m \leq m/s + O(1)$ [11, Def. 3.8] (in [11] the dimension is d).

Corollary 71 (Well-separated families in the sense of Dick, Goda and Suzuki). *Let $s \geq 2$ and $q \geq 2$ be integers and $I \subseteq \mathbb{N}$ infinite, and for $m \in I$ let $\mathcal{P}_m \subset [0, 1)^s$ be a $(0, m, s)$ -net in base q whose toroidal minimum distance satisfies $\delta \geq cq^{-m/s}$, with $c > 0$ independent of m . Then every $\mathcal{P}_m$ is κ_m -separated and toroidally κ_m -separated in base q [11, Def. 3.3], with*

$$\kappa_m = \left\lceil \frac{m}{s} + \log_q \frac{\sqrt{s}}{c} \right\rceil \leq \frac{m}{s} + \log_q \frac{\sqrt{s}}{c} + 1,$$

so $(\mathcal{P}_m)_{m \in I}$ is a well-separated and toroidally well-separated family on I [11, Def. 3.8]. In particular:

- (1) the nets $\mathcal{P}_{k,q}$ of Theorem 45, for every integer $q \geq 4$, are $(k+1)$ -separated, i.e. $\kappa_m = m/3 + 1$ on $I = \{3k : k \geq 2\}$;
- (2) the nets of Theorem A(2) are $(k+1)$ -separated on $I = \{sk : k \geq 1\}$;
- (3) the nets $\mathcal{H}_{k,p}^s$ of Theorem 116 are $(k+1)$ -separated for every prime $p \geq \max(2s, 2B_s + 4)$ (two more than in Theorem 116; see Step 3 of the proof) and every $k \geq 1$;
- (4) the nets $\mathcal{S}_{k,p,\rho}^1$ of Theorem 33, with $m = sk + s - 1$, are $(k+1)$ -separated, i.e. $\kappa_m = \lceil m/s \rceil$, if $(\rho - 1)^2 \geq s$ (for $\rho = \lfloor p^{1/s} \rfloor$ this holds when $p > (\lceil \sqrt{s} \rceil + 1)^s$), and $(k+2)$ -separated otherwise;
- (5) for every prime $p \geq 37$ the nets of Corollary 57 are $(\lfloor m/3 \rfloor + 1)$ -separated for every $m \geq 3$.

All of these hold toroidally as well, and for every digital shift (Definition 7) of the respective nets. For prime q the nets are digital nets over $\mathbb{F}_q$ in the sense of [11, Def. 2.1]; this covers (3)–(5) entirely and the prime instances of (1) and (2). For composite q the nets of (1) and (2) are digital over $\mathbb{Z}/q\mathbb{Z}$, which is not covered by [11, Def. 2.1]; Definitions 3.1 and 3.2 of [11] are stated for every integer base $b \geq 2$, and we read Definitions 3.3 and 3.8 in the same generality.

Proof. Step 1 ([11, Lemma 3.7], with strict inequality). Let $P \subset [0, 1)^s$ be finite and $\kappa \geq 0$, and suppose every two distinct points of P have toroidal ℓ^∞ -distance at least $q^{-\kappa}$. A toroidal shifted elementary interval $\tilde{J}_{\mathbf{c},a,e}$ with κ digits in every coordinate, $\mathbf{c} = (\kappa, \dots, \kappa)$ [11, Def. 3.2], is contained in a product of sets $I_j \bmod 1$, where $I_j = [\alpha_j, \alpha_j + q^{-\kappa})$ is half-open. If $x, y \in \tilde{J}_{\mathbf{c},a,e}$, then for each j there are $z, z' \in \mathbb{Z}$ with $x_j + z, y_j + z' \in I_j$, so $\min(|x_j - y_j|, 1 - |x_j - y_j|) \leq |(x_j + z) - (y_j + z')| < q^{-\kappa}$, and hence $x = y$. So P is toroidally κ -separated. A non-toroidal interval $J_{\mathbf{c},a,e}$ gives the same bound for $|x_j - y_j|$, which is at least the toroidal distance, so P is also κ -separated. This sharpens the contrapositive of [11, Lemma 3.7] to the strict bound $q_\infty(P) < 1/(2q^\kappa)$ for non-separated P , where $q_\infty(P)$ is the separation radius of [11] in the maximum norm; the strictness comes from the intervals being half-open.

Step 2. For distinct $x, y \in \mathcal{P}_m$ the toroidal coordinate distances t_j satisfy $\sum_j t_j^2 \geq \delta^2$, so $\max_j t_j \geq \delta/\sqrt{s} \geq (c/\sqrt{s})q^{-m/s} \geq q^{-\kappa_m}$ by the choice of κ_m . Since toroidal distances are at most $\sqrt{s}/2$, we have $cq^{-m/s} \leq \sqrt{s}/2$, so $\kappa_m \geq 1$. Step 1 gives the separation, and $\kappa_m - m/s \leq 1 + \log_q(\sqrt{s}/c)$ is bounded, which is the condition of [11, Def. 3.8].

Step 3 (the families). By Step 2 a net with $\delta \geq \theta q^{-\kappa}$ is κ -separated as soon as $\theta \geq \sqrt{s}$. (1) $m = 3k$ and $\delta \geq c(q)q^{-k}$ (Theorem 46); with $\kappa = k + 1$ we need $qc(q) \geq \sqrt{3}$, i.e. $\min\{(q-1)^2, (q-2)^2 + (q-4)^2, 3(q-3)^2\} \geq 3$, which holds for $q \geq 4$ (with equality at $q = 4$). (2) $\delta \geq (1 - a_s^*/q)q^{-k}$; with $\kappa = k + 1$ we need $q - a_s^* \geq \sqrt{s}$. From $q \geq 5a_s^* + 4$ we get $q - a_s^* \geq \frac{4}{5}(q+1)$, and from $\text{lpf}(q) \geq s - 1$ we get $q + 1 \geq s$, so $q - a_s^* \geq \frac{4}{5}s \geq \sqrt{s}$ for $s \geq 2$. (3) $\delta \geq c_p p^{-k}$ with

$c_p = \min(\sqrt{s}(\frac{1}{2} - \epsilon_p), \sqrt{2}(1 - \epsilon_p))$ and $\epsilon_p = (B_s + 1)/p$; with $\kappa = k + 1$ we need $p c_p \geq \sqrt{s}$. If $p \geq 2B_s + 4$, then $\sqrt{s}(\frac{1}{2} - \epsilon_p)p = \frac{\sqrt{s}}{2}(p - 2B_s - 2) \geq \sqrt{s}$ and $\sqrt{2}(1 - \epsilon_p)p \geq p/\sqrt{2} \geq \sqrt{2}s \geq \sqrt{s}$, since $\epsilon_p \leq \frac{1}{2}$ and $p \geq 2s$. (4) $m = sk + s - 1$ and $\delta \geq (\rho - 1)p^{-(k+1)}$ (Theorem 33(1)); $\kappa = k + 1$ needs $\rho - 1 \geq \sqrt{s}$, and otherwise $\kappa = k + 2$ needs $(\rho - 1)p \geq \sqrt{s}$, which holds as $p > 2^s$. If $p > (\lceil \sqrt{s} \rceil + 1)^s$, then $\rho = \lfloor p^{1/s} \rfloor \geq \lceil \sqrt{s} \rceil + 1$. (5) $m = 3$: $\delta \geq \sqrt{2/3}p^{-1}$ (Theorem 48), and $\kappa = 2$ needs $p\sqrt{2/3} \geq \sqrt{3}$, i.e. $p \geq 3/\sqrt{2}$. $m = 3k, k \geq 2$: part (1). $m = 3k + 1$: $\delta \geq (\rho^2 - 4)p^{-(k+1)}$ with ρ maximal subject to $\rho^2(\rho + 1) \leq p$ (Theorem 56), and $p \geq 37$ gives $\rho \geq 3$, so $\rho^2 - 4 \geq 5 \geq \sqrt{3}$ and $\kappa = k + 1$. $m = 3k + 2$: part (4) with $s = 3$ and $\rho = \lfloor p^{1/3} \rfloor \geq 3$, so $(\rho - 1)^2 = 4 \geq 3$ and $\kappa = k + 1$. In every case $\kappa_m = \lfloor m/3 \rfloor + 1$.

Digital shifts. By Proposition 68 the separation bounds used in (1)–(4) and, for $m \geq 4$, in (5) hold for every digitally shifted net. For $m = 3$, Proposition 52(3) gives $\delta \geq \frac{1}{\sqrt{3}}(1 - \frac{W+3}{p} + \frac{3}{p^2})p^{-1}$ with $W \leq 4$, and $\kappa = 2$ needs $p^2 - (W + 6)p + 3 \geq 0$, which holds for $p \geq 10$. $\square$

The nets of Theorem 64, with their shifts, are digitally shifted digital nets over $\mathbb{F}_b, b \in \{2, 3\}$, in the sense of [11, Def. 2.2], so the corollary applies to them as well, with $\kappa_m = \lceil m/3 + \log_b(\sqrt{3}/c) \rceil$: for every digital shift with the constants c of part (3), and with the larger constants of part (1) for its explicit shifts. Likewise the per-prime nets of Remark 58, with the constants of Table 10, are well separated under every digital shift (Remark 132).

Remark 72 (Finitely many resolutions). Definition 3.8 of [11] constrains only $m \in I$, and finitely many further resolutions can be added at no cost. If $\mathcal{Q} \subset q^{-m}\mathbb{Z}^s \cap [0, 1)^s$ is a $(0, m, s)$ -net in base q , the elementary boxes of shape $(m, 0, \dots, 0)$ each hold one point, so the first coordinates of the points are distinct elements of $q^{-m}\mathbb{Z} \cap [0, 1)$ and any two of them have toroidal distance at least q^{-m} ; by Step 1 of the proof of Corollary 71, $\mathcal{Q}$ is m -separated and toroidally m -separated. Adding finitely many such m to I changes the $O(1)$ of [11, Def. 3.8] by a constant. In dimension three digital $(0, m, 3)$ -nets over $\mathbb{Z}/q\mathbb{Z}$ exist for every integer $q \geq 2$ (over $\mathbb{F}_p$ for every prime p) and every $m \geq 1$: by Lemma 10, whose proof does not use $m \equiv 0 \pmod{s}$, every box minor of the frame of the places $\infty, 0, 1$ is ± 1 , a unit modulo every q , so the frame is one (Lemma 1; see also [46, Thm. 6.2, Cor. 6.3] and [14, Sec. 8.2]), and trivially for $m = 0$. Together, Theorems 45 and 49, Corollary 57, Remark 58 and Theorem 64 cover all but finitely many m in each prime base with a constant independent of m ; with the frame nets for the remaining m they give well-separated families on all of $\mathbb{N}$, in every prime base. The same holds under every digital shift: the constants survive every shift (Proposition 68, Corollary 69, Remark 132 and Theorem 64(3)), and a digitally shifted $(0, m, s)$ -net is again a $(0, m, s)$ -net on the grid $q^{-m}\mathbb{Z}^s$ (Lemma 67), so the argument above applies to it.

8.3. The maximum norm. [11] measure separation and mesh ratios also in the maximum norm. Since $\|x\|_\infty \geq \|x\|_2/\sqrt{3}$, the Euclidean bound gives $\delta_\infty \geq (1 - 1/q)q^{-k}/\sqrt{3}$ for the nets of Theorem 45; the sign analysis in the proof of Theorem 46 gives more:

Proposition 73 (Maximum norm). *Let $q \geq 4, k \geq 2$. For every digital shift τ , any two distinct points of $\mathcal{P}_{k,q} \oplus \tau$ have toroidal ℓ^∞ -distance at least $(1 - 3/q)q^{-k}$. Hence the ℓ^∞ mesh ratio of $\mathcal{P}_{k,q} \oplus \tau$ in the sense of [11], toroidal or not, is at most $2q/(q - 3)$, and $\mathcal{P}_{k,q} \oplus \tau$ is toroidally $(k + 1)$ -separated [11, Def. 3.3].*

Proof. By Proposition 68 the proof of Theorem 46 applies to $\mathcal{P}_{k,q} \oplus \tau$. In its sign analysis every step has a coordinate with $|\Delta_i| \geq 1 - 3/q$ ($= \beta_3$ in that proof): an own-axis step has β_1 ; for $\nu = 2$, (iv) gives a backward coordinate with $|\sigma| \leq 1$ or $\sigma = 0$; for $\nu = 3$, a forward coordinate or a backward one with $|\sigma| = 3$ forces a backward one with $|\sigma| \leq 1$ by (ii), (iii), and otherwise all three are backward with $|\sigma| \leq 2$. One point per cell gives $h_\infty \leq q^{-k}$, and $(1 - 3/q)q^{-k} \geq q^{-k-1}$ for $q \geq 4$; the separation statement is Step 1 of the proof of Corollary 71. $\square$

The constant 3 is the exact ℓ^∞ value of the relaxation of Lemma 4 for this geometric layer, attained at the step $e = 1$ with three carries. For a dominant design (Proposition 19) every moving coordinate is backward with $|\sigma_i| \leq 2a$, so the same argument gives $\delta_\infty \geq (1 - (2a + 1)/q)q^{-k}$ and an ℓ^∞ mesh ratio at most $2q/(q - 2a - 1)$ for every $q \geq 2a + 2$ and every digital shift, in particular below $10/3$ for the nets of Theorem A(2).

The sequence question. All nets here depend on m ; they are not prefixes of one sequence, and the question of [11] for sequences (a sequence whose first q^m points are well separated for every m , [11, Def. 3.8]) remains open in dimension $s \geq 3$ (Remark 123(10)).

Part II. Separation constants

Part I proves bounds $\delta N^{1/s} \geq c$ with explicit constants c . Part II asks how large c can be. At the resolutions $m = sk$ the bounds of Part I have the form $1 - K/q$, and for a family of nets with $\delta N^{1/s} = 1 - K/q + O(q^{-2})$ as $q \rightarrow \infty$ we call K its *first-order deficit*, or simply its deficit. Sections 9 and 10 bound the deficit from above for given designs and from below for whole classes of nets. Section 11 explains the deficits $\frac{1}{3}$ and $\frac{2}{3}$ of the column nets, whose geometric layers have entries of size about $q/3$. Section 12 shows why the cubic value 1, the value of $\mathbb{Z}^s$ with one point per cell, is a natural barrier when the cells are cubes, and Section 13 goes beyond it.

9. THE FIRST-ORDER DEFICIT: CERTIFICATES AND CEILINGS

This section works with designs. Its first subsection turns the one-digit relaxation into a number, the *certified deficit* $K(F)$ of a design F , and shows how a finite computation (a *certificate*) proves the bound $1 - K(F)/q$ at every admissible base (defined after Proposition 75). The second subsection proves *ceilings*: upper bounds on $\delta N^{1/s}$ that hold for a whole class of nets. The remaining subsections give the designs with the smallest certified deficits that we have, in dimension four and at $k = 1$. Section 10 shows why the deficit must grow with s .

9.1. The certified deficit of a design. Remark 5 expands the relaxation LB of Lemma 4 for a fixed design as $1 - K/q + O(q^{-2})$; we now define this K precisely. Let $F = (F_0, \dots, F_{L-1})$ be a design with integer partial sums $M^{(j)}$. A *configuration* (e, j) is a step $e \in \{-1, 0, 1\}^s \setminus \{0\}$ with carry depths $j_d \in \{0, \dots, L-1\}$ on its moving axes, with $\sigma_i = \sum_d e_d M^{(j_d)}[i][d]$ and jit_i as in Lemma 4. A moving coordinate is backward or forward as in Remark 5: a *backward* coordinate ($e_i \sigma_i \leq 0$) has its geometric digit move against the step, so its point lands about one cell away; a *forward* one has it move with the step, so its point may land almost on that of its neighbour.

Definition 74 (Certified first-order deficit). The *cost* of a configuration is $|\sigma_b| + \text{jit}_b$ if exactly one moving coordinate b is backward, 0 if at least two are, and $+\infty$ if none is. The *certified deficit* $K(F)$ is the maximum of the cost over all configurations, and $\sigma_{\max}(F)$ is the maximum of $|\sigma_i|$ over all configurations and all i .

The cost counts, in units of $1/q$ of a cell, by how much the step falls short of a full cell at first order. A one-axis step along a with carry depth j has cost $\alpha_a^{(j)} = -M^{(j)}[a][a]$ if this is ≥ 0 , and $+\infty$ otherwise. For a dominant design (Proposition 19) every moving coordinate is backward, so $K(F) = \max_c \alpha_c$, the number a of Proposition 19. Both $K(F)$ and $\sigma_{\max}(F)$ are maxima over the $(2L+1)^s - 1$ configurations, and $\sigma_{\max}(F) = \max_i \sum_d \max_j |M^{(j)}[i][d]|$. The certified deficit is an upper bound for the deficit of every family of nets that realizes F (Proposition 75); it need not equal it.

Proposition 75 (Certificate for all large q). *Let F be a design with $K = K(F) < \infty$ and $\sigma_{\max} = \sigma_{\max}(F)$, and put*

$$q_{\text{tail}}(K, \sigma_{\max}) = \max\left(\sigma_{\max} + 1, \left\lceil \frac{\sqrt{2}(\sigma_{\max} + 1) - K}{\sqrt{2} - 1} \right\rceil\right).$$

Then $\text{LB} \geq 1 - K/q$ for every $q \geq q_{\text{tail}}(K, \sigma_{\max})$, where LB is the relaxation of Lemma 4 for F or for any truncation $(F_0, \dots, F_{L'-1})$, $L' \leq L$.

Proof. Fix a configuration and let $q \geq q_{\text{tail}}$, so $q > \sigma_{\max} \geq |\sigma_i|$ for all i . For a moving backward coordinate i the bound b_i of Lemma 4 is $q - |\sigma_i| - \text{jit}_i \geq 0$: for $e_i = 1$ and $-q < \sigma_i < 0$, $\bar{\sigma}_i = q + \sigma_i$ and the two options give $|q + t| \in \{2q - |\sigma_i|, q - |\sigma_i|\}$; for $\sigma_i = 0$ the only option gives q ; $e_i = -1$ is symmetric. If at least two coordinates are backward, $\sum_i b_i^2 \geq 2(q - \sigma_{\max} - 1)^2 \geq (q - K)^2$, because $\sqrt{2}(q - \sigma_{\max} - 1) \geq q - K$ is the second condition on q_{tail} (and $K \leq \sigma_{\max} + 1 \leq q$). If exactly one coordinate b is backward, $\sum_i b_i^2 \geq (q - |\sigma_b| - \text{jit}_b)^2 \geq (q - K)^2$. No backward coordinate is excluded by $K < \infty$. So every configuration gives $(\sum_i b_i^2)^{1/2}/q \geq 1 - K/q$. The configurations of a truncation are among those of F , with the same σ (Lemma 4, capped carry depths), so its LB is at least that of F . $\square$

For a dominant design $K = a$ and $\sigma_{\max} \leq 2a$, and $q_{\text{tail}} \leq \lceil ((2\sqrt{2}-1)a + \sqrt{2})/(\sqrt{2}-1) \rceil < 5a+4$ for $a \geq 1$: Proposition 75 is the proof of Proposition 19 without the dominance hypothesis. It turns every statement “ $\text{LB} \geq x$ for every admissible $q \geq q_0$ ” about a fixed design into a finite computation (a certificate): $K(F)$ and $\sigma_{\max}(F)$, and the exact value of LB at the finitely many admissible $q < \max(q_{\text{tail}}, K/(1-x))$. Here the *admissible* bases of a design are those for which Corollary 15 gives a net, $\gcd(q, DD') = 1$ (Definition 14); on the places $\infty, 0, 1, \dots, s-2$ they satisfy $\text{lpf}(q) \geq s-1$. This is how the thresholds below are certified.

The relaxation never certifies a deficit below 1:

Lemma 76 (The relaxation stops at one). *Let F be a design with some nonzero off-diagonal entry $F_0[a][b]$. Then $K(F) \geq 1$.*

Proof. Write $M = F_0$ and consider the carry-free steps $e = \mathbf{e}_a + \varepsilon \mathbf{e}_b$, $\varepsilon = \pm 1$, along which only a and b move, with $\sigma_a = M_{aa} + \varepsilon M_{ab}$ and $\varepsilon \sigma_b = M_{bb} + \varepsilon M_{ba}$. If for some ε at most one of a, b is backward, that configuration costs at least $\text{jit} = 1$, or $+\infty$. Otherwise $M_{aa} + \varepsilon M_{ab} \leq 0$ for both signs, so $M_{aa} \leq -|M_{ab}| \leq -1$, and the one-axis step along a without carry costs $-M_{aa} \geq 1$. $\square$

By Lemma 98(ii) (Section 12) the off-diagonal entries of the geometric layer of a digital $(0, sk, s)$ -net are units modulo q , hence nonzero. So for every design with $|F_0| < q/2$, whose geometric layer is F_0 , the bounds of Lemma 4 and Proposition 75 certify at most $1 - 1/q$ at first order. This concerns what the relaxation certifies, not the true distance; ceilings for the true distance are Corollary 78 and the results of Section 10. Deficits below 1 need layers whose entries grow with q ; for the column nets of Section 6.5 the minimum distance is determined in closed form instead (Theorem 49, Section 11).

9.2. The first-order ceiling. The idea of the ceiling: a step to the neighbouring cell along an axis a moves coordinate a by about $1 + \tilde{M}_{aa}/p$ cells and every other coordinate u by about $\tilde{M}_{ua}/p$, unless a digit wraps; the $t = 0$ property lets us count cells and find one where the digits behave as required.

Proposition 77. *Let p be an odd prime, $k \geq 2$, and let $\mathcal{P}$ be a digital $(0, 3k, 3)$ -net over $\mathbb{F}_p$ with normalized minimum distance $c = \delta N^{1/3}$ (toroidal or not). Let a, b, b' be the three coordinates x, y, z in some order.*

- (i) *If $\tilde{M}_{aa} \leq -1$, then $c^2 < (1 - 1/p + p^{1-k})^2 + ((|\tilde{M}_{ba}| + 1)^2 + (|\tilde{M}_{b'a}| + 1)^2)/p^2$.*

(ii) If $\tilde{M}_{aa} \geq 1$, then $c^2 < ((\tilde{M}_{aa} + 1)^2 + (|\tilde{M}_{ba}| + 1)^2 + (|\tilde{M}_{b'a}| + 1)^2)/p^2$.

Proof. Let $\mu \in \{1, \dots, p-1\}$ be the least nonnegative residue of $(\Phi_{aa})_{0,k-1}$, so $\mu = p + \tilde{M}_{aa}$ in (i) and $\mu = \tilde{M}_{aa}$ in (ii). Take a cell n with $n_a = 0$ and its neighbour $n + e_a$; only the last digit of n_a changes, so each offset digit of each coordinate changes by a constant modulo p , the first one of coordinate u by $(\Phi_{ua})_{0,k-1}$. Require (A) the first $k-1$ offset digits of a all equal $p-1$, and (B) for $u \in \{b, b'\}$, the first offset digit of u is not in the set W_u of the $|\tilde{M}_{ua}|$ digit values on which adding $\tilde{M}_{ua}$ leaves $\{0, \dots, p-1\}$. Under (A) the first offset digit of a becomes $\mu-1$, the next $k-2$ (all $p-1$) can only decrease, and the remaining digits contribute less than p^{1-k} . So in cell units $\Delta_a = \mu/p + \theta$ with $-1/p < \theta < p^{1-k}$. Under (B), the first offset digit of u changes by exactly $\tilde{M}_{ua}$, so $|\Delta_u| < (|\tilde{M}_{ua}| + 1)/p$. In (i), $0 < \Delta_a < 1 - 1/p + p^{1-k}$; in (ii), $0 < \Delta_a < \tilde{M}_{aa}/p + p^{1-k} \leq (\tilde{M}_{aa} + 1)/p$ since $k \geq 2$. It remains to find such a cell. The p^{2k} indices with $n_a = 0$ are parametrized by $(n_b, n_{b'})$. By the $t = 0$ boxes $(2k-1, k+1, 0)$ and $(2k-1, 0, k+1)$ (order a, b, b'), exactly p^{k+1} of them satisfy (A), and among these the first offset digits of b and of b' each take every value exactly p^k times. Hence at most $(|W_b| + |W_{b'}|)p^k \leq (p-1)p^k < p^{k+1}$ of them violate (B), since $|\tilde{M}_{ua}| \leq (p-1)/2$. The pair $n, n + e_a$ lies inside the cube, so it bounds the toroidal and the Euclidean distance. $\square$

Corollary 78 (First-order ceiling in dimension three). *Let p be an odd prime and $k \geq 2$. Suppose the first offset digit of some coordinate a of a digital $(0, 3k, 3)$ -net over $\mathbb{F}_p$ depends on the last cell digit of a with a coefficient whose centred representative is nonzero, and the coefficients of the other two coordinates on that digit are bounded by $C \geq 1$ in absolute value. If that representative is ≤ -1 and $k \geq 3$, then $\delta N^{1/3} < 1 - 1/p + 7C^2/p^2$. If it lies in $[1, C]$, then $\delta N^{1/3} < 4C/p$.*

Proof. The coefficient of the corollary is $\tilde{M}_{aa}$; let $|\tilde{M}_{ba}|, |\tilde{M}_{b'a}| \leq C$, $C \geq 1$. In (i) of Proposition 77, with $k \geq 3$, put $\alpha = 1 - 1/p + p^{1-k} \geq 2/3$ and $\beta = ((|\tilde{M}_{ba}| + 1)^2 + (|\tilde{M}_{b'a}| + 1)^2)/p^2 \leq 8C^2/p^2$; then $c < \sqrt{\alpha^2 + \beta} \leq \alpha + \beta/(2\alpha) \leq \alpha + 6C^2/p^2$, and $p^{1-k} \leq 1/p^2 \leq C^2/p^2$, so $c < 1 - 1/p + 7C^2/p^2$. In (ii), with $1 \leq \tilde{M}_{aa} \leq C$, $c^2 < 3(C+1)^2/p^2 \leq 12C^2/p^2$, so $c < 4C/p$. (For $k = 2$ the term $p^{1-k} = 1/p$ cancels the $-1/p$; hence $k \geq 3$.) $\square$

For $\mathcal{P}_{k,p}$ ($\tilde{M} = M$), Proposition 77(i) gives $c^2 < (1 - 1/p + p^{1-k})^2 + 8/p^2$, i.e. $c < 1 - 1/p + 4/p^2 + O(p^{-3})$ for $k \geq 4$ ($5/p^2$ for $k = 3$). So the lower bound $c(p) = 1 - 1/p$ of Theorem 45 is sharp to first order for $p \geq 11$. For $\tilde{M}_{aa} = 0$ the same counting (now with $0 < \Delta_a < 1 + 1/p$) only gives $c^2 < (1 + 1/p)^2 + ((|\tilde{M}_{ba}| + 1)^2 + (|\tilde{M}_{b'a}| + 1)^2)/p^2$.

Corollary 79 (Ceiling in every dimension). *Let $s \geq 3$, $k \geq 2$, and let $\mathcal{P}$ be a digital $(0, sk, s)$ -net over $\mathbb{Z}/q\mathbb{Z}$, $q \geq 3$, in graph form, with geometric layer $\tilde{M}$ and $c = \delta N^{1/s}$ (toroidal or not). Let a be a coordinate with $\sum_{u \neq a} |\tilde{M}_{ua}| < q$.*

(i) If $\tilde{M}_{aa} \leq -1$, then

$$c^2 < \left(1 - \frac{|\tilde{M}_{aa}|}{q} + q^{1-k}\right)^2 + \sum_{u \neq a} \frac{(|\tilde{M}_{ua}| + 1)^2}{q^2}.$$

(ii) If $\tilde{M}_{aa} \geq 1$, then

$$c^2 < \frac{(\tilde{M}_{aa} + 1)^2 + \sum_{u \neq a} (|\tilde{M}_{ua}| + 1)^2}{q^2};$$

in particular $c < \sqrt{s}(C+1)/q$ if $|\tilde{M}| \leq C$.

Proof. The proof of Proposition 77 applies with all counts multiplied by $q^{(s-3)k}$ and $\Delta_a = \mu/q + \theta$, $\mu = q + \tilde{M}_{aa}$ in (i), $\mu = \tilde{M}_{aa}$ in (ii) (where $0 < \Delta_a < (\tilde{M}_{aa} + 1)/q$ as $k \geq 2$). The boxes used

have depth 0 off a and the transverse coordinate considered, and total depth $\leq 3k \leq sk$; no field structure is used; and the union bound over $u \neq a$ leaves a cell because $\sum_{u \neq a} |\tilde{M}_{ua}| < q$. $\square$

So for a design whose certified deficit is attained by a one-axis step, $K(F) = -F_0[a][a]$, Proposition 75 and Corollary 79(i) together give $\delta N^{1/s} = 1 - K(F)/q + O(q^{-2})$ for $k \geq 3$, and for $k \geq 2$ when the deeper rows of the diagonal blocks vanish ((H2) of Lemma 4), which removes the term q^{1-k} ; this is the sharpness argument in the proof of Theorem A.

Remark 80 (The sign of the diagonal; diagonal zero). Case (i) of the sign analysis in the proof of Theorem 46 uses the diagonal entry -1 of M : on a step along its own axis a coordinate moves by $1 - 1/q$ cells, slightly less than a full cell, never slightly more. Replacing it by $+1$ (in $\mathcal{P}_{k,q}$: row k of E becomes $(Ed)_k = -d_{k-1} + d_k$, which changes only the entry $(\Phi_{cc})_{0,k-1}$ keeps $t = 0$ (Lemma 2(a)), but for odd prime q Proposition 77(ii) caps the minimum distance at $O(1/q)$. If $\tilde{M}_{aa} = 0$ for all a , Proposition 77 does not apply; heuristically such layers stay below $1 - 1/p$ at first order too, but the argument would need a joint condition on three digits that is not a single box, and we have no proof (Remark 123(1)).

9.3. Designs with small deficit. The design U_s^* of Theorem A is fixed by a rule (for each column and carry depth, a short admissible design column reduced against the earlier ones, Definition 23) and is not optimized for K . A local search over admissible design columns (Lemma 20) and over diagonals, with $K(F)$ evaluated exactly, gives the designs of Table 6. Its row scalars are fixed in advance: $\lambda' \equiv 1$ for $s = 4$, and for $s \geq 5$ the values $\lambda'_\infty = \frac{1}{2}$, all other $\lambda'_c = 1$, a choice taken over from an earlier search over row scalars for designs with small entries; the other row scalars we tried did not give a smaller $K(F)$. Each column of the partial sums $M^{(j)}$ is taken from a precomputed pool of short admissible columns; a move replaces the column of one pair (column, carry depth) by another from the pool, flips its sign, or changes a diagonal entry by ± 1 , and a move is kept if it lowers $K(F)$, or keeps $K(F)$ without raising the number of configurations that attain it; the search stops after a fixed running time. The search program is not part of the software deposit. The search only proposes designs; every entry of the table is certified for the design found, independently of how it was found. Each is reachable (Proposition 17, checked by exact interpolation), so by Corollary 15 it gives digital $(0, sk, s)$ -nets for every admissible q and every $k \geq 1$; by Proposition 75 and an exact scan of the smaller admissible q their relaxations certify the thresholds of the table for every $k \geq 1$.

9.4. Dimension four. We work out the smallest case beyond dimension three: a design with certified deficit two, which is also the true deficit of its nets. Remark 82 below explains why its entries have size two. For $s = 4$ and the places $\infty, 0, 1, 2$ the place differences are $\pm 1, \pm 2$, so $R = \mathbb{Z}[\frac{1}{2}]$. In the normal form (Propositions 12 and 17) column d of the partial sum $M^{(j)}$ has the entries $\lambda'_c w_{cd} g_{d,j}(y_{cd})$: up to scalars, the values of a polynomial of degree j at the nodes y_{cd} . The nodes of column d are $y = (0, 1, \frac{1}{2})$ on the rows $(\infty, 1, 2)$ for $d = 0$, $(0, -1, 1)$ on $(\infty, 0, 2)$ for $d = 1$, $(0, -\frac{1}{2}, -1)$ on $(\infty, 0, 1)$ for $d = 2$, and $(0, 1, 2)$ on $(0, 1, 2)$ for $d = \infty$; so the recurrence after Proposition 13 reads $v_n = \frac{3}{2}v_{n-1} - \frac{1}{2}v_{n-2}$, $v_n = v_{n-2}$, $v_n = -\frac{3}{2}v_{n-1} - \frac{1}{2}v_{n-2}$ and $v_n = 3v_{n-1} - 2v_{n-2}$ for $n \geq 3$.

Proposition 81 (Dimension four, deficit two; computer-assisted). *Let F be the design of Appendix A on the places $\infty, 0, 1, 2$ with $\lambda' \equiv 1$, and for odd q and $k \geq 1$ let $\mathcal{P}_{k,q}^F$ be the net of Definition 14, $N = q^{4k}$. Then:*

- (1) $\mathcal{P}_{k,q}^F$ is a digital $(0, 4k, 4)$ -net over $\mathbb{Z}/q\mathbb{Z}$ for every odd $q \geq 3$ and every $k \geq 1$; every box minor of its generator matrices over $\mathbb{Z}[\frac{1}{2}]$ is $\pm 2^i$, every cell holds exactly one point, and $h \leq 2N^{-1/4}$;

s	4	5	6	7	8
certified deficit $K(F)$	2	5	10	33	127
$\sigma_{\max}(F)$; largest $ M^{(j)} $	7; 2	21; 8	63; 22	194; 104	754; 254
ring R'	$\mathbb{Z}[\frac{1}{2}]$	$\mathbb{Z}[\frac{1}{6}]$	$\mathbb{Z}[\frac{1}{6}]$	$\mathbb{Z}[\frac{1}{30}]$	$\mathbb{Z}[\frac{1}{30}]$
q_{tail} (Prop. 75)	23	64	195	587	2272
$\text{LB} \geq 1 - K/q$ for $q \geq$	17	31	61	197	461
$\text{LB} \geq .5/.8/.9$ for $q \geq$	11/15/21	23/29/53	41/59/91	107/187/323	331/631/1261
a_s^* (Table 3)	5	16	43	170	543
lower bound on $K(F)$ (Prop. 90)	1	2	6	12	60
status	c.-a.	c.-a.	c.-a.	computed	computed

TABLE 6. Searched designs on the places $\infty, 0, 1, \dots, s-2$ (data: Appendix A for $s \leq 6$; all in the deposit). The thresholds hold for every admissible q from the value shown and every $k \geq 1$ (least such admissible values; admissible means $\text{lpf}(q) \geq s-1$: odd q for $s=4$, $\gcd(q, 6) = 1$ for $s=5, 6$, $\gcd(q, 30) = 1$ for $s=7, 8$). *c.-a.*: computer-assisted, by full enumeration of the $(2L+1)^s - 1 = (2s-1)^s - 1$ configurations ($L = s-1$), the exact relaxation at every admissible q below the tail, and Proposition 75 beyond it, reproduced by an independent implementation. For $s=7, 8$ the same computations were run and reproduced, but we state these rows as computed values only: their designs are not printed here, and the deposit scripts do not rerun these enumerations. The searched K are upper bounds for the best certified deficit of a design on these places, not optimal values. The lower bound $\text{lcm}(1, \dots, s-3)$ applies to every design whose row scalars are constant on the finite places, these included.

- (2) for every odd $q \geq 17$ and every $k \geq 1$ the toroidal (hence also Euclidean) minimum distance satisfies $\delta N^{1/4} \geq 1 - 2/q$;
(3) for every odd $q \geq 17$ and every $k \geq 2$, toroidal or Euclidean, $\delta N^{1/4} < 1 - 2/q + 8/q^2$.

So for $k \geq 2$ the first-order deficit of these nets is exactly 2.

Proof. (1) Exact interpolation shows that every column of every partial sum $M^{(j)}$ is admissible (Proposition 17): its polynomial $g_{d,j}$ has degree j , coefficients in $\mathbb{Z}[\frac{1}{2}]$ and leading coefficient $\pm 2^i$. So the residual problem is solvable over $R' = \mathbb{Z}[\frac{1}{2}]$, and Corollary 15 gives the net property with box minors in $\mathbb{Z}[\frac{1}{2}]^\times = \{\pm 2^i\}$, units modulo every odd q ; a cell has diameter $2q^{-k} = 2N^{-1/4}$.

(2) (H1) and (H2) of Lemma 4 hold by Proposition 13 and Definition 14, with $L = \min(k, 3)$. Full enumeration of the 2400 configurations gives $K(F) = 2$ and $\sigma_{\max}(F) = 7$, so $q_{\text{tail}} = 23$ and Proposition 75 gives $\text{LB} \geq 1 - 2/q$ for $q \geq 23$ and every $k \geq 1$. For $q = 17, 19, 21$ the exact relaxation (with $L = 3$, which bounds those with $L < 3$) is $\text{LB} = (q-2)/q$. The bound is attained: the one-axis step along ∞ without carry has $\sigma = (-2, 1, 1, 1)$, so $b = q-2$ for the moving coordinate and $b = 0$ for the others.

(3) As $|F_0| \leq 2 < q/2$, the geometric layer is $\tilde{M} = F_0$, and column ∞ of F_0 is $(-2, 1, 1, 1)$. This is the sharpness argument of Theorem A (Section 4.3). Equivalently, it is Corollary 79(i) with $a = \infty$ without its term q^{1-k} : that term accounts for the deeper offset digits of the moving coordinate, and here they do not change, by (H2). So the own-axis step e_∞ from a cell whose last digit of n_∞ is not $q-1$ and whose first offset digit r_∞ is at least 2 moves coordinate ∞ by exactly $1 - 2/q$ cells, and as $\sum_{u \neq \infty} |F_0[u][\infty]| = 3 < q$, the union bound of that argument leaves such a cell at which every other coordinate u moves by less than $(|F_0[u][\infty]| + 1)/q$. Hence

$c^2 < (1 - 2/q)^2 + 12/q^2$ for every $k \geq 2$, toroidal and Euclidean (the pair lies inside the unit cube). With $\alpha = 1 - 2/q \geq 15/17$ we get $c < \alpha + 6/(\alpha q^2) \leq 1 - 2/q + \frac{102}{15}/q^2 < 1 - 2/q + 8/q^2$. $\square$

Computer-assisted are the interpolation in (1), the two finite maxima $K(F)$, $\sigma_{\max}(F)$ and the values at $q = 17, 19, 21$; the rest is Proposition 75 and Corollary 79. The proved bound is $\geq .5$ from $q = 11$ and $\geq .8$ from $q = 15$ (Table 6). Whether $K = 1$ is possible for $s = 4$ is open; the entries of size two are explained by the following remark.

Remark 82 (Why the entries have size two). *For any four places with unit differences and every base $q \geq 2$ other than 3, no Cauchy layer $\lambda_c \mu_d w_{cd}$ ($c \neq d$) has all twelve off-diagonal entries in $\{\pm 1\}$ modulo q . Indeed, the two terms of Lemma 18(X) would be ± 1 , and $\pm 1 \pm 1 = 1$ forces $1 = 0$ or $3 = 0$ in $\mathbb{Z}/q\mathbb{Z}$. So in dimension four no net in the frame orbit (the nets obtained from a frame by scrambles and gauge moves, Section 3) has a ± 1 layer like the layer M of dimension three; this does not decide whether $K = 1$ is possible.*

9.5. The case $k = 1$. At $k = 1$ ($m = s$, $N = q^s$) the nets are of practical size. There are no carries (Lemma 4 at $k = 1$), so only the geometric layer F_0 enters the separation, and it can be optimized alone: its diagonal is free (Lemma 2(a)), its row and column scalars need not fit deeper carry depths, and F_0 need not come from a frame at all.

Proposition 83 (Separation at $k = 1$). *Let $q \geq 3$ and let $\mathcal{P}$ be a digital net over $\mathbb{Z}/q\mathbb{Z}$ in graph form with depths $(1, \dots, 1)$ ($m = s$, $N = q^s$) whose first offset rows form an integer matrix F_0 (diagonal included, reduced modulo q) and whose deeper rows vanish in their own column (the offset digits after the first do not depend on the point's own cell digit: (H2) of Lemma 4). Let $\text{LB}_1(q)$ be the relaxation LB of Lemma 4 for the design (F_0) ($L = 1$, $\sigma = F_0 e$), and $K_1 = K((F_0))$, $\sigma_{\max,1} = \sigma_{\max}((F_0))$ (Definition 74). Then:*

- (1) $\delta N^{1/s} \geq \text{LB}_1(q)$ (toroidal, hence Euclidean), and $\text{LB}_1(q) \geq 1 - K_1/q$ for $q \geq q_{\text{tail}}(K_1, \sigma_{\max,1})$;
- (2) for a design F realized by Definition 14, $\text{LB}_1(q)$ is at least the relaxation of F at the same q for every $k \geq 2$; so the lower bounds of Propositions 19 and 75 and of Theorem A(2) hold at $k = 1$;
- (3) let a be a coordinate with $-F_0[a][a] = K_1$ and let $q > 2 \max |F_0|$. If $\gcd(\det F_0, q) = 1$, or if $\mathcal{P}$ is a $(0, s, s)$ -net with $s \geq 4$ and $\sum_{u \neq a} |F_0[u][a]| < q$, then

$$\delta N^{1/s} < \left(\left(1 - \frac{K_1}{q} \right)^2 + \sum_{u \neq a} \frac{(|F_0[u][a]| + 1)^2}{q^2} \right)^{1/2}$$

for the toroidal distance, in the second case also for the Euclidean one. With (1), $\delta N^{1/s} = 1 - K_1/q + O(q^{-2})$.

Proof. (1) The hypotheses are (H1) and (H2) of Lemma 4 with $k = L = 1$; then Proposition 75. (2) At $k = 1$ Definition 14 realizes the truncated design (F_0) with vanishing deeper diagonal rows, and its configurations are those of F with all $j_d = 0$, with the same σ and jitter (after Lemma 4). (3) As $q > 2 \max |F_0|$, the centred layer is F_0 . Take the step e_a from a cell with $r_a \geq K_1$ and $r_u + F_0[u][a] \in [0, q)$ for every $u \neq a$. Then $\Delta r_a = -K_1$ exactly and $\Delta f_a = 0$ (the deeper rows of a vanish on n_a), so coordinate a moves by exactly $1 - K_1/q$ cells, and every $u \neq a$ by $(F_0[u][a] + \Delta f_u)/q$, of absolute value less than $(|F_0[u][a]| + 1)/q$. Such a cell exists: if $\gcd(\det F_0, q) = 1$, $n \mapsto r = F_0 n$ is a bijection of $(\mathbb{Z}/q\mathbb{Z})^s$, so r can be prescribed. In the second case, for each $u \neq a$ the box with depths 2 on a and on u , 0 on two further coordinates and 1 elsewhere (total s) makes (n_a, r_a, r_u) uniformly distributed (Lemma 1); among the cells with $n_a \neq q - 1$ and $r_a \geq K_1$ the fraction on which r_u wraps is $|F_0[u][a]|/q$, and the union bound

leaves a cell as $\sum_{u \neq a} |F_0[u][a]| < q$. With $n_a \neq q - 1$ the pair does not cross the boundary of the cube, so the bound holds for the Euclidean distance too. $\square$

If $\gcd(\det F_0, q) = 1$, every choice of the wraps of r in a step is realized, so for $q \geq 4$ the point set obtained by truncating every coordinate of $\mathcal{P}$ after its second digit has normalized minimum distance exactly ν_1 if $\nu_1 \leq 1$ (and at least 1 otherwise), where $\nu_1 = \min_e (\sum_c \min_t |qe_c + t_c|^2)^{1/2}/q$ with t_c over the two representatives of σ_c ; only the jitter of the deeper digits separates LB_1 from the exact value.

Proposition 84 (Designs for $k = 1$; computer-assisted). (1) *Frame layers. With its diagonal re-chosen for $k = 1$, the geometric layer F_0 of U_4^* has $K_1 = 2$, and that of the $s = 5$ design of Table 6 has $K_1 = 3$; a choice of the row and column scalars of the Cauchy layer gives $K_1 = 6$ for $s = 6$.* (2) *Frameless layers. Integer layers F_0 with entries of size at most 3, chosen directly, without a frame (Appendix A), completed by deeper rows chosen per prime factor of q , give digital $(0, s, s)$ -nets over $\mathbb{Z}/q\mathbb{Z}$ with $K_1 = 2$ for $s = 5$ at every q with $\gcd(q, 30) = 1$, and with $K_1 = 3$ for $s = 6$ at every q with no prime factor in $\mathcal{E}_6 = \{2, 3, 5, 7, 11, 13, 17, 23, 31\}$, with $\delta N^{1/s} \geq 0.8$ for every such $q \geq 13$ ($s = 5$) resp. $q \geq 19$ ($s = 6$).*

Proof. (1) is a finite computation of K_1 . (2) At $k = 1$ the frame is not needed. By Lemma 2, a box minor of a graph form with depths $(1, \dots, 1)$ is the determinant of stacked offset rows restricted to the coordinates of depth 0; those that use only the first offset rows are the minors $F_0[T, Z]$ with disjoint T, Z . If a prime p divides none of them, every box minor is a nonzero polynomial over $\mathbb{F}_p$ in the entries of the deeper rows (it is not the zero polynomial: take the deeper rows it uses to be unit vectors that complete the independent rows of F_0), of degree at most the number of deeper rows it uses, and by the Schwartz–Zippel lemma deeper rows with all box minors nonzero exist modulo p once p exceeds the sum $\text{SZ}(s)$ of these degrees ($\text{SZ}(5) = 105$, $\text{SZ}(6) = 504$); below it we constructed them explicitly for each admissible prime and certified $t = 0$. Any integer lift of such a completion modulo p works modulo p^a : every box minor is an integer polynomial in the entries, so it is congruent modulo p to the minor modulo p , and a determinant prime to p is a unit modulo p^a . The Chinese remainder theorem combines the lifts for the prime powers of q , and Lemma 1 gives the net property. The separation bounds are Proposition 83 with exact scans below its tail. Computer-assisted are the layers, K_1 , the per-prime completions up to $\text{SZ}(s)$ and the finite scans. $\square$

In every layer of Table 7 the deficit K_1 is attained by a one-axis step, so by Proposition 83(3) it is exact at first order.

10. WHY THE DEFICIT GROWS WITH THE DIMENSION

Up to Section 10.1, $\mathcal{P}$ is any digital $(0, sk, s)$ -net over $\mathbb{Z}/q\mathbb{Z}$ in graph form, with geometric layer $\tilde{M}$, and $c = \delta N^{1/s}$. A step $e = \mathbf{e}_a + \varepsilon \mathbf{e}_b$ without carries changes the first offset digits by the constants $\sigma_c = \tilde{M}_{ca} + \varepsilon \tilde{M}_{cb}$. The following *pair ceiling*, an upper bound from steps along two axes, is proved by the counting argument of Proposition 77; the proof is in Appendix B.

Proposition 85 (Pair ceiling). *Let $s \geq 4$, $3k + 4 \leq sk$ (so that the boxes of the proof, of total depth $3k + 4$, fit into sk digits), $a \neq b$, $\varepsilon = \pm 1$, and suppose $\sigma_a > 0$, $\varepsilon \sigma_b < 0$ and $\sum_c |\sigma_c| < q$. Then*

$$c^2 < \left(1 - \frac{|\sigma_b|}{q} + \frac{1}{q^2}\right)^2 + \frac{(\sigma_a + 1)^2 + \sum_{u \neq a, b} (|\sigma_u| + 1)^2}{q^2}.$$

If instead $\sigma_a > 0$ and $\varepsilon \sigma_b > 0$, then $c^2 < \sum_c (|\sigma_c| + 1)^2 / q^2 \leq s(2C + 1)^2 / q^2$, $C = \max |\tilde{M}|$.

s layer	K_1	bases q	$c \geq .5$	$c \geq .8$	$c \geq .9$	status
3 $\mathcal{P}_{k,q}$, $k = 2$ (Thm. 45)	1	every q	5; $1.5 \cdot 10^4$	7; $1.1 \cdot 10^5$	10; 10^6	proved
4 U_4^* , F_0	2	odd	7; $2.4 \cdot 10^3$	11; $1.4 \cdot 10^4$	21; $1.9 \cdot 10^5$	c.-a.
5 frameless	2	$(q, 30) = 1$	11; $1.6 \cdot 10^5$	13; $3.7 \cdot 10^5$	23; $6.4 \cdot 10^6$	c.-a.
5 frame (Table 6), F_0	3	$(q, 6) = 1$	13; $3.7 \cdot 10^5$	19; $2.4 \cdot 10^6$	31; $2.8 \cdot 10^7$	c.-a.
6 frameless	3	no prime factor in $\mathcal{E}_6$	19; $4.7 \cdot 10^7$	19; $4.7 \cdot 10^7$	37; $2.5 \cdot 10^9$	c.-a.
6 frameless	5	$(q, 210) = 1$	17; $2.4 \cdot 10^7$	29; $5.9 \cdot 10^8$	53; $2.2 \cdot 10^{10}$	c.-a.
6 frame, scalars searched	6	$(q, 6) = 1$	23; $1.4 \cdot 10^8$	37; $2.5 \cdot 10^9$	61; $5.1 \cdot 10^{10}$	c.-a.

TABLE 7. Proved separation at practical sizes: $k = 1$, $N = q^s$ (for $s = 3$ the row lists the net of Theorem 45 at $k = 2$, $N = q^6$). Each entry “ $q_0; N$ ” means $\delta N^{1/s} \geq c$ for every admissible base $q \geq q_0$ of that layer, with $N = q_0^s$ the smallest such size; frameless layers are chosen directly, without a frame (Proposition 84(2)). Rows with $s \geq 4$ follow from Proposition 83 and exact scans below the tail of Proposition 75 (computer-assisted; the frameless layers also need the per-prime completions of Proposition 84); the layers are listed in Appendix A. A base excluded by one layer may be covered by another: $q = 23$ is admissible for the second and third $s = 6$ layers but not for the first, and there no layer here proves $c \geq .8$. For comparison, at $k = 2$ Table 6 gives $c \geq .8$ from $N = 15^8 \approx 2.5 \cdot 10^9$ ($s = 4$), $29^{10} \approx 4.2 \cdot 10^{14}$ ($s = 5$) and $59^{12} \approx 1.7 \cdot 10^{21}$ ($s = 6$).

Definition 86. Let $\tilde{M}$ be a layer with nonzero diagonal. If some diagonal entry is positive, or some carry-free step $\mathbf{e}_a + \varepsilon \mathbf{e}_b$ has both moving coordinates forward, let $K_{\text{pair}}(\tilde{M}) = \infty$. Otherwise $K_{\text{pair}}(\tilde{M})$ is the largest of

- (a) $|\tilde{M}_{aa}|$ over the coordinates a , and
- (b) $|\sigma_b|$ over the carry-free steps $\mathbf{e}_a + \varepsilon \mathbf{e}_b$ (as above) in which a is forward and b is the only backward coordinate, with $\varepsilon \sigma_b < 0$.

By Corollary 79(i), (ii) and Proposition 85, for a layer with nonzero diagonal, $s \geq 4$, $k \geq 3$, $3k + 4 \leq sk$ and $q > 4sC$, $C = \max |\tilde{M}|$,

$$(3) \quad \delta N^{1/s} < 1 - \frac{K_{\text{pair}}}{q} + \frac{6sC^2}{q^2} \quad (K_{\text{pair}} < \infty), \quad \delta N^{1/s} < \frac{3\sqrt{s}C}{q} \quad (K_{\text{pair}} = \infty),$$

the latter by Corollary 79(ii) for a positive diagonal entry and by Proposition 85 for two forward coordinates. As K_{pair} sees only carry-free steps (carry depth 0) along one or two axes, it bounds the deficit of the nets from below. It is neither their deficit nor the certified deficit $K(F)$ of a design.

Theorem 87 (The deficit grows with s). *Let $\mathcal{P}$ be a digital $(0, sk, s)$ -net over $\mathbb{Z}/q\mathbb{Z}$ with $q \geq 2$, $s \geq 4$ and $k \geq 1$, whose layer $\tilde{M}$ has no zero diagonal entry. Then $K_{\text{pair}}(\tilde{M}) \geq \sqrt{(s-3)/8}$ (Definition 86). Hence, by (3) (which includes the case $K_{\text{pair}} = \infty$), a family of such nets with $k \geq 3$ and $3k + 4 \leq sk$ whose layers stay bounded, $|\tilde{M}| \leq C$, has $\delta N^{1/s} < 1 - \sqrt{(s-3)/8}/q + 6sC^2/q^2$ for $q > 4sC$.*

Proof. Let $K = K_{\text{pair}} < \infty$. Every diagonal entry is $-\alpha_a$ with $1 \leq \alpha_a \leq K$. Every pair has a small entry: if $|x| = |\tilde{M}_{ab}| > K$, put $\varepsilon = \text{sgn } x$; then $\sigma_a = -\alpha_a + |x| > 0$, so b is backward, $\varepsilon \sigma_b = \varepsilon y - \alpha_b \leq 0$ for $y = \tilde{M}_{ba}$, and if it is negative the definition gives $\alpha_b - \varepsilon y \leq K$; so $|y| \leq \max(\alpha_b, K - \alpha_b) \leq K$. Orient $c \rightarrow d$ when $|\tilde{M}_{cd}| \leq K$, and let $\text{out}(c)$ be the number of $d \neq c$ with $c \rightarrow d$. Every pair carries at least one arc, so $\sum_c \text{out}(c) \geq \binom{s}{2}$, and by convexity $\sum_c \binom{\text{out}(c)}{2} \geq s \binom{(s-1)/2}{2} = s(s-1)(s-3)/8$. The left side counts the triples $(c, \{d, d'\})$ with

$c \rightarrow d$ and $c \rightarrow d'$, so averaging over the $\binom{s}{2}$ pairs $\{d, d'\}$, some two columns d, d' have at least $(s-3)/4$ common rows $c \notin \{d, d'\}$ with $|\tilde{M}_{cd}|, |\tilde{M}_{cd'}| \leq K$. By $t = 0$ and Lemma 2, the box with depths $k+1$ on two such rows c, c' , $k-1$ on d, d' and k elsewhere makes every 2×2 minor $\tilde{M}_{cd}\tilde{M}_{c'd'} - \tilde{M}_{cd'}\tilde{M}_{c'd}$ a unit, hence nonzero, and the 1×1 boxes make the entries nonzero. So these rows give pairwise non-proportional vectors in $([-K, K] \setminus 0)^2$, of which there are at most $2K^2$ directions: $(s-3)/4 \leq 2K^2$. $\square$

K_{pair} is an integer ≥ 1 for a nonzero diagonal, so Theorem 87 first gives $K \geq 2$ at $s = 12$; its content is that the deficit is unbounded in s for bounded layers. The same count with $K = 1$ shows: *for $s \geq 5$ no digital $(0, sk, s)$ -net over any $\mathbb{Z}/q\mathbb{Z}$ has a geometric layer with all off-diagonal entries in $\{\pm 1\}$* (three rows of ± 1 entries on two columns contain two proportional rows). Layers with zero diagonal are open, as in Remark 80.

Inside the frame orbit (Section 3), for an integer design reachable over $\mathbb{Q}$ from rational places, the geometric layer F_0 is a Cauchy matrix $\lambda_c \mu_d / D_{cd}$, so Lemma 18(C), (H) apply over $\mathbb{Q}$ to $\pi_{cd} = \tilde{M}_{cd}\tilde{M}_{dc}$. For instance, for an all- ± 1 layer on four rational places identity (H) would read $1 = 1 + 1$, so no such layer exists (modulo q : Remark 82).

Theorem 88 (Frame designs have $K_{\text{pair}} \geq 2$ for $s \geq 5$). *Let $s \geq 5$ and let F be an integer design (Section 2) whose residual problem is solvable over $\mathbb{Q}$ for a frame of rational places, with nonzero diagonal of F_0 . Then $K_{\text{pair}}(F_0) \geq 2$; hence for $k \geq 3$, $3k + 4 \leq sk$ and every $q > 4sC$ coprime to DD' (Definition 14), $C = \max |F_0|$, $\delta N^{1/s} < 1 - 2/q + 6sC^2/q^2$ (for $q > 2C$ the layer is $\tilde{M} = F_0$, and (3) applies, including the case $K_{\text{pair}} = \infty$).*

Proof. Suppose $K_{\text{pair}} \leq 1$. Then every diagonal entry is -1 , and the definition of K_{pair} forces the *pair rule*: each pair $(\tilde{M}_{ab}, \tilde{M}_{ba})$ is in $\{\pm 1\}^2$, or one entry x has $|x| \geq 2$ and the other is $\text{sgn } x$ (the step $e_a + \varepsilon e_b$ has $\sigma_a = -1 + \varepsilon x$, $\sigma_b = y - \varepsilon$ for $(x, y) = (\tilde{M}_{ab}, \tilde{M}_{ba})$; if $|x| \geq 2$ and $\varepsilon = \text{sgn } x$, a is forward, so b is backward with $|\sigma_b| \leq 1$ whenever $\varepsilon \sigma_b < 0$, which with $y \neq 0$ forces $y = \text{sgn } x$). So pairs in one class of Lemma 18(C) have $\pi = -1$, and pairs across classes have an integer $\pi = P \geq 1$. A class of size ≥ 4 contradicts (H) ($1 = 1 + 1$), so for $s = 5$ the classes are $X = \{x_1, x_2, x_3\}$ and $Y = \{y_1, y_2\}$. For $\{x_i, x_j, y_1, y_2\}$, (H) gives $1 = 1/u + 1/v$ with integers $u^2 = P_{i1}P_{j2}$, $v^2 = P_{i2}P_{j1}$; squaring shows $u, v \in \mathbb{Q}$, hence integers, hence $u = v = 2$; so $P_{i1}P_{j2} = 4$ for all $i \neq j$, which forces $P_{i1} = \alpha$ for all i . Then the three pairings of $\{x_1, x_2, x_3, y_1\}$ all have magnitude $\alpha^{-1/2}$, and $1 = 2$ is false. For $s = 6$ a class of size ≥ 4 again contradicts (H), so both classes have size 3, and any five of the coordinates form classes of sizes 3 and 2, to which the case $s = 5$ applies; for $s \geq 7$ some class has size ≥ 4 . Since K_{pair} is an integer, $K_{\text{pair}} \geq 2$. $\square$

The proof uses that the entries are integers; designs that are Cauchy only modulo q are not covered (an extension to them, for instance for q larger than a polynomial in C , is not proved here). The argument needs $s \geq 5$: for $s = 4$ two classes of size two are consistent with (C) and (H) ($u = v = 2$, $P_{11}P_{22} = P_{12}P_{21} = 4$), and Remark 82 excludes only layers with all off-diagonal entries ± 1 .

10.1. Lower bounds for the deficit of frame designs. For a design F realized on a frame, $K(F)$ (Definition 74) is the deficit that the relaxation certifies, for every k . We now bound $K(F)$ from below, for every design with $K(F) < \infty$ and any number L of carry depths.

Lemma 89 (Orientation). *Let F be a design with $K = K(F) < \infty$. Then for every pair $a \neq b$ of coordinates, $|M^{(j)}[a][b]| \leq K$ for all j , or $|M^{(j)}[b][a]| \leq K$ for all j .*

Proof. One-axis steps give $0 \leq \alpha_c^{(j)} \leq K$ for all c and j . Suppose $u = M^{(j_1)}[a][b]$ and $v = M^{(j_2)}[b][a]$ have $|u|, |v| > K$. Take the step along a and b with carry depths $j_a = j_2$, $j_b = j_1$

and $e_a e_b = \varepsilon := \operatorname{sgn} u$. Then $e_a \sigma_a = -\alpha_a^{(j_2)} + |u| > 0$, so a is forward, and $e_b \sigma_b = \varepsilon v - \alpha_b^{(j_1)}$. If $\operatorname{sgn} v = \operatorname{sgn} u$, then b is forward too and the cost is $+\infty$; otherwise b is the only backward coordinate, of cost $\alpha_b^{(j_1)} + |v| + 1 > K$. Both contradict the definition of K . $\square$

So in every pair of coordinates one of the two entries is small at every carry depth; orienting the pair towards it gives the orientation used below.

Proposition 90 (Constant row scalars). *Let $s \geq 4$ and let F be an integer design with $L \geq 1$ levels reachable over $\mathbb{Q}$ (Proposition 17) from the places $\infty, 0, 1, \dots, s-2$ with row scalars λ' that take one value on all finite places (λ'_∞ arbitrary). If $K(F) < \infty$, then $K(F) \geq \operatorname{lcm}(1, \dots, s-3)$.*

Proof. Let $\nu = s-2$ and λ the common value. By Proposition 17 at carry depth 0, $M^{(0)}[c][d] = \lambda'_c g_{d,0} w_{cd}$ with $g_{d,0} \neq 0$; put $\mu_d = \lambda g_{d,0}$. In column 0 the finite rows $c = 1, \dots, \nu$ give the integers μ_0/c , so $\operatorname{lcm}(1, \dots, \nu)$ divides μ_0 and $|M^{(0)}[1][0]| = |\mu_0| \geq \operatorname{lcm}(1, \dots, \nu)$. In column 1 the rows $c \in \{0, 2, \dots, \nu\}$ give the integers $\mu_1/(c-1)$, $c-1 \in \{-1, 1, \dots, \nu-1\}$, so $|M^{(0)}[0][1]| = |\mu_1| \geq \operatorname{lcm}(1, \dots, \nu-1)$. Lemma 89 for the pair $\{0, 1\}$ gives $K(F) \geq \operatorname{lcm}(1, \dots, \nu-1)$. $\square$

The class of Proposition 90 contains the monomial design U_s , the design U_s^* of Theorem A and the designs of Table 6; within it the certified deficit grows at least like $\operatorname{lcm}(1, \dots, s-3) = e^{(1+o(1))s}$, by the prime number theorem [21, 12]. Elementarily, $\operatorname{lcm}(1, \dots, s-3) \geq 2^{s-3}/(s-2)$ (Chebyshev): the central binomial coefficient $\binom{s-3}{\lfloor (s-3)/2 \rfloor} \geq 2^{s-3}/(s-2)$ divides $\operatorname{lcm}(1, \dots, s-3)$, as each of its prime-power factors is at most $s-3$ by Kummer's theorem. For arbitrary row scalars a divisor count gives the weaker bound $K(F) \geq s^{1-o(1)}$ (Theorem 92). Let $Q_K = \{x/y : x, y \in \mathbb{Z}, 1 \leq |x|, |y| \leq K\}$, let $\operatorname{div}(j)$ be the number of divisors of a positive integer j , and $\operatorname{div}^*(x) = \max_{1 \leq j \leq x} \operatorname{div}(j)$. For finite places $w_{cd}/w_{cd'} = (a_c - a_{d'})/(a_c - a_d)$ is a cross-ratio of $a_c, a_d, a_{d'}$ and ∞ , whence the title of the next lemma.

Lemma 91 (A cross-ratio count). *Take the places $\infty, 0, 1, \dots, \nu$, two distinct places d, d' and a rational $\varrho \neq 0$, and let w_{cd} be as in Proposition 12. If $\mathcal{C}$ is a nonempty set of places $c \notin \{d, d'\}$ with $w_{cd}/w_{cd'} \in \varrho Q_K$ for all $c \in \mathcal{C}$, then $|\mathcal{C}| \leq 1 + 2K \operatorname{div}^*(\nu) \operatorname{div}^*(\nu K)^2$.*

Proof. A rational lies in Q_K if and only if its numerator and denominator in lowest terms are at most K in absolute value. Put $\varphi(c) = w_{cd}/w_{cd'}$. One of d, d' is ∞ . As $\varphi \mapsto 1/\varphi$ and $Q_K = Q_K^{-1}$, we may take $d' = \infty$; then c is finite and $\varphi(c) = 1/t$ with $t = c-d \in [-\nu, \nu] \setminus 0$, and the condition says $tQ'/P' \in Q_K$ for $\varrho^{-1} = P'/Q'$ in lowest terms. With $e = \gcd(t, P')$ the lowest terms of tQ'/P' are $(tQ'/e)/(P'/e)$, so $t = et'$ with $e \mid P'$ and $|t'| \leq K$: at most $2K \operatorname{div}(P')$ values. Some $c_0 \in \mathcal{C}$ gives $\varrho^{-1} \in t_0 Q_K$, so $|P'| \leq \nu K$. d, d' finite. Row ∞ has $\varphi = 1$ and contributes at most one element. For finite c put $u = c-d$ and $g = d-d' \neq 0$, so $\varphi(c) = (u+g)/u$; with $h = \gcd(u, g)$, $u = hu'$, $g = hg'$, this is $(u'+g')/u'$ in lowest terms. Let $\varrho = P/Q$ in lowest terms, $A = \gcd(Q, u')$ and $B = \gcd(P, u'+g')$. Then $\varphi(c)/\varrho = (\frac{Q}{A} \cdot \frac{u'+g'}{B}) / (\frac{P}{B} \cdot \frac{u'}{A})$ is in lowest terms (each pair of factors is coprime, by $\gcd(P, Q) = \gcd(u', u'+g') = 1$ and $\gcd(Q/A, u'/A) = \gcd(P/B, (u'+g')/B) = 1$), so $u'+g' = B\beta$ with $1 \leq |\beta| \leq K$. For fixed (h, A, B) , β determines $u' = B\beta - g'$, hence $c = d + hu'$: at most $2K \operatorname{div}(g) \operatorname{div}(Q) \operatorname{div}(P)$ places, with $|g| \leq \nu$ and, as above, $|P|, |Q| \leq \nu K$. $\square$

Theorem 92 (Frame designs). *Let $s \geq 5$ and let F be an integer design with $L \geq 1$ levels reachable over $\mathbb{Q}$ (Proposition 17) from the places $\infty, 0, 1, \dots, s-2$, or from their image under an element of $\operatorname{PGL}_2(\mathbb{Q})$ that contains ∞ (as the places of every frame do, Section 3.2), with arbitrary row scalars. If $K = K(F) < \infty$, then*

$$\frac{s-3}{4} \leq 1 + 2K \operatorname{div}^*(s-2) \operatorname{div}^*((s-2)K)^2.$$

Proof. By Lemma 89 at carry depth 0 every pair $\{c, d\}$ has an entry $|M^{(0)}[c][d]| \leq K$; orient $c \rightarrow d$ for such an entry. The convexity count in the proof of Theorem 87 gives columns $d \neq d'$ and a set $\mathcal{C}$ of at least $(s-3)/4$ rows $c \notin \{d, d'\}$ with $1 \leq |M^{(0)}[c][d]|, |M^{(0)}[c][d']| \leq K$ (entries at carry depth 0 are nonzero integers). By Proposition 17, $M^{(0)}[c][d] = \lambda'_c g_{d,0} w_{cd}$, so $w_{cd}/w_{cd'} = (g_{d',0}/g_{d,0}) M^{(0)}[c][d]/M^{(0)}[c][d']$ lies in ϱQ_K with $\varrho = g_{d',0}/g_{d,0}$, and Lemma 91 with $n = s-2$ bounds $|\mathcal{C}|$. For the image of the places under $g \in PGL_2(\mathbb{Q})$, in normalized homogeneous coordinates every D_{cd} , hence every w_{cd} , is multiplied by a factor depending only on c times one depending only on d ; the first cancels in $w_{cd}/w_{cd'}$ and the second changes only ϱ . $\square$

By Wigert's divisor bound $\log \operatorname{div}(j) = O(\log j / \log \log j)$ [25, Thm. 317], Theorem 92 gives $K(F) \geq s^{1-O(1/\log \log s)}$. The proof of Theorem 87 finds a small entry in every pair from the ceilings, so the same count bounds $K_{\text{pair}}(F_0)$ for integer designs reachable over $\mathbb{Q}$ from these places (or a $PGL_2(\mathbb{Q})$ -image that contains ∞) with nonzero diagonal, under the hypotheses of Theorem 87 and for $q > 2 \max |F_0|$; there the bound $\sqrt{(s-3)/8}$ improves to $s^{1-o(1)}$. Theorem 92 uses the integer places: it says nothing about other rational frames, split frames (Proposition 113), or layers that are Cauchy only modulo q . So on these places the least certified deficit of the frame designs lies between $s^{1-o(1)}$ and $a_s^* \leq e^{s \log s + O(s)}$ (Theorem A). Proposition 90 shows that row scalars constant on the finite places force a certified deficit at least $\operatorname{lcm}(1, \dots, s-3)$, so a certified deficit polynomial in s would need row scalars that differ between the finite places. Whether such designs exist is open.

11. DRIFT AND JITTER

The deficits of Section 9 are at least 1: Corollary 78 bounds the true distance for bounded layers with negative diagonal, and Lemma 76 shows that the one-digit relaxation of Lemma 4 never certifies a deficit below 1. The column nets of Section 6.5 have the deficits $\frac{1}{3}$ and $\frac{2}{3}$ (Theorem 49); their layer $1a^\top$ has entries between $\frac{q-2}{3}$ and $\frac{q+2}{3}$, and their local configuration is the reflected cube $H\mathbb{Z}^3$ ($\mathbb{Z}^3$ reflected in the plane $\mathbf{1}^\perp$, Section 6.5), not a slightly rotated $\mathbb{Z}^3$. This section explains these two numbers. Going once around the torus along an axis takes q steps from column to column. The reflected cube wants every step to raise the height by a third of a cell, and q thirds of a cell is not a whole number of cells when $3 \nmid q$. So the steps of each such cycle must deviate from the ideal by a forced total, the *holonomy* of the cycle. The *drift* is this forced deviation spread evenly over the cycle, and the *jitter* is the further deviation caused by the third digit. Theorem 95 shows that the resulting deficits $\frac{1}{3}$ and $\frac{2}{3}$ are optimal among all column point sets that are $(0, 3, 3)$ -nets, digital or not. Section 13.7 applies the same bookkeeping to the half-integer layers of dimension five, where it lowers the base from which the constants exceed 1.

The two words are used in the same sense in the rest of Part II. The *drift* of a step is the part of the change of the offsets that comes from the geometric digits, beyond their limit as $q \rightarrow \infty$: it is of order $1/q$ of a cell per step, so the points deviate from the limit configuration by a ramp that is linear in the cell. The *jitter* is the part that comes from the deeper digits (Section 2). For the column nets the limit configuration is the reflected cube, and the drift of a step along $\mathbf{e}_i$ is $w_i/(3q)$ of a cell (Lemma 93).

11.1. Excess, drift and jitter. Let X be a column point set in base q (Section 6.5). On a step from the column $[n]$ to $[n + \mathbf{e}_i]$ the height changes by $\Delta_i([n]) = \varphi([n + \mathbf{e}_i]) - \varphi([n])$ (Theorem 48); let u be its representative modulo q^2 in $(-\frac{1}{6}q^2, \frac{5}{6}q^2]$, and call $\xi = u - \frac{1}{3}q^2$ the *excess* of the step. In $H\mathbb{Z}^3$ each step to a neighbouring column raises the height by a third of a cell, $\frac{1}{3}q^2$ at integer scale q^3 , so the excess measures the deviation from the reflected cube. If every excess lies in

$[-\frac{1}{6}q^2, \frac{1}{3}q^2]$, then $\text{dist}(u, \frac{2}{3}q^2 + q^2\mathbb{Z}) = \frac{1}{3}q^2 - \xi$, so in Theorem 48 $g = \frac{1}{3}q^2 - \eta$ with η the largest excess, and

$$d^2 = q^4 - 2q^2\eta + 3\eta^2, \quad \delta N^{1/3} = 1 - \frac{\eta}{q^2} + O\left(\frac{\eta^2}{q^4}\right).$$

The excesses are integers at scale q^3 , where a cell has side q^2 : an excess η costs η/q^2 of a cell, that is, a first-order deficit η/q . For the digital column nets whose shared second digit is $a \cdot n$ with $a = \frac{1}{3}(q\mathbf{1} + w) \approx \frac{q}{3}\mathbf{1}$, as in Definition 47, the excess splits into two terms.

Lemma 93 (Drift and jitter). *Let $q \geq 2$ with $3 \nmid q$, let $w \in \mathbb{Z}^3$ with $w_x + w_y + w_z = 0$ and $w_c \equiv -q \pmod{3}$, $a = \frac{1}{3}(q\mathbf{1} + w)$, and $b \in \mathbb{Z}^3$ with $b_x + b_y + b_z \equiv 0 \pmod{q}$ (the third-digit row, as in Definition 47); let X be the digital net over $\mathbb{Z}/q\mathbb{Z}$ whose point of cell n has, in every coordinate c , the digits n_c , $a \cdot n$, $b \cdot n$ (a digital column net; $\mathcal{C}_q$ is the case of Definition 47), and let $\bar{b}_i \in \{0, \dots, q-1\}$ be the residue of b_i (a third-digit step, not a geometric digit). Put $\varepsilon_i = \frac{1}{3}qw_i + \bar{b}_i$.*

- (1) *A step along $\mathbf{e}_i$ has $\Delta_i \equiv \frac{1}{3}q^2 + \varepsilon_i$ if the third digit $b \cdot n$ does not wrap (does not pass from $q-1$ to 0) and $\Delta_i \equiv \frac{1}{3}q^2 + \varepsilon_i - q$ if it wraps, modulo q^2 ; if $\bar{b}_i \neq 0$ both occur.*
- (2) *Along each cycle of q steps in the direction $\mathbf{e}_i$ the third digit wraps exactly $\bar{b}_i$ times. If moreover $|\varepsilon_i| < \frac{1}{2}q^2$ and $|\varepsilon_i - q| < \frac{1}{2}q^2$ (for instance if $|w_i| \leq 2$ and $q \geq 4$), the excesses of the cycle are ε_i and $\varepsilon_i - q$, and they sum to $\frac{1}{3}q^2w_i$.*
- (3) *If $q \geq 10$ and $|w_c| \leq 2$, then $\eta = \max_i \varepsilon_i$, so $d^2 = q^4 - 2q^2\eta + 3\eta^2$.*
- (4) *If X is a $(0, 3, 3)$ -net, then $\varepsilon_x + \varepsilon_y + \varepsilon_z \geq q$, and $\max_i \varepsilon_i \geq \frac{1}{3}q$; if moreover $q \equiv 1 \pmod{3}$, then $\max_i \varepsilon_i \geq \frac{2}{3}q$.*

Proof. (1) The digit $a \cdot n$ changes by a_i and $b \cdot n$ by $\bar{b}_i$ modulo q , so $\Delta_i \equiv qa_i + \bar{b}_i - q\omega = \frac{1}{3}q^2 + \frac{1}{3}qw_i + \bar{b}_i - q\omega$ modulo q^2 , with $\omega \in \{0, 1\}$ the wrap of the third digit (a wrap of $a \cdot n$ changes Δ_i by q^2). (2) Along a cycle the third digit takes the values $b \cdot n + t\bar{b}_i \pmod{q}$, $t = 0, \dots, q-1$, and returns after a total increase $q\bar{b}_i$, so it wraps exactly $\bar{b}_i$ times and does not wrap $q - \bar{b}_i \geq 1$ times; this also shows that both cases of (1) occur if $\bar{b}_i \neq 0$. Under the range condition the representatives $\frac{1}{3}q^2 + \varepsilon_i$ and $\frac{1}{3}q^2 + \varepsilon_i - q$ of (1) lie in the window $(-\frac{1}{6}q^2, \frac{5}{6}q^2]$, so the excesses are ε_i and $\varepsilon_i - q$, and those of the cycle sum to $q\varepsilon_i - q\bar{b}_i = \frac{1}{3}q^2w_i$. (Without it the identity can fail: for $q = 5$, $w = (-8, 4, 4)$ and $b = (0, 1, -1)$ the excesses of a cycle in the direction $\mathbf{e}_x$ sum to $\frac{175}{3}$, not $-\frac{200}{3}$.) (3) Then $-\frac{5}{3}q \leq \varepsilon_i - q < \varepsilon_i \leq \frac{5}{3}q$, and $\frac{5}{3}q \leq \frac{1}{6}q^2$ for $q \geq 10$, so every excess lies in $[-\frac{1}{6}q^2, \frac{1}{3}q^2]$ and the largest one is $\max_i \varepsilon_i$ (attained, since the third digit does not wrap on some step of each cycle, by (2)). (4) As $w_x + w_y + w_z = 0$, $\sum_i \varepsilon_i = \sum_i \bar{b}_i \equiv \sum_i b_i \equiv 0 \pmod{q}$, and $\bar{b} \neq 0$: otherwise $b \equiv 0$ and the box with depth 3 on a coordinate, whose minor is a 2×2 minor of (a, b) (Lemma 2), would be singular. So $\sum_i \bar{b}_i \geq q$ and $\max_i \varepsilon_i \geq \frac{1}{3}q$. For $q \equiv 1 \pmod{3}$, $w_c \equiv 2 \pmod{3}$ and $\sum_c w_c = 0$, so some $w_c \geq 2$ and $\varepsilon_c \geq \frac{2}{3}q$. $\square$

We call $\frac{1}{3}qw_i$, the mean excess per step of a cycle in the direction $\mathbf{e}_i$, the *drift* of that direction, and $\bar{b}_i$, the step of the third digit, its *jitter*: on the $q - \bar{b}_i$ steps of a cycle where the third digit does not wrap the excess is the drift plus $\bar{b}_i$, and on the $\bar{b}_i$ steps where it wraps it is the drift plus $\bar{b}_i - q$. By (3) and (4), the digital column nets with $|w_c| \leq 2$ have $\eta \geq \frac{1}{3}q$, so their deficit is at least $\frac{1}{3}$, or $\frac{2}{3}$ for $q \equiv 1 \pmod{3}$: by (4) the net property forces the third-digit steps $\bar{b}_x + \bar{b}_y + \bar{b}_z$ to add up to at least q , which the three directions share, and for $q \equiv 1 \pmod{3}$ the integrality of a alone forces some direction to have drift at least $\frac{2}{3}q$. For $\mathcal{C}_q$ (Definition 47), $\bar{b} = (q-1, 1, 0)$ and

$$\begin{aligned} \varepsilon &= \left(\frac{1}{3}q - 1, \frac{1}{3}q + 1, \frac{1}{3}q\right) & (q \equiv 2, w = (-2, 1, 1)), \\ \varepsilon &= \left(\frac{2}{3}q - 1, 1 - \frac{1}{3}q, \frac{2}{3}q\right) & (q \equiv 1, w = (-1, -1, 2)), \end{aligned}$$

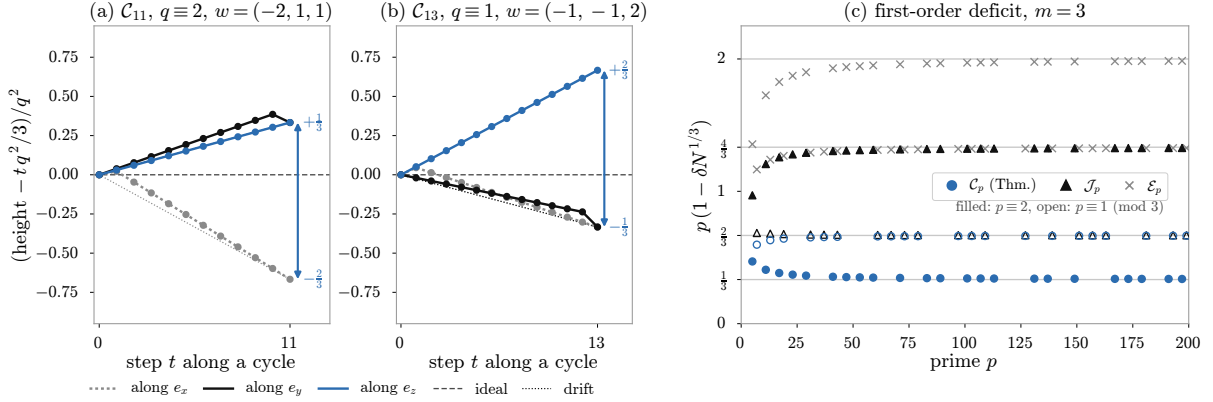


FIGURE 10. Drift and jitter. (a), (b) The holonomy: along the three cycles of q steps through the column of the cell 0, the heights φ (each step value taken near $\frac{1}{3}q^2$) minus the ideal $\frac{1}{3}q^2$ per step of the reflected cube, in units of q^2 . After q steps the ideal heights would end at $\frac{q}{3}$, not an integer, but the heights must return modulo q^2 : the heights of the cycles of C_{11} end at 3, 4, 4 (times q^2) and those of C_{13} at 4, 4, 5, so the excess sums to the forced leftover $\frac{1}{3}w_c$ (accent arrows). Thin dotted: the drift, $\frac{1}{3}w_c$ spread evenly over the cycle; the jitter adds the residue $\bar{b}_c$ of the third digit on the steps where it does not wrap and subtracts $q - \bar{b}_c$ where it does (Lemma 93). The first-order deficit is η/q , with η the largest step excess, $\frac{q}{3} + 1$ resp. $\frac{2}{3}q$. (c) The first-order deficit $p(1 - \delta N^{1/3})$ at the primes $5 \leq p \leq 199$: the column nets C_p (exact, Theorem 49) tend to $\frac{1}{3}$ ($p \equiv 2$) and $\frac{2}{3}$ ($p \equiv 1 \pmod 3$). For comparison two nets that share the second digit $\lfloor p/3 \rfloor \Sigma n$ in all coordinates, so that their drift vector is fixed at $w = -\gamma \mathbf{1}$, $\gamma \in \{1, 2\}$ (computed exact values): $\mathcal{J}_p$ with the third digit $\frac{1}{2}(-n_c - n_{c+1} + n_{c+2})$ tends to $\frac{2}{3}$ and $\frac{4}{3}$, and $\mathcal{E}_p$ with the third digit n_{c+1} to $\frac{4}{3}$ and 2. Interactive version: [explainers/anatomy.html](#) (Section 1).

so $\eta = \frac{1}{3}q + 1$ resp. $\frac{2}{3}q$, in agreement with Theorem 49. Both nets put the residue $q - 1$ (a third digit that wraps on $q - 1$ of the q steps of each cycle and adds $q - 1$ to the excess on the remaining step, Lemma 93(2)) on a direction with the most negative drift, $w_x = -2$ resp. $w_x = -1$, where the excess stays below the maximum, and the residue 0 on a direction with the largest drift. Figure 10(a) shows the excesses along the three cycles through one column.

11.2. The holonomy, and the optimum among column nets. No column point set beats the cubic value $\delta N^{1/3} = 1$, and among those that are $(0, 3, 3)$ -nets the column nets of Definition 47 are optimal.

Corollary 94 (Column ceiling). *Every column point set in base $q \geq 2$ has $g \leq \frac{1}{3}q^2$ in Theorem 48, i.e. toroidal minimum distance at most q^2 at integer scale q^3 : $\delta N^{1/3} \leq 1$.*

Proof. If $g > \frac{1}{3}q^2$, every step value $\Delta_i([n])$ has distance more than $\frac{1}{3}q^2$ from $\frac{2}{3}q^2 + q^2\mathbb{Z}$, so its residue modulo q^2 lies in the open interval $(0, \frac{1}{3}q^2)$. The three steps $[n] \rightarrow [n + \mathbf{e}_x] \rightarrow [n + \mathbf{e}_x + \mathbf{e}_y] \rightarrow [n + \mathbf{1}] = [n]$ have step values that sum to 0, so their residues sum to a multiple of q^2 ; but that sum lies in $(0, q^2)$. $\square$

So a net at $m = 3$ with $\delta N^{1/3} > 1$ cannot be a column point set. Proposition 103 shares the geometric digit between two coordinates only, and Proposition 104 uses a layer of rank one, not of the column form $\mathbf{1}a^\top$, under which all three coordinates still wrap together (Section 13.3).

Theorem 95 (Column optimum). *Let $q \geq 2$.*

- (1) *A column point set, with the set of columns $\mathbb{T}$ and the heights φ of Section 6.5, is a $(0, 3, 3)$ -net in base q if and only if φ is a bijection from $\mathbb{T}$ onto $\{0, \dots, q^2 - 1\}$ and $\lfloor \varphi/q \rfloor$ is injective on every line of $\mathbb{T}$ in the directions $[\mathbf{e}_x]$, $[\mathbf{e}_y]$, $[\mathbf{e}_z]$.*
- (2) *If q is even, no column point set is a $(0, 3, 3)$ -net in base q .*
- (3) *If $q \geq 5$ is odd and $3 \nmid q$, every column point set that is a $(0, 3, 3)$ -net in base q has toroidal minimum distance d with $d^2 \leq d^2(\mathcal{C}_q)$, the value of Theorem 49(2); equivalently $\eta \geq \frac{1}{3}q + 1$ for $q \equiv 2$ and $\eta \geq \frac{2}{3}q$ for $q \equiv 1 \pmod{3}$, where $\eta = \frac{1}{3}q^2 - g$.*

Proof. (1) The point of cell n has the digits n_c , $\lfloor \varphi/q \rfloor$, $\varphi \bmod q$ in every coordinate. The box of shape $(1, 1, 1)$ holds one point per cell. A box with depth 3 on c prescribes n_c and φ ; the q^2 cells with a given n_c meet every column exactly once ($n + t\mathbf{1}$ for the one t with $n_c + t$ given), so these boxes hold one point each if and only if φ is a bijection. A box with depth 2 on c , 1 on c' and 0 on c'' prescribes n_c , $n_{c'}$ and $\lfloor \varphi/q \rfloor$; the q cells with given $n_c, n_{c'}$ form a line in the direction $\mathbf{e}_{c''}$, whose columns form a line of $\mathbb{T}$ in the direction $[\mathbf{e}_{c''}]$, and every such line of $\mathbb{T}$ arises. These are all box shapes.

(2) Identify $\mathbb{T}$ with $(\mathbb{Z}/q\mathbb{Z})^2$ by $[n] \mapsto (n_x - n_z, n_y - n_z)$; the lines in the directions $[\mathbf{e}_x]$, $[\mathbf{e}_y]$, $[\mathbf{e}_z]$ become the horizontal lines, the vertical lines and the lines of slope 1 of $(\mathbb{Z}/q\mathbb{Z})^2$. A level set $\{\lfloor \varphi/q \rfloor = v\}$ has q elements and meets each of these lines once, by (1). So it is the graph of a permutation π of $\mathbb{Z}/q\mathbb{Z}$ (once on every horizontal and every vertical line) such that $y \mapsto \pi(y) - y$ is a permutation too (once on every line of slope 1). Then $\sum_y (\pi(y) - y) \equiv 0$, while the sum over all residues is $\frac{q}{2} \not\equiv 0 \pmod{q}$ for even q . In other words, $y \mapsto \pi(y) - y$ is a complete mapping of $\mathbb{Z}/q\mathbb{Z}$, and this is the classical argument that a cyclic group of even order has none [48, Thm. 1 and its corollary]; more generally, no finite group with a nontrivial cyclic Sylow 2-subgroup has one [29, Thm. 5]. In the language of Latin squares, (1) says that each level set is a transversal of the cyclic Latin square $(a, b) \mapsto b - a$, and that the array $\lfloor \varphi/q \rfloor$ on $(\mathbb{Z}/q\mathbb{Z})^2$ is a Latin square orthogonal to it.

(3) Put $\eta = \frac{1}{3}q^2 - g$. By Corollary 94, $0 \leq \eta \leq \frac{1}{3}q^2$, and by Theorem 48 $d^2 = q^4 - 2q^2\eta + 3\eta^2$, which decreases in η on this interval and equals $d^2(\mathcal{C}_q)$ at $\eta_0 = \frac{1}{3}q + 1$ ($q \equiv 2$) resp. $\eta_0 = \frac{2}{3}q$ ($q \equiv 1$). So it suffices to show $\eta \geq \eta_0$. Suppose $\eta < \eta_0$.

Then $\eta < \frac{1}{12}q^2$. For $q \geq 8$ this holds because $\eta_0 \leq \frac{1}{12}q^2$. For $q = 5$ and 7 : $3g = |3U + q^2|$ for an integer U , which is not divisible by 3 since $q^2 \equiv 1 \pmod{3}$, so $3\eta = q^2 - 3g \equiv 0$ or $2 \pmod{3}$; hence $\eta < \frac{8}{3}$ gives $\eta \leq 2 < \frac{25}{12}$ at $q = 5$, and $\eta < \frac{14}{3}$ gives $\eta \leq 4 < \frac{49}{12}$ at $q = 7$.

Windows and triangles. Every step value has distance at least $\frac{1}{3}q^2 - \eta$ from $\frac{2}{3}q^2 + q^2\mathbb{Z}$, so it has a unique representative u in the window $[-\eta, \frac{1}{3}q^2 + \eta]$ modulo q^2 (narrower than the window of Section 11.1). As $[\mathbf{e}_x] + [\mathbf{e}_y] + [\mathbf{e}_z] = 0$ in $\mathbb{T}$, for every column and every order of the three directions the three steps around the triangle $[n] \rightarrow [n + \mathbf{e}_i] \rightarrow [n + \mathbf{e}_i + \mathbf{e}_{i'}] \rightarrow [n]$ have values summing to 0, so their representatives sum to a multiple of q^2 in $[-3\eta, q^2 + 3\eta]$, i.e. to 0 or q^2 . In a triangle with sum 0 every u lies in $[-\eta, 2\eta]$, and in one with sum q^2 every u lies in $[\frac{1}{3}q^2 - 2\eta, \frac{1}{3}q^2 + \eta]$; as $\eta < \frac{1}{12}q^2$ these ranges are disjoint, so two triangles that share a step have the same sum. The step $([n], i)$ shares a triangle with $([n + \mathbf{e}_i], i')$ for both $i' \neq i$, and two such moves give $([n + \mathbf{e}_i + \mathbf{e}_{i'}], i) = ([n - \mathbf{e}_{i''}], i)$; and the classes $[\mathbf{e}_{i''}]$, $i'' \neq i$, generate $\mathbb{T}$; so all steps are connected through shared triangles, and all triangles have the same sum. Sum q^2 means that every step is close to $\frac{1}{3}q^2$, the configuration of the reflected cube $H\mathbb{Z}^3$; sum 0 means that every step is close to 0, the configuration of $\mathbb{Z}^3$.

Sum q^2 (the reflected cube). Put $\xi = u - \frac{1}{3}q^2 \in [-2\eta, \eta]$, the excess; then $\text{dist}(u, \frac{2}{3}q^2 + q^2\mathbb{Z}) = \frac{1}{3}q^2 - \xi$, so η is the largest excess, and every triangle has excess sum 0. The class $[\mathbf{e}_i]$ has order q in $\mathbb{T}$, so the steps in the direction $\mathbf{e}_i$ form q cycles γ of length q . Along a cycle the step values telescope to 0, so $\sum_{\gamma} u \in q^2\mathbb{Z}$, and the *cycle excess* $\Xi_{\gamma} = \sum_{\gamma} \xi \in q^2\mathbb{Z} - \frac{1}{3}q^3$. Summing the excess over the triangles $[n] \rightarrow [n + \mathbf{e}_x] \rightarrow [n + \mathbf{e}_x + \mathbf{e}_y] \rightarrow [n]$ for all $[n] \in \mathbb{T}$ counts every step once, so the $3q$ cycle excesses sum to 0. Also $-2q\eta \leq \Xi_{\gamma} \leq q\eta$. If $q \equiv 1 \pmod{3}$, then $\Xi_{\gamma} = q^2 z_{\gamma} - \frac{1}{3}q^2$ with integers z_{γ} (as $\frac{1}{3}q^3 \equiv \frac{1}{3}q^2$), and the cycle excesses sum to 0 only if $\sum_{\gamma} z_{\gamma} = q$. So some $z_{\gamma} \geq 1$, $\Xi_{\gamma} \geq \frac{2}{3}q^2$, and $q\eta \geq \frac{2}{3}q^2$: $\eta \geq \frac{2}{3}q$, a contradiction. If $q \equiv 2 \pmod{3}$, then $\Xi_{\gamma} = q^2 z_{\gamma} - \frac{2}{3}q^2$ and $\sum_{\gamma} z_{\gamma} = 2q$. Every excess lies in $\mathbb{Z} + \frac{2}{3}$ (as $u \in \mathbb{Z}$ and $\frac{1}{3}q^2 \in \mathbb{Z} + \frac{1}{3}$), and so does $\frac{1}{3}q$; hence $\eta < \frac{1}{3}q + 1$ gives $\eta \leq \frac{1}{3}q$, and then every $\Xi_{\gamma} \in [-\frac{2}{3}q^2, \frac{1}{3}q^2]$, i.e. $\Xi_{\gamma} \in \{-\frac{2}{3}q^2, \frac{1}{3}q^2\}$. A cycle excess $\frac{1}{3}q^2 \leq q\eta$ forces $\xi = \eta = \frac{1}{3}q$ on each step of its cycle, and a cycle excess $-\frac{2}{3}q^2 \geq -2q\eta$ forces $\xi = -2\eta = -\frac{2}{3}q$ on each step. So every step has $u = \frac{1}{3}q(q+1)$ or $\frac{1}{3}q(q-2)$, a multiple of q , and φ is constant modulo q on $\mathbb{T}$. This contradicts (1): φ takes every value in $\{0, \dots, q^2 - 1\}$.

Sum 0 (the cube). Now $u \in [-\eta, 2\eta]$ and $\text{dist}(u, \frac{2}{3}q^2 + q^2\mathbb{Z}) = u + \frac{1}{3}q^2$, so $\min u = -\eta$. The cycle sums $\sum_{\gamma} u$ lie in $q^2\mathbb{Z}$ and add up to 0. If one of them is nonzero, one is at most $-q^2$; it is at least $-q\eta$, so $\eta \geq q$. Otherwise every cycle closes: the partial sums S_t of u along a cycle are integers with $S_t \equiv \varphi(c_t) - \varphi(c_0) \pmod{q^2}$, where c_t are its columns. By (1) the q values $\varphi(c_t)$ lie in q different blocks $[kq, kq+q)$, so the q values $\varphi(c_0) + S_t$ meet all q blocks modulo q^2 ; an interval of integers of length rg meets at most $\text{rg}/q + 2$ of them, so the range of the walk is $\text{rg} \geq q(q-2)$. Here $\eta > 0$, since $\eta = 0$ would make every step value 0 and $\text{rg} = 0 < q(q-2)$. A closed walk whose up-steps are at most 2η and whose down-steps are at least $-\eta$ needs at least $\text{rg}/(2\eta) + \text{rg}/\eta$ steps, so $q \geq 3\text{rg}/(2\eta)$ and $\eta \geq \frac{3}{2}(q-2)$. Both q and $\frac{3}{2}(q-2)$ are at least $\frac{2}{3}q \geq \eta_0$ for $q \geq 4$, a contradiction.

Equality holds for $\mathcal{C}_q$ by Theorem 49(2). $\square$

So among column nets the first-order deficits $\frac{1}{3}$ ($q \equiv 2$) and $\frac{2}{3}$ ($q \equiv 1 \pmod{3}$) are optimal, and $\mathcal{C}_q$ attains the optimum exactly, second order included. Within the class this answers why the deficits are what they are. Whether some digital $(0, 3, 3)$ -net that is not a column point set has a deficit below $\frac{1}{3}$ (resp. $\frac{2}{3}$) is open (Remark 123(5)).

The holonomy. The ideal step $\frac{1}{3}q^2$ of the reflected cube cannot close up: q steps around a cycle of $\mathbb{T}$ give $\frac{1}{3}q^3$, but the heights live modulo q^2 , and $\frac{1}{3}q^3 \notin q^2\mathbb{Z}$ when $3 \nmid q$. So every cycle carries a forced total excess, its *holonomy*, and some step must carry at least its share. Formally, in the case of sum q^2 the excess is a closed 1-form on the triangulated torus $\mathbb{T}$ (its sum around every triangle vanishes), and its sums around the cycles of $\mathbb{T}$ are prescribed modulo q^2 . For $q \equiv 2 \pmod{3}$ every cycle total is $\frac{1}{3}q^2$ modulo q^2 (the smallest choices are $\frac{1}{3}q^2$ and $-\frac{2}{3}q^2$), and as the totals add up to zero, some cycle has at least $\frac{1}{3}q^2$; for $q \equiv 1$ every cycle total is $-\frac{1}{3}q^2$ modulo q^2 , and the totals add up to zero only if some cycle has at least $\frac{2}{3}q^2$ (the balance $\sum_{\gamma} z_{\gamma} = q$ of the proof). Spread over the q steps of that cycle, this is at least $\frac{1}{3}q$ resp. $\frac{2}{3}q$ per step: the deficits $\frac{1}{3}$ and $\frac{2}{3}$ are these per-step shares of a forced holonomy. (The $+1$ in $\eta \geq \frac{1}{3}q + 1$ is not holonomy but the net property.) For the digital nets of Lemma 93 with $|w_c| \leq 2$ (Lemma 93(2)) the total excess of a cycle in the direction $\mathbf{e}_i$ is $\frac{1}{3}q^2 w_i$, so the drift $\frac{1}{3}q w_i$ is exactly the per-step share of the holonomy, and the jitter decides how evenly the cycle spreads it. As a rule for constructions: spread the forced excess evenly over the directions that attain the minimum distance, and give the largest third-digit steps to the directions with the smallest drift. Theorem 95 proves this rule optimal for column nets; beyond them it is a heuristic. Two comparisons show what each term does (Figure 10(c)). Fixing the drift at $w = -\gamma \mathbf{1}$, $\gamma \in \{1, 2\}$, by the shared second digit $\lfloor q/3 \rfloor \Sigma n$ (its row $\lfloor q/3 \rfloor \mathbf{1}$ sums to $3 \lfloor q/3 \rfloor \not\equiv 0 \pmod{q}$, so the shared digit is not constant on a

column, and the points do not lie on columns) and choosing only the jitter residues, at every prime $q = p$, $5 \leq p \leq 199$, the third digit $\frac{1}{2}(-n_c - n_{c+1} + n_{c+2})$ gives $p(1 - \delta N^{1/3})$ close to $\frac{2}{3}$ ($p \equiv 1$) and $\frac{4}{3}$ ($p \equiv 2$), and the third digit n_{c+1} close to $\frac{4}{3}$ and 2 (computed exactly at every such prime; within 0.06 of these values for every prime $53 \leq p \leq 199$); the column nets reach $\frac{2}{3}$ ($p \equiv 1$) and $\frac{1}{3}$ ($p \equiv 2$).

Dimension five. The same bookkeeping applies to half-integer layers (Section 13.7). There the holonomy is a parity: p steps of $\frac{p}{2}$ do not close up modulo the odd p . The net property excludes the cheapest sign patterns, a skew-symmetric layer balances the steps with all coordinates moving, and a second offset row with few harmful entries keeps the jitter off the steps that attain the minimum. Theorem 120 shows that the drift dr of such a layer is at least $\frac{17}{2}$, where dr is measured in units of $1/p$ of a cell on the squared length, $(\delta N^{1/5})^2 \approx \frac{5}{4} - dr/p$; a layer attains it, and with a suitable second row it gives $(0, 5, 5)$ -nets with $\delta N^{1/5} > 1$ for every prime $p \geq 37$ (Proposition 118).

12. ONE POINT PER CUBE: CUBE TILINGS AND THE VALUE 1

The lattice picture uses only that the geometric digit is linear in the cell digits. This section makes precise what that linearity forces: offsets that are affine in the cell between wraps, so locally a lattice, but broken at the slip planes where a geometric digit wraps, so globally not a lattice. It also shows what the cube cells of the resolutions $m = sk$ cost. Call the position of a point inside its cell its *phase*; for a digital net it is, to first order, r/q with r the geometric digits. By the cube-tiling theorems of Hajós and Keller, configurations with one point per unit cube whose phases vary independently are no better than $\mathbb{Z}^s$ (Proposition 100). In Lemma 96 and Corollary 97 only, the digits of an integer $0 \leq P < q^j$ are counted from the least significant one: $P = \sum_{i < j} d_i(P) q^i$.

Lemma 96 (Additive digit functionals). *Let $q \geq 2$, $j \geq 1$, $\beta_0, \dots, \beta_{j-1} \in \mathbb{Z}/q\mathbb{Z}$, and $\phi(P) = \sum_{i < j} \beta_i d_i(P)$ for $P \in \mathbb{Z}/q^j\mathbb{Z}$ (digits of the representative in $[0, q^j)$). Then ϕ is a homomorphism $\mathbb{Z}/q^j\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ if and only if $\beta_i = 0$ for every $i \geq 1$.*

Proof. If $\beta_i = 0$ for $i \geq 1$, then $\phi(P) = \beta_0 (P \bmod q)$, a homomorphism. Conversely, a homomorphism on the cyclic group $\mathbb{Z}/q^j\mathbb{Z}$ satisfies $\phi(P) = P \phi(1) = \beta_0 P = \beta_0 d_0(P)$ in $\mathbb{Z}/q\mathbb{Z}$; at $P = q^i$, $i \geq 1$, this gives $\beta_i = \phi(q^i) = \beta_0 d_0(q^i) = 0$. $\square$

So a linear function of the digits is additive in the integer only through the lowest digit; at every higher digit, carries break additivity. The geometric digit is a linear function of the last cell digits, one level above it: it is additive, hence affine and lattice-like, between carries and wraps, and it breaks where they occur.

Corollary 97 (Linear offsets). *Let $q \geq 2$.*

- (a) *One level.* Let a set of integer vectors $Y \in \mathbb{Z}^s$ consist of all Y whose lowest base- q digits $(Y_c \bmod q)_c$ satisfy a system of linear equations over $\mathbb{Z}/q\mathbb{Z}$, with solution set $y_0 + C$ for a linear code $C \subset (\mathbb{Z}/q\mathbb{Z})^s$, all higher digits being free. Then the set is the coset $y_0 + C + q\mathbb{Z}^s$ of the Construction A lattice $C + q\mathbb{Z}^s$.
- (b) *Two levels.* For an $s \times s$ matrix B over $\mathbb{Z}/q\mathbb{Z}$ let $\mathcal{D}_B = \{q\ell + (B\ell \bmod q) : \ell \in \{0, \dots, q-1\}^s\} \subset (\mathbb{Z}/q^2\mathbb{Z})^s$ (the two-digit set of B ; ℓ plays the part of the last cell digits), with $B\ell \bmod q$ taken in $[0, q)^s$. Then $\mathcal{D}_B$ is a subgroup if and only if $Bc \equiv 0 \pmod{q}$ for every carry vector $c = (\lfloor (v_i + v'_i)/q \rfloor)_i$ of two vectors $v, v' \in \{B\ell \bmod q\}$. If B is invertible, $\mathcal{D}_B$ is not a subgroup.
- (c) *Locally a lattice.* Let a digital net over $\mathbb{Z}/q\mathbb{Z}$ be in graph form with depths $(k, \dots, k)$ and geometric layer $\tilde{M}$, and let the cells n, n' differ only in their last level, by $n' - n = E \in \mathbb{Z}^s$

(no carry). If the geometric digits r of n satisfy $r + \tilde{M}E \in [0, q)^s$, then in cell units the points of n' and n differ by $(I + \tilde{M}/q)E + (f' - f)/q$, with $f, f' \in [0, 1)^s$ the contributions of the deeper digits.

Proof. (a) The set of $Y \in \mathbb{Z}^s$ with $Y \bmod q \in y_0 + C$ is $y_0 + C + q\mathbb{Z}^s$. (b) Let $Y = q\ell + v$ and $Y' = q\ell' + v'$ be in $\mathcal{D}_B$, and let c be the carry vector of v, v' . Then $Y + Y' = q(\ell + \ell' + c) + (v + v' - qc)$ with $v + v' - qc \in [0, q)^s$, and $v + v' \equiv B(\ell + \ell')$; so $Y + Y' \in \mathcal{D}_B$ if and only if $Bc \equiv 0$. A nonempty finite subset of a group that is closed under addition is a subgroup. If B is invertible, its image contains $v = v' = \lceil q/2 \rceil \mathbf{e}_i$, whose carry vector is $\mathbf{e}_i$; then $B\mathbf{e}_i \equiv 0$ would be needed, which is false. (c) Only the last digits of the cells change, so r changes by $\tilde{M}E$ modulo q , and $r' = r + \tilde{M}E$ exactly since both sides lie in $[0, q)^s$; the cell digits change by E . $\square$

At $m = s$, $\mathcal{D}_B$ is the set of the first two digits of all points of the graph form with geometric layer B , so (b) says that the configuration of an invertible layer is never a lattice: it is a lattice coset cut at slip planes (Figure 11). What digitality forces is therefore *linear offsets*: by (c), away from the wraps the offset of a point is an affine function of its cell, so locally the points form a coset of the lattice $(I + \tilde{M}/q)\mathbb{Z}^s$ up to the jitter. Finite unions of lattice cosets are not excluded, and they occur: D_s^+ for odd s and the configuration of Proposition 103.

At $m = s$ (one cell digit per coordinate) write B for the geometric layer modulo p . The phase of the cell n is then given by its geometric digits $r(n) = Bn \bmod p$, and the phase decides which coordinates wrap on a step (Lemma 98(i)). An invertible layer realizes every wrap pattern, and every square minor of the layer of a $(0, sk, s)$ -net with disjoint row and column sets is a unit (Lemma 98(ii)).

Lemma 98 (Wrap patterns; rank of the layer). (i) Let p be a prime and consider a graph form over $\mathbb{F}_p$ with depths $(1, \dots, 1)$: coordinate c of the point with index $n \in \mathbb{F}_p^s$ has the digits n_c , $r_c(n) = (Bn)_c$ and deeper digits, with $B \in \mathbb{F}_p^{s \times s}$. For $E \in \mathbb{Z}^s$ let $\beta = BE \bmod p \in \{0, \dots, p-1\}^s$ and $n' \equiv n + E$. Then $r(n') = r(n) + \beta - p\omega$ with $\omega_c = \lceil r_c(n) + \beta_c \rceil$, and $\omega_c = 0$ whenever $\beta_c = 0$. If B is invertible, then every $\omega \in \{0, 1\}^s$ with $\omega_c = 0$ whenever $\beta_c = 0$ is the wrap vector of some cell n . (ii) Let a digital $(0, sk, s)$ -net over $\mathbb{Z}/q\mathbb{Z}$, $k \geq 1$, be in graph form with depths $(k, \dots, k)$ and geometric layer $\tilde{M}$. For disjoint $T, Z \subset \{1, \dots, s\}$ with $|T| = |Z|$, $\det \tilde{M}_{T,Z}$ is a unit of $\mathbb{Z}/q\mathbb{Z}$. In particular $\tilde{M}$ has rank at least $\lfloor s/2 \rfloor$ modulo every prime factor of q .

Proof. (i) $r(n') \equiv B(n + E) \equiv r(n) + \beta$, and $r(n') \in [0, p)^s$, which gives ω ; if $\beta_c = 0$, then $r_c(n) + \beta_c < p$. If B is invertible, take $n = B^{-1}y$ with $y_c = p - 1$ if $\omega_c = 1$ (then $\beta_c \geq 1$ and $y_c + \beta_c \geq p$) and $y_c = 0$ if $\omega_c = 0$. (ii) The box with depths $k + 1$ on T , $k - 1$ on Z and k elsewhere has total depth sk ; by Lemma 2 its minor is, up to sign, the determinant of the first offset rows of T on the last level of Z , which is $\det \tilde{M}_{T,Z}$ modulo q , and by Lemma 1 it is a unit. Disjoint T, Z of size $\lfloor s/2 \rfloor$ exist. $\square$

So in (i), at the representative with cell difference E , the points of n and n' differ in cell units by $E + b - \omega$, $b = \beta/p$, plus less than $1/p$ per coordinate of jitter. We call $b \in [0, 1)^s$ the *glue* of the step E : to first order, the change of the phase on the step, in cell units and modulo 1. Call the wraps of a layer *free* if every wrap vector allowed by (i) occurs, as for every invertible layer. Then, up to the jitter, the minimum distance is the least *fully folded length* over the steps $E \neq 0$: the length $|E + b - \omega|$ minimized over the allowed wrap vectors ω , whose coordinate c is $\min(|E_c + b_c|, |E_c + b_c - 1|)$ if $\beta_c \neq 0$ and $|E_c|$ if $\beta_c = 0$. Part (ii) contains the 2×2 minors used for Theorem 87.

Remark 99 (Glue under free wraps). A coordinate with $E_c = 0$ and $\beta_c \neq 0$ contributes $\min(b_c, 1 - b_c) \leq \frac{1}{2}$ to the fully folded length, with equality only for $b_c = \frac{1}{2}$: a step keeps its

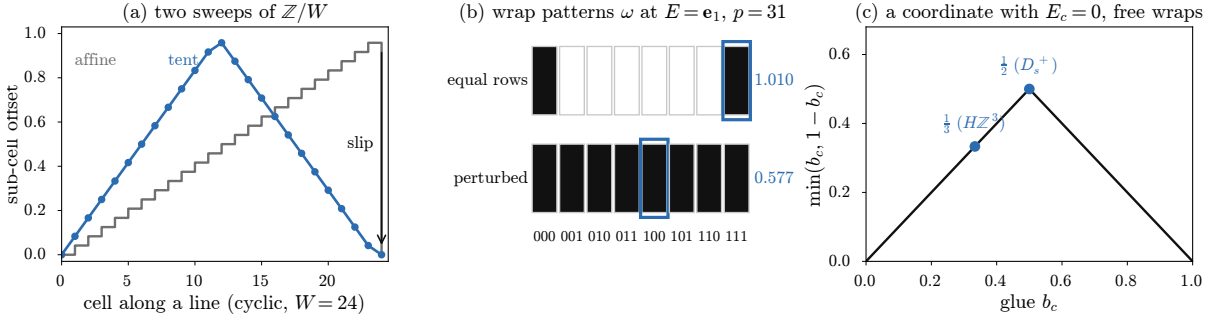


FIGURE 11. What linearity forces (Section 12). (a) Two bijections of $\mathbb{Z}/W$, $W = 24$, as sub-cell offsets along a cyclic line of cells: the affine bijection $i \mapsto i$ (grey), the kind that a linear offset gives, jumps once, by $W - 1$, and this jump sits at a slip plane (Corollary 97); every affine bijection of $\mathbb{Z}/W$ has a step of size at least $W/2$, since its steps are congruent modulo W and sum to zero. A tent-shaped bijection (accent), available only to nets that are not digital, moves by at most 2 between neighbouring cells (Remark 123(11)). (b) The wrap vectors ω of Lemma 98(i) that occur for the step $E = \mathbf{e}_1$ over all p^3 cells, $p = 31$ (filled), for the equal-row layer $\mathbf{1}a^\top$, $a = (10, 10, 11)$, of the column net $\mathcal{C}_{31}$ (Definition 47) and for the invertible layer obtained by adding $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{pmatrix}$; framed, the pattern of least length $|E + b - \omega|$, printed on the right (computed: 1.010 and 0.577). The shared wrap allows only 000 and 111; the perturbed layer realizes all eight, and with the glue $b \approx \frac{1}{3}\mathbf{1}$ (Lemma 98) the fully folded length drops to $1/\sqrt{3}$. (c) A coordinate that does not move contributes $\min(b_c, 1 - b_c)$ under free wraps, at most $\frac{1}{2}$, attained only at $b_c = \frac{1}{2}$ (Remark 99).

full length under free wraps only if its glue in each coordinate that does not move is $\frac{1}{2}$, the only value that is its own negative modulo 1. So half-integer layers do not need the wraps of different coordinates to be correlated: for odd s the differences between the two cosets of D_s^+ fill $(\mathbb{Z} + \frac{1}{2})^s$, a set that free wraps (integer changes of single coordinates) map to itself, so these steps keep a length of at least $\sqrt{s}/2$, and the relaxation of Proposition 115 at $k = 1$, which allows every wrap, tends to $\min(\sqrt{s}/2, \sqrt{2})$ for dominant layers. The glue $\frac{1}{3}\mathbf{1}$ of the reflected cube does not survive: with free wraps the step $E = \mathbf{e}_1$ of the layer $\frac{p}{3}\mathbf{1}\mathbf{1}^\top$ would have fully folded length $1/\sqrt{3} = .5773\dots$, and bounded perturbations of the equal rows $\mathbf{1}a^\top$ of the column nets make the wraps independent (computed instance: Figure 11(b)). Wraps that are correlated across coordinates because the layer is singular (*locked* wraps, Section 13.3) are needed otherwise: the column nets (Theorem 49) share one geometric digit among all three coordinates, Proposition 103 between two, and in Proposition 104 a layer of rank one locks all three, one coordinate reading half of the digit of the others; literally equal rows exist only at $(s, m) = (3, 3)$ (Lemma 50). Locked wraps are what produces the coherent phases defined before Proposition 100. The half-integer rule concerns coordinates whose wraps are free: a coordinate whose wraps are locked to those of the others can carry other glue and a step longer than one cell along its own axis (in the net $\mathcal{W}_p$ of Section 13.3, the glue $\frac{1}{2} + 3\varepsilon$ and the step $1 + 2\varepsilon$ along $\mathbf{e}_z$, with $\varepsilon = \rho/(2p)$). The rule concerns the length of a single step under free wraps; it is a heuristic for the choice of glue, not an optimality statement for the minimum, even for free coordinates (the remark on $\sqrt{233}/15$ in Section 13.3).

At the resolutions $m = sk$ the cells are cubes. Call $S \subset \mathbb{R}^s$ a *one-per-cube set* if every unit cube $n + [0, 1]^s$, $n \in \mathbb{Z}^s$, contains exactly one point of S , and *periodic* with period lattice Π (of full rank) if $S + \Pi = S$; write $\mu(S)$ for its minimum distance. The *phase group* of a lattice L is $Y = (L + \mathbb{Z}^s)/\mathbb{Z}^s \subset (\mathbb{R}/\mathbb{Z})^s$, the set of fractional offsets (the phases) of its points. Say that the phases of L *vary independently* if Y is dense in $(\mathbb{R}/\mathbb{Z})^s$ (equivalently, $\mathbb{Z}^s + L$ is dense), or finite and equal to $\pi_1(Y) \times \cdots \times \pi_s(Y)$, the product of its projections to the coordinate circles; the lattices in $\mathbb{Q}^s$ are those with a finite phase group, and we do not treat lattices whose phase group is neither dense nor finite. A lattice whose phase group is finite and smaller than the product of its projections has *coherent* phases. For every $(0, sk, s)$ -net P in base q , digital or not, $S = q^k(P + \mathbb{Z}^s)$ is a periodic one-per-cube set with $\Pi \supset q^k\mathbb{Z}^s$, and $\min(\delta N^{1/s}, q^k) = \mu(S)$ for the toroidal δ of P .

Proposition 100 (One point per cube). *Let S be a periodic one-per-cube set in $\mathbb{R}^s$ with period lattice Π .*

- (i) *If $S = L$ is a lattice and $\mathbb{Z}^s + L$ is dense in $\mathbb{R}^s$, then L contains a unit vector $\mathbf{e}_c$; so $\mu(L) \leq 1$.*
- (ii) *If $S = L \subset \mathbb{Q}^s$ is a lattice whose phase group Y equals $\pi_1(Y) \times \cdots \times \pi_s(Y)$, the product of its projections to the coordinate circles, then L contains a unit vector $\mathbf{e}_c$; so $\mu(L) \leq 1$.*
- (iii) *If $s \leq 7$ and $\mathbb{Z}^s + \Pi$ is dense in $\mathbb{R}^s$, then two points of S differ by a unit vector; so $\mu(S) \leq 1$.*
- (iv) *If $S - x \subset \mathbb{Q}^s$ for some x , all squared distances in S are rational. Hence $\mu(S) < (4/3)^{1/4}$ for $s = 2$ and $\mu(S) < 2^{1/6}$ for $s = 3$, the optimal packing values at density 1; and for $4 \leq s \leq 7$, $\mu(S)$ differs from the value of the densest known packing at density 1 (D_4 , D_5 , E_6 , E_7 , with squared minima $\sqrt{2}$, $2^{3/5}$, $2 \cdot 3^{-1/6}$, $2^{6/7}$).*

Proof. Let $f(x) = \#(S \cap (x + [0, 1]^s))$. Then $f(x + \pi) = f(x)$ for $\pi \in \Pi$ and $f(n) = 1$ for $n \in \mathbb{Z}^s$, so $f = 1$ on $\mathbb{Z}^s + \Pi$. For every x there is $\varepsilon > 0$ such that f is constant on $x - [0, \varepsilon]^s$: S is locally finite, so we may choose ε below every positive difference $x_c - \sigma_c$ and $x_c + 1 - \sigma_c$ for the finitely many $\sigma \in S$ near the cube, and then shifting the cube by $-t$, $t \in [0, \varepsilon]^s$, neither adds nor removes a point. If $f \equiv 1$, the cubes $\sigma + (-1, 0]^s$, $\sigma \in S$, tile $\mathbb{R}^s$, since $x \in \sigma + (-1, 0]^s$ if and only if $\sigma \in x + [0, 1]^s$. (i) Density gives a point of $\mathbb{Z}^s + L$ in every $x - [0, \varepsilon]^s$, so $f \equiv 1$, and the cubes form a lattice tiling. By Hajós's theorem (Minkowski's conjecture) [22] two of them share a facet, so L contains some $\mathbf{e}_c$. (ii) For each c , $\pi_c(L) + \mathbb{Z}$ is a finitely generated subgroup of $\mathbb{Q}$ containing $\mathbb{Z}$, hence equal to $\frac{1}{e_c}\mathbb{Z}$ for an integer $e_c \geq 1$. For $x_c \in (\frac{j-1}{e_c}, \frac{j}{e_c}]$ and $\sigma \in L$ the condition $x_c \leq \sigma_c < x_c + 1$ is equivalent to $\frac{j}{e_c} \leq \sigma_c \leq \frac{j-1}{e_c} + 1$, which does not depend on x_c ; so f is constant on every box $\prod_c(\frac{j_c-1}{e_c}, \frac{j_c}{e_c}]$, and its value there is that at the corner $(j_c/e_c)_c$. By hypothesis the corner lies in $\mathbb{Z}^s + L$, so $f \equiv 1$, and Hajós's theorem applies as in (i). (iii) As in (i), $f \equiv 1$ and the cubes $\sigma + (-1, 0]^s$ tile $\mathbb{R}^s$. Keller's conjecture holds for $s \leq 7$ (Perron [49] for $s \leq 6$, Brakensiek, Heule, Mackey and Narváez [1] for $s = 7$): two cubes of the tiling share a complete facet, so their corners differ by some $\mathbf{e}_c$. (iv) The differences are rational vectors. As S is a finite union of Π -cosets, $\mu(S)$ is a minimum over the finitely many Π -orbits of pairs, so it is attained and $\mu(S)^2$ is rational. A periodic set of density 1 with minimum μ is a packing of balls of radius $\mu/2$ with density $\text{vol}(B_{\mu/2})$, so μ^2 is at most $4\vartheta_s^{2/s}$ with ϑ_s the optimal centre density; this is $2/\sqrt{3}$ for $s = 2$ [9, Ch. 1] and $2^{1/3}$ for $s = 3$ [23], both irrational. The four squared minima for $4 \leq s \leq 7$ are $4\vartheta_s^{2/s}$ with the centre densities $\frac{1}{8}$, $\frac{1}{8\sqrt{2}}$, $\frac{1}{8\sqrt{3}}$, $\frac{1}{16}$ [9], and they are irrational. $\square$

Parts (i)–(iii) say that a one-per-cube lattice whose phases vary independently, and for $s \leq 7$ any periodic one-per-cube set with dense phases, is no better than $\mathbb{Z}^s$. So a rational one-per-cube lattice with minimum above 1 has coherent phases. $H\mathbb{Z}^3$ and D_s^+ for even s have coherent

phases, and D_s^+ beats the cubic value for even $s \geq 6$. The configuration Γ of Section 13.2 and D_s^+ for odd $s \geq 5$, both unions of two lattice cosets, beat it too, and so do, in the limit, the rank-one nets of Proposition 104, whose phases lie on one line.

These statements concern idealized configurations. For a net P in a fixed base, $S = q^k(P + \mathbb{Z}^s) \subset q^{k-m}\mathbb{Z}^s$ is rational, so $\mathbb{Z}^s + \Pi$ is discrete, and (i) and (iii) never apply to the net itself; they apply to idealized models of its local configuration, the sets $\{n + \{An + y\} : n \in \mathbb{Z}^s\}$ obtained in the limit $q \rightarrow \infty$ with $\tilde{M}/q \rightarrow A$, when their phases are irrational. Part (ii) applies to rational lattices, among them the limits as $q \rightarrow \infty$ of the local configurations ($\mathbb{Z}^s$ in regime I of Section 2, $H\mathbb{Z}^3$, and D_s^+ for even s), and to a net itself only when S is a lattice; at $m = s$ the first two digits of an invertible layer never form a group (Corollary 97(b)). Part (iv) applies to every net. For $s \geq 8$ part (iii) says nothing (Keller's conjecture fails [41, 42]), and at $s = 8$ the squared minimum 2 of E_8 is rational; Theorem 116 reaches it in the limit. Part (iv) needs $S \subset x + \mathbb{Q}^s$: for a periodic set whose period lattice is merely rational, cross-coset distances can be irrational.

Remark 101 (What the cube costs; computed). The largest minimum of a periodic one-per-cube set is not known. In dimension three an exhaustive enumeration of the lattices of covolume 1 in $\frac{1}{e}\mathbb{Z}^3$, $e \leq 11$, finds one-per-cube lattices with minimum up to $\sqrt{29/25} = 1.0770\dots$ (computed), for instance the lattice with basis $\frac{1}{5}(3, -4, -2)$, $\frac{1}{10}(6, 2, -9)$, $\frac{1}{2}(1, 0, 2)$. It has covolume 1; its Gram matrix $100^{-1} \begin{pmatrix} 116 & 56 & -10 \\ 56 & 121 & -60 \\ -10 & -60 & 125 \end{pmatrix}$ is Minkowski-reduced, so its minimum is $\sqrt{116/100}$; and a finite check over one period shows that every unit cube holds exactly one of its points. So the largest minimum lies between 1.0770 and $2^{1/6} = 1.1224\dots$ [23]. The maximizers found have offsets that are not affine modulo 1 in the cell, so no digital net realizes them through its geometric digit (Corollary 97(c)); the best digital value at $m = 3$ in this paper is $\sqrt{281}/16 = 1.0476\dots$ (Proposition 104). For $s \leq 9$, restricting to lattices is not known to lose anything: lattices hold the packing records there and are optimal for $s = 3, 8$ [9, 23, 67]. The constraints visible here are the *cube constraint* (one point in every cube of side q^{-k} , at $m \equiv 0 \pmod{s}$), the linearity of the offsets and, in the frame orbit, Lemma 18. The skeleton regime ($m \not\equiv 0 \pmod{s}$), whose cells are not cubes, is not bound by the cube constraint (Table 8).

Scope. What uses the linearity of the geometric digit: Lemma 96, Corollary 97 and Lemma 98; Corollaries 78 and 79 and Proposition 85, whose proofs use that a carry-free step changes every offset digit by a constant; Theorem 87 (box minors of the layer, and carry-free steps); and, inside the frame orbit, where the layer is a Cauchy matrix (Proposition 12), Lemma 18 and its consequences (Remark 82, Theorem 88, Corollary 39, Proposition 109).

What holds for every net, digital or not: Proposition 100, which applies to the periodic set S of every $(0, sk, s)$ -net within the limits stated after it, and the box count of Lemma 50: if, for every point of a $(0, m, s)$ -net in base q , the digits with index k (counted from the most significant, as everywhere outside Lemma 96 and Corollary 97) of two coordinates agree, or one is a fixed function of the other, then $2(k+1) > m$. For nets that are not digital only these constraints and the other box conditions remain (Remark 123(11)).

13. BEYOND THE CUBIC VALUE: EUCLIDEAN SKELETONS AND HALF-INTEGER LAYERS

By Proposition 100, a set with one point per unit cube can have minimum distance above the cubic value 1 only if the phases of its points are correlated (coherent, in the idealized setting of that proposition). For an invertible layer every pattern of wraps occurs (Lemma 98(i)), so a step to a neighbouring cell keeps its full length only if its glue is $\frac{1}{2}$ in every coordinate that does not move (Remark 99). Three ways above 1 occur in this paper.

- (i) *Euclidean skeletons* (Section 13.1). At $m \not\equiv 0 \pmod{s}$ the cells are boxes, longer in the skeleton coordinates, not cubes, so the cube constraint does not apply (Section 5). In the

Euclidean norm the certified constants exceed 1 at $m \equiv -1 \pmod{s}$ at the large primes of Table 8; whether this persists for all large p is open (Remark 124).

- (ii) *Locked wraps at $m = 3$* (Sections 13.2 and 13.3). A singular layer can force coordinates to wrap together. In $\mathcal{T}_p$ two coordinates share one geometric digit, and the points lie on a union of two lattice cosets; in $\mathcal{W}_p$ the layer has rank one, and all three coordinates wrap together.
- (iii) *Half-integer layers* (Sections 13.4–13.7). Layers whose entries are half-integers, read modulo q via $\frac{1}{2} \equiv (q+1)/2$, so that each centred entry is about $\pm q/2$ plus a bounded amount (regime III, Figure 7), put the points locally on the packing D_s^+ . For $k \geq 2$ the frame orbit cannot provide them (Proposition 109: for rational designs, and over $\mathbb{F}_p$ for large p), but split frames give them at every resolution $m = sk$ (Theorem 116); at $k = 1$ no frame is needed (Section 13.7).

13.1. Euclidean skeletons. *Euclidean form.* The bound of Theorem 33(1) measures the centred difference a of the fine-cell positions of two points (Lemma 25) in the maximum norm. Every skeleton digit $S_z = \sum_d \kappa_d x_{d,k}$ with all $\kappa_d \neq 0$ can be realized (Proposition 27(ii)), and in the Euclidean norm the best choice is not $\kappa_d = \rho^d$ (Remark 32(c)).

Proposition 102 (Euclidean form of Theorem 33(1)). *Let $s \geq 3$, let $p \geq s - 1$ be a prime, $k \geq 0$, $m = sk + s - 1$, and let $\kappa_1, \dots, \kappa_{s-1}$ be units of $\mathbb{F}_p$. The recipe of Proposition 27(ii) on the frame of Definition 34 gives a digital $(0, m, s)$ -net over $\mathbb{F}_p$ with the skeleton digit $S_z = \sum_d \kappa_d x_{d,k}$, and every graph form with the depths $(k + 1, \dots, k + 1, k)$ and this skeleton digit satisfies, for the toroidal distance,*

$$\delta N^{1/s} \geq p^{-1/s} \lambda_{\text{jit}}(\kappa) \geq p^{-1/s} (\lambda_2(\Lambda_\kappa) - \sqrt{s}), \quad \lambda_{\text{jit}}(\kappa) = \min_{0 \neq a \in \Lambda_\kappa} \|(|a| - 1)_+\|_2,$$

where $\Lambda_\kappa = \{a \in \mathbb{Z}^s : a_z \equiv \sum_d \kappa_d a_{x_d} \pmod{p}\}$ and $(|a| - 1)_+$ is taken coordinatewise. (So λ_{jit} is the length of the shortest nonzero lattice vector after one fine cell of jitter is subtracted from each coordinate.)

Proof. The net property is Proposition 27(ii); the s places of Definition 34 are distinct because $p \geq s - 1$. As in the proof of Theorem 33(1), $P_z \equiv \sum_d \kappa_d P_{x_d} \pmod{p}$ for every point, and the centred difference $a \neq 0$ of the fine positions of two distinct points lies in Λ_κ . By Lemma 25(i) in each coordinate c , the two points are at toroidal distance at least $(|a_c| - 1)_+ \varpi$ in coordinate c , so their distance is at least $\varpi \|(|a| - 1)_+\|_2 \geq \varpi \lambda_{\text{jit}}(\kappa)$, and $\varpi N^{1/s}/N = p^{-1/s}$. Finally $|a| \leq (|a| - 1)_+ + 1$ coordinatewise gives $\|(|a| - 1)_+\|_2 \geq \|a\|_2 - \sqrt{s}$. $\square$

For $\kappa_d = \rho^d$ some $|a_c|$ is at least ρ , so $\lambda_{\text{jit}} \geq \rho - 1$ and the proposition contains Theorem 33(1). Every index- p sublattice of $\mathbb{Z}^s$ without unit vectors is a Λ_κ after a permutation of the coordinates: it is the kernel of a functional h modulo p , it contains no unit vector exactly when h has full weight (all entries nonzero modulo p), and then h can be scaled to $h_z = -1$. So the proposition can use the best of these lattices. Table 8 lists certified values for searched κ ; λ_{jit}^2 is an integer, computed exactly by lattice reduction and complete enumeration and also checked in Lean (Appendix F). At $p = 1009$ they already beat Table 4 for $s = 3, 4, 5$. The limit of the certified values as $p \rightarrow \infty$ is discussed in Remark 124.

13.2. Resolution $m = 3$: a layer of two cosets. The column nets of Section 6.5 share the geometric digit among all three coordinates, and no column point set beats the cubic value (Corollary 94). Sharing it between two coordinates only, and letting the geometric digit of the third coordinate have coefficients $h \equiv -\frac{1}{2}$, so that it moves by about half a cell between neighbouring cells, produces a local configuration that is not a lattice and whose minimum exceeds 1, the minimum of the reflected cube $H\mathbb{Z}^3$ of the column nets (Section 6.5; Figure 12).

s	searched κ , at $p =$				rounded root lattice, $p' \approx$		$\sqrt{\gamma_s}$	root lattice
	1009	10007	10^6+3	10^8+7	10^6	10^{10}		
3	.940	1.027	1.090	1.097	1.106	1.121	1.122	A_3
4	.813	.948	1.034	1.110	1.128	1.183	1.189	D_4
5	.752	.823	.989	1.069	1.098	1.208	1.231	D_5
6	.631	.714	.938	1.036	1.047	1.235	1.290	E_6
7	.372	.599	.867	.984	.974	1.238	1.345	E_7
8	.421	.547*	.814	.953	.881	1.219	1.414	E_8

TABLE 8. Certified lower bounds $\lambda_{\text{jit}}(\kappa)p^{-1/s}$ for $\delta N^{1/s}$ (Proposition 102; toroidal, every $k \geq 0$), truncated to three digits; every entry except those of the last two columns is such a certified bound. Left: κ found by a random and local search; compare Table 4 at $p = 1009, 10007, 10^6+3$. *Here the search is weaker than $\kappa_d = \rho^d$, which gives .632. Right: κ obtained by rounding a randomly rotated copy of the root lattice to an integer matrix of prime determinant p' ; the primes are $p' = 996001, 1006301, 1025909, 1033493, 1138273, 1071337$ and $10002435263, 10040205517, 10123347709, 10136355487, 10660100951, 11556622703$ for $s = 3, \dots, 8$. The last two columns give $\sqrt{\gamma_s}$ (truncated) and the lattice that attains it. The κ are listed in Table 13 (Appendix D); they are also fixed data of the Lean formalization (Appendix F).

Proposition 103 (Two-coset nets at $m = 3$). *Let $p \geq 5$ be a prime, $h = (p-1)/2$, let r be the integer nearest to $p/8$, and let $\theta = 8r - p \in \{\pm 1, \pm 3\}$. Let $\mathcal{T}_p$ be the digital net over $\mathbb{F}_p$ whose generator matrices C_x, C_y, C_z have the rows*

$$C_x : \mathbf{e}_x, (0, h, h), (0, 1, 2); \quad C_y : \mathbf{e}_y, (r, -1, 1), (3, 0, 1); \quad C_z : \mathbf{e}_z, (r, -1, 1), (1, 5, 0).$$

- (1) $\mathcal{T}_p$ is a $(0, 3, 3)$ -net if and only if $p \neq 23$, and every cell of side p^{-1} holds one point.
- (2) For $p \geq 41$ its toroidal (hence also Euclidean) minimum distance satisfies

$$\delta N^{1/3} \geq \sqrt{\frac{33}{32} - \frac{41}{16p}} - \frac{\sqrt{3}}{p}.$$

The bound exceeds $\sqrt{66}/8 - 3.014/p$ for $p \geq 83$, and it exceeds 1 for $p \geq 197$.

- (3) For $p \geq 7$ the points of the cells 0 and $(p-1)\mathbf{1}$ have toroidal distance d_* at integer scale p^3 , where $d_*^2 = (p^2 - 2p + 3)^2 + ((r-1)p + 4)^2 + ((r-1)p + 6)^2$. So $\delta N^{1/3} \leq d_*/p^2$, and $d_*/p^2 < \sqrt{66}/8 - 2/p$ for $p \geq 53$. In particular $\delta N^{1/3} \rightarrow \sqrt{66}/8 = 1.0155\dots$ as $p \rightarrow \infty$.

So y and z read the same geometric digit $rn_x - n_y + n_z$ (here r is a parameter, not a geometric digit), and x reads $h(n_y + n_z)$, with $h \equiv -\frac{1}{2}$. The third rows only add jitter: part (2) holds for any third rows, and only the minors in part (1) use them. In this section and the next, $g(n)$ denotes the vector of geometric digits of the cell n and $f(n)$ that of its third digits, both in $\{0, \dots, p-1\}^3$.

Proof. Net property. The first rows are $\mathbf{e}_x, \mathbf{e}_y, \mathbf{e}_z$, so $\mathcal{T}_p$ is a graph form with the depths $(1, 1, 1)$, and we use Lemma 2: the box of shape $(1, 1, 1)$ has determinant 1 and puts one point in every cell. A box with depth 2 on a , 1 on b and 0 on c has, up to sign, the determinant $(C_a)_{2,c}$, the entry of the second row of C_a in column c ; these off-diagonal entries of the second rows are $h, h, r, 1, r, -1$. The box with depth 3 on a has, up to sign, the 2×2 minor of the second and third rows of C_a off column a ; it is $2h - h = h$, $r - 3$ and $5r + 1$ for $a = x, y, z$. Here $1 \leq r < p$. Since $r \leq p/8 + \frac{1}{2}$, $0 < 5r + 1 < p$ for $p \geq 11$, and $5r + 1 = 6$ for $p = 5, 7$, a unit modulo 5 and

7. Finally $r - 3 \equiv 0$ means $r = 3$, as $-2 \leq r - 3 < p$, i.e. $p/8 \in (\frac{5}{2}, \frac{7}{2})$; among primes this holds only for $p = 23$, where the box with depth 3 on y is singular. Lemma 1 concludes.

Separation: reduction. At integer scale p^3 the point of cell $n \in \{0, \dots, p-1\}^3$ is $X(n) = p^2n + pg(n) + f(n)$, with the geometric digits $g(n)$ and the third digits $f(n)$ in $\{0, \dots, p-1\}^3$. Let $n \neq n'$, and let $D = p^2E + p\Delta g + \Delta f$ be a representative of $X(n') - X(n)$ modulo p^3 , where $E \equiv n' - n \pmod{p}$ is an integer vector, $\Delta g = g(n') - g(n)$ and $\Delta f = f(n') - f(n) \in (-p, p)^3$; the toroidal distance is the least $|D|$ over these representatives. If some $|E_c| \geq 3$, then $|D_c| \geq 3p^2 - p(p-1) - (p-1) > 2p^2$. So let $E \in \{-2, \dots, 2\}^3 \setminus \{0\}$, and put $S = E_y + E_z$ and $T = E_y - E_z$ (so $|S| \leq 4$, and $|S| \leq 3$ if T is odd). As C_y and C_z have the same second row, $g_y(n) = g_z(n)$ for every cell, so $\Delta g = (\xi, \eta, \eta)$ with integers $\xi, \eta \in (-p, p)$: *the y - and z -digits wrap together*. Since $\xi \equiv hS$, $2h \equiv -1$, $\eta \equiv rE_x - T$ and $8r = p + \theta$, there are integers i, j with

$$2\xi = jp - S, \quad 8\eta = ip + \theta E_x - 8T.$$

Reducing modulo 2 and modulo 8, with p odd and $\theta \equiv -p \pmod{8}$, gives $j \equiv S \pmod{2}$ and $i \equiv E_x \pmod{8}$. As $|\xi| < p$ and $|S| < p$, $|j| \leq 2$, and $j = \pm 2$ only if $\pm S > 0$. If $|T| \leq 1$, then $|\theta E_x - 8T| \leq 14 < p$, so likewise $|i| \leq 8$, $i = \pm 8$ only if $\mp(\theta E_x - 8T) > 0$, and $i = 0$ if $E_x = T = 0$.

In cell units $D/p^2 = V + \Delta f/p^2$, with $|\Delta f| < \sqrt{3}p$ and $V = E + (\xi, \eta, \eta)/p$. So $|D|/p^2 > |V| - \sqrt{3}/p$, and it suffices to show $|V|^2 \geq \frac{33}{32} - \frac{41}{16p}$. With the half-integer $\alpha = E_x + \frac{j}{2}$ and the quarter-integer $\beta = S + \frac{i}{4}$ (the limits of V_x and $V_y + V_z$ as $p \rightarrow \infty$),

$$V_x = \alpha - \frac{S}{2p}, \quad V_y + V_z = \beta + \frac{\theta E_x - 8T}{4p}, \quad V_y - V_z = T, \quad |V|^2 = V_x^2 + \frac{1}{2}((V_y + V_z)^2 + T^2).$$

The terms of order $1/p$ are the drift (Section 11): the deviation of the geometric digits from their limit values. Each numerical estimate below increases with p and is evaluated at $p = 41$.

The cases. (a) $|T| \geq 2$: $|V|^2 \geq T^2/2 \geq 2$.

(b) $T = 0$, $E_x = 0$: then $S \neq 0$ is even and $i = 0$, so $V_y = V_z = E_y$ and $|V|^2 \geq S^2/2 \geq 2$.

(c) $|T| = 1$, $E_x = 0$: j is odd, so $|\alpha| = \frac{1}{2}$ and $|V_x| \geq \frac{1}{2} - \frac{3}{2p}$; $i \in \{0, \pm 8\}$, so β is an odd integer and $|V_y + V_z| \geq 1 - \frac{2}{p}$. Hence $|V|^2 \geq (\frac{1}{2} - \frac{3}{2p})^2 + \frac{1}{2}(1 - \frac{2}{p})^2 + \frac{1}{2} > 1.16$.

(d) $|E_x| = 2$. If $|T| = 1$, then $j = \pm 1$, $|\alpha| \geq \frac{3}{2}$ and $|V|^2 \geq (\frac{3}{2} - \frac{3}{2p})^2 > 2$. If $T = 0$, then S and hence j are even, so α is an integer, and $\alpha \neq 0$ (which would need $j = \mp 4$); so $|V_x| \geq 1 - \frac{2}{p}$; and $4\beta = 4S + i \equiv E_x \equiv 2 \pmod{4}$, so $|\beta| \geq \frac{1}{2}$ and $|V_y + V_z| \geq \frac{1}{2} - \frac{3}{2p}$. Hence $|V|^2 \geq (1 - \frac{2}{p})^2 + \frac{1}{2}(\frac{1}{2} - \frac{3}{2p})^2 = \frac{9}{8} - \frac{19}{4p} + \frac{41}{8p^2}$, which is at least $\frac{33}{32} - \frac{41}{16p}$ for $p \geq 24$.

(e) $|E_x| = 1$, $T = 0$: $\alpha \in \mathbb{Z}$, $i \in \{E_x, -7E_x\}$, and $4\beta = 4S + i \equiv E_x \pmod{8}$, so $|\beta| \in \{\frac{1}{4}, \frac{7}{4}, \frac{9}{4}, \dots\}$; moreover $|V_x - \alpha| \leq \frac{2}{p}$ and $|V_y + V_z - \beta| \leq \frac{3}{4p}$. If $\alpha = 0$, then $j = -2E_x$, so $E_x S \leq -2$ and $E_x \beta = E_x S + E_x i/4 \leq -\frac{7}{4}$; then $|V|^2 \geq \frac{1}{2}(\frac{7}{4} - \frac{3}{4p})^2 > 1.4$. If $|\alpha| \geq 2$, or $|\alpha| = 1$ and $|\beta| \geq \frac{7}{4}$, then also $|V|^2 > 1.4$. There remains $|\alpha| = 1$, $|\beta| = \frac{1}{4}$. Since $S = \beta - \frac{i}{4}$ is an even integer, $\beta = \frac{E_x}{4}$ and $S \in \{0, 2E_x\}$, and if $S = 2E_x$ then $\alpha = E_x$ (as $|j| \leq 2$). With $(a - b)^2 \geq a^2 - 2ab$,

$$|V|^2 \geq \alpha^2 - \frac{\alpha S}{p} + \frac{1}{2}\left(\beta^2 + \frac{\beta \theta E_x}{2p}\right) = \frac{33}{32} - \frac{\alpha S - \theta/16}{p} \geq \frac{33}{32} - \frac{35}{16p},$$

as $\alpha S \in \{0, 2\}$ and $\theta \geq -3$.

(f) $|E_x| = 1$, $|T| = 1$: $j = \pm 1$, so $\alpha \in \{\pm \frac{1}{2}, \pm \frac{3}{2}\}$; $i \in \{E_x, -7E_x\}$, and $4\beta = 4S + i \equiv 4 + E_x \pmod{8}$, so $|\beta| \in \{\frac{3}{4}, \frac{5}{4}, \frac{11}{4}, \dots\}$; moreover $|V_x - \alpha| \leq \frac{3}{2p}$ and $|V_y + V_z - \beta| \leq \frac{11}{4p}$, as $|\theta E_x - 8T| \leq 11$. If $|\alpha| = \frac{3}{2}$, then $|V|^2 \geq (\frac{3}{2} - \frac{3}{2p})^2 > 2$. If $|\beta| \geq \frac{5}{4}$, then $|V|^2 \geq (\frac{1}{2} - \frac{3}{2p})^2 + \frac{1}{2}(\frac{5}{4} - \frac{11}{4p})^2 + \frac{1}{2} > 1.41$. There remains $|\alpha| = \frac{1}{2}$, $|\beta| = \frac{3}{4}$. Then $\alpha = \frac{E_x}{2}$ and, from $4\beta \equiv 4 + E_x \pmod{8}$, $\beta = -\frac{3}{4}E_x$; and

$S = \beta - \frac{i}{4} = \pm E_x$. As in (e),

$$|V|^2 \geq \alpha^2 - \frac{\alpha S}{p} + \frac{1}{2} \left(\beta^2 + \frac{\beta(\theta E_x - 8T)}{2p} + T^2 \right) = \frac{33}{32} - \frac{\frac{1}{2}E_x S - \frac{3}{2}E_x T + \frac{3}{16}\theta}{p} \geq \frac{33}{32} - \frac{41}{16p},$$

as $E_x S, E_x T \in \{\pm 1\}$ and $\theta \leq 3$.

So $|V|^2 \geq \frac{33}{32} - \frac{41}{16p}$ in every case, which proves (2). The bound increases with p ; it is $1.0002\dots$ at $p = 197$ and below 1 at $p = 193$. For $p \geq 83$ we have $\frac{33}{32} - \frac{41}{16p} \geq 1$, and $\sqrt{a} - \sqrt{a-x} = x/(\sqrt{a} + \sqrt{a-x}) \leq x/2$ gives the bound $\sqrt{66}/8 - (\frac{41}{32} + \sqrt{3})/p$, with $\frac{41}{32} + \sqrt{3} < 3.014$.

The pair. For $n' = (p-1)\mathbf{1} \equiv -\mathbf{1}$ one has $g(n') = (1, p-r, p-r)$ and, as the entries of the third rows sum to 3, 4, 6, $f(n') = (p-3, p-4, p-6)$; also $g(0) = f(0) = 0$. The representative with $E = -1$ is $D_* = -(p^2 - 2p + 3, (r-1)p + 4, (r-1)p + 6)$. Since $|D_{*,c}| < p^2 \leq p^3/2$ in every coordinate, this representative is the toroidal one, so the toroidal distance is d_* and $\delta N^{1/3} \leq |D_*|/p^2 = d_*/p^2$. With $r = (p+\theta)/8$,

$$p^4 \left(\frac{\sqrt{66}}{8} - \frac{2}{p} \right)^2 - d_*^2 = \left(\frac{9}{2} - \frac{\theta}{16} - \frac{\sqrt{66}}{2} \right) p^3 - \left(\frac{21}{2} - \frac{\theta}{2} + \frac{\theta^2}{32} \right) p^2 + \left(32 - \frac{5\theta}{2} \right) p - 61,$$

and for $|\theta| \leq 3$ the three coefficients exceed $\frac{1}{4}$, -12.3 and 24 , so the difference is positive for $p \geq 53$. With (2) this gives the limit. $\square$

The two-coset packing. Since $h/p = \frac{1}{2} - \frac{1}{2p}$ and $r/p = \frac{1}{8} + \frac{\theta}{8p}$, the point of cell n sits, in cell units, at

$$n + \left(\left\{ \frac{n_y + n_z}{2} \right\}, \left\{ \frac{n_x}{8} \right\}, \left\{ \frac{n_x}{8} \right\} \right)$$

up to the drift and the jitter, both of order $1/p$ for bounded cell differences. Call this set Γ . Each slab $n_x = \text{const}$ of Γ is a square grid in (y, z) , *puckered*: the points of the cells with $n_y + n_z$ odd are raised by $\frac{1}{2}$ in x , so neighbours within a slab are $\sqrt{5}/2$ apart. Consecutive slabs are *sheared* by $(\frac{1}{8}, \frac{1}{8})$ in (y, z) . For a shear (t, t) a point has two kinds of nearest neighbours in the next slab: the point of the same parity above it, at $(1, t, t)$, and two points of the other parity diagonally above, at $(\frac{1}{2}, t-1, t)$ and $(\frac{1}{2}, t, t-1)$. The squared lengths $1 + 2t^2$ and $\frac{1}{4} + (1-t)^2 + t^2$ agree exactly at $t = \frac{1}{8}$, with the value $\frac{33}{32}$. This is the minimum of Γ , and the two kinds of shortest difference vectors are its *contacts*; cases (e) and (f) of the proof are these two contacts at finite p , and the explicit pair of (3) is the first one, across the corner of the torus. Γ is the union of the two cosets of the lattice $\langle (1, \frac{1}{8}, \frac{1}{8}), (0, 1, 1), (0, 1, -1) \rangle$ (covolume 2) given by the parity of $n_y + n_z$, and it is not a lattice: $(\frac{1}{2}, 1, 0)$ is a difference of two of its points, but $(1, 2, 0)$ is not.

Why the parity glue helps. If the slabs $n_x = \text{const}$ are flat translates of $\mathbb{Z}^2$, as for $\mathbb{Z}^3$ and for the small-entry layers, neighbours within a slab are at distance 1, whatever the shear between slabs. The offset $(\frac{1}{2}, 0, 0)$ of the odd coset relative to the even one lifts the in-slab distance to $\sqrt{5}/2$, at the price of halving the gap in x between points of opposite parity in consecutive slabs; the shear $\frac{1}{8}$ pays exactly that price. In odd dimension $s \geq 5$ the packings D_s^+ below are also unions of two cosets. The mechanism of Figure 1 is unchanged: one point per cell, the pattern Γ placed by the geometric digit, minus the cost of the jitter ($\sqrt{3}/p$) and of the drift.

Why the shared digit, and why only $m = 3$. The shear is one shift in y and in z , and the two offsets must wrap together. If the y - and z -digits wrapped at different cells, then in a slab where only the z -offset wraps the cells n and $n + (1, 0, 1)$ would hold points about $(\frac{1}{2}, \frac{1}{8}, \frac{1}{8})$ apart, at distance about $\sqrt{9/32} < 0.54$. Equal rows exclude this; in the proof it is the identity $V_y - V_z = T$. By Lemma 50, two coordinates of a $(0, m, 3)$ -net share the row of their first offset digit only for $m = 3$, so the construction does not extend to $m > 3$ in this form. Other mechanisms that correlate the wraps at $k \geq 2$, not through equal rows, are not ruled out (Remark 123(7)).

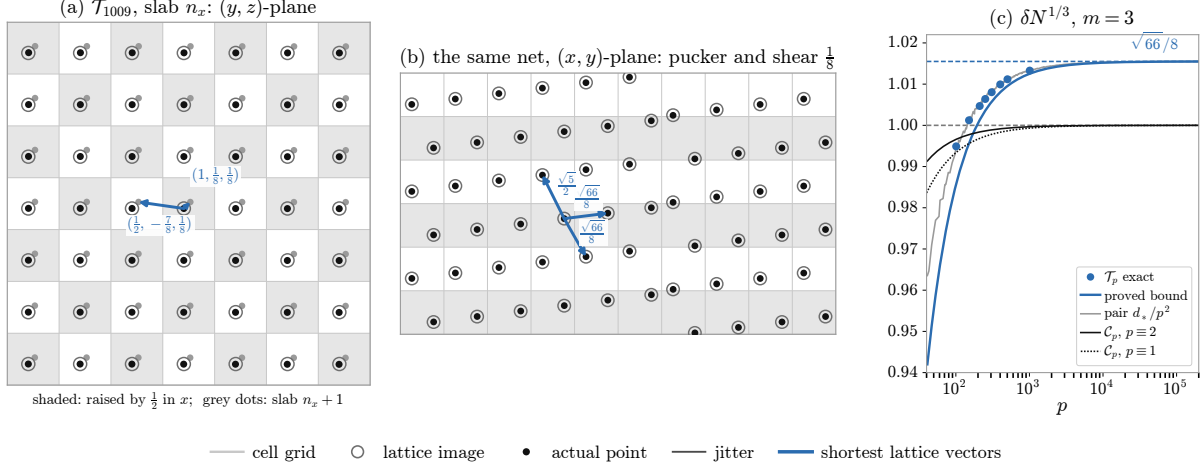


FIGURE 12. A two-coset layer at $m = 3$: the net $\mathcal{T}_{1009}$ of Proposition 103 ($h = 504$, $r = 126$), in cell units. (a) The (y, z) -plane of the slab of cells $n_x = 661$, 7×7 cells around $(n_y, n_z) = (309, 171)$. The coordinates y and z read the same geometric digit $rn_x - n_y + n_z$, so the points of a slab lie, up to drift and jitter, on a translate of $\mathbb{Z}^2$ (open circles: the pattern Γ anchored at the central point); the geometric digit $h(n_y + n_z)$ of x , with $h \equiv -\frac{1}{2}$, raises the points of every other cell (shaded) by $\frac{1}{2}$ in x . Grey dots: the next slab $n_x + 1$, shifted by $(\frac{1}{8}, \frac{1}{8})$. Accent: from a raised point, the two kinds of shortest vectors to the next slab, $(1, \frac{1}{8}, \frac{1}{8})$ and $(\frac{1}{2}, -\frac{7}{8}, \frac{1}{8})$, both of length $\sqrt{66}/8$. (b) The (x, y) -plane of the cells with $n_z = 171$: along y the points alternate between the two heights (the pucker; in-slab neighbours are $\sqrt{5}/2$ apart), and from column to column the y -offset grows by $\frac{1}{8}$ (the shear) and wraps after eight columns. Accent: the same two shortest vectors (their z -components $\frac{1}{8}$ are not visible) and an in-slab neighbour. In (a) and (b) every point is within 0.01 of its site of Γ in each coordinate, and Γ has one site in each cell; it is the union of two cosets of a lattice of covolume 2 and is not a lattice. (c) $\delta N^{1/3}$ against p : exact values for $\mathcal{T}_p$ at 8 primes $101 \leq p \leq 1009$ (dots; computed, Appendix G), the lower bound of Proposition 103(2) (for $p \geq 41$), the pair value d_*/p^2 of (3), and for comparison the exact values of the column nets $\mathcal{C}_p$ (Theorem 49; solid for $p \equiv 2$, dotted for $p \equiv 1 \pmod{3}$), which stay below 1 (Corollary 94); dashed: 1 and $\sqrt{66}/8$.

Computed values. At eight primes $101 \leq p \leq 1009$ the exact minimum distance of $\mathcal{T}_p$ is attained by the pair of (3), from $\delta N^{1/3} = 0.9949\dots$ at $p = 101$ to $1.0132\dots$ at $p = 1009$ (computed; Figure 12(c), Appendix G). The column nets have, exactly, $0.9966\dots$ at $p = 101$ and $0.9978\dots$ at $p = 307$ (Theorem 49). Compared at every prime $7 \leq p \leq 199$ other than 23 (computed), $\mathcal{T}_p$ is ahead at 103, 109 and at every prime $127 \leq p \leq 199$, and $\mathcal{C}_p$ at the other primes, all of them $p \leq 113$. For $p \geq 197$ the bound of Proposition 103(2) exceeds 1, so by Corollary 94 $\mathcal{T}_p$ is ahead of every column point set at every prime $p \geq 197$. The rank-one nets $\mathcal{W}_p$ of the next subsection are ahead of every column point set already at every prime $p \geq 17$, and of $\mathcal{T}_p$ (Section 13.3).

13.3. Resolution $m = 3$: a rank-one layer. In $\mathcal{T}_p$ the coordinates y and z wrap together, and x wraps independently of them. Such a coordinate must move by exactly one cell along its own axis, and its glue must be $\frac{1}{2}$ (Remark 99; see *Why locking pays* below). Making all three coordinates wrap together removes this restriction and gives a larger constant. We first say what locked wraps are, for any layer at $m = 3$. In this section the *layer* is the matrix B over $\mathbb{F}_p$ of the geometric digits, $r(n) = Bn \bmod p$.

Locked wraps. Write a digital $(0, 3, 3)$ -net over $\mathbb{F}_p$ in graph form with depths $(1, 1, 1)$, as in Lemma 98(i): coordinate c of the point of cell n has the digits n_c , $r_c(n) = (Bn)_c$ and a third digit. The phase of a cell is given by its geometric digits $r(n)$, which run exactly over the image $W = B\mathbb{F}_p^3$, and by Lemma 98(i) coordinate c wraps on the step E if and only if $r_c(n) \geq p - \beta_c$. So the wrap vectors ω that occur on the step E are exactly those for which W meets the box $\prod_c I_c$, with $I_c = [p - \beta_c, p)$ if $\omega_c = 1$ and $I_c = [0, p - \beta_c)$ if $\omega_c = 0$. If B is invertible, $W = \mathbb{F}_p^3$ and every wrap vector occurs: the free wraps of Lemma 98(i). If B is singular, every integer vector $\mathbf{h}$ with $\mathbf{h}^\top B \equiv 0 \pmod{p}$ (a *relation*) gives $\mathbf{h} \cdot r(n) \equiv 0$ at every cell, and wrap vectors can be excluded: the wraps are *locked*. These statements are exact for every p .

The limit model (heuristic). To explain the constants we also use a limit model, which no proof below uses. Suppose $B = pA + O(1)$ with A fixed, with a fixed finite set of relations $\mathbf{h}$ of bounded $|\mathbf{h}|_\infty$, every other relation having $|\mathbf{h}|_\infty \rightarrow \infty$ with p . Then the phases $r(n)/p$ become dense in the subtorus $Y \subset (\mathbb{R}/\mathbb{Z})^3$ cut out by the bounded relations (it is connected: if $k\mathbf{h}$ is a relation and $0 < |k| < p$, so is $\mathbf{h}$), the wrap vectors that occur are those of the open boxes that meet Y , and in cell units the step E joins two points at $E + \beta - \omega$, $\beta = AE \bmod 1$, up to $O(1/p)$. The *model value* of (A, Y) is the least $|E + \beta - \omega|$ over the steps $E \neq 0$ and these wrap vectors. Locked wraps mean $\dim Y < 3$.

Examples. (a) For $\mathcal{T}_p$ the relation $(0, 1, -1)$ gives $Y = \{\psi \in (\mathbb{R}/\mathbb{Z})^3 : \psi_y = \psi_z\}$, of dimension 2: y and z wrap together, and the model value is $\sqrt{66}/8$, the minimum of Γ . (b) A layer of rank one, $B \equiv \mathbf{w}u^\top \pmod{p}$ with a fixed primitive integer vector $\mathbf{w}$, has the relations $\mathbf{h} \perp \mathbf{w}$ and $Y = \{\vartheta \mathbf{w} : \vartheta \in \mathbb{R}/\mathbb{Z}\}$, of dimension 1: all three wraps follow one parameter ϑ . The column nets have $\mathbf{w} = \mathbf{1}$, and the net $\mathcal{W}_p$ below has $\mathbf{w} = (2, 2, 1)$. (c) The rank alone does not determine Y : $\mathbf{w} = (1, t, t^2)$ with $t \approx p^{1/3}$ gives layers of rank one whose phases become dense in $(\mathbb{R}/\mathbb{Z})^3$ as $p \rightarrow \infty$.

Why locking pays. A coordinate whose wraps are free cannot move by $1 + \alpha$ with a small $\alpha \neq 0$ along its own axis: at a cell where it wraps alone, the same step moves it by α only, which shortens the step (Remark 99). So in $\mathcal{T}_p$ the free coordinate x moves by exactly one cell along $\mathbf{e}_x$, and the balance of its two contacts sits at $\frac{33}{32}$. A coordinate whose wraps are locked can move by more. In $\mathcal{W}_p$ the coordinate z reads half of the geometric digit that x and y share, so z wraps only where x and y wrap too. The step along $\mathbf{e}_z$ moves z by $1 + 2\varepsilon$, with $\varepsilon = \rho/(2p) \rightarrow \frac{1}{48}$, and x and y by 4ε ; at a wrap of z it is $(-1 + 4\varepsilon, -1 + 4\varepsilon, 2\varepsilon)$, long, because x and y wrap with z . If z wrapped alone it would be $(4\varepsilon, 4\varepsilon, 2\varepsilon)$, of length $6\varepsilon \rightarrow \frac{1}{8}$. The longer step along $\mathbf{e}_z$ lifts the other contact as well. In $\mathcal{W}_p$ the coordinate z plays the part of x in $\mathcal{T}_p$, and the analogue of the diagonal contact $(\frac{1}{2}, -\frac{7}{8}, \frac{1}{8})$ of Γ is $(1 - 6\varepsilon, -6\varepsilon, -\frac{1}{2} - 3\varepsilon)$. Its z -component now exceeds $\frac{1}{2}$ in absolute value, so this contact is longer than in Γ . At $\varepsilon = \frac{1}{48}$ the two contacts have the squared lengths $\frac{281}{256}$ and $\frac{211}{192}$ (Table 9, rows (a) and (b)); Figure 13 shows both nets and the short step that locked wraps avoid.

Proposition 104 (A rank-one layer at $m = 3$; (4) computer-assisted). *Let $p \geq 5$ be a prime, $h = (p - 1)/2$, $r = \lfloor p/48 \rfloor$ and $\rho = 2r + 1$. Let $\mathcal{W}_p$ be the digital net over $\mathbb{F}_p$ whose generator matrices C_x, C_y, C_z have the rows*

$$C_x : \mathbf{e}_x, \rho(-1, -1, 2), (0, 1, 2); \quad C_y : \mathbf{e}_y, \rho(-1, -1, 2), (1, 0, 1);$$

$$C_z : \mathbf{e}_z, (h-r, h-r, \rho), (0, 1, 0).$$

- (1) $\mathcal{W}_p$ is a $(0, 3, 3)$ -net, and every cell of side p^{-1} holds one point.
- (2) For $p \geq 53$ its toroidal (hence also Euclidean) minimum distance satisfies, for any third rows,

$$\delta N^{1/3} \geq \sqrt{\frac{281}{256} - \frac{345}{128p}} - \frac{\sqrt{3}}{p}.$$

The bound increases with p ; it exceeds 1 for $p \geq 67$ and $\sqrt{66}/8$ for $p \geq 97$.

- (3) For $p \geq 53$ the points of the cells $(1, 0, 0)$ and $(2, 0, p-1)$ have toroidal distance d_* at integer scale p^3 , where $d_*^2 = (p^2 - (6r+2)p - 2)^2 + (6r+3)^2 p^2 + (h+3r+2)^2 p^2$, and $d_*/p^2 < \sqrt{281}/16 + 5/(2p)$. So $\delta N^{1/3} \rightarrow \sqrt{281}/16 = 1.0476 \dots$ as $p \rightarrow \infty$.
- (4) $\delta N^{1/3} > 1$ for every prime $p \geq 17$, and $\delta N^{1/3} > \sqrt{66}/8$ for every prime $p \geq 53$.

Since $2(h-r) \equiv -\rho$, the second rows of C_x and C_y are twice that of C_z modulo p : z reads the digit $\zeta(n) = u \cdot n \bmod p$, $u = (h-r, h-r, \rho)$, and x and y both read $2\zeta(n) \bmod p$. The layer is $(2, 2, 1)u^\top$, of rank one, and as $u/p \rightarrow (\frac{23}{48}, \frac{23}{48}, \frac{1}{24})$, in cell units the point of cell n sits near $n + \{\vartheta_n(2, 2, 1)\}$ with $\vartheta_n = \frac{23}{48}(n_x + n_y) + \frac{1}{24}n_z$, up to the drift and the jitter. Part (3) bounds δ from above by one explicit pair, which is not a closest pair: at every prime $53 \leq p \leq 199$ and at $p = 307, 353$ the exact $\delta N^{1/3}$ is smaller than d_*/p^2 (computed).

The proof of (2) rests on an exact description of the wraps of the shared digit.

Lemma 105 (Wraps of a doubled digit). *Let $p \geq 5$ be a prime, $h = (p-1)/2$, $u \in \mathbb{F}_p^3 \setminus \{0\}$, and $\zeta(n) = u \cdot n \bmod p \in \{0, \dots, p-1\}$ for $n \in \mathbb{F}_p^3$. For $E \in \mathbb{Z}^3$ and $n' \equiv n + E$ put $\Delta\zeta = \zeta(n') - \zeta(n)$ and $\omega = [2\zeta(n') \geq p] - [2\zeta(n) \geq p]$, so that the digit $2\zeta \bmod p$ changes by $2\Delta\zeta - p\omega$. Let $\sigma \in \{0, \dots, p-1\}$ be the residue of $u \cdot E$. As n runs over $\mathbb{F}_p^3$, the pairs $(\Delta\zeta, \omega)$ that occur are exactly: $(0, 0)$ if $\sigma = 0$; and if $\sigma \neq 0$, for each $\Delta\zeta \in \{\sigma, \sigma - p\}$ the pair $(\Delta\zeta, \text{sgn } \Delta\zeta)$, and also $(\Delta\zeta, 0)$ if $|\Delta\zeta| \leq h$.*

Proof. As $u \neq 0$, ζ takes every value, and $\zeta(n') \equiv \zeta(n) + \sigma$; so $\Delta\zeta = \sigma$ for $\zeta(n) \leq p-1-\sigma$ and $\Delta\zeta = \sigma - p$ otherwise, and both occur if $\sigma \neq 0$. Reversing the pair exchanges $(\Delta\zeta, \omega)$ and $(-\Delta\zeta, -\omega)$, so let $\Delta\zeta = d > 0$ and $\zeta = \zeta(n) \in [0, p-1-d]$. As $2\zeta \geq p$ if and only if $\zeta \geq h+1$, $\omega \in \{0, 1\}$, and $\omega = 1$ if and only if $\zeta \leq h < \zeta + d$; such ζ form the interval $[\max(0, h+1-d), \min(h, p-1-d)]$, which is not empty, as $1 \leq d \leq p-1$ and $h+2 \leq p$. And $\omega = 0$ if and only if $\zeta + d \leq h$, possible if and only if $d \leq h$, or $\zeta \geq h+1$, possible if and only if $h+1 \leq p-1-d$, i.e. $d \leq h-1$. $\square$

The lemma holds for $u = 0$ as well: then $\sigma = 0$ for every E , $\zeta \equiv 0$, and only $(0, 0)$ occurs. We call each pair $(\Delta\zeta, \omega)$ that occurs for a step E an *option* of E .

Proof of Proposition 104. (1) The first rows are $\mathbf{e}_x, \mathbf{e}_y, \mathbf{e}_z$, so $\mathcal{W}_p$ is a graph form with the depths $(1, 1, 1)$, and we use Lemma 2: the box of shape $(1, 1, 1)$ has determinant 1 and puts one point in every cell. A box with depth 2 on a , 1 on b and 0 on c has, up to sign, the determinant $(C_a)_{2,c}$; these off-diagonal entries of the second rows are $-\rho, 2\rho, -\rho, 2\rho, h-r, h-r$. The box with depth 3 on a has, up to sign, the 2×2 minor of the second and third rows of C_a off column a : $\det \begin{pmatrix} -\rho & 2\rho \\ 1 & 2 \end{pmatrix} = -4\rho$, $\det \begin{pmatrix} -\rho & 2\rho \\ 1 & 1 \end{pmatrix} = -3\rho$ and $\det \begin{pmatrix} h-r & h-r \\ 0 & 1 \end{pmatrix} = h-r$ for $a = x, y, z$. As $1 \leq \rho \leq \frac{p}{24} + 1 < p$, $1 \leq h-r < p$ and $p \geq 5$, all these are units, and Lemma 1 concludes.

(2) *Reduction.* At integer scale p^3 the point of cell n is $X(n) = p^2 n + p g(n) + f(n)$, with the second digits $g(n) = (2\zeta(n) \bmod p, 2\zeta(n) \bmod p, \zeta(n))$ and the third digits $f(n)$. As in the proof of Proposition 103, a representative of $X(n') - X(n)$ is $D = p^2 E + p \Delta g + \Delta f$ with $E \equiv n' - n$, $|\Delta f| < p$, and only $E \in \{-2, \dots, 2\}^3 \setminus \{0\}$ can give $|D| \leq 2p^2$; then $|D|/p^2 > |V| - \sqrt{3}/p$

row	A	steps E	(ν, ω)	Q	$ V ^2$	at $\varepsilon = \frac{1}{48}$	slope
(a)	$(1, 0, -\frac{1}{2})$	$(1, 0, -1)$	$(\frac{1}{2}, 1)$	3	$\frac{5}{4} - 9\varepsilon + 81\varepsilon^2$	$\frac{281}{256}$	$-\frac{45}{8}$
(b)	$(0, 0, 1)$	$(0, 0, 1)$	$(0, 0)$	-2	$1 + 4\varepsilon + 36\varepsilon^2$	$\frac{211}{192}$	$\frac{11}{2}$
		$(1, 1, 2)$	$(-1, -1)$				
(c)	$(1, 0, \frac{1}{2})$	$(1, 0, 0)$	$(\frac{1}{2}, 1)$	1	$\frac{5}{4} - 5\varepsilon + 9\varepsilon^2$	$\frac{883}{768}$	$-\frac{37}{8}$
(d)	$(1, 0, -\frac{1}{2})$	$(1, 0, 0)$	$(-\frac{1}{2}, -1)$	1	$\frac{5}{4} - 3\varepsilon + 9\varepsilon^2$	$\frac{305}{256}$	$-\frac{21}{8}$
		$(0, -1, -1)$	$(\frac{1}{2}, 0)$				
(e)	$(1, 0, \frac{1}{2})$	$(1, 0, 1)$	$(-\frac{1}{2}, -1)$	-1	$\frac{5}{4} + 5\varepsilon + 9\varepsilon^2$	$\frac{1043}{768}$	$\frac{43}{8}$
(f)	$(1, 1, 0)$	$(1, 1, 0)$	$(0, 0)$	2	$2 - 16\varepsilon + 36\varepsilon^2$	$\frac{323}{192}$	$-\frac{29}{2}$
		$(0, 0, -1)$	$(1, 1)$				
(g)	$(1, -1, 0)$	$(1, -1, 0)$	$(0, 0)$	0	2	2	0

TABLE 9. The short options in the proof of Proposition 104(2): every step E and every (ν, ω) allowed by the rules of the proof with $|A|^2 \leq \frac{9}{4}$, up to the reversal $(E, \nu, \omega, A, Q) \mapsto (-E, -\nu, -\omega, -A, -Q)$ and the exchange of x and y . Here E is a cell step, $Q = E_x + E_y - 2E_z$, $\nu \in \frac{E_x + E_y}{2} + \mathbb{Z}$ the integer part of the change of ζ/p , ω the wrap of the digit $2\zeta \bmod p$, $A = E + (2\nu - \omega)(1, 1, 0) + \nu \mathbf{e}_z$ the limit step, $\mathbf{w} = (2, 2, 1)$, $V = A - Q\varepsilon \mathbf{w}$ the step in cell units without the jitter, $\varepsilon = \rho/(2p)$, and the last columns give $|V|^2 = |A - Q\varepsilon \mathbf{w}|^2$, its value and its derivative in ε at the limit $\varepsilon = \frac{1}{48}$. Row (a) is the diagonal contact, row (b) the step along $\mathbf{e}_z$, and the second step of row (f) the step along $-\mathbf{e}_z$ at a wrap of z , where x and y wrap too.

with $V = E + \Delta g/p$, and by Lemma 105 $\Delta g = (2\Delta\zeta - p\omega, 2\Delta\zeta - p\omega, \Delta\zeta)$. It suffices to show $|V|^2 \geq \frac{281}{256} - \frac{345}{128p}$.

Parametrization. Put $S = E_x + E_y$, $Q = S - 2E_z$ and $\varepsilon = \rho/(2p)$. As $2(h - r) = p - \rho$, $2u \cdot E = pS - \rho Q$, so $\Delta\zeta = p(\nu - Q\varepsilon)$ with $\nu \in \frac{S}{2} + \mathbb{Z}$, and

$$V = A - Q\varepsilon \mathbf{w}, \quad A = E + (2\nu - \omega)(1, 1, 0) + \nu \mathbf{e}_z, \quad \mathbf{w} = (2, 2, 1),$$

$$|V|^2 = |A|^2 - 2Q(A \cdot \mathbf{w})\varepsilon + 9Q^2\varepsilon^2.$$

With $\theta = 48r - p$, an odd integer in $[-47, -1]$ (here θ is not that of Proposition 103), we have $\rho = (p + \theta)/24 + 1$, so $\varepsilon = \frac{1}{48} + \frac{\theta+24}{48p}$ and $|\varepsilon - \frac{1}{48}| \leq \frac{23}{48p}$; for $p \geq 53$, $\varepsilon \leq \frac{19}{636} < \frac{3}{100}$. The drift of the layer is this deviation of ε from its limit.

Which (ν, ω) occur. Let $p \geq 53$. Then $|Q| \leq 8$ and $4\rho \leq \frac{p}{6} + 4 < h$. By Lemma 105: if $\nu = 0$, then $\Delta\zeta = -Q\rho/2$, $|\Delta\zeta| \leq h$, and $\omega \in \{0, -\text{sgn } Q\}$ (only $\omega = 0$ if $Q = 0$); if $\nu = \pm\frac{1}{2}$, then $\Delta\zeta = \frac{1}{2}(\pm p - Q\rho)$ has the sign of ν , $\omega = \text{sgn } \nu$ occurs, and $\omega = 0$ occurs if and only if $\nu Q > 0$; if $\nu = \pm 1$, the step occurs only if $\nu Q > 0$, and then $|\Delta\zeta| > h$ and $\omega = \text{sgn } \nu$; and $|\nu| \geq \frac{3}{2}$ gives $|\Delta\zeta| \geq \frac{3}{2}p - 4\rho > p$, which does not occur. None of these rules depends on p or on its class.

Long options. A lies in the lattice $\Lambda_{\mathcal{W}} = \{A : A_x, A_y \in \mathbb{Z}, 2A_z \in \mathbb{Z}, A_x + A_y \equiv 2A_z \pmod{2}\}$, as $A_x + A_y \equiv S \equiv 2\nu \equiv 2A_z$. By the rules $|2\omega - 2\nu| \leq 2$, and $Q = (A_x + A_y - 2A_z) - 2\nu + 2\omega$, so $|Q| \leq \sqrt{6}|A| + 2$. Hence $|V| \geq |A| - 3|Q|\varepsilon \geq (1 - \frac{9\sqrt{6}}{100})|A| - \frac{9}{50} > 1.05$ if $|A|^2 \geq 3$, and $1.05^2 > \frac{281}{256}$.

Short options. Since $2A_z \in \mathbb{Z}$, $|A|^2$ is an integer or an integer plus $\frac{1}{4}$, and $|A|^2 = \frac{9}{4}$ would need $A = (\pm 1, \pm 1, \pm\frac{1}{2})$ or $\pm\frac{3}{2}\mathbf{e}_z$, which violate the parity condition; so the vectors of $\Lambda_{\mathcal{W}}$ with $0 < |A|^2 < 3$ are those with $|A|^2 \leq 2$: $\pm\mathbf{e}_z$, $(\pm 1, 0, \pm\frac{1}{2})$, $(0, \pm 1, \pm\frac{1}{2})$ and $(\pm 1, \pm 1, 0)$. For each of them $E = A - (2\nu - \omega)(1, 1, 0) - \nu \mathbf{e}_z$, with $\nu \equiv A_z \pmod{1}$ and $|\nu| \leq 1$, so at most three values

of ν , and checking the rules for these values and their ω leaves the options of Table 9; $A = 0$ does not occur (it would need $E = \omega(1, 1, 0)$ with $\nu = 0$, $\omega = -\operatorname{sgn} Q = -\operatorname{sgn}(2\omega)$, or $E = -\nu \mathbf{1}$ with $|\nu| = 1$ and $Q = 0$). The squared length $q(\varepsilon) = |V|^2$ of each row is a convex quadratic in ε , so it lies above its tangent line at $\frac{1}{48}$, and as $|\varepsilon - \frac{1}{48}| \leq \frac{23}{48p}$, $q(\varepsilon) \geq q(\frac{1}{48}) - |q'(\frac{1}{48})| \cdot \frac{23}{48p} =: T(p)$. For the diagonal contact (a), $T(p) = \frac{281}{256} - \frac{345}{128p}$, as $\frac{45}{8} \cdot \frac{23}{48} = \frac{345}{128}$. For the step (b) along $\mathbf{e}_z$, $T(p) = \frac{211}{192} - \frac{253}{96p}$, which is larger, as $\frac{211}{192} > \frac{281}{256}$ and $\frac{253}{96} < \frac{345}{128}$. For the rows (c)–(g), $q(\frac{1}{48}) > \frac{281}{256}$, so $p(T(p) - \frac{281}{256}) = p(q(\frac{1}{48}) - \frac{281}{256}) - \frac{23}{48}|q'(\frac{1}{48})|$ is affine in p with positive slope, and at $p = 53$ it is positive (for row (c), $53 \cdot \frac{5}{96} - \frac{23}{48} \cdot \frac{37}{8} > 0$, and the other rows have more room); so these options have $|V|^2 > \frac{281}{256}$. This proves (2). The constant $\frac{345}{128}$ is the slope of the diagonal contact (a) times the largest drift $\frac{23}{48p}$, which is attained for $p \equiv 1 \pmod{48}$; exactly, with $x = \varepsilon - \frac{1}{48} = \frac{\theta+24}{48p}$,

$$|V_a|^2 = \frac{281}{256} - \frac{45}{8}x + 81x^2.$$

The bound increases with p ; it is 1.0024... at $p = 67$, below 1 at $p = 61$, 1.0164... at $p = 97$ and below $\sqrt{66}/8 = 1.01550...$ at $p = 89$.

(3) Here $\zeta(1, 0, 0) = h - r$ and $\zeta(2, 0, p - 1) = p - 2 - 4r$, so the second digits of the two points are $(p - 1 - 2r, p - 1 - 2r, h - r)$ and $(p - 4 - 8r, p - 4 - 8r, p - 2 - 4r)$ (as $p \geq 8r + 4$), and the third digits are $(0, 1, 0)$ and $(p - 2, 1, 0)$. Hence $D = (p^2 - (6r + 2)p - 2, -(6r + 3)p, -(h + 3r + 2)p)$ is a representative of the difference with $|D_c| < p^3/2$, i.e. the toroidal one. As $6r + 3 = 3\rho$ and $h + 3r + 2 = \frac{1}{2}(p + 3\rho)$, $D/p^2 = (1 - 6\varepsilon, -6\varepsilon, -\frac{1}{2} - 3\varepsilon) + (\frac{1}{p} - \frac{2}{p^2}, 0, 0)$: the contact (a) with the step $E = (1, 0, -1)$, plus a jitter. So $d_*/p^2 \leq |V_a| + \frac{1}{p}$, where by the display in (2), with $|x| \leq \frac{23}{48p}$, $|V_a|^2 \leq \frac{281}{256} + \frac{345}{128p} + \frac{4761}{256p^2} < \frac{281}{256} + \frac{3.05}{p}$ for $p \geq 53$; with $\sqrt{a+x} \leq \sqrt{a} + x/(2\sqrt{a})$ this gives $d_*/p^2 < \sqrt{281}/16 + 2.46/p$, slightly more than (3) states. Together with (2), $\delta N^{1/3} \rightarrow \sqrt{281}/16$.

(4) By (2), $\delta N^{1/3} > 1$ for every prime $p \geq 67$ and $> \sqrt{66}/8$ for every prime $p \geq 97$. The remaining primes are settled by the exact minimum distances (Appendix G): at every prime $17 \leq p \leq 61$, $\delta N^{1/3} \geq 1.0009...$ (least at $p = 47$), and at every prime $53 \leq p \leq 89$, $\delta N^{1/3} \geq 1.0257...$ (least at $p = 89$). $\square$

The balance. In the limit the two shortest contacts are rows (a) and (b) of Table 9: the diagonal contact, lifted by the glue $\frac{1}{2} + 3\varepsilon$, and the step along $\mathbf{e}_z$, lengthened to $1 + 2\varepsilon$ in z . Their squared lengths

$$q_a(\varepsilon) = \frac{5}{4} - 9\varepsilon + 81\varepsilon^2, \quad q_b(\varepsilon) = 1 + 4\varepsilon + 36\varepsilon^2$$

are equal where $45\varepsilon^2 - 13\varepsilon + \frac{1}{4} = 0$. The smaller root is $\varepsilon^* = (13 - 2\sqrt{31})/90 = 0.02071...$, and there both equal μ^{*2} , where $\mu^* = \sqrt{(72 - 8\sqrt{31})/25} = 1.0480...$; on $[0, \frac{1}{18}]$, q_a decreases and q_b increases. The limit $\varepsilon = \frac{1}{48} = 0.02083...$ of $\mathcal{W}_p$ is not a balance: it lies just above ε^* , on the side of the diagonal contact, with $q_a(\frac{1}{48}) = \frac{281}{256} < q_b(\frac{1}{48}) = \frac{211}{192}$, and its length $\sqrt{281}/16$ is 0.030 % below μ^* . Since ρ is an integer, the drift $\varepsilon - \frac{1}{48}$ cannot vanish; the choice $\rho = 2\lfloor p/48 \rfloor + 1$ centres it, $|\varepsilon - \frac{1}{48}| \leq \frac{23}{48p}$, and it gives the first-order constant $\frac{345}{128}$ of (2). The balance μ^* is the optimum of the whole family of layers of this shape.

Proposition 106 (Optimum of the rank-one layers with image $(2, 2, 1)$). *Let $p \geq 5$ be a prime, $\mathbf{w} = (2, 2, 1)$, and let P be a digital $(0, 3, 3)$ -net over $\mathbb{F}_p$ in graph form with the depths $(1, 1, 1)$ whose layer is $B = \mathbf{w}u^\top$ for some $u \in \mathbb{F}_p^3$, with any third rows: z reads the second digit $\zeta(n) = u \cdot n \bmod p$, and x and y read $2\zeta(n) \bmod p$. For $\psi \in (\mathbb{R}/\mathbb{Z})^3$ let $F(\psi)$ be the least value of $|E + \xi\mathbf{w} - \omega(1, 1, 0)|^2$ over the steps $E \in \mathbb{Z}^3 \setminus \{0\}$ and the pairs (ξ, ω) with $\xi \in (-1, 1)$, $\xi \equiv \psi \cdot E \pmod{1}$, and $\omega = \operatorname{sgn} \xi$, or $\omega = 0$ if $|\xi| < \frac{1}{2}$. Let $\psi^* = (\frac{1}{2} - \varepsilon^*, \frac{1}{2} - \varepsilon^*, 2\varepsilon^*)$.*

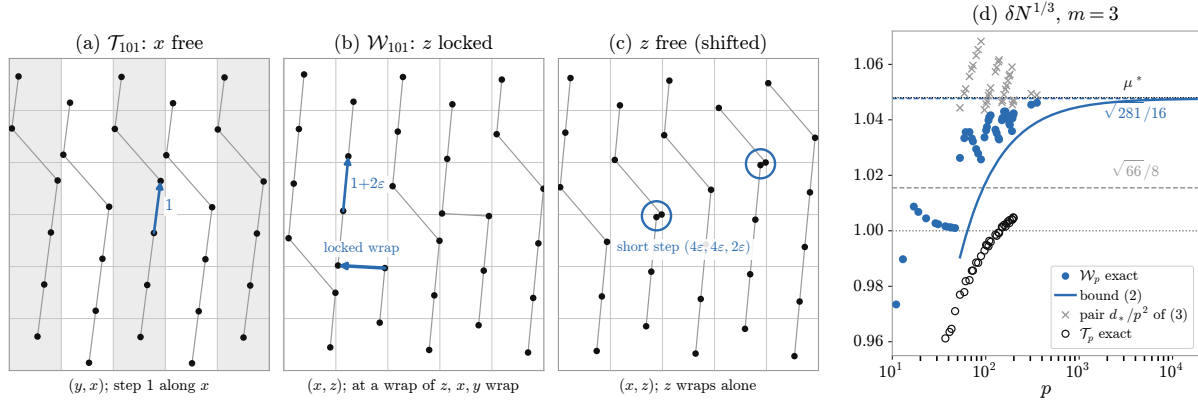


FIGURE 13. Locked and free wraps at $m = 3$, from points generated by the generator matrices, in cell units. Grey segments join the points of consecutive cells along the vertical axis. (a) $\mathcal{T}_{101}$ (Proposition 103), a slab $n_z = \text{const}$ seen in the (y, x) -plane, with the free coordinate x vertical (shaded: cells raised by about $\frac{1}{2}$ in x): the step along $\mathbf{e}_x$ moves x by exactly one cell, up to the jitter, whatever the cell. (b) $\mathcal{W}_{101}$ (Proposition 104, $\varepsilon = \rho/(2p) = 5/202$), a slab $n_y = \text{const}$ in the (x, z) -plane, with the locked coordinate z vertical: the step along $\mathbf{e}_z$ is $(4\varepsilon, 4\varepsilon, 1 + 2\varepsilon)$, longer than one cell (accent arrow); where z wraps, x and y wrap too and the step becomes $(-1 + 4\varepsilon, -1 + 4\varepsilon, 2\varepsilon)$, still long (thick accent arrow; checked at every cell of the window). (c) The same net after the digital shift that adds 1 to the second digit of z : the wraps of z are no longer locked, z now wraps alone at some cells (the cells with $\zeta = p - 1 - \rho$), and the step along $\mathbf{e}_z$ there shrinks to $(4\varepsilon, 4\varepsilon, 2\varepsilon)$ up to the third digits (circles; length 0.148); the shifted net has $\delta N^{1/3} = .1355\dots$, against $1.0362\dots$ without the shift (computed, Remark 108). (d) $\delta N^{1/3}$ of $\mathcal{W}_p$ (exact at the primes $11 \leq p \leq 199$ and at 307, 353; above 1 exactly from $p = 17$ on), the bound of Proposition 104(2) and the explicit pair of (3), which is not a closest pair; open circles: $\mathcal{T}_p$ (exact, $17 \leq p \leq 199$); dotted: the optimum μ^* of the family (Proposition 106), $3.1 \cdot 10^{-4}$ above $\sqrt{281}/16$. Interactive version: explainers/beyond.html (Section 1).

- (1) Let $F_p(u)$ be the squared toroidal minimum distance of the points $p^2n + pg(n)$ at integer scale p^3 , divided by p^4 , where $g(n) = (2\zeta(n) \bmod p, 2\zeta(n) \bmod p, \zeta(n))$ are the second digits: the value of $(\delta N^{1/3})^2$ without the third digits. Then $F_p(u) = F(u/p)$, and $|\delta N^{1/3} - \sqrt{F_p(u)}| < \sqrt{3}/p$ for any third rows.
- (2) For $0 < \varepsilon \leq \frac{3}{100}$, $F(\frac{1}{2} - \varepsilon, \frac{1}{2} - \varepsilon, 2\varepsilon) = \min(q_a(\varepsilon), q_b(\varepsilon))$.
- (3) $F(\psi) \leq \mu^{*2}$ for every $\psi \in (\mathbb{R}/\mathbb{Z})^3$, with equality only at $\psi = \psi^*$. As ψ^* has irrational coordinates, $F_p(u) < \mu^{*2}$, and $\delta N^{1/3} < \mu^* + \sqrt{3}/p$.

So no digital $(0, 3, 3)$ -net whose layer has rank one with image $\mathbb{F}_p(2, 2, 1)$ exceeds $\mu^* + \sqrt{3}/p$, at any prime and with any third rows, and the supremum μ^{*2} of the value without the third digits is attained by no net. Permuting the coordinates gives the isometric families with the images $\mathbb{F}_p(2, 1, 2)$ and $\mathbb{F}_p(1, 2, 2)$.

Proof. Call a step E with a pair (ξ, ω) as in the definition of F an *option* of ψ , with the vector $V = E + \xi\mathbf{w} - \omega(1, 1, 0)$. Every option has $|\xi| < 1$ and $|2\xi - \omega| < 1$, so $|V| > 2$ if some

$|E_c| \geq 3$. The step $\mathbf{e}_z$ gives $V = \mathbf{e}_z$ if $\psi_z \equiv 0$, and otherwise, with $\xi = \{\psi_z\} - 1$ and $\omega = -1$, it gives $V = (2\xi + 1, 2\xi + 1, 1 + \xi)$, whose entries lie in $(-1, 1)$. Hence $F \leq 3$, and only the steps $E \in \{-2, \dots, 2\}^3 \setminus \{0\}$ matter.

(1) At integer scale p^3 the point of cell n is $p^2n + pg(n) + f(n)$ with the third digits $f(n)$. As in the proof of Proposition 104(2), the representatives of the difference of the points of the cells n and n' are $D = p^2E + p\Delta g + \Delta f$ with $E \equiv n' - n \pmod{p}$ and $|\Delta f_c| < p$; without the third digits they are p^2V with $V = E + \Delta g/p$, and $||D|/p^2 - |V|| \leq |\Delta f|/p^2 < \sqrt{3}/p$. Comparing a pair that attains δ with one that attains $\sqrt{F_p(u)}$ gives $|\delta N^{1/3} - \sqrt{F_p(u)}| < \sqrt{3}/p$. By Lemma 105 (which holds for every u ; part (1) uses neither $u \neq 0$ nor the net property), $\Delta g = (2\Delta\zeta - p\omega, 2\Delta\zeta - p\omega, \Delta\zeta)$, and the pairs $(\Delta\zeta, \omega)$ that occur for the step E are those of the lemma. With $\xi = \Delta\zeta/p$ they are exactly the pairs of the definition of F for $\psi = u/p$: $\Delta\zeta \in \{\sigma, \sigma - p\}$ (only 0 if $\sigma = 0$) means $\xi \in (-1, 1)$ and $\xi \equiv u \cdot E/p \pmod{1}$, and, as p is odd, $|\Delta\zeta| \leq h$ means $|\xi| < \frac{1}{2}$. Then $V = E + \xi\mathbf{w} - \omega(1, 1, 0)$. As $p \geq 5$, every step $E \in \{-2, \dots, 2\}^3 \setminus \{0\}$ joins two distinct cells, so $F_p(u) = F(u/p)$.

(2) Let $\psi = (\frac{1}{2} - \varepsilon, \frac{1}{2} - \varepsilon, 2\varepsilon)$ with $0 < \varepsilon \leq \frac{3}{100}$. With $S = E_x + E_y$ and $Q = S - 2E_z$, $\psi \cdot E = \frac{S}{2} - Q\varepsilon$, so $\xi = \nu - Q\varepsilon$ with $\nu \in \frac{S}{2} + \mathbb{Z}$, and $V = A - Q\varepsilon\mathbf{w}$ with $A = E + (2\nu - \omega)(1, 1, 0) + \nu\mathbf{e}_z$. This is the parametrization of the proof of Proposition 104(2), where u/p is of this form with $\varepsilon = \rho/(2p)$. As $|Q\varepsilon| \leq 8\varepsilon < \frac{1}{2}$, the pairs that occur follow the rules stated there: for $\nu = 0$, $|\xi| < \frac{1}{2}$ and $\omega \in \{0, -\text{sgn } Q\}$; for $\nu = \pm\frac{1}{2}$, ξ has the sign of ν , $\omega = \text{sgn } \nu$ occurs, and $\omega = 0$ occurs if and only if $\nu Q > 0$; $\nu = \pm 1$ occurs only if $\nu Q > 0$, and then $\omega = \text{sgn } \nu$; and $|\nu| \geq \frac{3}{2}$ does not occur. The rest of that proof uses only $\varepsilon \leq \frac{3}{100}$: the options with $|A|^2 \geq 3$ have $|V| > 1.05$, and the others are the rows of Table 9. On $(0, \frac{3}{100}]$ the rows (c), (d) and (f) decrease, to 1.1081, 1.1681 and 1.5524, and the rows (e) and (g) are at least $\frac{5}{4}$; all of these, and $1.05^2 = 1.1025$, exceed μ^{*2} , while $\min(q_a(\varepsilon), q_b(\varepsilon)) \leq \mu^{*2}$, as q_a decreases and q_b increases through ε^* . The rows (a) and (b) occur, since $(\nu, \omega) = (\frac{1}{2}, 1)$ and $(0, 0)$ are always allowed. So $F(\psi) = \min(q_a(\varepsilon), q_b(\varepsilon))$.

(3) Let $\psi \in (\mathbb{R}/\mathbb{Z})^3$ with $F(\psi) \geq \mu^{*2}$, and represent ψ_x, ψ_y, ψ_z by numbers in $[0, 1)$. We use only options with $\omega = \text{sgn } \xi$, which always occur, and options with $\omega = 0$ and $|\xi| < \frac{1}{2}$. The numbers $\frac{246}{225} = 1.0933\dots$, $\frac{17}{16}$ and $\frac{9}{25}$ are below $\mu^{*2} = 1.0983\dots$.

The step $\mathbf{e}_z$. If $\psi_z = 0$, then $V = \mathbf{e}_z$ and $|V|^2 = 1$. Otherwise $\xi = \psi_z - 1$, $\omega = -1$ gives $V = (2\psi_z - 1, 2\psi_z - 1, \psi_z)$ with $|V|^2 = 9\psi_z^2 - 8\psi_z + 2$, a convex function with the values $\frac{246}{225}$ at $\psi_z = \frac{2}{15}$ and $\frac{17}{16}$ at $\psi_z = \frac{3}{4}$; so $\psi_z \notin [\frac{2}{15}, \frac{3}{4}]$. If $\psi_z > \frac{3}{4}$, then $\xi = \psi_z - 1$, $\omega = 0$ gives $|V|^2 = 8(1 - \psi_z)^2 + \psi_z^2 \leq \frac{17}{16}$. So $0 < \psi_z < \frac{2}{15}$, and $\xi = \psi_z$, $\omega = 0$ gives $V = (2\psi_z, 2\psi_z, 1 + \psi_z)$ with $|V|^2 = q_b(\psi_z/2)$; as q_b increases, $\psi_z \geq 2\varepsilon^*$.

The steps $\mathbf{e}_x$ and $\mathbf{e}_y$. If $\psi_x = 0$, then $|V|^2 = 1$. Otherwise $\xi = \psi_x$, $\omega = 1$ gives $V = (2\psi_x, 2\psi_x - 1, \psi_x)$ with $|V|^2 = 9\psi_x^2 - 4\psi_x + 1$, a convex function with the values 1 at $\psi_x = 0$ and $\frac{246}{225}$ at $\psi_x = \frac{7}{15}$; so $\psi_x > \frac{7}{15}$. If $\psi_x > \frac{1}{2}$, then $\xi = \psi_x - 1$, $\omega = 0$ gives $V = (1 - 2t, -2t, -t)$ with $t = 1 - \psi_x$, and $|V|^2 = 9t^2 - 4t + 1$ is the same function, so $t > \frac{7}{15}$. Hence $\alpha = \frac{1}{2} - \psi_x \in (-\frac{1}{30}, \frac{1}{30})$, and likewise $\beta = \frac{1}{2} - \psi_y \in (-\frac{1}{30}, \frac{1}{30})$. Put $\gamma = \psi_z$.

The step 1 (the lock). Here $\psi \cdot \mathbf{1} \equiv \gamma - \alpha - \beta =: \tilde{\sigma} \in (-\frac{1}{15}, \frac{1}{5})$. If $\tilde{\sigma} > 0$, then $\xi = \tilde{\sigma} - 1$, $\omega = -1$ gives $V = (2\tilde{\sigma}, 2\tilde{\sigma}, \tilde{\sigma})$ with $|V|^2 = 9\tilde{\sigma}^2 < \frac{9}{25}$. So $\alpha + \beta \geq \gamma$.

The diagonal steps $(1, 0, -1)$ and $(0, 1, -1)$. For $E = (1, 0, -1)$, $\psi \cdot E \equiv \psi_x - \psi_z = \frac{1}{2} - \lambda$ with $\lambda = \alpha + \gamma \in (2\varepsilon^* - \frac{1}{30}, \frac{1}{6}) \subset (0, \frac{1}{6})$, and $\xi = \frac{1}{2} - \lambda$, $\omega = 1$ gives $V = (1 - 2\lambda, -2\lambda, -\frac{1}{2} - \lambda)$ with $|V|^2 = \frac{5}{4} - 3\lambda + 9\lambda^2 = q_a(\lambda/3)$: row (a) of Table 9 with $\varepsilon = \lambda/3$. Likewise $E = (0, 1, -1)$ gives $q_a(\lambda'/3)$ with $\lambda' = \beta + \gamma$. As q_a decreases on $[0, \frac{1}{18}]$ and $q_a(\varepsilon^*) = \mu^{*2} \leq F(\psi)$, we get $\lambda \leq 3\varepsilon^*$ and $\lambda' \leq 3\varepsilon^*$. But $\lambda + \lambda' = \alpha + \beta + 2\gamma \geq 3\gamma \geq 6\varepsilon^*$, by the lock and the step $\mathbf{e}_z$. So equality holds throughout: $\lambda = \lambda' = 3\varepsilon^*$, $\alpha + \beta = \gamma$ and $\gamma = 2\varepsilon^*$, hence $\alpha = \beta = \varepsilon^*$, i.e. $\psi = \psi^*$.

Hence $F(\psi) \geq \mu^{*2}$ only at $\psi = \psi^*$, where $F(\psi^*) = \mu^{*2}$ by (2): $F \leq \mu^{*2}$ everywhere, with equality only at ψ^* . As ε^* is irrational, $u/p \neq \psi^*$, so $F_p(u) = F(u/p) < \mu^{*2}$, and by (1) $\delta N^{1/3} < \sqrt{F_p(u)} + \sqrt{3}/p < \mu^* + \sqrt{3}/p$. $\square$

How six contacts fix the optimum. The proof uses six steps. Along $\mathbf{e}_x$, $\mathbf{e}_y$ and $\mathbf{e}_z$ a coordinate can wrap alone, which shortens the step. This forces ψ_x and ψ_y to stay within $\frac{1}{30}$ of $\frac{1}{2}$ ($|\alpha|, |\beta| < \frac{1}{30}$), and z to move by at least $1 + 2\varepsilon^*$ along $\mathbf{e}_z$ ($\gamma \geq 2\varepsilon^*$), or the step along $\mathbf{e}_z$ is short. The step **1** is the one along which all three coordinates can wrap together, and these offsets must not shorten it: $\alpha + \beta \geq \gamma$. The diagonal contacts then balance against the step along $\mathbf{e}_z$, at an irrational point. The optimum lies on the plane $\psi \cdot \mathbf{1} \equiv 0$, i.e. $u \cdot \mathbf{1} \equiv 0$, where the step **1** has no phase change; $\mathcal{W}_p$ lies on it, as $2(h-r) + \rho = p$. Proposition 106 covers only the image $\mathbb{F}_p(2, 2, 1)$ and its permutations; other rank-one images, layers of rank two and non-digital point sets are not covered (Remark 123(7)).

Remark 107 (Reaching μ^*). Let $\mathcal{W}_p^*$ be the net of Proposition 104 with $r = \lfloor p\varepsilon^* \rfloor$ in place of $\lfloor p/48 \rfloor$. Then $\rho = 2r + 1$ is the odd integer nearest to $2p\varepsilon^*$, and $\varepsilon_p = \rho/(2p)$ satisfies $|\varepsilon_p - \varepsilon^*| < \frac{1}{2p}$ (both use that $p\varepsilon^*$ is never an integer, as ε^* is irrational). $\mathcal{W}_p^*$ is a $(0, 3, 3)$ -net for every prime $p \geq 5$, since the proof of Proposition 104(1) needs only $1 \leq \rho < p$ and $1 \leq h - r < p$. Its layer is $\mathbf{w}u^\top$ with $u/p = (\frac{1}{2} - \varepsilon_p, \frac{1}{2} - \varepsilon_p, 2\varepsilon_p)$, and $\varepsilon_p \leq \frac{3}{100}$ for $p \geq 17$ ($\varepsilon_p = \frac{1}{2p}$ for $p \leq 47$, $\varepsilon_{53} = \frac{3}{106}$, and $\varepsilon^* + \frac{1}{118} < \frac{3}{100}$). So for $p \geq 17$ Proposition 106(1), (2) gives the value $\min(q_a(\varepsilon_p), q_b(\varepsilon_p))$ without the third digits. Both q_a and q_b are convex, so each lies above its tangent line at ε^* ; there q_a decreases and q_b increases, and $q'_b(\varepsilon^*) < |q'_a(\varepsilon^*)|$; hence

$$\delta N^{1/3}(\mathcal{W}_p^*) > \sqrt{\mu^{*2} - \frac{K}{p}} - \frac{\sqrt{3}}{p}, \quad K = \frac{|q'_a(\varepsilon^*)|}{2} = \frac{9\sqrt{31} - 36}{5} = 2.8219\dots,$$

for every prime $p \geq 17$. With Proposition 106(3), $\delta N^{1/3}(\mathcal{W}_p^*) \rightarrow \mu^*$: the optimum of the family is attained in the limit. The bound exceeds 1 from $p = 67$ on and $\sqrt{66}/8$ from $p = 97$ on, as that of Proposition 104(2). It exceeds $\sqrt{281}/16$ from $p = 9791$ on, and the upper bound $\sqrt{281}/16 + 5/(2p)$ of Proposition 104(3) from $p = 17737$ on; only from there on is $\mathcal{W}_p^*$ provably ahead of $\mathcal{W}_p$.

The optimum is reached only asymptotically: at moderate p , $\mathcal{W}_p^*$ is not ahead of $\mathcal{W}_p$. $\mathcal{W}_p^* = \mathcal{W}_p$ for $p < 193$ (computed), and $\mathcal{W}_p^* \neq \mathcal{W}_p$ for $p > 8548$: as $\frac{1}{48} - \varepsilon^* = \frac{96\sqrt{31}-534}{4320} > \frac{1}{8549}$, for $p \geq 8549$ we have $p/48 - p\varepsilon^* > 1$, so $\lfloor p/48 \rfloor > \lfloor p\varepsilon^* \rfloor$, and the two nets have different $\rho < p$. At the primes $p \leq 1009$ where they differ, namely 193, 241, 337, 433, 577, 673, 769 and 1009, $\mathcal{W}_p$ has the larger $\delta N^{1/3}$ (computed; 1.0405... against 1.0355... at $p = 193$, and 1.0463... against 1.0458... at $p = 1009$). At these primes $\varepsilon_p < \varepsilon^*$ for $\mathcal{W}_p^*$, so without the third digits its minimum is the step (b) along $\mathbf{e}_z$, while $\mathcal{W}_p$ has $\varepsilon > \varepsilon^*$ and its minimum is the diagonal contact (a). A heuristic reading of the computed values is that the third rows of Proposition 104 cost the step (b) more than the contact (a): at moderate p the jitter, not the drift, decides, and the value that $\mathcal{W}_p$ gives up by its limit $\varepsilon \rightarrow \frac{1}{48}$ instead of ε^* is small, $\mu^{*2} - \frac{281}{256} < 7 \cdot 10^{-4}$.

Computed values. The exact $\delta N^{1/3}$ of $\mathcal{W}_p$ is 1.0087... at $p = 17$, 1.0262... at $p = 53$, 1.0362... at $p = 101$ and 1.0461... at $p = 353$, and below 1 for $p \leq 13$ (computed). By (4) and Corollary 94, $\mathcal{W}_p$ is ahead of every column point set at every prime $p \geq 17$. It is ahead of $\mathcal{T}_p$ at every prime $17 \leq p \leq 199$ other than 23 (computed), and for $p \geq 53$ also by (4) and Proposition 103(3), as $\delta(\mathcal{T}_p)N^{1/3} \leq d_*(\mathcal{T}_p)/p^2 < \sqrt{66}/8$. Nor is $\sqrt{66}/8$ the best value for layers in which two coordinates share a geometric digit: in the limit model the layer $A = \frac{1}{15} \begin{pmatrix} 0 & 6 & 6 \\ 2 & -1 & -1 \end{pmatrix}$

with $Y = \{\psi \in (\mathbb{R}/\mathbb{Z})^3 : \psi_y = \psi_z\}$ has the value $\sqrt{233}/15 = 1.0176\dots$ (computed), and its realization $B_x = (0, a, a)$, $B_y = B_z = (2r', -r', -r')$, $a = \text{round}(2p/5)$, $r' = \text{round}(p/15)$, with the third rows of $\mathcal{T}_p$, is a $(0, 3, 3)$ -net at $p = 307$ with $\delta N^{1/3} = 1.0160\dots > \sqrt{66}/8$ (computed). Its free coordinate x carries the glue $\frac{2}{5}$. So Remark 99, which concerns the length of a single step under free wraps, does not decide which glue is optimal for the minimum, even for free coordinates.

Only at $m = 3$. At $m = 3k$, $k \geq 2$, the geometric digits of any two coordinates of a $(0, m, 3)$ -net are jointly uniformly distributed (Lemma 50), so no coordinate can read half, or any function, of the geometric digit of another: the lock of $\mathcal{W}_p$, like that of $\mathcal{T}_p$, exists only at $m = 3$ (Remark 123(7)).

Remark 108 (Digital shifts of $\mathcal{T}_p$ and $\mathcal{W}_p$). As for the column nets (Remark 70), a digital shift translates the wrap windows of the coordinates independently, so bounds that use locked wraps need not survive it. The bound of Proposition 103(2) does not extend to shifts whose second digits differ in y and z , the two coordinates that share their geometric digit, for instance at $p = 41, 53, 101$ (computed). If they agree, $\tau_{y,2} = \tau_{z,2}$ (all other shift digits arbitrary), the bound holds for the shifted net, for every prime $p \geq 41$. Indeed, by Lemma 67 the shifted net, indexed by its own cells, is $\mathcal{T}_p$ with constants added to the offset digits. As C_y and C_z have the same second row, the geometric digits of y and z of each cell differ by the constant $\tau_{y,2} - \tau_{z,2} = 0$, so $g_y = g_z$ at every cell; and the differences of the geometric digits of two cells satisfy the same congruences $\xi \equiv hS$, $\eta \equiv rE_x - T$ as for $\mathcal{T}_p$, since the constants cancel. The proof of Proposition 103(2) uses the geometric digits only through these congruences and through $g_y = g_z$, and the third digits only through $|\Delta f_c| < p$; so it applies verbatim. The lock of $\mathcal{W}_p$ (Proposition 104) is more fragile, because z reads half of the digit of x and y . In the notation of Lemma 105 (z reads $\zeta(n) = u \cdot n \bmod p$, and x and y read $2\zeta(n) \bmod p$), let the second shift digits be $\tau_{x,2} = \tau_{y,2} = t$ and $\tau_{z,2} = t'$. Re-indexing the cells by $n' = n + n_0$, for a cell n_0 with $u \cdot n_0 \equiv t'$ (a translation of the torus by $-n_0$ cells, together with a shift of the third digits), turns the shifted net into the one in which z reads $\zeta(n)$ and x and y read $(2\zeta(n) + t - 2t') \bmod p$. For $t \equiv 2t'$ this is $\mathcal{W}_p$ with shifted third digits. For $t \equiv 2t' + 1$ the digit $(2\zeta + 1) \bmod p$ wraps, i.e. $2\zeta + 1 \geq p$, if and only if $\zeta \geq h$, one step earlier than 2ζ , and with $\omega = [2\zeta(n') + 1 \geq p] - [2\zeta(n) + 1 \geq p]$ the pairs $(\Delta\zeta, \omega)$ that occur are exactly those of Lemma 105. Indeed, the proof of the lemma goes through with h in place of $h + 1$: the values of $\Delta\zeta$ and the reversal are unchanged, and for $\Delta\zeta = d > 0$ and $\zeta = \zeta(n) \in [0, p - 1 - d]$ we have $\omega \in \{0, 1\}$; $\omega = 1$ if and only if $\zeta \leq h - 1 < \zeta + d$, which holds for $\zeta = \max(0, h - d)$, so it occurs for every d ; and $\omega = 0$ if and only if $\zeta + d \leq h - 1$, possible if and only if $d \leq h - 1$ (both digits below the wrap), or $\zeta \geq h$, possible if and only if $h \leq p - 1 - d$, i.e. $d \leq h$ (both at or above it). So $\omega = 0$ occurs if and only if $d \leq h$, as in the lemma. The proof of Proposition 104(2) uses the second digits only through these pairs and allows any third digits, so its bound holds for the shifted net whenever $t \equiv 2t'$ or $t \equiv 2t' + 1$; the exact value need not be kept, since the third digits move. Other second digits break the lock in every case computed: at $p = 101$ the shifts $(\tau_{x,2}, \tau_{y,2}, \tau_{z,2}) = (0, 0, 1)$ and $(7, 7, 7)$ give $\delta N^{1/3} = .1355\dots$, against $1.0362\dots$ without a shift, and every shift $(t, t, 0)$ with $2 \leq t \leq 100$ gives $\delta N^{1/3} < 0.1356$, while $(1, 1, 0)$, $(3, 3, 1)$ and $(5, 5, 2)$ keep $1.0362\dots$ (computed). That only $t \equiv 2t'$ and $t \equiv 2t' + 1$ keep the lock is computed, not proved. In the computed cases where the lock breaks, the step along $\mathbf{e}_z$ at a wrap of z alone shrinks to $(4\varepsilon, 4\varepsilon, 2\varepsilon)$ up to the third digits. Proposition 104 is a statement about unshifted nets.

13.4. No half-integer layer in the frame orbit. By Section 3, every net obtained from a frame by per-coordinate lower-triangular scrambles has a geometric layer of Cauchy form, $\tilde{M}_{cd} = \lambda_c \mu_d / D_{cd}$ ($c \neq d$), with units λ_c, μ_d and the homogeneous place differences D_{cd} ; this holds over $\mathbb{Q}$, and verbatim over $\mathbb{F}_p$ for places in $\mathbb{P}^1(\mathbb{F}_p)$. The deepest carry depth $s - 2$ of row 0

is free by Proposition 17 up to one condition per column d (the polynomial $g_{d,s-2}$ there, which the $s-1$ off-diagonal entries of the column determine, must have a unit leading coefficient) and can be made half-integer. But the geometric layer F_0 , which every carry-free step sees, sits at carry depth 0, where the Cauchy form leaves only the row and column scalars free.

Proposition 109 (No half-integer frame layer). *Let $\tilde{M}$ be a layer of this Cauchy form over a field $\mathbb{K}$, and let a, b, c, d be four distinct coordinates.*

- (1) *If $\mathbb{K} = \mathbb{F}_p$, p prime, and $2\tilde{M}_{ij} \equiv h_{ij} \pmod{p}$ for all twelve ordered pairs $i \neq j$ in $\{a, b, c, d\}$, with odd integers $|h_{ij}| \leq \Omega$, then p divides a nonzero odd integer Z with $|Z| \leq 13\Omega^{16}$. In particular this is impossible for $p > 13\Omega^{16}$.*
- (2) *If $\mathbb{K} = \mathbb{Q}$, then the twelve entries $\tilde{M}_{ij}$, $i \neq j$ in $\{a, b, c, d\}$, do not all lie in $\frac{1}{2} + \mathbb{Z}$.*

Proof. By Lemma 18(P) over $\mathbb{K}$, with $\pi_{ij} = \tilde{M}_{ij}\tilde{M}_{ji}$, the numbers $\chi^2 = \pi_{ab}\pi_{cd}/(\pi_{ac}\pi_{bd})$ and $\psi^2 = \pi_{ab}\pi_{cd}/(\pi_{ad}\pi_{bc})$ satisfy $(\chi^2 - \psi^2 - 1)^2 = 4\psi^2$. (1) The entries of a layer of Cauchy form are units, so for odd p the $h_{ij} \equiv 2\tilde{M}_{ij}$ are units modulo p (for $p = 2$ the hypothesis fails, the h_{ij} being odd), and $4\pi_{ij} \equiv h_{ij}h_{ji}$. Let $A_1 = |h_{ab}h_{ba}h_{cd}h_{dc}|$, $A_2 = |h_{ac}h_{ca}h_{bd}h_{db}|$, $A_3 = |h_{ad}h_{da}h_{bc}h_{cb}|$, odd integers at most Ω^4 . Then $\chi^2 \equiv \varepsilon_2 A_1/A_2$ and $\psi^2 \equiv \varepsilon_3 A_1/A_3$ with signs $\varepsilon_2, \varepsilon_3 \in \{\pm 1\}$, and multiplying the last relation by $A_2^2 A_3^2$ shows that p divides

$$Z = (\varepsilon_2 A_1 A_3 - \varepsilon_3 A_1 A_2 - A_2 A_3)^2 - 4\varepsilon_3 A_1 A_2^2 A_3.$$

The bracket is a sum of three odd numbers, hence odd, so Z is odd and in particular nonzero, and $|Z| \leq (3\Omega^8)^2 + 4\Omega^{16} = 13\Omega^{16}$. (2) Over $\mathbb{Q}$ the same computation with $h_{ij} = 2\tilde{M}_{ij}$, odd integers by assumption, gives $Z = 0$ exactly, contradicting that Z is odd. $\square$

So a rational design never has a half-integer geometric layer in the frame orbit (on four coordinates, hence for $s \geq 4$), and a design over $\mathbb{F}_p$ with $|2\tilde{M}| \leq \Omega$ has none once $p > 13\Omega^{16}$. Proposition 109 reads the Plücker relation of Lemma 18(P) modulo powers of 2: it is the 2-adic counterpart of Lemma 18(H), which reads it in absolute value, and of Remark 82, which reads it modulo q .

13.5. The split frame. The ceilings of Theorems 87 and 88 concern bounded layers. A geometric layer with half-integer entries escapes them: locally the points form the packing $D_s^+ = D_s \cup (D_s + \frac{1}{2}\mathbf{1})$ [9, Ch. 4], whose minimum $\min(\sqrt{s}/2, \sqrt{2})$ exceeds 1 for $s \geq 5$ and equals the E_8 value $\sqrt{2}$ at $s = 8$. At the resolution $m = s$ no frame is needed (Section 13.7). For $k \geq 2$ the layer sits at carry depth 0 of a design, and there a Plücker relation between the places excludes rational half-integer layers in the frame orbit (Proposition 109). To escape it, the split frame lets each coordinate c read its cell digits at one point v_c and its offset digits at a different point u_c . Its box minors are still confluent Vandermonde determinants, its geometric layer is the non-symmetric Cauchy matrix $\lambda'_c \mu_d / (u_c - v_d)$ in two unrelated point sets, and with u_c even and v_d odd it can be half-integer at every carry depth.

Definition 110. Let $v_0, \dots, v_{s-1}$ (*cell points*) and $u_0, \dots, u_{s-1}$ (*offset points*) be $2s$ pairwise distinct rational numbers, let D be the product of their denominators and of the numerators of their pairwise differences, $R = \mathbb{Z}[1/D]$ and $m = sk$. For $V \in R[t]_{<m}$ let coordinate c have the m digits

$$[(t - v_c)^j] V \quad (j < k), \quad \text{followed by} \quad [(t - u_c)^j] V \quad (j < m - k).$$

Put $\vartheta_{cd} = u_c - v_d$, $\Pi(t) = \prod_d (t - v_d)^k$, $\Pi_d = \Pi / (t - v_d)^k$ and $\Theta_c = \prod_d \vartheta_{cd}$, so that $\Pi(u_c) = \Theta_c^k$.

With $u = v$ (and one place at ∞) this would be the frame of Section 3.2. Here the cell of coordinate c is the k -jet of V at v_c and its offset is the jet at a different point u_c (Figure 14).

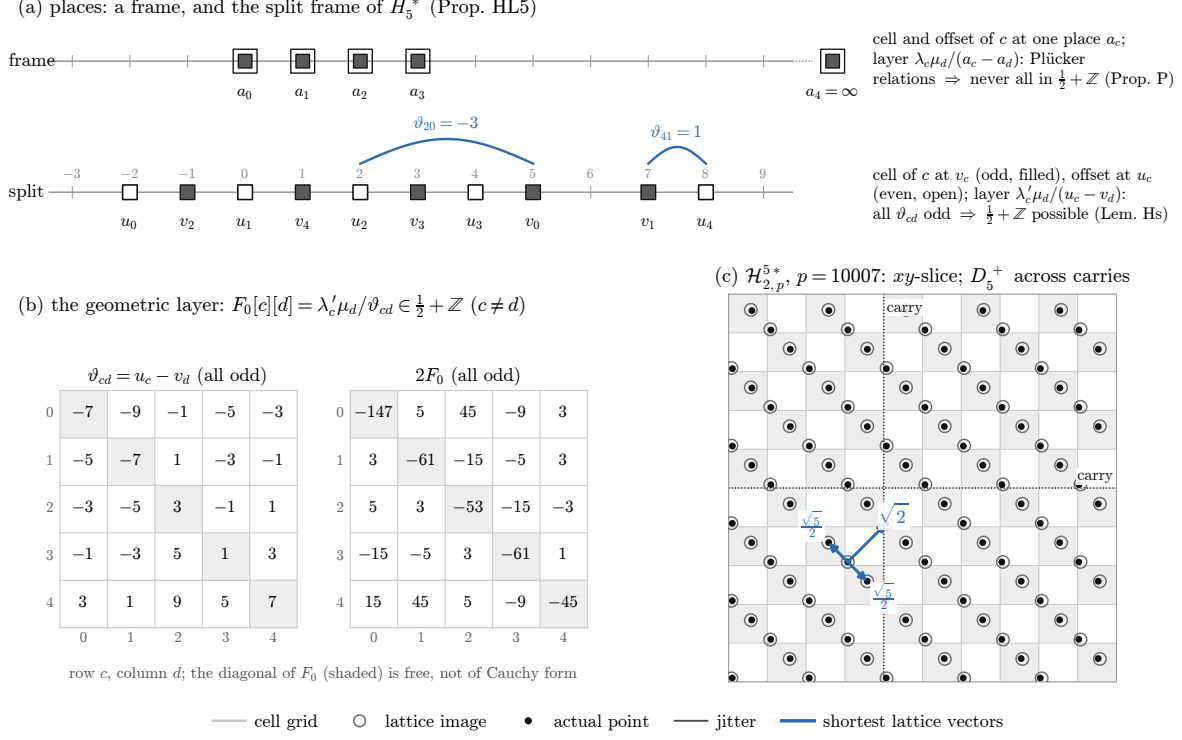


FIGURE 14. Split frames (Definition 110). (a) Top: a frame reads the cell and the offset of coordinate c at one place a_c , so its geometric layer is a symmetric Cauchy matrix, and a Plücker relation among four places rules out a half-integer layer (Proposition 109). Bottom: the split frame of H_5^* (Proposition 122), $u = (-2, 0, 2, 4, 8)$ even, $v = (5, 7, -1, 3, 1)$ odd: coordinate c reads its cell at v_c (filled) and its offset at u_c (open); arcs: two entries $v_{cd} = u_c - v_d$. The box minors are confluent Vandermonde determinants in the ten places (Lemma 111). (b) The geometric layer is the non-symmetric Cauchy matrix $\lambda'_c \mu_d / (u_c - v_d)$ (Proposition 113); every v_{cd} is odd, so the layer can be put in $\frac{1}{2} + \mathbb{Z}$ (Lemma 114; for the explicit H_s , $u_c = 2c$, $v_d = 2d + 1$). Shown: v and $2F_0$ of H_5^* . (c) The net $\mathcal{H}_{2,p}^{5*}$, $p = 10007$: the xy -slice of a 10×10 window of cells that crosses a carry in x and in y (dotted), the other three cells fixed. Every partial sum $M^{(j)}$ of the design lies in $\frac{1}{2} + \mathbb{Z}$, so the corner/centre parity pattern of D_5^+ (minimum $\sqrt{5}/2 > 1$) continues across the carries (Proposition 115); drift and jitter stay below 0.05 of a cell.

Lemma 111 (Box minors of the split frame). *For depths (d_c) with $\sum_c d_c = m$ the box matrix of the split frame consists of the $\min(d_c, k)$ -jets of V at v_c and the $(d_c - k)_+$ -jets at u_c , and its determinant is, up to sign, the confluent Vandermonde product $\prod_{\{P, Q\}} (x_Q - x_P)^{\alpha_P \alpha_Q}$ over the $2s$ points x_P with these multiplicities α_P . In particular, for $s \geq 4$, every $k \geq 1$ and q coprime to the denominators of the points, the split frame is a $(0, sk, s)$ -net over $\mathbb{Z}/q\mathbb{Z}$ if and only if the $2s$ points are pairwise distinct modulo every prime factor of q (which needs every prime factor of q to be at least $2s$).*

Proof. The box matrix is the Hermite matrix of Lemma 8 for the $2s$ points with the multiplicities α_P , $\sum_P \alpha_P = \sum_c d_c = m$ (no point at ∞); this gives the value, a unit modulo p if the points

are distinct modulo p . Conversely, a coincidence modulo p puts two equal rows into some box: $V(v_c)$ and $V(v_d)$ for $v_c \equiv v_d$ (the box $(k, \dots, k)$); $V(u_c)$ and $V(v_d)$ for $u_c \equiv v_d$, $c = d$ allowed (depth $k + 1$ on c , at least 1 on d); $V(u_c)$ and $V(u_d)$ for $u_c \equiv u_d$, $c \neq d$ (depths $k + 1$ on c and d , $k - 1$ on two other coordinates, k elsewhere; here $s \geq 4$ is used). Then Lemma 1. $\square$

So the $t = 0$ property of split frames is Lemma 8 with two points per coordinate (the exact sign is recorded in Appendix F). As for frames, the $(k, \dots, k)$ box is invertible over R , so the split frame has a graph form Φ^S with depths $(k, \dots, k)$ and entries in R , whose box minors are those of Lemma 111 divided by the unit $(k, \dots, k)$ minor.

Lemma 112 (First offset rows of the split frame). *For every $k \geq 1$ and $c \neq d$, row 0 of Φ_{cd}^S has, with x^n marking carry depth n , the generating function*

$$\frac{\Theta_c^k}{\Pi_d(v_d + x)(\vartheta_{cd} - x)}.$$

Proof. As $\deg V < sk = \deg \Pi$, partial fractions give $V = \sum_d \Pi_d N_d$ with $\deg N_d < k$; as $V \equiv \Pi_d N_d \pmod{(t - v_d)^k}$ and $\Pi_d(v_d)$ is a unit, the cell of d determines N_d and conversely. The first offset digit of c is $V(u_c)$. For the column (level j of the cell of d , all other cells 0) we have $V = \Pi_d N_d$ with $N_d \equiv (t - v_d)^j / \Pi_d \pmod{(t - v_d)^k}$, i.e. $N_d = \sum_{j \leq i < k} \varphi_{i-j} (t - v_d)^i$ with $\varphi(x) = \sum_n \varphi_n x^n = 1 / \Pi_d(v_d + x)$. Hence, with $\vartheta = \vartheta_{cd}$, $V(u_c) = \Pi_d(u_c) \sum_{j \leq i < k} \varphi_{i-j} \vartheta^i$. Weighting the level $j = k - 1 - n$ by x^n gives $\Pi_d(u_c) \vartheta^{k-1} \varphi(x) \sum_{r \geq 0} (x/\vartheta)^r = \Pi_d(u_c) \vartheta^k \varphi(x) / (\vartheta - x)$ modulo x^k , and $\Pi_d(u_c) \vartheta^k = \Pi(u_c) = \Theta_c^k$. $\square$

Proposition 113 (Normal form and reachable designs of the split frame). *Apply the gauge move of Lemma 2(c) with $L_c = \text{diag}(\Theta_c^{-k}, 1, \dots, 1)$ and $U_d = \text{Toep}(\Pi_d(v_d + x))$. Then row 0 of every off-diagonal block becomes $w_{cd} / (1 - y_{cd}x)$ with*

$$w_{cd} = y_{cd} = \frac{1}{\vartheta_{cd}} = \frac{1}{u_c - v_d} \quad (c \neq d),$$

independently of k , and within each column d the y_{cd} ($c \neq d$) are pairwise distinct with unit differences $y_{cd} - y_{c'd} = (u_{c'} - u_c) / (\vartheta_{cd} \vartheta_{c'd})$. Consequently Propositions 13 and 17, Definition 14 and Corollary 15 hold verbatim for the split frame, with Q_c replaced by Θ_c and Lemma 10 by Lemma 111. In particular a design is reachable with row scalars λ' if and only if, for every column d and every $j \leq s - 2$,

$$M^{(j)}[c][d] = \lambda'_c \frac{g_{d,j}(y_{cd})}{u_c - v_d} \quad (c \neq d)$$

for polynomials $g_{d,j}$ of degree j with unit leading coefficient; and then, for every $k \geq 1$ and every q coprime to DD' , where D' collects the primes of the units λ'_c , of the leading coefficients of the $g_{d,j}$ and of the denominators, the graph form $\mathcal{P}_{k,q}^{u,v,F}$ of Definition 14 (on the split frame) is a digital $(0, sk, s)$ -net over $\mathbb{Z}/q\mathbb{Z}$ with one point in every cell, whose row 0 equals the design on the levels $k - 1, \dots, k - \min(k, s - 1)$ and vanishes below.

Proof. The normal form is Lemma 112 times Θ_c^{-k} and $\Pi_d(v_d + x)$, as in Proposition 12, with unit diagonal entries of L_c and U_d . The proofs of Propositions 13 and 17 use only that the w_{cd} are units and that the y_{cd} of a column are distinct with unit differences (the matrix $(w_{cd} y_{cd}^n)_{c \neq d, n \leq s-2}$ is then a unit diagonal times an invertible Vandermonde matrix), and the proof of Corollary 15 uses only the unit box minors of the frame, here Lemma 111. $\square$

Only the leading coefficients of the $g_{d,j}$ with $j < \min(k, s - 1)$ enter at a given k ; if a prime p divides the leading coefficient of some $g_{d,j}$, the design cannot be realized modulo p at carry depth j , so modulo p the net exists only for $k \leq j$ (this is also verified in Lean). The geometric

layer is now $M_{cd}^{(0)} = \lambda'_c \mu_d / (u_c - v_d)$ with $\mu_d = g_{d,0}$: a general, non-symmetric Cauchy matrix in two different sets of points. There is no Plücker relation between the row points u_c and the column points v_d , so Proposition 109 does not apply, and parities can be prescribed.

Lemma 114 (Half-integer designs). *Let the u_c be even and the v_d odd integers, so that every $\vartheta_{cd} = u_c - v_d$ is odd, put $\Lambda_c = \prod_{d \neq c} \vartheta_{cd}^{s-1}$, and take $\lambda'_c = \frac{1}{2} \Lambda_c$, $g_{d,0} = 1$ and $g_{d,j}(y) = 1 + 2y^j$ for $1 \leq j \leq s-2$. Then*

$$M^{(0)}[c][d] = \frac{\Lambda_c}{2\vartheta_{cd}}, \quad M^{(j)}[c][d] = \frac{\Lambda_c}{2\vartheta_{cd}} + \frac{\Lambda_c}{\vartheta_{cd}^{j+1}} \quad (1 \leq j \leq s-2),$$

all in $\frac{1}{2} + \mathbb{Z}$ ($c \neq d$), so the off-diagonal part of F_0 lies in $\frac{1}{2} + \mathbb{Z}$ and $F_j = M^{(j)} - M^{(j-1)}$ is an integer matrix for $j \geq 1$. Complete the design by $F_0[c][c] = -\alpha_c$, with α_c the least element of $\frac{1}{2} + \mathbb{Z}$ that is at least $A_c = \sum_{d \neq c} \max_{j \leq s-2} |M^{(j)}[c][d]|$, and $F_j[c][c] = 0$ for $j \geq 1$. The primes of DD' are 2 and the primes of the point differences and of the Λ_c . For $u_c = 2c$, $v_d = 2d + 1$ they are all at most $2s - 1$.

We write H_s for the design of Lemma 114 with $u_c = 2c$, $v_d = 2d + 1$.

Proof. By Proposition 113, $M^{(0)}[c][d] = \frac{1}{2} \Lambda_c \vartheta_{cd}^{-1}$ and $M^{(j)}[c][d] = \frac{1}{2} \Lambda_c \vartheta_{cd}^{-1} (1 + 2\vartheta_{cd}^{-j})$ for $1 \leq j \leq s-2$. For $1 \leq i \leq s-1$, $\Lambda_c / \vartheta_{cd}^i$ is a product of odd integers, hence an odd integer; so the first term lies in $\frac{1}{2} + \mathbb{Z}$ and the second in $\mathbb{Z}$. The leading coefficients are 1 and 2, and $\mu_d = 1$. For H_s the differences $u_c - u_{c'}$, $v_d - v_{d'}$ and $\vartheta_{cd} = 2(c-d) - 1$ have absolute value at most $2s - 1$. $\square$

13.6. Separation with carries. For a design with half-integer F_0 , every partial sum $M^{(j)}$ lies in $\frac{1}{2} + \mathbb{Z}$, and this parity is all that the separation argument needs, at every carry pattern. As in Lemma 4, we bound each coordinate by the smallest of the possible changes of its geometric digit (its *options*); all numbers below use this form.

Proposition 115 (Half-integer layers with carries). *Let p be an odd prime, $s \geq 3$, $k \geq 1$, $L = \min(k, s-1)$, and let a graph form over $\mathbb{F}_p$ be given (a digital net or not; no part uses $t = 0$) with depths $(k, \dots, k)$ whose row 0 of every block, diagonal included, equals a design $(F_0, \dots, F_{L-1})$ on the levels $k-1, \dots, k-L$ and vanishes below (the rows ≥ 1 are arbitrary). Assume*

$$(Half) \quad F_0 \in (\tfrac{1}{2} + \mathbb{Z})^{s \times s}, \quad F_i \in \mathbb{Z}^{s \times s} \quad (1 \leq i \leq L-1),$$

with $\frac{1}{2} \equiv (p+1)/2$. For $0 \neq E \in \{-2, \dots, 2\}^s$ (steps of two cells are included, because an offset change of about $\pm \frac{p}{2}$ can bring the points of cells two apart to about 1.5 cells apart, below the cap 2 of LB) and carry depths $j_d \in \{0, \dots, L-1\}$ on the moving axes put $\Sigma E = \sum_c E_c$,

$$\sigma_c = \sum_{d: E_d \neq 0} \left(E_d F_0[c][d] + \text{sgn}(E_d) \sum_{i=1}^{j_d} F_i[c][d] \right)$$

(so $\sigma_c = \sum_d E_d M^{(j_d)}[c][d]$ if $|E|_\infty \leq 1$), let the options of coordinate c be $O_c = \{\sigma_c + \frac{p}{2}, \sigma_c - \frac{p}{2}\}$ if ΣE is odd, $O_c = \{\sigma_c, \sigma_c - p \text{sgn } \sigma_c\}$ if ΣE is even ($O_c = \{0\}$ if $\sigma_c = 0$), $b_c = \min_{t \in O_c} \max(0, |pE_c + t| - 1)$, and $\text{LB} = \min(2, \min_{E,j} |b|/p)$.

- (1) If $p > 2 \max |\sigma_c|$ (over all E , j and c), then $\delta N^{1/s} \geq \text{LB}$ (toroidal distance), for every choice of the rows ≥ 1 .
- (2) Suppose moreover that $F_i[c][c] = 0$ for $i \geq 1$ and $F_0[c][c] = -\alpha_c$ with

$$\alpha_c \geq A_c := \sum_{d \neq c} \max_{j < L} |M^{(j)}[c][d]|.$$

Let $B = \max_c(2\alpha_c + 2A_c)$ (the dominance constant) and $\epsilon_p = (B+1)/p$. If $p > 2B$, then $\delta N^{1/s} \geq \min(\sqrt{s}(\frac{1}{2} - \epsilon_p), \sqrt{2}(1 - \epsilon_p))$.

(3) Let $C = \max_{c,d} |F_0[c][d]|$. If $p > 4sC + 2$, then $\delta N^{1/s} \leq \min(\sqrt{s}/2, \sqrt{2}) + \sqrt{s}(2C+1)/p$.

Proof. (1) In cell units, coordinate c of the point of cell n is $n_c + (r_c + f_c)/p$ with r_c the first offset digit and $f_c \in [0, 1)$. Let $n \neq n'$ and let E be a torus representative of $n' - n$ (modulo p^k in each coordinate). If some $|E_c| \geq 3$, then the two points differ by $|D_c| > |E_c| - 1 \geq 2$ cells in coordinate c , with D their difference in cell units, since $(r'_c + f'_c) - (r_c + f_c) \in (-p, p)$. Otherwise adding E_d to the cell integer n_d changes its level $k-1$ by E_d and the levels $k-1-i$, $1 \leq i \leq j_d$, by $\text{sgn}(E_d)$ (carries or borrows; a carry is at most 1 since $|E_d| \leq 2 < p$, and the torus wrap is the full carry); since row 0 vanishes below level $k-L$, capping j_d at $L-1$ is exact. So $\Delta r_c = r'_c - r_c \equiv \sigma_c \pmod{p}$ with $\Delta r_c \in (-p, p)$. As $F_0 \in (\frac{1}{2} + \mathbb{Z})^{s \times s}$ and F_i is integral, $\sigma_c \in \Sigma E/2 + \mathbb{Z}$. If ΣE is odd, $\sigma_c \pm \frac{p}{2}$ are the integers congruent to σ_c (with $\frac{1}{2} \equiv (p+1)/2$), and as $|\sigma_c| < p/2$ they are the only ones in $(-p, p)$; if ΣE is even, σ_c is an integer with $|\sigma_c| < p$, and the integers in $(-p, p)$ congruent to it are σ_c and $\sigma_c - p \text{sgn } \sigma_c$ (only 0 if $\sigma_c = 0$). So $\Delta r_c \in O_c$, and $p|D_c| = |pE_c + \Delta r_c + \Delta f_c| > |pE_c + \Delta r_c| - 1$, i.e. $p|D_c| \geq b_c$.

(2) First $|\sigma_c| \leq 2\alpha_c + 2A_c \leq B$, since the own term is $-E_c\alpha_c$ and the term of an axis $d \neq c$ is $E_d M^{(j_d)}[c][d]$ ($|E_d| = 1$) or $\text{sgn}(E_d)(M^{(0)} + M^{(j_d)}[c][d])$ ($|E_d| = 2$); so (1) applies. Let $e = |E|_\infty \leq 2$ and $|E_c| = e$. Then $E_c\sigma_c \leq -e^2\alpha_c + e \cdot eA_c \leq 0$: every coordinate of maximal size is backward. If ΣE is odd, every coordinate has $|pE_c + t| \geq p|E_c \pm \frac{1}{2}| - |\sigma_c| \geq p/2 - |\sigma_c|$ for $t \in O_c$, so $|D_c| \geq \frac{1}{2} - \epsilon_p$ for all s coordinates. If ΣE is even, a backward coordinate c with $|E_c| = e$ has $\text{sgn } \sigma_c \neq \text{sgn } E_c$, so both options give $|pE_c + t| \geq pe - |\sigma_c|$ and $|D_c| \geq e - \epsilon_p$. For $e = 2$ this is at least $2 - \epsilon_p \geq \sqrt{2}(1 - \epsilon_p)$; for $e = 1$ an even ΣE needs at least two nonzero coordinates, each of maximal size, so $|D| \geq \sqrt{2}(1 - \epsilon_p)$.

(3) Since $|2F_0[c][d]| \leq 2C < p$ is odd, every entry of F_0 is a unit modulo p , and $C < p/2 - 1$. First take the step $E = \mathbf{e}_a$ from a cell in which the last digit of n_a is not $p-1$ (no carry) and r_a wraps, i.e. $\Delta r_a = F_0[a][a] - \frac{p}{2}$; such cells exist, because r_a depends on the last digit of n_d , $d \neq a$, with the unit coefficient $F_0[a][d]$. Then $|D_a| \leq \frac{1}{2} + (C+1)/p$, and every other coordinate has $\Delta r_c = F_0[c][a] \pm \frac{p}{2}$ and $|D_c| \leq \frac{1}{2} + (C+1)/p$; so $\delta N^{1/s} \leq \sqrt{s}(\frac{1}{2} + (C+1)/p)$. Next take $E = \mathbf{e}_a - \mathbf{e}_b$, with the last digit of n_a not $p-1$ and that of n_b not 0 (no carries); then $\sigma_c = \beta_c := F_0[c][a] - F_0[c][b]$ is an integer with $|\beta_c| \leq 2C$. Fix these two digits. For every c , r_c depends with a unit coefficient on the last digit of some n_g , $g \notin \{a, b\}$ (as $s \geq 3$), so it is uniformly distributed on the remaining cells, and the fraction of them on which $r_c + \beta_c \notin [0, p)$ is $|\beta_c|/p$. As $\sum_c |\beta_c| \leq 2sC < p$, some cell has no wrap; there $|D_c - E_c| \leq (|\beta_c| + 1)/p \leq (2C+1)/p$ for every c , so $|D| \leq \sqrt{2} + \sqrt{s}(2C+1)/p$. $\square$

Only the parity class of the partial sums enters: the deeper digits, including whatever deeper rows are needed for $t = 0$, act only as jitter. Each option in b_c has the form $|\alpha p + \sigma_c|$ with $\alpha \in \{E_c \pm \frac{1}{2}\}$ resp. $\{E_c, E_c - \text{sgn } \sigma_c\}$ independent of p ; replacing it by $|\alpha|p - |\sigma_c|$ gives a lower bound $\text{LB}^* \leq \text{LB}$ that is nondecreasing in p , so $\text{LB}^*(p_1) > x$ implies $\delta N^{1/s} > x$ for every prime $p \geq p_1$ (as long as the net exists modulo p and the hypothesis of (1) holds). In (1) the hypothesis implies $p \geq 7$: the step $E_d = 2 \text{sgn } F_0[c][d]$ ($d = 0, \dots, s-1$) without carries has $\sigma_c = 2 \sum_d |F_0[c][d]| \geq s \geq 3$. Parts (1)–(3) are formally verified as stated, (3) for the Euclidean distance; for the split-frame nets (1) and (2) also over $\mathbb{Z}/q\mathbb{Z}$ with composite q (Appendix F).

Theorem 116 (Beyond the cubic lattice). *Let $s \geq 4$. For the explicit design H_s on the split frame $u_c = 2c$, $v_d = 2d + 1$ (Lemma 114) there are constants $B_s = e^{O(s^2 \log s)}$ and C_s such that for every prime $p \geq \max(2s, 2B_s + 2)$ and every $k \geq 1$ the net $\mathcal{H}_{k,p}^s$ is a digital $(0, sk, s)$ -net over $\mathbb{F}_p$ with one point in every cell, and*

$$\min\left(\sqrt{s}\left(\frac{1}{2} - \epsilon_p\right), \sqrt{2}(1 - \epsilon_p)\right) \leq \delta N^{1/s} \quad \left(\epsilon_p = \frac{B_s + 1}{p}\right),$$

toroidal, hence Euclidean; if also $p > 4sC_s + 2$, then $\delta N^{1/s} \leq \min(\sqrt{s}/2, \sqrt{2}) + \sqrt{s}(2C_s + 1)/p$. So $\delta N^{1/s} \rightarrow \min(\sqrt{s}/2, \sqrt{2})$ as $p \rightarrow \infty$, uniformly in k .

Theorem A already gives non-decaying separation along $N = q^{sk}$; Theorem 116 adds the value: above the cubic value 1 for $s \geq 5$, at every resolution $m = sk$, beyond the first-order ceiling $1 - 2/q$ that Theorem 88 proves for bounded layers of frame designs. Unlike a_s^* , the constant B_s is enormous ($B_4 = 1787594$, $B_5 = 1413079078321$); searched designs have much smaller constants (Section 13.7). For $s = 4$ nothing is gained, since D_4^+ is a rotated copy of $\mathbb{Z}^4$.

Proof of Theorem 116. Let H_s be the design of Lemma 114 on $u_c = 2c$, $v_d = 2d + 1$, let $\mathcal{H}_{k,p}^s = \mathcal{P}_{k,p}^{u,v,H_s}$, $B_s = \max_c(2\alpha_c + 2A_c)$ and $C_s = \max_c \alpha_c$, which is the largest entry of F_0 in absolute value, since $|F_0[c][d]| \leq A_c \leq \alpha_c$. For a prime $p \geq 2s$ and every $k \geq 1$, Lemma 114 and Proposition 113 make $\mathcal{H}_{k,p}^s$ a digital $(0, sk, s)$ -net with one point in every cell, whose row 0 is H_s truncated to $L = \min(k, s - 1)$ levels and 0 below. It satisfies (Half) and the dominance hypothesis of Proposition 115(2) (with A_c over all $j \leq s - 2 \geq L - 1$), so Proposition 115(2) gives the lower bound (as $p \geq 2B_s + 2 > 2B_s$; for $p \leq 2B_s + 2$ it would not be positive) and Proposition 115(3) the upper bound, both independent of k . Finally $|\vartheta_{cd}| \leq 2s - 1$, so $|\Lambda_c| \leq (2s - 1)^{(s-1)^2}$, $|M^{(j)}[c][d]| \leq \frac{3}{2}|\Lambda_c|$ (absolute values, as Λ_c is negative for some c when s is even), $\alpha_c \leq A_c + 1$ and $B_s \leq 6(s - 1) \max_c |\Lambda_c| + 2 = e^{O(s^2 \log s)}$. $\square$

By Proposition 109, the nets of Theorem 116 lie outside the frame orbit of every frame with rational places (they cannot be obtained from it by per-coordinate lower-triangular scrambles and gauge moves), and outside that of every frame over $\mathbb{F}_p$ with $|2\tilde{M}| \leq \Omega$ once $p > 13\Omega^{16}$.

13.7. One resolution, and searched designs. *One resolution.* At $m = s$ ($k = 1$) no frame is needed: for a layer F_0 in $(\frac{1}{2} + \mathbb{Z})^{s \times s}$ (with $\frac{1}{2} \equiv (p + 1)/2$) and any deeper rows, Proposition 115 with $k = 1$ gives the bound, and the point of cell n sits, up to the drift, which grows like $|n - n_0|/p$ away from a reference cell n_0 , and the jitter, at n or at $n + \frac{1}{2}\mathbf{1}$ according to the parity of $\sum_c n_c$: locally the classical packing $D_s^+ = D_s \cup (D_s + \frac{1}{2}\mathbf{1})$ [9, Ch. 4], with one point per unit cube and minimum $\min(\sqrt{s}/2, \sqrt{2})$ (a lattice for even s ; $D_4^+ \cong \mathbb{Z}^4$, $D_8^+ = E_8$). As for the frameless layers of Proposition 84, deeper rows that give $t = 0$ exist for all but finitely many p when the minors of F_0 with disjoint row and column sets are nonzero. For $s = 5$ an explicit such layer gives digital $(0, 5, 5)$ -nets with $\delta N^{1/5} > 1$ for every prime $p \geq 37$ (Proposition 118 below). These limits are not the best packing values for $4 \leq s \leq 7$. The best known lattices D_4, D_5, E_6, E_7 have normalized minima 1.189, 1.231, 1.290, 1.345, and D_s^+ reaches the fractions .84, .90, .94, .98 of them; the Cohn–Elkies bound [3] caps every periodic configuration (hence the toroidal separation of any point set) at about 1.204, 1.261, 1.315, 1.366. At $s = 8$, $D_8^+ = E_8$ is optimal among all packings [67], so there the limit $\sqrt{2}$ of Theorem 116 is sharp for the toroidal separation of every point set.

Drift and jitter at one resolution. The bookkeeping of Section 11 decides how small the base can be. Let $s = 5$, $k = 1$ and $F_0 \in (\frac{1}{2} + \mathbb{Z})^{5 \times 5}$. Call a step $E \in \{-1, 0, 1\}^5$ with odd ΣE *binding*: in the limit these steps land on the minimal vectors of D_5^+ , of length $\sqrt{5}/2$, so they decide the separation. For a binding step Proposition 115(1) offers each coordinate the two options $\beta_c \pm \frac{p}{2}$,

$\beta = F_0 E$, and in the limit every coordinate has length $\frac{1}{2}$. At finite p one option is shorter than $\frac{p}{2}$: for $E_c \neq 0$ the one with $|pE_c + t| \approx \frac{p}{2}$, for $E_c = 0$ the one of sign $\varsigma_c(E) := -\text{sgn } \beta_c$; for $E_c \neq 0$ put $\varsigma_c(E) = E_c$. In units of $1/p$ of a cell it is shorter by the *drift* (the drift of Section 11 in this setting: the first-order shortening of a binding step caused by the bounded part of F_0)

$$\text{dr}_c(E) = |\beta_c| \quad (E_c = 0), \quad \text{dr}_c(E) = -E_c \beta_c \quad (E_c \neq 0), \quad \text{dr}(E) = \sum_c \text{dr}_c(E) = -\varsigma(E)^\top F_0 E,$$

and $\text{dr}(F_0)$ is the maximum of $\text{dr}(E)$ over the binding steps. Every entry of F_0 is $\equiv \frac{1}{2}(p+2F_0[c][d]) \pmod{p}$: the ideal step $\frac{p}{2}$ plus an excess of at least $\frac{1}{2}$ in absolute value, since p steps of $\frac{p}{2}$ do not add up to a multiple of p when p is odd. This is the closing-up obstruction of Section 11, here a parity (the *parity holonomy*), and it is why $|\beta_c| \geq \frac{1}{2}$ when $E_c = 0$. A second offset row D_1 (integer) adds the *jitter*: with $v = D_1 E$, coordinate c is *harmful* for E if $v_c \neq 0$ and $\text{sgn } v_c = \varsigma_c(E)$, since then the second digit can wrap in the direction that shortens coordinate c by a further $1/p$, whereas otherwise the second digit costs $O(p^{-2})$. Put $\text{dj}(F_0, D_1) = \max_E (\text{dr}(E) + \#\{c \text{ harmful}\})$ over the binding steps. Here the first-order constants are measured on the squared value, $(\delta N^{1/5})^2 = \frac{5}{4} - \text{dr}/p + \dots$, equivalently $\delta N^{1/5} = \frac{\sqrt{5}}{2} (1 - \frac{2\text{dr}}{5p}) + \dots$; they are not deficits in the sense of Definition 74. Proposition 115(1) charges a jitter of 1 to every coordinate, so its constant is $\text{dr} + 5$. The second offset digit can be included in the relaxation:

Lemma 117 (Two-digit relaxation). *Let p be an odd prime, $s \geq 3$, and let a graph form over $\mathbb{F}_p$ (a digital net or not) with the depths $(1, \dots, 1)$ have first offset rows $F_0 \in (\frac{1}{2} + \mathbb{Z})^{s \times s}$ and second offset rows $D_1 \in \mathbb{Z}^{s \times s}$; the deeper rows are arbitrary. For $0 \neq E \in \{-2, \dots, 2\}^s$ let $\beta = F_0 E$, $v = D_1 E$, let O_c be the options of Proposition 115 (with $\sigma_c = \beta_c$), $U_c = \{v_c, v_c - p \text{sgn } v_c\}$ ($U_c = \{0\}$ if $v_c = 0$), and*

$$b_c = \min_{t \in O_c, u \in U_c} \max(0, |p^2 E_c + pt + u| - 1), \quad \text{LB}_2(p) = \min \left(2, \min_E |b|/p^2 \right).$$

If $p > \max |2\beta_c|$ and $p > \max |v_c|$ over these E and c , then $\delta N^{1/s} \geq \text{LB}_2(p)$ for the toroidal distance.

Proof. In cell units coordinate c of the point of cell n is $n_c + r_c/p + (d_c + g_c)/p^2$, with r_c and d_c the first and second offset digits and $g_c \in [0, 1)$. For two distinct points and a torus representative E of their cell difference with some $|E_c| \geq 3$, coordinate c differs by more than 2, as in the proof of Proposition 115(1). Otherwise, as there (at $k = 1$ there are no carries), $\Delta r_c \in O_c$. As $d = D_1 n \pmod{p}$ is linear in the cell, $\Delta d_c \equiv v_c \pmod{p}$ with $\Delta d_c \in (-p, p)$ and $|v_c| < p$, so $\Delta d_c \in U_c$; and $|\Delta g_c| < 1$. So $p^2 |D_c| = |p^2 E_c + p \Delta r_c + \Delta d_c + \Delta g_c| \geq b_c$. The comparison with the toroidal distance is that of the proof of Proposition 115(1). $\square$

Each option in b_c has the form $|p^2 \alpha + p \beta' + v_c|$ with $\alpha \in \{E_c \pm \frac{1}{2}\}$ resp. $\{E_c, E_c - \text{sgn } \beta_c\}$ and $\beta' \in \{\beta_c, \beta_c - \text{sgn } v_c\}$ independent of p ; replacing it by $\max(0, p^2 |\alpha| - p |\beta'| - |v_c| - 1)$ (and by 0 if $\alpha = 0$) gives a lower bound $\text{LB}_2^* \leq \text{LB}_2$ that is nondecreasing in p , as for LB^* after Proposition 115. At first order the lemma charges exactly the harmful coordinates, so its constant is dj (Remark 119). The lemma holds verbatim over $\mathbb{Z}/q\mathbb{Z}$ for every odd q , like Proposition 115(1), as its proof uses only that p is odd. We call the second row D_1 *lean* for F_0 if $\text{dj}(F_0, D_1) = \text{dr}(F_0)$: its harmful coordinates do not raise the maximum above the drift. A layer with small drift and a lean second row give:

Proposition 118 (Dimension five, one resolution; computer-assisted). *Let F_0^* , D_1 , D_2 , D_3 be the matrices*

$$2F_0^* = \begin{pmatrix} -3 & -3 & -3 & -1 & -1 \\ 3 & -3 & -1 & -3 & 1 \\ 3 & 1 & -3 & 1 & -1 \\ 1 & 3 & -1 & -3 & -1 \\ 1 & -1 & 1 & 1 & -1 \end{pmatrix}, \quad D_1 = \begin{pmatrix} -2 & 0 & -1 & -1 & 1 \\ 0 & -1 & -1 & -1 & -1 \\ 2 & -1 & -3 & 1 & 0 \\ -1 & 2 & -1 & -2 & 0 \\ -1 & -1 & 3 & 2 & -5 \end{pmatrix},$$

$$D_2 = \begin{pmatrix} 0 & -1 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 & -1 \\ -1 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 \end{pmatrix}, \quad D_3 = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

and, for an odd prime p , let $\mathcal{Q}_p^*$ be the digital net over $\mathbb{F}_p$ whose point with index $n \in \mathbb{F}_p^5$ has, in coordinate c , the digits $n_c, (F_0^*n)_c, (D_1n)_c, (D_2n)_c, (D_3n)_c$ (with $\frac{1}{2} \equiv (p+1)/2$).

- (1) $\mathcal{Q}_p^*$ is a $(0, 5, 5)$ -net for every prime $p \geq 7$.
- (2) For every prime $p \geq 37$, $\delta N^{1/5} > 1$ (toroidal), and $\delta N^{1/5} \rightarrow \sqrt{5}/2 = 1.1180\dots$ as $p \rightarrow \infty$.
- (3) For every prime $p \geq 53$, every graph form over $\mathbb{F}_p$ with the depths $(1, \dots, 1)$ and first offset rows F_0^* (deeper rows arbitrary) has $\delta N^{1/5} > 1$ (toroidal).

Proof (computer-assisted). (1) The generator matrix of coordinate c has the rows $\mathbf{e}_c$ and row c of F_0^*, D_1, D_2, D_3 . By Lemma 2 its box minors are the minors of the stacked offset rows with disjoint row and column sets; each of the 126 of them, computed in exact rational arithmetic, is a nonzero rational whose numerator and denominator have no prime factors other than 2, 3 and 5. Lemma 1 concludes.

(2) Over $E \in \{-2, \dots, 2\}^5$, $\max |2(F_0^*E)_c| = 22$ and $\max |(D_1E)_c| = 24$, so Lemma 117 applies for $p \geq 29$. Evaluated exactly, $\text{LB}_2(p) > 1$ for every prime $37 \leq p < 200$ (the least value is 1.0127..., at $p = 37$; and $\text{LB}_2(31) = 0.9918\dots$), and $\text{LB}_2^*(200)^2 = 1.1877\dots > 1$, so $\text{LB}_2(p) \geq \text{LB}_2^*(p) \geq \text{LB}_2^*(200) > 1$ for every $p \geq 200$. For the limit, with the row-sum norm $\|F_0^*\|_\infty = \max_c \sum_d |F_0^*[c][d]| = \frac{11}{2}$ every option of Proposition 115(1) is at least $p \ell_c(E) - (2\|F_0^*\|_\infty + 1)$, where

$$\ell_c(E) = \min(|E_c + \tfrac{1}{2}|, |E_c - \tfrac{1}{2}|) \quad (\Sigma E \text{ odd}), \quad \ell_c(E) = \min_\omega |E_c - \omega| \quad (\Sigma E \text{ even}),$$

ω over $\{0, \text{sgn } \beta_c\}$ (over $\{0\}$ if $\beta_c = 0$). So $\delta N^{1/5} \geq \lambda - \sqrt{5}(2\|F_0^*\|_\infty + 1)/p$ with $\lambda = \min_E |\ell(E)|$. If ΣE is odd, every coordinate gives at least $\frac{1}{2}$, with equality exactly on the binding steps; if ΣE is even, $|\ell(E)|^2$ is an integer, and a finite check over the $5^5 - 1$ vectors shows that it is at least 2. So $\lambda = \sqrt{5}/2$, and Proposition 115(3) with $C = \frac{3}{2}$ gives $\delta N^{1/5} \leq \sqrt{5}/2 + 4\sqrt{5}/p$ for $p > 32$.

(3) Proposition 115(1) with $k = 1$ and $F_0 = F_0^*$ applies for $p > 22$. Evaluated exactly, $\text{LB} > 1$ for every prime $53 \leq p < 200$ ($\text{LB}(47) = 0.9906\dots$, $\text{LB}(53) = 1.0049\dots$), and the nondecreasing bound LB^* after Proposition 115 has $\text{LB}^*(200)^2 = 1.1689\dots > 1$. (The monotone bounds already exceed 1 from $p = 50$ for LB_2^* and from $p = 63$ for LB^* , so the exact scans up to 200 in (2) and (3) are more than needed.) $\square$

The threshold 37 is that of the net itself: its exact normalized minimum distances are 0.9928 at $p = 31$ and 1.0134 at $p = 37$ (computed), and the relaxation of Lemma 117 follows the exact values closely (Figure 15). The second row D_1 is *lean*: $\text{dj}(F_0^*, D_1) = \text{dr}(F_0^*) = \frac{17}{2}$, i.e. the harmful residues of D_1 lie on steps whose drift leaves room for them. Whether some $(0, 5, 5)$ -net over $\mathbb{F}_p$ with $p \leq 31$ has $\delta N^{1/5} > 1$ is open.

Remark 119 (First-order accounting). Let $F_0 \in (\frac{1}{2} + \mathbb{Z})^{5 \times 5}$ with $\det F_0 \neq 0$ satisfy

$$(\text{Gap}) \quad |\ell(E)| > \sqrt{5}/2 \text{ for every } 0 \neq E \in \{-2, \dots, 2\}^5 \text{ that is not a binding step,}$$

with ℓ as in the proof of Proposition 118, let D_1, D_2, D_3 be fixed integer matrices, and let $K_{\text{eff}}(p) = \frac{5p}{2}(1 - \delta N^{1/5}/\frac{\sqrt{5}}{2})$ for the digital net with these rows over $\mathbb{F}_p$, normalized so that $K_{\text{eff}} \rightarrow \text{dr}$ when the second row is lean. Then

$$\text{dr}(F_0) \leq \liminf_{p \rightarrow \infty} K_{\text{eff}}(p) \leq \limsup_{p \rightarrow \infty} K_{\text{eff}}(p) \leq \text{dj}(F_0, D_1).$$

In particular, if $\text{dj}(F_0, D_1) = \text{dr}(F_0)$, then $\delta N^{1/5} = \frac{\sqrt{5}}{2} \left(1 - \frac{2\text{dr}(F_0)}{5p}\right) + O(p^{-2})$. For $\mathcal{Q}_p^*$ the finite checks give $\text{dr} = \text{dj} = \frac{17}{2}$, $\det 2F_0^* = -880$ and $|\ell(E)|^2 \geq 2$ on the non-binding steps, so $\delta N^{1/5} = \frac{\sqrt{5}}{2} \left(1 - \frac{17}{5p}\right) + O(p^{-2})$.

Proof. Upper bound for K_{eff} : on a binding step each option of Lemma 117 is $p^2(\frac{1}{2} - x/p) + O(1)$ in absolute value, and the smallest has $x = \text{dr}_c(E) + [c \text{ harmful}]$: the shorter option of the geometric digit r shortens by $\text{dr}_c(E)$, a second-digit wrap of the sign $\varsigma_c(E)$ by 1 more, a residue of the other sign by $O(1)$ only, and for $E_c = 0$ the longer r -option combined with a harmful wrap is not shorter, as $|\beta_c| \geq \frac{1}{2}$. So these steps give $|b|^2/p^4 = \frac{5}{4} - (\text{dr}(E) + \#\text{harmful})/p + O(p^{-2})$. By (Gap) the other steps of $\{-2, \dots, 2\}^5$ have $|b|/p^2 \rightarrow |\ell(E)| > \sqrt{5}/2$. Hence $\text{LB}_2(p) = \frac{\sqrt{5}}{2} \left(1 - \frac{2\text{dj}}{5p}\right) + O(p^{-2})$, and $\delta N^{1/5} \geq \text{LB}_2(p)$ gives $\limsup K_{\text{eff}} \leq \text{dj}$. Lower bound: fix a binding E with $\text{dr}(E) = \text{dr}(F_0)$. For p large ($p \nmid \det 2F_0$, p larger than the entries of D_1 and than $2|2\beta_c| + 2$) F_0 is invertible modulo p , so $n \mapsto r = F_0 n \bmod p$ is a bijection, and the cells whose five first offset digits all take the shorter option for E form a box in the r -coordinates with at least $(\frac{p}{2} - O(1))^5$ cells. A second-digit wrap $\Delta d_c \neq v_c$ needs $d_c(n)$ in a set of $|v_c|$ residues, which happens on $|v_c|p^4$ cells if $v_c \neq 0$ (as d_c is a nonzero linear form) and never if $v_c = 0$. So for p large some cell has the shorter options and $\Delta d = v$, and its step E gives $|D|^2 = \frac{5}{4} - \text{dr}(F_0)/p + O(p^{-2})$, i.e. $\liminf K_{\text{eff}} \geq \text{dr}(F_0)$. In the same way Proposition 115(1) has $\text{LB} = \frac{\sqrt{5}}{2} \left(1 - \frac{2(\text{dr}(F_0)+5)}{5p}\right) + O(p^{-2})$.

(Gap) is a genuine hypothesis. The layer

$$2F_0 = \begin{pmatrix} -3 & 1 & -1 & -3 & -3 \\ -3 & -3 & 3 & 1 & -1 \\ -3 & 1 & -3 & 3 & 1 \\ 1 & -1 & 3 & -3 & 1 \\ 1 & 1 & 1 & 1 & -1 \end{pmatrix}$$

satisfies (B2) and (MIN), defined before Theorem 120, and has $\det 2F_0 = 560$, but the even step $E = (1, -1, -2, -1, -1)$ has $\beta = (2, -3, -1, -1, -1)$ and $|\ell(E)| = 1$: its coordinates with $E_c = \pm 1$ move forward, so the step is short (length 1). Each half of the remark uses only one hypothesis: (Gap) only the upper bound $\limsup K_{\text{eff}} \leq \text{dj}$, and $\det F_0 \neq 0$ only the lower bound; the deeper rows are arbitrary in both. With (Gap) the accounting is an identity for the relaxations and a two-sided bound for the nets, exact when the second row is lean. Cauchy–Schwarz, $\sum_c (\frac{1}{2} - x_c/p)^2 \geq \frac{1}{5}(\frac{5}{2} - K/p)^2$, makes $\delta N^{1/5} > 1$ plausible once $p \gtrsim \frac{2K}{5(1-2/\sqrt{5})} \approx 3.79 K$; this is a first-order estimate, not a threshold. It predicts 51 for F_0^* with Proposition 115(1) ($K = \frac{17}{2} + 5$) and 32 for $\mathcal{Q}_p^*$ ($K = \frac{17}{2}$), against the certified 53 and 37.

How small can the drift be? Two conditions on the layer are natural. Every minor of F_0 with disjoint row and column sets is a box minor at $s = 5$ (Lemma 2); its denominator is a power of 2, so a zero minor kills $t = 0$ at every odd p . At $s = 5$ these minors are the off-diagonal entries and the 2×2 minors on two rows $\{a, b\}$ and two columns outside $\{a, b\}$, and we require

$$\begin{aligned} \text{(MIN)} \quad & \text{all these minors are nonzero;} \\ \text{(B2)} \quad & \alpha_c := -F_0[c][c] \geq m_c := \max_{d \neq c} |F_0[c][d]| \text{ for every } c. \end{aligned}$$

(B2) is the backward condition of Remark 5: it says that on every two-axis step $\mathbf{e}_c \pm \mathbf{e}_d$ coordinate c is backward (its geometric digit does not move with its cell step); if $\alpha_c < |F_0[c][d]|$, coordinate c moves forward on one of the steps $\mathbf{e}_c \pm \mathbf{e}_d$.

Theorem 120 (The least drift). *Every $F_0 \in (\frac{1}{2} + \mathbb{Z})^{5 \times 5}$ with (B2) and (MIN), with entries of any size, has $\text{dr}(F_0) \geq \frac{17}{2}$, and $\text{dr}(F_0^*) = \frac{17}{2}$. The part of the proof for layers whose off-diagonal part is not skew-symmetric is computer-assisted.*

Proof. Diagonal. $\text{dr}(E)$ contains α_c exactly for the coordinates with $E_c \neq 0$, since $-E_c\beta_c = \alpha_c - E_c \sum_{d \neq c} F_0[c][d]E_d$, and β_c does not involve α_c when $E_c = 0$. So $\text{dr}(F_0)$ does not increase when every α_c is lowered to m_c , which keeps (B2) and (MIN); we assume $\alpha = m$.

Minor tax. At most one row of F_0 has all its off-diagonal entries in $\{\pm \frac{1}{2}\}$: if rows $a \neq b$ did, the three ratios $F_0[a][c]/F_0[b][c]$, $c \notin \{a, b\}$, would lie in $\{\pm 1\}$, two would be equal, and the 2×2 minor on those two columns would vanish. So at most one m_c is $\frac{1}{2}$: at most one row is *light*, with all off-diagonal entries $\pm \frac{1}{2}$, and the others are *heavy*, and $\sum_c \alpha_c \geq 4 \cdot \frac{3}{2} + \frac{1}{2} = \frac{13}{2}$.

Balance on the full steps. A *full* step has all $E_c = \pm 1$. For $E \in \{\pm 1\}^5$ (binding, as 5 is odd), $\text{dr}(E) = -E^\top F_0 E = \sum_c \alpha_c + \phi(E)$ with $\phi(E) = \sum_{c < d} \gamma_{cd} E_c E_d$ and $\gamma_{cd} = -(F_0[c][d] + F_0[d][c]) \in \mathbb{Z}$. The function ϕ has mean 0 over $\{\pm 1\}^5$, and it vanishes identically if and only if the off-diagonal part of F_0 is skew-symmetric; otherwise $\max \phi \geq 1$, as ϕ is integer-valued. So $\text{dr}(F_0) \geq \sum_c \alpha_c$, and $\text{dr}(F_0) \geq \sum_c \alpha_c + 1$ if the off-diagonal part is not skew.

Skew layers. If some entry has $|F_0[c][d]| \geq \frac{5}{2}$, it occurs in the rows c and d , and with the minor tax $\sum \alpha \geq \frac{5}{2} + \frac{5}{2} + \frac{3}{2} + \frac{3}{2} + \frac{1}{2} = \frac{17}{2}$. Otherwise all off-diagonal entries are $\pm \frac{1}{2}$ or $\pm \frac{3}{2}$; let G be the graph on the five coordinates with the edges $\{c, d\}$ where $|F_0[c][d]| = \frac{3}{2}$. For two coordinates x, y and the set S of the other three, the binding steps with $E_x = E_y = 0$ and $E_S \in \{\pm 1\}^3$ have, as the skew terms inside S cancel, $\text{dr}(E) = \sum_{c \in S} \alpha_c + |u \cdot E_S| + |w \cdot E_S|$ with $u = F_0[x, S]$, $w = F_0[y, S]$. The step with $E_S = \text{sgn } u$ (coordinatewise) has $u \cdot E_S = \|u\|_1$ and $w \cdot E_S \in \frac{1}{2} + \mathbb{Z}$, as w has three entries in $\frac{1}{2} + \mathbb{Z}$; so

$$\max_{E_S} (|u \cdot E_S| + |w \cdot E_S|) \geq \|u\|_1 + \frac{1}{2}, \quad \|u\|_1 = \frac{3}{2} + \deg_S(x).$$

(i) If there is a light row ℓ , then $\sum \alpha = \frac{13}{2}$, the other four rows have degree at least 1 in G , and ℓ is isolated. G is not a perfect matching on the four heavy rows: for an edge $\{a, b\}$ of such a matching, the rows a and b would be $\pm \frac{1}{2}$ on the three columns outside $\{a, b\}$, which (MIN) excludes as in the minor tax. So some heavy h has degree at least 2, and the pair $\{x, y\} = \{h, \ell\}$ gives $\text{dr}(F_0) \geq \frac{9}{2} + (\frac{3}{2} + 2 + \frac{1}{2}) = \frac{17}{2}$. (ii) If there is no light row, $\sum \alpha = \frac{15}{2}$ and every degree is at least 1; as 5 is odd, G is not a perfect matching, so some x has degree at least 2, and with y outside x and its neighbours if $\deg x = 2$ (any $y \neq x$ otherwise) we get $\deg_S(x) \geq 2$ and again $\text{dr}(F_0) \geq \frac{9}{2} + 4 = \frac{17}{2}$.

Layers that are not skew. If some entry has absolute value at least $\frac{5}{2}$, then $\sum \alpha \geq \frac{5}{2} + 3 \cdot \frac{3}{2} + \frac{1}{2} = \frac{15}{2}$, and balance gives $\text{dr} \geq \frac{17}{2}$; the same holds if $\sum \alpha \geq \frac{15}{2}$. There remain the layers with entries in $\{\pm \frac{1}{2}, \pm \frac{3}{2}\}$, one light row and four heavy rows with $\alpha = \frac{3}{2}$. Conjugation by permutation matrices and by diagonal sign matrices preserves the binding steps, dr , (B2) and (MIN), so we may take the light row to be row 4, equal to $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2})$. Each heavy row then has 240 possibilities, and an exhaustive enumeration with the (MIN) conditions finds 1,004,544 layers satisfying (MIN), none with $\text{dr} \leq \frac{15}{2}$. Finally $\text{dr}(F_0^*) = \frac{17}{2}$ is a finite check over the 61 binding steps up to sign. $\square$

F_0^* is skew, with the minimal diagonal: one light row (row 4) and its heavy entries on a path 2–0–1–3, the leanest graph the proof allows (a vertex of degree 3 would cost $\frac{3}{2} + 3 + \frac{1}{2} = 5$ on its pair). Its full steps all cost $\frac{13}{2}$, and the three binding steps of drift $\frac{17}{2}$, up to sign $(0, 1, 1, 1, 0)$, $(1, 0, -1, -1, 0)$ and $(1, 1, 0, 0, -1)$, have weight three. Among the skew layers with entries $\pm \frac{1}{2}, \pm \frac{3}{2}$ and minimal diagonal, 39,168 satisfy (MIN), and the 3840 with drift $\frac{17}{2}$ form two orbits of 1920 under permutations and sign changes, each with one light row and a path of heavy entries (computed).

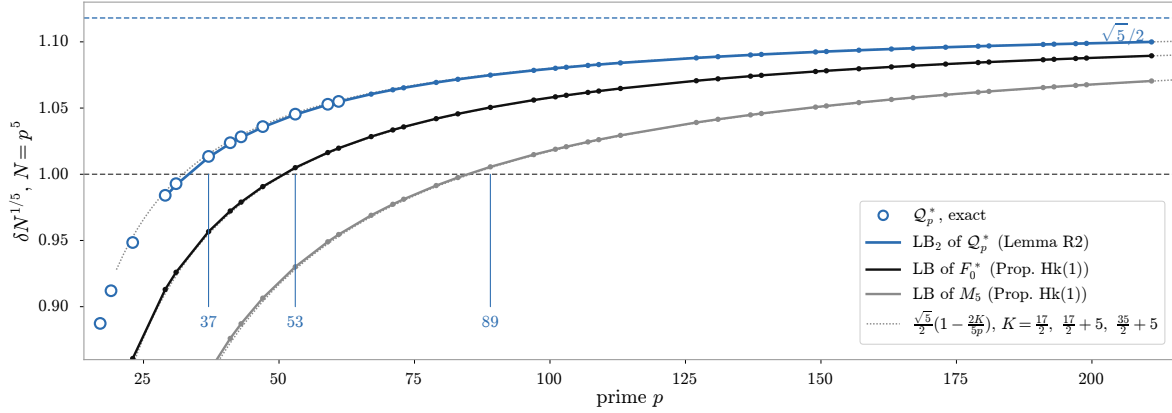


FIGURE 15. Dimension five, one resolution, $N = p^5$: the layer F_0^* of Proposition 118 against the dominant layer M_5 of Remark 121. Open circles: the exact $\delta N^{1/5}$ of Q_p^* at the primes $17 \leq p \leq 61$ (computed); it exceeds 1 from $p = 37$ on (0.9928 at $p = 31$, 1.0134 at $p = 37$). Lines: the proved lower bounds, computed exactly at every prime: Lemma 117 for Q_p^* (from $p = 29$, where its hypotheses hold), which exceeds 1 from $p = 37$ on, and Proposition 115(1), which charges a jitter of 1 to every coordinate, for every graph form with the first offset rows F_0^* (from $p = 53$ on) and M_5 (from $p = 89$ on). Dotted: the first-order lines $\frac{\sqrt{5}}{2}(1 - \frac{2K}{5p})$ with $K = \text{dr} = \frac{17}{2}$ (lean second row, Remark 119), $K = \frac{17}{2} + 5$ and $K = \frac{35}{2} + 5$: the drift of the layer and the jitter decide the base. Interactive version: explainers/beyond.html (Section 1).

Remark 121 (Accounting for a dominant layer). For comparison, the layer

$$2M_5 = \begin{pmatrix} -5 & 3 & 1 & -3 & 1 \\ -3 & -3 & 3 & -1 & -1 \\ 1 & -1 & -5 & -3 & 3 \\ -1 & -1 & 3 & -7 & 1 \\ 3 & -1 & 1 & -1 & -3 \end{pmatrix}$$

satisfies (B2) with room to spare: $\alpha = \frac{1}{2}(5, 3, 5, 7, 3)$, $\sum \alpha = \frac{23}{2}$, against $\sum m = \frac{15}{2}$; and its symmetric part has $\max \phi = 6$. Its drift $\text{dr}(M_5) = \frac{35}{2}$ is attained on full steps, and as an accounting identity

$$\frac{35}{2} = \frac{13}{2} + 1 + 4 + 6 :$$

$\frac{13}{2}$, the least possible $\sum_c m_c$ under (MIN) (the minor tax of the proof of Theorem 120); 1, the excess of the actual $\sum_c m_c = \frac{15}{2}$ of M_5 over it; 4, its diagonal above m ; and 6, the asymmetric part ($\max \phi$). This is an accounting, not a causal decomposition: the drift of M_5 is attained on full steps, that of F_0^* on steps of weight three. With the diagonal lowered to m the drift of M_5 would be $\frac{27}{2}$. Proposition 115(1) applies to M_5 for $p > 26$ and gives $\delta N^{1/5} > 1$ only from $p = 89$ on (LB(83) = 0.9975..., LB(89) = 1.0056..., computed), against 53 for F_0^* (Figure 15). Dominance, which Proposition 115(2) and Theorem 116 use to obtain a bound for all designs at once, is what the accounting says to avoid: by the diagonal step of the proof of Theorem 120 it costs $\sum_c (\alpha_c - m_c)$ in drift.

Searched designs. Smaller constants than B_s come from searched split-frame designs: random integer points with u even and v odd, then, column by column and level by level, short reachable columns (Proposition 113) in the coset $\frac{1}{2}\mathbf{h} + \mathbb{Z}^{s-1}$ for a vector $\mathbf{h}$ of odd integers, found by

lattice reduction; the diagonal is then chosen by evaluating the exact relaxation LB of Proposition 115(1), and it need not be dominant. The bound of Proposition 122 is the exact value of the relaxation of Proposition 115(1); its design H_5^* is also the one drawn in Figures 7(c) and 14.

Proposition 122 (Dimension five; computer-assisted). *Let $\mathcal{H}_{k,p}^{5*} = \mathcal{P}_{k,p}^{u,v,F}$ for the split frame $u = (-2, 0, 2, 4, 8)$, $v = (5, 7, -1, 3, 1)$ and the design $F = H_5^*$ of Appendix A. For every prime $p \notin \{2, 3, 5, 7, 97, 101\}$ and every $k \geq 1$ it is a digital $(0, 5k, 5)$ -net over $\mathbb{F}_p$ with one point in every cell ($p = 97, 101$ enter only for $k \geq 4$), and for every prime $p \geq 1511$ and every $k \geq 1$,*

$$\delta N^{1/5} > 1.0265.$$

Proof (computer-assisted). The design H_5^* satisfies (Half); its geometric layer F_0 has the row scalars $\lambda' = \frac{1}{2}(-9, -3, -3, 3, 9)$ and the column scalars $\mu = (5, 5, 5, -5, 1)$. The primes of the point differences, of the units $\lambda'_c \mu_d$ and of the leading coefficients of the column polynomials $g_{d,j}$ (exact interpolation) are 2, 3, 5, 7 and 97, 101, the last two only in leading coefficients at carry depth $j = 3$; Proposition 113 gives the net statement. For the separation, $\max |\sigma_c| = 253$, so Proposition 115(1) applies for $p > 506$; the monotone bound LB^* , minimized over the number of design levels $L = \min(k, 4) \in \{1, 2, 3, 4\}$ (that is, over k), is $1.026529\dots$ at $p = 1511$, the same value as LB (attained at $L = 4$, i.e. $k \geq 4$). As LB^* is nondecreasing in p for each L , $\delta N^{1/5} \geq \text{LB}^*(p) \geq \text{LB}^*(1511) = 1.026529\dots > 1.0265$ for every prime $p \geq 1511$ and every k . $\square$

Dimension three. D_3^+ has minimum $\sqrt{3}/2 < 1$, so the mechanism above gives nothing at $s = 3$; whether other layers with entries of order p and a rational limit $A = \lim \tilde{M}/p$ can be realized for every k in dimension three is open (Remark 123(7)).

14. VERIFICATION STATUS

Every result is proved in the text, by hand or, where stated, with a computer-assisted finite certificate. The numbers in the paper fall into three classes.

- *Computer-assisted proofs* rest on exact finite certificates: Propositions 40, 81, 122 and 118; part (4) of Proposition 104 (exact minimum distances at the primes $17 \leq p \leq 89$); the part of Theorem 120 for layers that are not skew; the rows $s \leq 6$ of Table 6 and $s \geq 4$ of Table 7 (with Proposition 84); the values of Table 8; the per-prime certificates of Remark 58 (Appendix C); and Theorem 64 (Table 5). The certificates of Propositions 40, 81, 122 and 118, of part (4) of Proposition 104, of Theorem 120, of Table 8, of Appendix C, of parts (2) and (3) of Theorem 64 and the per-prime completions of Proposition 84 are also checked in the Lean kernel. Part (1) of Theorem 64, the entries .4699 and .2586 of Table 5, and the thresholds and scans of Tables 6 and 7 are checked by scripts only (Appendix F). The certificates of Theorems 64 and 120, Propositions 81, 118, 104 and 84 and Tables 6 and 7 were moreover reproduced by two independent implementations, that is, by two separately written programs (for Theorem 64, two C++ checkers written from the mathematics, without shared code). The scripts of the accompanying software deposit (Appendix G) rerun the certificates of Theorem 64, Propositions 118 and 104 and Theorem 120.
- *Computed values* are labelled where they occur and are used in no proof: the decay of the net of [20] (Section 1); the bracket of Remark 101; the exact minimum distances of Table 12; the values a_s^* of Table 3; the rows $s = 7, 8$ of Table 6; the effect of Remark 16; the per-prime nets listed after Corollary 39 other than the one of Proposition 40; the computed values after Proposition 103, including the comparison with the column nets; those after Proposition 104, including the layer at $m = 3$ in which two coordinates

share their geometric digit (value $\sqrt{233}/15$ in the limit model of Section 13.3); the shifts of Remark 108 that break the lock; the comparison of $\mathcal{W}_p^*$ with $\mathcal{W}_p$ in Remark 107; the comparison nets of Figure 10(c), whose second digit is the same in all coordinates (Section 11); the exact minimum distances of $\mathcal{Q}_p^*$ after Proposition 118; the orbits after Theorem 120; and the values for M_5 in Remark 121. Appendix G lists the scripts that reproduce them.

- *Heuristic statements* are marked as such where they occur (for instance in Remarks 99, 80, 37, 125 and 124, and the limit model of Section 13.3).

Lean. Every theorem, proposition, lemma and corollary, every definition except Definition 3 (which only introduces names), and the proved statements of the remarks listed in Table 15 are formalized in Lean 4 [13] with Mathlib [44], apart from finite computations that are checked by scripts instead: part (1) of Theorem 64, the tables of designs and the computed values above (the list is in Appendix F). One formalized result, Proposition 100, uses classical theorems that are not in Mathlib as explicit hypotheses: Hajós’s theorem, Keller’s conjecture for $s \leq 7$ and the optimal packing bounds in dimensions two and three; so does the growth statement for the design U_s of Remark 24 (the prime number theorem). Consequences of other cited theorems, such as the asymptotics after Proposition 90 and Theorem 92, are cited and not formalized. Appendix F describes the method and maps the sections of the paper to the statement files and proof modules of the formalization (Table 15). The formal proofs complement, and do not replace, the arguments in the text.

15. OPEN PROBLEMS

We list what remains open, by the regimes of the lattice picture (Section 2): (I) geometric layers $\tilde{M}$ with entries bounded independently of q , at $m = sk$; (II) lattice skeletons, $m \not\equiv 0 \pmod{s}$; (III) layers with entries of size $\Theta(q)$. Results stated earlier are not repeated. Recall that the (first-order) deficit of a family of nets is the K in $\delta N^{1/s} = 1 - K/q + O(q^{-2})$, and the certified deficit $K(F)$ of a design is the value that the one-digit relaxation certifies (Definition 74).

Remark 123 (Open problems). (I) *Bounded layers.* (1) *Growth of the deficit.* Let $K(s)$ be the best first-order deficit K in $\delta N^{1/s} = 1 - K/q + O(q^{-2})$, $q \rightarrow \infty$, over families of digital $(0, sk, s)$ -nets over $\mathbb{Z}/q\mathbb{Z}$ whose geometric layers have entries bounded independently of q and no zero diagonal entry. Lower bounds: $K(s) \geq \sqrt{(s-3)}/8$ (Theorem 87). For designs on the places $\infty, 0, \dots, s-2$: $K(F) \geq s^{1-o(1)}$ (Theorem 92); if moreover the row scalars λ'_c (Proposition 17) take one value on the finite places, $K(F) \geq \text{lcm}(1, \dots, s-3)$ (Proposition 90); and the two-axis bound K_{pair} is at least 2 for $s \geq 5$ (Theorem 88). Upper bounds: the constructions here achieve 1 for $s = 3$, 2 for $s = 4$ (Proposition 81), 5 and 10 for $s = 5, 6$ (Table 6), and a certified deficit at most $a_s^* \leq e^{s \log s + O(s)}$ for every $s \geq 4$ (Theorem A). Does $K(s)$ grow polynomially or exponentially? On these places a certified deficit polynomial in s would need row scalars that differ between the finite places (Proposition 90). Also open: $K = 1$ for $s = 4$; whether layers with zero diagonal do better (Remark 80); and the optimal second-order constant C in $\delta N^{1/3} = 1 - 1/p + C/p^2 + o(p^{-2})$ in dimension three. For nets with the layer of $\mathcal{P}_{k,p}$ it is at most 4 for $k \geq 4$ (after Corollary 78); for other bounded layers Proposition 77(i) bounds it by $\frac{1}{2}((|\tilde{M}_{ba}| + 1)^2 + (|\tilde{M}_{b'a}| + 1)^2)$ for a coordinate a with $\tilde{M}_{aa} = -1$, and for zero diagonals (Remark 80) we have no bound. (2) *Small bases.* Theorem A needs $q \geq 5a_s^* + 4$, and the designs of Table 6 certify smaller bases only by finite scans; for $s = 4$ the bases $q \leq 15$ have only weaker proved constants, and for $s \geq 4$ Theorem A excludes even q (it needs $\text{lpf}(q) \geq s-1$; for $q = 2$ no $(0, m, s)$ -net with $s \geq 4$ exists, as $s \leq q+1$). In dimension three the bases 2 and 3 are covered for every m (Theorem 64, computer-assisted); at $m = 3$ the column nets cover every base coprime

to 6 (Theorem 49), column nets do not exist in even bases (Theorem 95), and the other bases $q \geq 4$ divisible by 2 or 3 are open at $m = 3$.

(II) *Lattice skeletons.* (3) For $s \geq 5$ the residues $1 \leq r \leq s - 3$ ($\ell \geq 3$ skeleton coordinates) are open for all p ; per-prime nets exist for $s = 5$, $r = 2$ at seven primes (computed, after Corollary 39), and a family for all large p is open. Lattices with the optimal minimum order $p^{\ell/s}$ exist by a counting argument (after Lemma 29); explicit ones are known here only for $\ell = 1$, $\ell = 2$ and $r = 1$, and for $3 \leq \ell \leq s - 2$ an explicit family is open (a mixed radix in the ring of integers of a degree- ℓ field is a natural candidate). The bottleneck is to realize such a skeleton with bounded faults: inside the frame orbit Lemma 38 excludes the Korobov skeleton digits of $\mathcal{B}^1$ with small faults (Corollary 39); other Korobov vectors, faults growing slowly with p , and completions outside the frame orbit are not excluded, and per prime frame-orbit skeletons with faults ± 1 work (Proposition 40). For one skeleton coordinate it is open whether the certified Euclidean constants tend to $\sqrt{\gamma_s}$ (Remark 124) and which explicit κ attain it; for two skeleton coordinates, Euclidean (rather than maximum-norm) bounds are open. (4) In dimension four: $m \equiv 1 \pmod{4}$ for primes $p > 83$ (no closed form is known; per-prime nets are known at every prime $7 \leq p \leq 83$, after Corollary 39 (computed), Proposition 40 works out $p = 13$, and we know of no obstruction for larger p), $m = 4$, and small primes ($m \equiv 1$ at $p = 5$, $m \equiv 2$ at $p \leq 19$, $m \equiv 3$ at $p \leq 13$). Also open: an explicit $p_0(s)$ in Theorem 35 for $s \geq 9$, and a covering radius uniform in p for $\ell \geq 2$. (5) In dimension three: a mesh ratio uniform in p for $m \equiv 1$; $m \in \{4, 7\}$ for $p \leq 31$ and $m = 5$ for $p \leq 7$; and an explicit family for all large primes with limit > 1 at the resolutions $m \geq 4$ (at $m = 3$ the nets $\mathcal{T}_p$ and $\mathcal{W}_p$ of Propositions 103 and 104 are such families). At $m = 3$, among constants below 1: whether digital $(0, 3, 3)$ -nets that are not column point sets have smaller deficits than $\frac{1}{3}$ and $\frac{2}{3}$ (Theorem 95 settles this among column point sets; outside them the drift-and-jitter bookkeeping of Section 11 is only a heuristic).

(III) *Large-entry layers.* (6) (a) Smaller bases for $s \geq 5$: Proposition 122 needs $p \geq 1511$, and at one resolution it is open whether some $(0, 5, 5)$ -net over $\mathbb{F}_p$ with $p \leq 31$ has $\delta N^{1/5} > 1$ (Proposition 118). (b) The drift-and-jitter bookkeeping for half-integer layers at $k \geq 2$, where the split-frame layers are Cauchy matrices, and for $s \geq 6$. (c) Split-frame designs with explicit constants of moderate size for $s = 6, 7, 8$. (d) Half-integer layers at the resolutions $m \not\equiv 0 \pmod{s}$. (e) Other split-frame layers beyond D_s^+ . (7) In dimension three: whether a geometric layer $\tilde{M} \approx qA$ with a fixed rational matrix A can be realized for every k with $\delta N^{1/3}$ bounded above 1. At $k = 1$, layers whose geometric digits wrap together in two or three coordinates (locked wraps, Section 13.3) give the limits $\sqrt{66}/8$ (Proposition 103), $\sqrt{281}/16$ (Proposition 104) and $\mu^* = 1.0480\dots$ (Remark 107), the optimum of the layers of rank one with image $\mathbb{F}_p(2, 2, 1)$ (Proposition 106); the optimum over the other images of rank one, over layers of rank two and over non-digital point sets is open. At $k \geq 2$ the geometric digits of any two coordinates are jointly uniformly distributed (Lemma 50, as $2(k+1) \leq 3k$), so no relation between the geometric digits of two coordinates survives, and neither the two-coordinate lock of $\mathcal{T}_p$ nor the three-coordinate lock of $\mathcal{W}_p$ extends to $k \geq 2$. For digital nets the only linear relation among the three geometric digits of one index that this count leaves is one of full support, $h_x r_x + h_y r_y + h_z r_z \equiv 0$ with all $h_c \neq 0$; whether such a relation, or a correlation that involves digits of other indices, can raise the constant above 1 is open.

The case $k = 1$ and digital shifts. (8) At $k = 1$: whether $K_1 = 1$ is possible for $s = 5$, or $K_1 = 2$ for $s = 6$ (Proposition 84); frameless layers (F_0 chosen directly, not from a frame, Proposition 84(2)) for $s \geq 7$; and the choice of the deeper rows, which are free at $k = 1$ apart from $t = 0$ and change the exact separation at small q (Proposition 83 and the remark after it). (9) In the bases two and three the constants of Theorem 64(3) are certified lower bounds, not exact values; for $b = 3$ and $m \equiv 2 \pmod{3}$ the infimum over m and τ for these nets lies between

0.0770 and 0.0901, the latter the exact value at $m = 20$ (computed). Whether other seeds or lift parameters give larger every-shift constants in base three is open.

Sequences. (10) All nets here depend on m ; they are not prefixes of one sequence, and the question of [11] for sequences remains open in dimension $s \geq 3$.

Beyond digital nets. (11) Can nets that are not digital, for instance permutation nets, exceed the constants of the digital nets here, for instance by avoiding the slip planes that linear offsets force (Corollary 97)?

16. RELATION TO PRIOR WORK

Where we say below that we found no prior work, this reflects a literature search (web searches of October 2026) that was not exhaustive; it is not a claim of priority. *The frame and unit minors.* The unit-minor criterion over any finite commutative ring is Niederreiter's [46, Thm. 6.1]; the Möbius frame (T^2, I, T) of Section 3, which by Proposition 9 is the net with the generator matrices (J, P, I) up to scrambles, is his construction [46, Thm. 6.2] with the elements $\beta = (0, 1)$ of $\mathbb{F}_q$, whose box determinants are $\pm \prod (\beta_k - \beta_h)^{d_h d_k} = \pm 1$, and [46, Cor. 6.3] gives $(0, m, 3)$ -nets in every base (Theorem 6.2 is stated over a product of finite fields; since the determinant identity is polynomial, the same integer matrices work over $\mathbb{Z}/q$ by Theorem 6.1). For integer systems the reduction to prime-power and prime moduli is [39, Lemmas 8–9], and the admissible dimensions over a ring, in particular $s \leq \text{lpf}(q) + 1$ over $\mathbb{Z}/q\mathbb{Z}$, are [39, Thm. 2, Cor. 2]; Lemmas 8 and 10 are therefore classical in substance. The same matrices reappear as universally decodable matrices in coding theory [66]. *Scrambles and t -preserving moves.* That lower-triangular scrambles preserve t is standard [43, 62, 14] (as do Owen's nested scrambles [47], a nonlinear family that contains the lower-triangular ones); Proposition 9 places $\mathcal{P}_{k,q}$ in Tezuka's generalized Faure class (for each m). Lemma 2 (the gauge moves, which preserve t) is elementary; the block scalings are not per-coordinate lower-triangular scrambles (whether they leave the orbit of the nested scrambles we have not checked), and the nets $\mathcal{B}^1$ use them. The occupied fine cells of $\mathcal{B}^1$ form, per coarse block, cosets of a Korobov lattice [34, 55]. *Separation.* In two dimensions, well-separated nets are known: the Larcher–Pillichshammer net [40, 11] and, in coding language, a digitally shifted Hammersley set with a product-distance bound [63]. In every dimension Sobol' and Shukhman [58] bound the minimum distance of Sobol' points from below, by a bound that decays faster than $N^{-1/s}$. Without the digital structure, quasi-uniform low-discrepancy point sets are known in every dimension: Frolov point sets [10, Thm. 3.1], Kronecker sequences [10, Thm. 3.9 and the text after Cor. 3.13] (with discrepancy $N^{-1+\varepsilon}$), and (by an existence argument) rank-1 lattices [10, Thm. 3.7]. These are not digital nets in a fixed base (Section 1), and we do not claim the broad statement. In two dimensions the even- m permutation nets of [20, Sec. 3] follow the pattern of this paper: a lattice of lines, van der Corput slides along these lines carrying $t = 0$, and a torus tiling adapted to that lattice (Remark 6; their net property is proved in [53]). *Large-entry layers.* The packings D_s^+ and E_8 are classical [9], and so are the bounds of Cohn and Elkies [3] and the optimality of E_8 [67]. We found no digital nets with a D_s^+ or E_8 local structure, and no construction that reads the cell and the offset of a coordinate at different points, as the split frames of Section 13 do. Their box-minor lemma (Lemma 111) is classical in substance: it is the confluent Vandermonde determinant of Hermite interpolation, as in Niederreiter's frames [46, Thm. 6.2]. Suzuki [60] studies the separation of scrambled digital nets: under full Owen scrambling fixed- t nets are not quasi-uniform (the mesh ratio is $\Omega(N^{1/(2s)})$ in probability), and matrix (linear) scrambling of binary fixed- t digital nets gives mesh ratio $O(\log N)$ in probability in every dimension $s \geq 2$. Both results are in probability, for randomized nets, and short of quasi-uniformity; they do not overlap with the explicit constructions here. They concern random scrambles; a particular nested scramble can be well separated: the two-dimensional nets of

Remark 6 are a nested scrambling [47] of the Hammersley net (Remark 6(iv)), and they are not digital [20, 53]. The closest work we found is: [11], whose quasi-uniform digital example is two-dimensional; He [26, 28], who builds rotated sphere packing designs and designs from rotated lattices (rotated $\mathbb{Z}^s$, densest packings including E_8 , thinnest coverings, interleaved lattices) with quasi-optimal separation distance on all projections, which are not digital nets; He [27], who builds maximin designs from interleaved lattices (unions of shifted copies of a lattice), which are not nets; and the search for (t, m, s) -nets with maximized minimum distance [19, 20]. D_s is Construction A of the even-weight code, and for even s , $2D_s^+$ is Construction D applied to the repetition code contained in the even-weight code [2]; whether such one-point-per-cube descriptions have been used for nets before we have not checked systematically. *One point per cube.* The theorems behind Proposition 100 are classical: Hajós's theorem on lattice cube tilings [22], Keller's conjecture, proved for $s \leq 6$ by Perron [49] and for $s = 7$ by Brakensiek, Heule, Mackey and Narváez [1], and false for $s \geq 8$ [41, 42], and the optimality of the face-centred cubic packing [23], of E_8 [67] and of the Leech lattice [4]. We found no prior use of the cube-tiling theorems for the separation of nets. Maximin Latin hypercube designs, in which every coordinate takes each of N grid values exactly once, have separation bounds under this marginal one-per-row constraint [64, 65]; we found no prior separation analysis under the constraint of one point per cube. *Codes.* Each ingredient of Remark 32 is classical: Construction A and Construction D [9, 2], the characterization of MDS codes by nonsingular submatrices [45] and of generalized Reed–Solomon codes by Cauchy redundancy matrices [51], the spectral test [5, 32], and the equivalence of $t = 0$ with the MDS property in the Rosenbloom–Tsfasman metric, with Reed–Solomon codes of that metric [52, 56, 46]; over a field, the zero count after Lemma 8 is Skrikanov's MDS proof for these codes. We found no prior work that relates the Euclidean separation of digital nets to Construction A, Lee-metric codes or the spectral test, and no treatment of digital-net skeletons as generalized Reed–Solomon Construction A lattices or of geometric layers $\tilde{M} \approx qA$ with A rational of denominator e as codes over $\mathbb{Z}/e^2$. The carry criterion of Corollary 97(b) is the analogue, for carries, of the criterion of Kositwattanarerk and Oggier [33]: the code formula $C_0 + 2C_1 + \dots + 2^{a-1}C_{a-1} + 2^a\mathbb{Z}^n$ of nested binary linear codes is a lattice if and only if the codes are closed under the Schur product, whereas Construction D always gives a lattice. *What is new.* We did not find the following in the literature.

- Part I: the scramble L ; the residue description of the geometric digits (Proposition 43 and Lemma 11); a single choice of scrambles that realizes a design for every number k of cell digits (Proposition 13); a separation bound of the optimal order $N^{-1/s}$ for a family of digital nets in a fixed base ($N = q^m$, $m \rightarrow \infty$) in any dimension $s \geq 3$ (decaying lower bounds are known [58]); the lattice of admissible design columns with its adelic Chebyshev identity (Lemmas 20, 21); the deep-shift lift $m \rightarrow m+3$ (Definition 60), which carries a separation certificate (Lemma 62); and lattice skeletons of digital nets for the resolutions $m \not\equiv 0 \pmod{s}$ (Section 5; the lattices themselves are classical congruence and Korobov lattices).
- Column nets: column nets themselves and an exact minimum-distance formula for point sets on lines parallel to the body diagonal (Theorems 48 and 49); their two-dimensional analogue is the union of translated diagonals with van der Corput slides of [20, Sec. 3], and exact formulas are known for particular two-dimensional nets: the ℓ^∞ separation of the Sobol' points [59] and the dispersion of the Hammersley net [35]. Also the optimality of the column nets among column point sets and the column ceiling (Theorem 95(3), Corollary 94; part (2) of Theorem 95 is classical in substance [48, 29]).
- Part II: ceilings of the type of Proposition 77 and Theorem 87; lower bounds for the certified deficit of frame designs by counting cross-ratios (Theorem 92); the bookkeeping

of the first-order deficit by drift and jitter with its holonomy obstruction (Lemma 93); the description of the local configurations of digital nets by linear offsets, with the one-point-per-cube ceilings of Section 12; split frames with their non-symmetric Cauchy layers, and digital nets whose separation exceeds the cubic value 1 at every resolution $m = sk$ (Theorem 116); digital $(0, 5, 5)$ -nets with $\delta N^{1/5} > 1$, and the least drift $\text{dr} = \frac{17}{2}$ over the half-integer layers of Theorem 120 (Proposition 118); explicit digital $(0, 3, 3)$ -nets whose local configuration is a union of two lattice cosets, with separation above the cubic value (Proposition 103); and a digital $(0, 3, 3)$ -net with a layer of rank one and $\delta N^{1/3} \rightarrow \sqrt{281}/16$, with the optimum μ^* of its family (Propositions 104 and 106).

More generally, we found no digital $(0, 3, 3)$ -net (polynomial lattice point sets included, as they are digital nets) with separation above the cubic value in the literature; the closest constructions we found are lattices, not nets: lattice designs [26, 28], some of them built from packings denser than the cubic lattice, and the quasi-uniform rank-1 and Korobov lattice designs of Sakai and Goda [54].

Use of AI systems. The constructions, proofs and Lean formalization were produced by AI systems (Anthropic Claude Opus 5.5; some early exploratory results used Claude Fable 5.1) under the author's direction. The author selected the problems, steered the research and reviewed the formal statements, but has not verified every proof by hand. AI systems are not listed as authors; responsibility for the deposit rests with the author.

APPENDIX A. DESIGNS

A design $(F_0, \dots, F_{L-1})$ prescribes, for each pair of coordinates (c, d) , how the geometric digit of c depends on the last L cell digits of d (Section 2). With Definition 14 each design below defines the nets $\mathcal{P}_{k,q}^F$; the deficits and base thresholds they certify are in Table 6, and the values at $k = 1$ in Table 7. Conventions: entry (c, d) is in row c and column d , with the coordinates in the order of the places listed; F_n is the target at carry depth n (the level $k - 1 - n$) of row 0 of the block (c, d) , diagonal included.

A.1. The designs of Table 6. $s = 4$, places $(\infty, 0, 1, 2)$, row scalars $\lambda' \equiv 1$; this is the deficit-two design of Proposition 81:

$$F_0 = \begin{pmatrix} -2 & -2 & -1 & -2 \\ 1 & -2 & 1 & 1 \\ 1 & -2 & -2 & 2 \\ 1 & -1 & -1 & -1 \end{pmatrix}, \quad F_1 = \begin{pmatrix} 0 & 3 & 1 & 1 \\ 0 & 1 & -2 & -1 \\ -1 & 1 & 0 & -3 \\ -2 & 1 & 0 & 0 \end{pmatrix}, \quad F_2 = \begin{pmatrix} 0 & -2 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

$s = 5$, places $(\infty, 0, 1, 2, 3)$, row scalars $\lambda' = (\frac{1}{2}, 1, 1, 1, 1)$ (Proposition 17; the $\frac{1}{2}$ needs q odd):

$$F_0 = \begin{pmatrix} -4 & -3 & 1 & -1 & 3 \\ -1 & -5 & -2 & 1 & -2 \\ -1 & -6 & -5 & 2 & -3 \\ -1 & -3 & 2 & -5 & -6 \\ -1 & -2 & 1 & -2 & -5 \end{pmatrix}, \quad F_1 = \begin{pmatrix} -1 & 5 & -1 & 1 & -8 \\ 1 & 0 & -2 & -2 & 4 \\ 0 & -2 & 0 & -6 & 5 \\ -1 & 2 & -6 & 1 & 4 \\ -2 & 2 & -2 & -2 & 1 \end{pmatrix},$$

$$F_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 4 \\ -1 & 1 & 1 & 0 & -3 \\ 1 & 5 & 1 & 3 & -4 \\ 2 & 2 & 1 & 0 & 1 \\ 2 & 1 & 1 & 3 & 1 \end{pmatrix}, \quad F_3 = \begin{pmatrix} 0 & -2 & -1 & -1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ -1 & 3 & 0 & 1 & 1 \\ -1 & -3 & 3 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 \end{pmatrix}.$$

$s = 6$, places $(\infty, 0, 1, 2, 3, 4)$, $\lambda' = (\frac{1}{2}, 1, 1, 1, 1, 1)$:

$$F_0 = \begin{pmatrix} -8 & -6 & 3 & 1 & -3 & 6 \\ 2 & -9 & -6 & -1 & 2 & -3 \\ 2 & -12 & -8 & -2 & 3 & -4 \\ 2 & -6 & 6 & -7 & 6 & -6 \\ 2 & -4 & 3 & 2 & -9 & -12 \\ 2 & -3 & 2 & 1 & -6 & -9 \end{pmatrix}, \quad F_1 = \begin{pmatrix} -1 & 7 & -7 & -1 & 7 & -13 \\ -1 & -1 & 2 & 0 & -6 & 5 \\ -2 & -10 & 0 & -2 & -10 & 6 \\ -3 & 1 & -26 & -1 & -26 & 7 \\ -4 & 2 & -10 & -6 & 2 & 2 \\ -5 & 2 & -6 & -2 & 2 & 1 \end{pmatrix}, \quad F_2 = \begin{pmatrix} 0 & -4 & 0 & 1 & -9 & 10 \\ 1 & 4 & 2 & 0 & 7 & -1 \\ 0 & 20 & 1 & 4 & 11 & 0 \\ 0 & 9 & 26 & -1 & 23 & 3 \\ 1 & 4 & 5 & 0 & -2 & 8 \\ 3 & 2 & 2 & 1 & -1 & 1 \end{pmatrix},$$

$$F_3 = \begin{pmatrix} 1 & 8 & 7 & -1 & 2 & -4 \\ -2 & -3 & -1 & 0 & -4 & 0 \\ 1 & 3 & 0 & -1 & -7 & 0 \\ 1 & -3 & -6 & 3 & -3 & 1 \\ 0 & -1 & -1 & 3 & 3 & 0 \\ 0 & 0 & 1 & -1 & 2 & 0 \end{pmatrix}, \quad F_4 = \begin{pmatrix} -1 & -3 & -3 & -3 & 3 & 1 \\ 0 & 4 & 0 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 3 & -2 \\ 0 & -1 & 0 & -2 & 0 & -5 \\ 3 & -1 & 3 & 1 & -1 & 1 \\ 0 & -1 & 1 & 1 & 0 & 3 \end{pmatrix}.$$

Each design is reachable: the interpolating polynomials $g_{d,j}$ of Proposition 17 have degree j and leading coefficients that are units of the ring R' of Definition 14 (checked by exact interpolation). The designs for $s = 7, 8$ are in the software deposit (Appendix G).

A.2. The layers of Table 7. At $k = 1$ a design is a single geometric layer F_0 , of two kinds (Proposition 84). The *frame layers* are, off the diagonal, the Cauchy layers $\lambda'_c \mu_d w_{cd}$ that every scrambled frame on the places $\infty, 0, 1, \dots, s-2$ has (Proposition 12), with a diagonal chosen for $k = 1$: for $s = 4$ the off-diagonal part of U_4^* , for $s = 5$ that of the $s = 5$ design of Table 6, and for $s = 6$ the searched scalars $\lambda' = (1, \frac{2}{3}, -2, -\frac{2}{3}, \frac{2}{3}, -2)$, $\mu = (\frac{3}{2}, 18, 3, 3, 9, 6)$:

$$\begin{pmatrix} -1 & 2 & 1 & 2 \\ 1 & -1 & -1 & -1 \\ 1 & 2 & -2 & -2 \\ 1 & 1 & 1 & -2 \end{pmatrix}, \quad \begin{pmatrix} -3 & -3 & 1 & -1 & 3 \\ -1 & -3 & -2 & 1 & -2 \\ -1 & -6 & -3 & 2 & -3 \\ -1 & -3 & 2 & -3 & -6 \\ -1 & -2 & 1 & -2 & -3 \end{pmatrix}, \quad \begin{pmatrix} -6 & 18 & 3 & 3 & 9 & 6 \\ 1 & -4 & -2 & -1 & -2 & -1 \\ -3 & -36 & -6 & 6 & 9 & 4 \\ -1 & -6 & -2 & -6 & 6 & 2 \\ 1 & 4 & 1 & 2 & -4 & -4 \\ -3 & -9 & -2 & -3 & -18 & -3 \end{pmatrix}.$$

The *frameless layers*, integer matrices chosen directly, for which a $t = 0$ completion exists for each admissible prime ($s = 5$, $K_1 = 2$; $s = 6$, $K_1 = 3$; $s = 6$, $K_1 = 5$), are

$$\begin{pmatrix} -2 & 1 & -1 & -2 & -1 \\ -1 & -2 & -2 & 2 & -1 \\ -1 & 1 & -1 & -1 & 2 \\ -2 & 1 & -2 & -2 & 1 \\ -1 & -2 & 1 & 1 & -2 \end{pmatrix}, \quad \begin{pmatrix} -3 & -3 & 2 & -1 & 2 & 1 \\ 1 & -3 & 2 & 1 & 3 & -2 \\ 1 & -2 & -3 & 3 & -1 & -1 \\ 2 & 3 & 1 & -2 & -1 & 1 \\ -3 & -2 & 1 & 1 & -3 & 2 \\ -1 & -1 & 3 & 2 & 2 & -3 \end{pmatrix}, \quad \begin{pmatrix} -4 & 1 & 3 & -1 & 2 & 4 \\ -2 & -4 & 1 & -1 & 1 & 3 \\ -4 & -2 & -4 & 4 & 1 & -2 \\ -2 & 4 & -2 & -4 & -4 & -2 \\ 1 & -3 & 3 & 1 & -5 & 2 \\ -1 & 4 & 4 & -2 & 1 & -5 \end{pmatrix};$$

their deeper rows are chosen per prime factor of q (Proposition 84). For the finitely many admissible primes below the Schwartz–Zippel bound $SZ(s)$ of that proof, where the generic argument does not apply, explicit completions with $t = 0$ were constructed and checked; they are in the deposit.

A.3. The five-dimensional split-frame design H_5^* . This design gives the nets $\mathcal{H}_{k,p}^{5*}$ of Proposition 122, with $\delta N^{1/5} > 1.0265$ for every prime $p \geq 1511$. Its split frame (Definition 110) has the offset points $u = (-2, 0, 2, 4, 8)$ and the cell points $v = (5, 7, -1, 3, 1)$; the conventions are those stated at the start of this appendix:

$$2F_0 = \begin{pmatrix} -147 & 5 & 45 & -9 & 3 \\ 3 & -61 & -15 & -5 & 3 \\ 5 & 3 & -53 & -15 & -3 \\ -15 & -5 & 3 & -61 & 1 \\ 15 & 45 & 5 & -9 & -45 \end{pmatrix}, \quad F_1 = \begin{pmatrix} 0 & 23 & 21 & 12 & -1 \\ -2 & 0 & 38 & 5 & -2 \\ -3 & 15 & 0 & -10 & -1 \\ 4 & -28 & -4 & 0 & 0 \\ -14 & -18 & -6 & 21 & 0 \end{pmatrix},$$

$$F_2 = \begin{pmatrix} 0 & -19 & -54 & -7 & -2 \\ -1 & 0 & -39 & -2 & 1 \\ -2 & -13 & 0 & 19 & 2 \\ 2 & 26 & 0 & 0 & -1 \\ 5 & -6 & -1 & -18 & 0 \end{pmatrix}, \quad F_3 = \begin{pmatrix} 0 & -7 & 10 & -1 & 1 \\ 1 & 0 & 8 & -1 & -1 \\ 2 & -4 & 0 & -2 & 0 \\ 1 & 4 & 2 & 0 & 0 \\ 1 & 1 & 4 & 1 & 0 \end{pmatrix}.$$

Off the diagonal, the geometric layer is $M_{cd}^{(0)} = \lambda'_c \mu_d / (u_c - v_d)$ with $\lambda' = \frac{1}{2}(-9, -3, -3, 3, 9)$ and $\mu = (5, 5, 5, -5, 1)$; all partial sums $M^{(j)}$ lie in $\frac{1}{2} + \mathbb{Z}$ (off-diagonal entries of absolute value at most $\frac{87}{2}$), and $M^{(3)} = -\frac{1}{2}$ off the diagonal. The interpolating polynomials $g_{d,j}$ of Proposition 113 have degree j , and their leading coefficients have only the primes 2, 3, 5, 7, except -97 ($d = 1$, $j = 3$) and $\frac{101}{12}$ ($d = 2$, $j = 3$). This is why Proposition 122 excludes $p \in \{2, 3, 5, 7, 97, 101\}$, and why 97 and 101 matter only from $k \geq 4$ on, when carry depth 3 is used.

APPENDIX B. DEFERRED PROOFS AND SIDE RESULTS

This appendix holds one deferred proof and two heuristic remarks.

B.1. Proof of Proposition 85.

Proof. Let $e = \mathbf{e}_a + \varepsilon \mathbf{e}_b$ be the step of the proposition, from the cell n to the cell $n + e$. Write ρ'_b and ρ''_b for the second offset digit of b at n and at $n + e$; along e it changes by a constant σ'_b modulo q . Count the cells n with the following properties:

- (a) the last digits of n_a and n_b cause no carry along e ;
- (b) $r_a + \sigma_a \geq q$, so that a wraps (σ_a values of r_a);
- (c) r_b does not wrap ($q - |\sigma_b|$ values);
- (d) ρ'_b lies in a nonempty set $\mathcal{V}_b$ of digit values chosen so that $\varepsilon(\rho''_b - \rho'_b) \leq 0$;
- (e) $r_u + \sigma_u \in [0, q)$ for every coordinate $u \notin \{a, b\}$.

For one u at a time, the digits involved form a box with depths $k + 1$ on a , $k + 2$ on b , $k + 1$ on u and 0 elsewhere, of total $3k + 4 \leq sk$, so they are jointly uniform; the conditions (a)–(d) have positive density and the fraction of cells violating (e) at u is $|\sigma_u|/q$, so some cell satisfies all of them, because $\sum_u |\sigma_u| < q$. For such a cell, $|\Delta_a| < (\sigma_a + 1)/q$, $|\Delta_u| < (|\sigma_u| + 1)/q$ and $\varepsilon \Delta_b < 1 - |\sigma_b|/q + 1/q^2$. The second part of the proposition (the case $\varepsilon \sigma_b > 0$) uses, in the same way, the boxes with depths $k + 1$ on a , b and u and 0 elsewhere (total $3k + 3 \leq sk$), with r_a and r_b both wrapping, so that $|\Delta_a| < (\sigma_a + 1)/q$ and $|\Delta_b| < (|\sigma_b| + 1)/q$. The pair lies inside the cube, so the bound holds for the toroidal and the Euclidean distance. $\square$

B.2. A conjectural limit for one skeleton coordinate (heuristic).

Remark 124 (The limit $\sqrt{\gamma_s}$). Table 8 suggests that $\max_\kappa \lambda_{\text{jit}}(\kappa) p^{-1/s} \rightarrow \sqrt{\gamma_s}$, the square root of the Hermite constant (1.122, 1.189, 1.231, 1.290, 1.345, $\sqrt{2}$ for $s = 3, \dots, 8$); here $\lambda_{\text{jit}}(\kappa)$ is the Euclidean minimum of the skeleton lattice Λ_κ after one fine cell of jitter is subtracted in each coordinate (Proposition 102). The upper bound holds by the definition of γ_s , since $\lambda_{\text{jit}} \leq \lambda_2(\Lambda_\kappa) \leq \sqrt{\gamma_s} p^{1/s}$. For the lower bound it would suffice that the index- p sublattices of $\mathbb{Z}^s$, scaled to covolume 1, equidistribute in $\text{SL}_s(\mathbb{Z}) \backslash \text{SL}_s(\mathbb{R})$ as $p \rightarrow \infty$. Indeed, the set of unimodular lattices with $\lambda_1 > \sqrt{\gamma_s} - \varepsilon$ is open and nonempty, so for large p it would contain a scaled Λ_κ (λ_1 is continuous, and the sublattices containing a unit vector have normalized minimum at most $p^{-1/s}$), and then $\lambda_{\text{jit}} \geq \lambda_2 - \sqrt{s}$. Such equidistribution is a theorem of Clozel, Oh and Ullmo on Hecke points [7], but as usually stated it is for simply connected G and Hecke operators T_a with $a \in G(\mathbb{Q})$, which does not literally contain the index- p correspondence of $\text{diag}(p, 1, \dots, 1) \notin \text{SL}_s(\mathbb{Q})$. The version of Eskin and Oh [15, Thm. 1.2] allows a in the commensurator of the arithmetic group; we have not carried out the reduction in detail, so we do not state the limit as a theorem. The limit would hold at the residue $m \equiv -1 \pmod{s}$, as $p \rightarrow \infty$ uniformly in k , and would exceed the limit $\min(\sqrt{s}/2, \sqrt{2})$ of Theorem 116 (at the residue $m \equiv 0$) for $4 \leq s \leq 7$ and equal it at $s = 8$.

B.3. Size of the constants in Theorem 35 (heuristic).

Remark 125 (Constants). $B(p)$ and $\rho(p)$ are nondecreasing, so the bounds are positive for every $p \geq p_0$. For $s \geq 5$ a rough count gives $B \approx (p/\sqrt{2})^{2/s}$, i.e. $\delta N^{1/s} \rightarrow 2^{-1/s}$ (heuristic). For $s \geq 9$ the route of Lemma 31(c) needs B of order $(2s/\pi)^2$, which suggests $p_0(s) = e^{O(s \log s)}$ (heuristic). Nothing is optimized: the faults cost g^* cells at small p , and for even r a *block radix*, in which each of the two rows of A is a radix chain on its own group of the full coordinates, has a better constant.

APPENDIX C. PER-PRIME DESIGNS IN DIMENSION THREE

With Theorem 64 ($p = 2, 3$) and Corollary 57 ($p \geq 37$), these designs give well-separated families of digital $(0, m, 3)$ -nets in every prime base (Remark 72). Proposition 131 reduces the separation bound of Table 10, for every k and every graph form with the prescribed rows, to one finite computation per

design; Propositions 128 and 129 show by hand that a net with the prescribed rows exists for every k if the design satisfies finitely many polynomial conditions modulo p , which hold for the 37 designs. All of this is formally verified (Proposition 129 for odd p ; every tabulated design has $p \geq 5$). The appendix sets up the notation, defines the invariants of the moves, proves existence for every k , proves the separation bound for every k , and lists the finite checks.

Setting. We use the notation of Section 6.6: p is prime, $m = 3k + r$, $r \in \{1, 2\}$, the depths are $\mathbf{k} = (k + 1, k, k)$ resp. $(k + 1, k + 1, k)$, and Φ^F is the integer graph form of the frame with depths $\mathbf{k}$; all its box minors are ± 1 . An offset row is named by its coordinate and its position: $X0$ is the first offset row of x , $Y1$ the second offset row of y , and so on. The *prescribed rows* are the first offset row of a full coordinate and the first two offset rows of a skeleton coordinate: $X0, Y0, Z0 = S_z, Z1$ for $r = 2$, and $X0, Y0 = S_y, Y1, Z0 = S_z, Z1$ for $r = 1$. The first offset row of a skeleton coordinate is its skeleton digit (Section 5). The other prescribed row of each coordinate gives its *inner digit*: the first digit after the fine cell of the point (Section 5.1), which places the point inside its fine cell up to $1/p$ of the fine unit. For a full coordinate the inner digit is the first offset digit, the analogue of the geometric digit (Definition 3); Lemma 25 counts it among the deeper digits, whereas the designs below prescribe it. $R|d_l$ is the coefficient of an offset row R on level l of the cell of d , and for rows R, R' and columns c, c' (levels, possibly of different coordinates) $[R, R' | c, c'] = R|c R'|c' - R|c' R'|c$. The *window* of the cell of d is its last L_d levels, $L_x = 4$ if $r = 1$ and $L_d = 3$ otherwise.

Definition 126. A *per-prime design* for (p, r) assigns to each prescribed row R and each coordinate d integers $R|d^{(i)}$, $0 \leq i < L_d$. A graph form over $\mathbb{F}_p$ with depths $\mathbf{k}$ carries it if (i) each prescribed row R has the coefficient $R|d^{(i)} \bmod p$ on level $k_d - 1 - i$ of d and 0 on the higher levels of d , and (ii) each offset row of c below its prescribed rows has the coefficient 0 on the cell of c .

A per-prime design is the analogue, for the unequal depths $\mathbf{k}$, of a design with L_d levels (Section 2): $R|d^{(i)}$ is the target at carry depth i of d , diagonal included. In this appendix “design”, “configuration”, “certificate” and “relaxation” always mean the per-prime notions defined here. The upper index i counts the levels from the last one and does not depend on k ; in the proofs, which work at a fixed k , we write the entries with the level names of that k instead (e.g. $Y0|x_{k-1}$ for $Y0|x^{(1)}$). Entries of a row of c on the cell of c are diagonal entries (Lemma 2); they matter for separation, not for existence. The 11 designs that the coverage of every prime base needs ($m \equiv 1$ for $5 \leq p \leq 31$, $m \equiv 2$ for $p = 5, 7$; Remark 72) are printed in Table 11. The other 26 designs of Table 10 are at primes that other results already cover; they give larger constants there (Remark 58). All 37 designs are fixed data of the formalization (Table 15, statement file **Appendix**). For instance, for $p = 5$, $r = 2$ the skeleton digit is $S_z = 2x_k - y_k$, so the occupied fine cells are those of the index-5 lattice $P_z \equiv 2P_x - P_y \pmod{5}$, as for $\mathcal{B}^2$. The designs were found by a finite search scored by the relaxation of Definition 130; no optimality is claimed.

Invariants of the frame. The moves of Lemma 2 scale and combine rows and levels. So a design can be carried by a graph form obtained from Φ^F by the moves only if every quantity that the moves do not change has the same value at the design as at Φ^F . The following ratios are such quantities (Lemma 127). Propositions 128 and 129 show that their values, together with finitely many conditions of vanishing and nonvanishing, suffice for existence at every k . For $r = 2$ let $\tilde{x} = x_{k-1} - (Z0|x_{k-1}/Z0|x_k)x_k$ (a combination of columns), define $\tilde{y}$ likewise, and

$$\chi_1 = \frac{Z1|\tilde{y} \cdot Y0|\tilde{x} \cdot X0|y_k \cdot Z0|x_k}{Z1|\tilde{x} \cdot Y0|x_k \cdot X0|\tilde{y} \cdot Z0|y_k}, \quad \chi_2 = \left(\frac{Z1|x_k}{Z0|x_k} - \frac{Z1|y_k}{Z0|y_k} \right) \frac{Z0|x_k \cdot Y0|\tilde{x}}{Z1|\tilde{x} \cdot Y0|x_k}.$$

For $r = 1$ write $\xi_i = x_{k-i}$, $\eta_i = y_{k-1-i}$, $\zeta_i = z_{k-1-i}$; let $R_Y = Y1 - (Y1|\xi_0/Y0|\xi_0)Y0$ and $R_Z = Z1 - (Z1|\xi_0/Z0|\xi_0)Z0$ (combinations of rows), $d_x = [Y0, Z0|\xi_0, \xi_1]$, $\tilde{\zeta} = \zeta_1 - (X0|\zeta_1/X0|\zeta_0)\zeta_0$, $\tilde{\eta} = \eta_1 - (X0|\eta_1/X0|\eta_0)\eta_0$, and $\tilde{\xi} = \xi_2 + a\xi_1 + b\xi_0$ with $Y0|\tilde{\xi} = Z0|\tilde{\xi} = 0$, and put

$$J_1 = \frac{R_Y|\xi_1 \cdot Z0|\xi_0 \cdot Y0|\zeta_0}{R_Y|\zeta_0 \cdot d_x}, \quad J_2 = \frac{R_Z|\xi_1 \cdot Y0|\xi_0 \cdot Z0|\eta_0}{R_Z|\eta_0 \cdot d_x}, \quad J_3 = \frac{R_Y|\tilde{\zeta} \cdot Y0|\zeta_0}{Y0|\tilde{\zeta} \cdot R_Y|\zeta_0},$$

$$J_4 = \frac{R_Z|\tilde{\eta} \cdot Z0|\eta_0}{Z0|\tilde{\eta} \cdot R_Z|\eta_0}, \quad J_5 = \frac{R_Z|\tilde{\xi} \cdot Y0|\xi_0 \cdot Z0|\eta_0 \cdot R_Y|\zeta_0}{R_Y|\tilde{\xi} \cdot Z0|\xi_0 \cdot Y0|\zeta_0 \cdot R_Z|\eta_0}.$$

They read only the prescribed rows on the windows, so they are defined for designs as well (when the divisors are nonzero, as (U2), (U1) below guarantee).

Lemma 127 (Invariants). (a) Where defined, χ_1, χ_2 and $J_1, \dots, J_5$ are unchanged by the moves (a), (c) of Lemma 2 and the block scalings (b). (b) For every prime p , Φ^F has $\chi_1 = \chi_2 = -1$ for every $k \geq 1$ ($r = 2$), and $(J_1, \dots, J_5) = (1, -1, 2, 2, 1)$ for every $k \geq 2$ ($r = 1$).

Proof. (a) Diagonal blocks are not read. A move (c) scales the last level of a cell and adds to every other level multiples of deeper ones; so $\tilde{x}, \tilde{y}, \tilde{\zeta}, \tilde{\eta}, \tilde{\xi}$, each fixed by its leading level and a vanishing condition, are multiplied by units, and d_x by the product of the factors of ξ_0, ξ_1 . L_c scales the first offset row of c and replaces the second by a unit multiple of itself plus a multiple of the first; so R_Y, R_Z (the combinations vanishing on ξ_0) and $Z1$ restricted to $\tilde{x}, \tilde{y}$ (where $Z0$ vanishes) are multiplied by units, and the bracket in χ_2 is invariant under $Z1 \mapsto Z1 + \lambda Z0$ and scales like $Z1/Z0$. In each quantity every row, column and off-diagonal block occurs equally often in numerator and denominator, so all unit factors, including the block scalings, cancel.

(b) Let $\varphi_\infty(V), \varphi_0(V), \varphi_1(V)$ be the coefficient vectors of $V \in \mathbb{F}_p[t]_{<m}$ with respect to $t^{m-1}, t^{m-2}, \dots$, resp. $1, t, \dots$, resp. $1, (t-1), \dots$. The first d digits of $[\Psi^2 V]_m$ vanish iff $\deg V < m - d$ (as $\Psi^2 V(t) = (-t)^{m-1} V((t-1)/t)$), i.e. iff the first d entries of $\varphi_\infty(V)$ do; those of $[\Psi V]_m$ vanish iff $(t-1)^d \mid V$ (proof of Proposition 9), i.e. iff those of $\varphi_1(V)$ do. Invertible matrices whose leading d rows have equal kernels for every d differ by a lower-triangular left factor; so the frame readings are $(T_x \varphi_\infty, \varphi_0, T_z \varphi_1)$, up to the unit s_k , with T_x, T_z lower-triangular. Multiplying the reading of c by such a T_c changes Φ_{cd} into $T_c'' \Phi_{cd} (T_d')^{-1}$ ($d \neq c$; T_d', T_c'' the leading $k_d \times k_d$ block of T_d and the trailing diagonal block of T_c) and changes Φ_{cc} , i.e. it is a combination of moves (a), (c). By (a) we may use the readings $(\varphi_\infty, \varphi_0, \varphi_1)$. Then the column of level j of d is the offset part of the unique V , $\deg V < m$, whose cell digits (the top k_x coefficients, the coefficients of $t^0, \dots, t^{k_y-1}$, those of $(t-1)^0, \dots, (t-1)^{k_z-1}$) are 1 at (d, j) and 0 elsewhere; $X0$ reads the coefficient of t^{m-2-k} , the first offset rows of y those of t^{k_y}, t^{k_y+1} , and $Z0, Z1$ those of $(t-1)^k, (t-1)^{k+1}$. Let $\bar{t} = t - 1$, $\epsilon = (-1)^k$ and $\beta_i = \binom{k-1+i}{i}$, the coefficients of $(1-t)^{-k}$.

For $r = 2$ the degree bound, the vanishing orders at 0 and 1 (for $\tilde{x}, \tilde{y}$ one more factor $\bar{t}$, as $Z0 = 0$) and one normalization give $x_k : t^{k+1} \bar{t}^k, \tilde{x} : t^{k+1} \bar{t}^{k+1}, y_k : \epsilon t^k \bar{t}^k, \tilde{y} : -\epsilon t^{k-1} \bar{t}^{k+1}$. So $(Y0, Z0, Z1)|x_k = (\epsilon, 1, k+1)$, $(Y0, Z1)|\tilde{x} = (-\epsilon, 1)$, $(X0, Z0, Z1)|y_k = (\epsilon, \epsilon, k\epsilon)$, $(X0, Z1)|\tilde{y} = (-\epsilon, -\epsilon)$, and

$$\chi_1 = \frac{(-\epsilon)(-\epsilon)\epsilon \cdot 1}{1 \cdot \epsilon(-\epsilon)\epsilon} = -1, \quad \chi_2 = ((k+1) - k) \frac{1 \cdot (-\epsilon)}{1 \cdot \epsilon} = -1.$$

For $r = 1$, inverting t^k resp. $\bar{t}^k$ as a power series at the other finite place, the columns are

$$\xi_j : t^k \bar{t}^k \sum_{i \leq j} \beta_i t^{j-i}, \quad \eta_j : \epsilon \bar{t}^k t^{k-1-j} \sum_{i \leq j} \beta_i t^i, \quad \zeta_j : t^k \bar{t}^{k-1-j} \sum_{i \leq j} (-1)^i \beta_i \bar{t}^i,$$

with the entries

	$X0$	$Y0$	$Y1$	$Z0$	$Z1$
ξ_0		ϵ	$-k\epsilon$	1	k
ξ_1		$k\epsilon$	$-(k^2-1)\epsilon$	$k+1$	k^2+k+1
ξ_2		$\epsilon \binom{k+1}{2}$	$-\epsilon k(k-1)(k+2)/2$	$\binom{k+2}{2}$	$(k+2)(k^2+k+2)/2$
η_0, η_1	$\epsilon, k\epsilon$			$\epsilon, (k+1)\epsilon$	$(k-1)\epsilon, (k^2-2)\epsilon$
ζ_0, ζ_1	1, $-k$	$-\epsilon, (k+1)\epsilon$	$(k-1)\epsilon, (2-k^2)\epsilon$		

Hence $d_x = \epsilon$, $R_Y = Y1 + kY0$, $R_Z = Z1 - kZ0$, $\tilde{\zeta} = \zeta_1 + k\zeta_0$, $\tilde{\eta} = \eta_1 - k\eta_0$, $\tilde{\xi} = \xi_2 - (k+1)\xi_1 + \binom{k+1}{2}\xi_0$,

$$R_Y|(\xi_1, \zeta_0, \tilde{\zeta}, \tilde{\xi}) = (\epsilon, -\epsilon, 2\epsilon, -\epsilon), \quad R_Z|(\xi_1, \eta_0, \tilde{\eta}, \tilde{\xi}) = (1, -\epsilon, -2\epsilon, 1), \quad Y0|\tilde{\zeta} = Z0|\tilde{\eta} = \epsilon,$$

and substituting gives $(J_1, \dots, J_5) = (1, -1, 2, 2, 1)$. All entries are integers and all divisors are ± 1 , so this holds for every k and every p . $\square$

The values do not depend on k because the invariants compare consecutive binomial coefficients: χ_2 contains $(k+1) - k = 1$, and J_3, J_4 contain $(k+2) - k = 2$; the rest are signs.

Existence for every k .

Proposition 128 (Existence, $m \equiv 2$). *Let D be a per-prime design for $(p, 2)$ with*

- (V2) $Z0|x_{k-1} = Z0|x_{k-2} = Z0|y_{k-1} = Z0|y_{k-2} = 0$ and $X0|z_{k-3} = Y0|z_{k-3} = 0$;
- (U2) *the following are nonzero modulo p : the entries $Z0|x_k, Z0|y_k, Y0|x_k, Y0|x_{k-1}, Z1|x_{k-1}, X0|y_k, X0|y_{k-1}, X0|z_{k-1}, Y0|z_{k-1}$ and the brackets $[Y0, Z1 | x_{k-2}, x_{k-1}], [X0, Z1 | y_{k-2}, y_{k-1}], [X0, Y0 | z_{k-2}, z_{k-1}]$;*
- (I2) $\chi_1(D) = \chi_2(D) = -1$ in $\mathbb{F}_p$.

Then for every $k \geq 2$ the moves of Lemma 2 turn Φ^F into a digital $(0, 3k+2, 3)$ -net over $\mathbb{F}_p$ that carries D .

Proof. All moves are moves (a)–(c), so every intermediate graph form has unit box minors; each pivot below is nonzero because, given the entries already normalized, it is a box minor or a quotient of two (box in brackets). An entry is *set* when it is made equal to its value in D .

Step 1 (windows). $Y0, Z0, Z1$ on x_{k-2}, x_{k-1}, x_k form an invertible matrix (box $(k-2, k+2, k+2)$); subtracting combinations of these levels from the levels $x_l, l < k-2$, clears the three rows there. Likewise $X0, Z0, Z1$ on y_{k-2}, y_{k-1}, y_k (box $(k+2, k-2, k+2)$), and $X0, Y0$ on $z_l, l < k-2$, with z_{k-2}, z_{k-1} (box $(k+2, k+2, k-2)$). Then subtract multiples of x_k from x_{k-1}, x_{k-2} to clear $Z0$ there (pivot $Z0|x_k$, box $(k, k+1, k+1)$), and likewise in y (box $(k+1, k, k+1)$); now $x_{k-1} = \tilde{x}, y_{k-1} = \tilde{y}$.

Step 2. Scale Φ_{yx} to set $Y0|x_k$ (box $(k, k+2, k)$) and the level x_{k-1} to set $Y0|x_{k-1}$ (box $(k-1, k+2, k+1)$); apply L_z : $Z0 \mapsto \ell Z0, Z1 \mapsto \ell' Z1 + \lambda Z0$, to set $Z0|x_k, Z1|x_{k-1}$ (box $(k-1, k+1, k+2)$) and $Z1|x_k$.

Step 3. Scale Φ_{xy} to set $X0|y_k$ (box $(k+2, k, k)$), the level y_{k-1} to set $X0|y_{k-1}$ (box $(k+2, k-1, k+1)$), and Φ_{zy} to set $Z0|y_k$ (box $(k+1, k, k+1)$).

Step 4 (forced entries). This is where the invariants enter. All entries read by χ_1, χ_2 are now set except $Z1|y_{k-1}, Z1|y_k$. By Lemma 127 and (I2) the current χ_1, χ_2 equal those of D ; as χ_1 is a nonzero multiple of $Z1|y_{k-1}$ and χ_2 is affine with nonzero slope in $Z1|y_k$, these entries already have their values in D , and no move is needed (or possible) to set them.

Step 5. Replace x_{k-2} by $a x_{k-2} + b x_{k-1}$ so as to set $Y0|x_{k-2}, Z1|x_{k-2}$; the matrix $[Y0, Z1 | x_{k-2}, x_{k-1}]$ is invertible (box $(k-2, k+2, k+2)$, divided by $Z0|x_k$), and $Z0$ stays 0 on x_{k-2} . Afterwards the bracket is a times its old value and equals that of D , nonzero by (U2); so $a \neq 0$ and this is a move (c). The same for y_{k-2} (box $(k+2, k-2, k+2)$).

Step 6. Scale Φ_{xz}, Φ_{yz} to set $X0|z_{k-1}, Y0|z_{k-1}$ (boxes $(k+2, k+1, k-1), (k+1, k+2, k-1)$), and replace z_{k-2} by $a z_{k-2} + b z_{k-1}$ to set $X0|z_{k-2}, Y0|z_{k-2}$ (box $(k+2, k+2, k-2)$; $a \neq 0$ as in Step 5).

Step 7. By move (a), give each coordinate's prescribed rows their values in D on the window of its own cell (0 above it) and its other offset rows the value 0 on its own cell.

Steps 2–6 only combine window levels, so the prescribed rows still vanish above the windows (as Definition 126(i) requires), and the graph form carries D . Lemma 1 completes the proof. $\square$

Proposition 129 (Existence, $m \equiv 1$). *Let D be a per-prime design for $(p, 1)$ with*

- (V1) $Y0, Z0$ vanish on x_{k-2}, x_{k-3} ; $X0, Z0$ on y_{k-3} ; $X0, Y0$ on z_{k-3} ;
- (U1) *the following are nonzero modulo p : the entries $Y0|x_k, Z0|x_k, X0|y_{k-1}, Z0|y_{k-1}, X0|z_{k-1}, Y0|z_{k-1}, Y1|x_{k-2}, Z1|y_{k-3}, Y1|z_{k-3}$ and the brackets*
 $[Y0, Z0 | x_{k-1}, x_k], [X0, Z0 | y_{k-2}, y_{k-1}], [X0, Y0 | z_{k-2}, z_{k-1}],$
 $[Y1, Z1 | x_{k-3}, x_{k-2}], [Y1, Y0 | x_k, z_{k-1}], [Z1, Z0 | x_k, y_{k-1}];$
- (II) $(J_1, \dots, J_5)(D) = (1, -1, 2, 2, 1)$ in $\mathbb{F}_p$.

Then for every $k \geq 3$ the moves of Lemma 2 turn Φ^F into a digital $(0, 3k+1, 3)$ -net over $\mathbb{F}_p$ that carries D .

Proof. As for Proposition 128; in each solve below, $a \neq 0$ because the corresponding bracket of D is nonzero (U1).

Step 1 (windows). Clear $Y0, Y1, Z0, Z1$ on $x_l, l < k-3$ (box $(k-3, k+2, k+2)$), $X0, Z0, Z1$ on $y_l, l < k-3$ (box $(k+2, k-3, k+2)$), and $X0, Y0, Y1$ on $z_l, l < k-3$ (box $(k+2, k+2, k-3)$). Then clear $Y0, Z0$ on x_{k-2}, x_{k-3} with x_{k-1}, x_k (box $(k-1, k+1, k+1)$), $X0, Z0$ on y_{k-3} with y_{k-2}, y_{k-1} (box $(k+2, k-2, k+1)$), and $X0, Y0$ on z_{k-3} with z_{k-2}, z_{k-1} (box $(k+2, k+1, k-2)$).

Step 2 ($X0, Y0, Z0$). Scale Φ_{yx}, Φ_{zx} to set $Y0|x_k, Z0|x_k$ (boxes $(k, k+1, k), (k, k, k+1)$) and replace x_{k-1} by $ax_{k-1} + bx_k$ to set $Y0|x_{k-1}, Z0|x_{k-1}$ (box $(k-1, k+1, k+1)$). In the same way set $X0|y_{k-1}, Z0|y_{k-1}$ by Φ_{xy}, Φ_{zy} and $X0|y_{k-2}, Z0|y_{k-2}$ by $y_{k-2} \mapsto ay_{k-2} + by_{k-1}$ (boxes $(k+2, k-1, k), (k+1, k-1, k+1), (k+2, k-2, k+1)$), and $X0|z_{k-1}, Y0|z_{k-1}, X0|z_{k-2}, Y0|z_{k-2}$ by Φ_{xz}, Φ_{yz} and z_{k-2} (boxes $(k+2, k, k-1), (k+1, k+1, k-1), (k+2, k+1, k-2)$).

Step 3 ($Y1, Z1$). Apply $L_y: Y1 \mapsto aY1 + bY0$ to set $Y1|x_k, Y1|z_{k-1}$ (matrix $[Y1, Y0|x_k, z_{k-1}]$, box $(k, k+2, k-1)$), and $L_z: Z1 \mapsto cZ1 + dZ0$ to set $Z1|x_k, Z1|y_{k-1}$ (box $(k, k-1, k+2)$).

Step 4 (*forced entries*). All entries read by $J_1, \dots, J_4$ are now set except $Y1|x_{k-1}, Z1|x_{k-1}, Y1|z_{k-2}, Z1|y_{k-2}$, and $J_1, \dots, J_4$ are affine with nonzero slope in one of them each (through $R_Y|\xi_1, R_Z|\xi_1, R_Y|\zeta, R_Z|\eta$). By Lemma 127 and (I1) they already have their values in D .

Step 5. Scale the levels $z_{k-3}, y_{k-3}, x_{k-2}$ to set $Y1|z_{k-3}, Z1|y_{k-3}, Y1|x_{k-2}$ (boxes $(k+2, k+2, k-3), (k+2, k-3, k+2), (k-2, k+2, k+1)$). Now $\tilde{\xi} = \xi_2$, as $Y0, Z0$ vanish on x_{k-2} , and J_5 is affine with nonzero slope in $Z1|x_{k-2}$; by Lemma 127 and (I1) this entry has its value in D . Finally replace x_{k-3} by $ax_{k-3} + bx_{k-2}$ to set $Y1|x_{k-3}, Z1|x_{k-3}$ (box $(k-3, k+2, k+2)$).

Step 6 is *Step 7* of Proposition 128. $\square$

Which of these conditions are necessary? Given (V1) resp. (V2), each quantity in (U1), (U2) is, up to sign and factors from the same list, the box minor of the box named where it is used, for every graph form carrying D ; so (U1), (U2) are necessary for a net carrying D . (I1) and (I2) hold, by Lemma 127, for every design carried at a single k by a graph form obtained from Φ^F by the moves. Only (V1), (V2) are hypotheses of Propositions 129 and 128 that are not shown to be necessary. Hence, for a design satisfying (V1) resp. (V2), reachability from the frame does not depend on k ($k \geq 3$ resp. $k \geq 2$). With the checks below, Propositions 128 and 129 prove by hand that the per-prime nets exist for every k .

Separation for every k . Let $g_0 = p^{m-k-2} = \varpi/p$, one p -th of the fine unit ϖ of Section 5.1. A point with cells n_c , skeleton digits S_c and inner digits ρ_c has $X_c = g_0(pn_c + \rho_c) + \theta_c$ (c full) resp. $X_c = g_0(p(pn_c + S_c) + \rho_c) + \theta_c$ (c skeleton), where $0 \leq \theta_c < g_0$ comes from the digits after the inner digit.

Definition 130 (Per-prime relaxation). Let D be a per-prime design for (p, r) and $B \in \mathbb{Z}_{>0}^3$ a search radius. A *configuration* is a pair (E, j) of a cell difference $E \in \mathbb{Z}^3 \setminus \{0\}$, $|E_c| \leq B_c$, and carry depths $j_c \in \{0, \dots, L_c - 1\}$, with $j_c = 0$ if $E_c = 0$. Put $\Delta_{d,0} = E_d$, $\Delta_{d,i} = \text{sgn}(E_d) [i \leq j_d]$ for $1 \leq i < L_d$, and let σ_c resp. $\iota_c \in \{0, \dots, p-1\}$ be the residue of $\sum_{d,i} R|d^{(i)} \Delta_{d,i}$, where R is the skeleton row resp. the row of the inner digit of c . With $\mathcal{A}(v) = \{v, v-p\}$ for $v \neq 0$, $\mathcal{A}(0) = \{0\}$, and $\varepsilon_c = 0$ if $E_d = 0$ for all $d \neq c$, $\varepsilon_c = 1$ otherwise, let

$$t_c = \min_{\beta \in \mathcal{A}(\iota_c)} (|pE_c + \beta| - \varepsilon_c)^+ \quad (c \text{ full}), \quad t_c = \min_{\alpha \in \mathcal{A}(\sigma_c), \beta \in \mathcal{A}(\iota_c)} (|p(pE_c + \alpha) + \beta| - \varepsilon_c)^+ \quad (c \text{ skeleton}).$$

A *certificate* is a pair (T, B) with $T \leq t_x^2 + t_y^2 + t_z^2$ for every configuration, $B_c < p$ for all c , $T \leq p^2 B_c^2$ for full c , and $B_c = 1, T \leq p^4$ for skeleton c .

Here E plays the role of the step E and j that of the carry depths of Lemma 4; α and β run over the two possible changes of the skeleton digit and of the inner digit.

Proposition 131 (Separation). *Let p be odd, D a per-prime design for (p, r) with a certificate (T, B) , and $k \geq 3$ ($r = 1$) resp. $k \geq 2$ ($r = 2$). Every graph form over $\mathbb{F}_p$ with depths $\mathbf{k}$ carrying D , net or not, has $\|X(w) - X(v)\|_{\text{torus}}^2 \geq Tg_0^2$ for all indices $v \neq w$ (integer coordinates on the torus of side N). Hence $\delta N^{1/3} \geq \sqrt{T} p^{-5/3}$ ($r = 1$) resp. $\sqrt{T} p^{-4/3}$ ($r = 2$).*

Proof. Let E_c be the centred residue of $n_c(w) - n_c(v)$ modulo p^{k_c} ; as the cells are the index, $E \neq 0$. The proof of Lemma 25(i) only uses $X_c = gn_c + \theta$, $0 \leq \theta < g$, $N = gp^{k_c}$ and the centring; with $g = pg_0$ (full) resp. p^2g_0 (skeleton) the toroidal distance in coordinate c is at least $(|E_c| - 1)g$. So if $|E_c| > B_c$ for a full c , or $|E_c| \geq 2$ for a skeleton c , the claim follows from $T \leq p^2 B_c^2$ resp. $T \leq p^4$.

Otherwise $|E_c| \leq B_c < p$ for all c . For $E_c \neq 0$ the digits of $n_c(w)$ and $n_c(v)$ differ, modulo p , by E_c on the last level, by $\text{sgn } E_c$ on the next $j'_c \geq 0$ levels (a carry chain, cf. Lemma 25(ii)), and not above; with $j_c = \min(j'_c, L_c - 1)$, (E, j) is a configuration. As the prescribed rows have the coefficients of D on the windows and 0 above, the skeleton and inner digits of c change by σ_c resp. ι_c modulo p , and since they

p	5	7	11	13	17	19	23	29	31	37
$m \equiv 1$	.6306	.7407	.8544	.8569	.8890	.9023	.9354	.9767	.9608	.9738
$m \equiv 2$	.5098	.6380	.8426	.8599	.8286	.8363	.9695	.9839	.9752	.9520
p	41	43	47	53	59	61	67	71	73	79
$m \equiv 1$	.9530	.9903	1.0092	1.0150	1.0242	1.0137	.9972	1.0207	1.0257	1.0352
$m \equiv 2$	1.0032	1.0034	.9962	.9733	1.0150	1.0079	–	–	–	1.0210

TABLE 10. Certified lower bounds for $\delta N^{1/3}$ of the per-prime designs of Remark 58, for every $m = 3k + 1 \geq 10$ resp. $m = 3k + 2 \geq 8$ (that is, $k \geq 3$ resp. $k \geq 2$, as Propositions 129, 128 and 131 require; the finitely many smaller m are covered by the frame nets of Remark 72). They are $\sqrt{T_p} p^{-5/3}$ resp. $\sqrt{T_p} p^{-4/3}$ for the integers T_p of the formal statements, truncated (not rounded) to four digits. For $m \equiv 2$ there is no per-prime design at $p = 67, 71, 73$ (–); there Remark 55 gives .717–.738 ($\rho = 4$).

lie in $[0, p)$, $S_c(w) - S_c(v) \in \mathcal{A}(\sigma_c)$ and $\rho_c(w) - \rho_c(v) \in \mathcal{A}(\iota_c)$. Further $|\theta_c(w) - \theta_c(v)| < g_0$, with equality $\theta_c(w) = \theta_c(v)$ if $\varepsilon_c = 0$: the deeper digits of c have coefficient 0 on the cell of c (Definition 126(ii)), and no other cell changes. Hence $X_c(w) - X_c(v) \equiv g_0 y_c + \theta_c(w) - \theta_c(v) \pmod{N}$ with $y_c = pE_c + \beta$ resp. $p(pE_c + \alpha) + \beta$ for some $\alpha \in \mathcal{A}(\sigma_c)$, $\beta \in \mathcal{A}(\iota_c)$; as $|y_c| < 3p^2$ and $N/g_0 = p^{k+2} \geq p^4$, the toroidal distance is at least $g_0(|y_c| - \varepsilon_c)^+ \geq g_0 t_c$. Summing squares gives $\|X(w) - X(v)\|_{\text{torus}}^2 \geq g_0^2 \sum_c t_c^2 \geq T g_0^2$. Finally $\delta N^{1/3} \geq \sqrt{T} g_0 N^{-2/3} = \sqrt{T} p^{(m-3k-6)/3}$. $\square$

The relaxation keeps only the cell difference of a pair, its carry depths on the windows and the two possible changes of each prescribed digit. Nothing in it depends on k , so one finite computation covers every m . At large p the minimum in the relaxation is attained by short vectors of the skeleton lattice, reduced by the inner digits and the deeper digits.

Remark 132 (Digital shifts). Proposition 131 holds verbatim, with the same certificate (T, B) , for every digital shift (Definition 7) of every graph form carrying D . So the constants of Table 10 hold for every digitally shifted per-prime net.

Proof. By Lemma 67 the shifted point set is indexed by its own cells n , one point per cell, and its offsets are $\Phi n + \gamma$, with the blocks Φ of the unshifted graph form and a constant γ . Each coordinate still has the form $X_c = g_0(pn_c + \rho_c) + \theta_c$ resp. $g_0(p(pn_c + S_c) + \rho_c) + \theta_c$ with $S_c, \rho_c \in [0, p)$ and $0 \leq \theta_c < g_0$. So the first paragraph of the proof of Proposition 131 applies, and E and the carry chains are those of the shifted cells, so (E, j) is a configuration. The prescribed rows applied to $n(w) - n(v)$ give $S_c(w) - S_c(v) \equiv \sigma_c$ and $\rho_c(w) - \rho_c(v) \equiv \iota_c \pmod{p}$, since γ cancels. As both digits lie in $[0, p)$, the differences lie in $\mathcal{A}(\sigma_c)$ resp. $\mathcal{A}(\iota_c)$. A shift may change which of the two representatives occurs, but t_c is the minimum over both. If $\varepsilon_c = 0$, the deeper digits of c are given by rows with coefficient 0 on the cell of c (Definition 126(ii)) plus the same constants, so $\theta_c(w) = \theta_c(v)$; otherwise $|\theta_c(w) - \theta_c(v)| < g_0$ as before. The rest of the proof is unchanged. $\square$

The finite checks. (1) *Certificates.* For each of the 37 designs, (T_p, B) with T_p as in Table 10, $B_c = \lceil \sqrt{T_p}/p \rceil \leq 20$ for full and $B_c = 1$ for skeleton coordinates is a certificate (at most $1.4 \cdot 10^4$ configurations per design). This check is evaluated by `decide` in the Lean kernel and, with the formalized Proposition 131, gives the separation bounds. Each T_p is attained by a configuration (also checked in the kernel), so it is the exact value of the relaxation. Table 10 lists $\sqrt{T_p} p^{-5/3}$ resp. $\sqrt{T_p} p^{-4/3}$, truncated. (2) *Existence conditions.* (V1), (U1), (I1) for the 20 designs with $r = 1$ and (V2), (U2), (I2) for the 17 designs with $r = 2$ hold in exact arithmetic modulo p ; this is also checked in the Lean kernel.

p	R	$R x^{(\cdot)}$	$R y^{(\cdot)}$	$R z^{(\cdot)}$	p	R	$R x^{(\cdot)}$	$R y^{(\cdot)}$	$R z^{(\cdot)}$
$m \equiv 1$: rows $X0, Y0 = S_y, Y1, Z0 = S_z, Z1$									
5	$X0$	(0, 0, 0, 0)	(-1, -1, 0)	(1, 1, 0)	7	$X0$	(0, 0, 0, 0)	(-1, 1, 0)	(1, -1, 0)
	$Y0$	(2, 1, 0, 0)	(0, 0, 0)	(-2, 0, 0)		$Y0$	(3, 1, 0, 0)	(0, 0, 0)	(-3, 0, 0)
	$Y1$	(0, 2, -1, -1)	(0, 0, 0)	(1, -1, 1)		$Y1$	(-3, -3, -1, 1)	(0, 0, 0)	(-3, 1, -1)
	$Z0$	(-1, -1, 0, 0)	(1, 0, 0)	(1, 0, 0)		$Z0$	(-2, 0, 0, 0)	(-1, 0, 0)	(2, 0, 0)
	$Z1$	(0, -2, -1, 1)	(1, -1, 1)	(0, 0, 0)		$Z1$	(0, -3, -2, -1)	(-1, -1, 1)	(0, 0, 0)
11	$X0$	(-1, 0, 0, 0)	(-1, 1, 0)	(-1, -1, 0)	13	$X0$	(-1, 0, 0, 0)	(1, 1, 0)	(-1, -1, 0)
	$Y0$	(-2, 0, 0, 0)	(0, 0, 0)	(2, 0, 0)		$Y0$	(5, 1, 0, 0)	(0, 0, 0)	(-1, 0, 0)
	$Y1$	(2, -3, -1, 1)	(0, 0, 0)	(-1, -1, 1)		$Y1$	(-5, -2, 1, -1)	(0, 0, 0)	(0, 1, 1)
	$Z0$	(-4, -1, 0, 0)	(1, 0, 0)	(4, 0, 0)		$Z0$	(-3, 0, 0, 0)	(1, 0, 0)	(0, 0, 0)
	$Z1$	(0, 1, -4, 1)	(1, 1, -1)	(0, 0, 0)		$Z1$	(0, -2, -2, 1)	(-1, 1, 1)	(0, 0, 0)
17	$X0$	(-1, 0, 0, 0)	(-1, -1, 0)	(1, 1, 0)	19	$X0$	(-1, 0, 0, 0)	(-1, -1, 0)	(-1, 1, 0)
	$Y0$	(3, 1, 0, 0)	(-1, 0, 0)	(-1, 0, 0)		$Y0$	(4, 1, 0, 0)	(4, 0, 0)	(-1, 0, 0)
	$Y1$	(-3, 0, -1, -1)	(1, 0, 0)	(2, -1, 1)		$Y1$	(-4, -7, 1, -1)	(-4, 0, 0)	(2, 1, 1)
	$Z0$	(6, 0, 0, 0)	(1, 0, 0)	(0, 0, 0)		$Z0$	(6, 1, 0, 0)	(6, 0, 0)	(0, 0, 0)
	$Z1$	(-6, -2, -2, 1)	(-2, 1, -1)	(0, 0, 0)		$Z1$	(0, -8, 5, -1)	(-1, 1, -1)	(0, 0, 0)
23	$X0$	(0, 0, 0, 0)	(-1, 1, 0)	(1, 1, 0)	29	$X0$	(0, 0, 0, 0)	(-1, -1, 0)	(-1, -1, 0)
	$Y0$	(3, 0, 0, 0)	(-3, 0, 0)	(-3, 0, 0)		$Y0$	(3, 1, 0, 0)	(0, 0, 0)	(3, 0, 0)
	$Y1$	(0, -5, -1, -1)	(0, 0, 0)	(1, -1, 1)		$Y1$	(0, 3, -1, -1)	(0, 0, 0)	(1, -1, 1)
	$Z0$	(9, -1, 0, 0)	(-9, 0, 0)	(-9, 0, 0)		$Z0$	(9, 1, 0, 0)	(1, 0, 0)	(9, 0, 0)
	$Z1$	(-9, 6, -1, 1)	(10, 1, -1)	(9, 0, 0)		$Z1$	(0, -2, 9, -1)	(-1, 1, -1)	(0, 0, 0)
31	$X0$	(0, 0, 0, 0)	(-1, 1, 0)	(-1, -1, 0)					
	$Y0$	(3, 1, 0, 0)	(0, 0, 0)	(2, 0, 0)					
	$Y1$	(0, -15, -1, -1)	(0, 0, 0)	(-1, 1, -1)					
	$Z0$	(-11, 0, 0, 0)	(1, 0, 0)	(-11, 0, 0)					
	$Z1$	(0, -14, 3, -1)	(1, 1, -1)	(0, 0, 0)					
$m \equiv 2$: rows $X0, Y0, Z0 = S_z, Z1$									
5	$X0$	(-2, 0, 0)	(2, -1, -1)	(-1, 1, 0)	7	$X0$	(2, 0, 0)	(3, -1, 0)	(-1, 1, 0)
	$Y0$	(2, -1, 0)	(-1, 0, 0)	(-1, 0, 0)		$Y0$	(1, -1, 0)	(-1, 0, 0)	(-1, 0, 0)
	$Z0$	(2, 0, 0)	(-1, 0, 0)	(0, 0, 0)		$Z0$	(3, 0, 0)	(2, 0, 0)	(0, 0, 0)
	$Z1$	(-2, -1, 1)	(0, 2, 0)	(0, 0, 0)		$Z1$	(2, -1, 1)	(2, 1, -1)	(0, 0, 0)

TABLE 11. The 11 per-prime designs of Appendix C that the coverage of every prime base needs (Remark 72; fixed data of the formalization, Table 15). Rows are named as in the appendix: $X0$ is the first offset row of x , $Y1$ the second offset row of y , and so on. For each prescribed row R the three tuples are $(R|d^{(0)}, \dots, R|d^{(L_d-1)})$ for $d = x, y, z$, the coefficients on the levels $k_d-1, k_d-2, \dots$ of the cell of d (so $R|x^{(0)}$ is the coefficient on x_k); entries on the cell of the row's own coordinate are diagonal entries. With the certificates T_p they give the corresponding entries of Table 10.

APPENDIX D. TABLES

This appendix collects data behind statements in the text: the certified bound of Theorem 45 against exact separations of $\mathcal{P}_{2,q}$ (Table 12, dimension three, $m \equiv 0 \pmod{3}$), the vectors κ of Table 8 (Table 13), and the seeds of the lift of Section 7 (Table 14).

APPENDIX E. PICTURES

Figure 16 shows slabs $n_z = \text{const}$ of cells of the nets $\mathcal{P}_{k,q}$; for large N only the points shown are generated, each directly from its cell.

q	4	5	6	7	8	9	10	11	12	13	16
certified $c(q)$, all $k \geq 2$	.4330	.6324	.7453	.8329	.8750	.8888	.9000	.9090	.9166	.9230	.9375
exact c of $\mathcal{P}_{2,q}$	.5964	.7322	.8183	.8578	.8753	.8891	.9001	.9091	.9167	.9231	.9375

TABLE 12. First row: the lower bound $c(q)$ of Theorem 45, certified for every $k \geq 2$ (truncated). Second row: the exact normalized toroidal minimum distance $c = \delta N^{1/3}$ of $\mathcal{P}_{2,q}$ ($m = 6$), computed by an exact neighbour-cell scan of all N points (truncated). The cubic lattice has $c = 1$.

s	p	$\kappa = (\kappa_1, \dots, \kappa_{s-1})$
3	1009	(194, 927)
3	10007	(7263, 512)
3	996001°	(386012, 289649)
3	1000003	(480737, 456115)
3	100000007	(35938453, 38104672)
3	10002435263°	(6351393446, 2689022248)
4	1009	(60, 942, 427)
4	10007	(7789, 6790, 2749)
4	1000003	(906828, 842915, 540337)
4	1006301°	(488116, 625468, 981379)
4	100000007	(75429390, 71818190, 91631379)
4	10040205517°	(5572254466, 6450656159, 2352780990)
5	1009	(97, 590, 862, 326)
5	10007	(4287, 291, 6535, 8776)
5	1000003	(814550, 377607, 542427, 841650)
5	1025909°	(448199, 390598, 84034, 101647)
5	100000007	(10605878, 95749095, 74073896, 86459444)
5	10123347709°	(9581363571, 7859938370, 4587520169, 3357307811)
6	1009	(1006, 434, 303, 379, 336)
6	10007	(3959, 5172, 482, 4657, 4647)
6	1000003	(898060, 73290, 548128, 694268, 723193)
6	1033493°	(692761, 511602, 86731, 102710, 280758)
6	100000007	(38304664, 72775107, 78968817, 72577778, 12520865)
6	10136355487°	(67990745, 4455545937, 5539174410, 2022757295, 4530764856)
7	1009	(364, 903, 266, 189, 5, 32)
7	10007	(5416, 7655, 1613, 8456, 1914, 5199)
7	1000003	(219819, 595664, 349551, 501112, 415995, 657791)
7	1138273°	(977285, 895703, 570465, 140992, 1065215, 1028731)
7	100000007	(92652368, 47992472, 45324136, 56540409, 38423666, 54604852)
7	10660100951°	(8069839213, 5273863583, 6436724208, 2404140741, 1832389919, 1010034693)
8	1009	(135, 889, 105, 367, 892, 986, 321)
8	10007	(6121, 8133, 3883, 760, 6795, 3843, 1579)
8	1000003	(59285, 987228, 779534, 118614, 216758, 621532, 892678)
8	1071337°	(516035, 106020, 316101, 49825, 432533, 18773, 319711)
8	100000007	(21187390, 39864196, 90193868, 30228904, 687983, 29614392, 68077957)
8	11556622703°	(8648308921, 2075022356, 3012831926, 5980481396, 3082196750, 808709099, 2210083677)

TABLE 13. The vectors κ behind Table 8: for the searched κ at $p = 1009, 10007, 10^6+3, 10^8+7$, and, at the primes p' (marked °), for the vectors obtained by rounding a randomly rotated copy of a root lattice to an integer matrix of determinant p' (Table 8). The skeleton lattice is $\Lambda_\kappa = \{a \in \mathbb{Z}^s : a_z \equiv \sum_d \kappa_d a_{x_d} \pmod{p}\}$ (Proposition 102).

b	$m \bmod 3$	M	rows of A_y	rows of A_z	(τ_y, τ_z)
2	0	9	135, 45, 3, 498, 194, 440, 335, 219, 392	481, 146, 111, 183, 386, 325, 223, 361, 358	(414, 211)
2	1	10	209, 382, 805, 151, 314, 829, 673, 883, 1010, 361	947, 597, 575, 978, 901, 1020, 856, 754, 73, 687	(570, 524)
2	2	11	983, 1182, 492, 1089, 1674, 1177, 538, 1803, 1473, 939, 333	701, 54, 431, 771, 1929, 1550, 1860, 1141, 1802, 734, 1278	(62, 919)
3	0	6	404, 542, 48, 70, 11, 52	316, 557, 650, 282, 551, 247	(626, 448)
3	1	7	1495, 822, 993, 989, 391, 477, 1366	1192, 1811, 657, 430, 705, 1663, 87	(614, 1328)
3	2	8	2902, 3540, 5732, 4163, 4228, 2472, 696, 593	5695, 1981, 2605, 6323, 2624, 3996, 209, 3923	(703, 1559)

TABLE 14. The seeds of Theorem 64, at the seed resolutions m_0 of Table 5 (m_0 is the number of digits of the seed). With the index $u \in \mathbb{F}_b^{m_0}$ taken to be the vector of x -digits, the shifted seed is $\{(u, A_y u + \tau_y, A_z u + \tau_z) : u \in \mathbb{F}_b^{m_0}\}$ (digit vectors, digit 0 the most significant, addition modulo b without carries) and the unshifted one has the generator matrices (I, A_y, A_z) . Row d of A_y is printed as the integer $\sum_j (A_y)_{dj} b^{m_0-1-j}$, the shift τ_y as $\sum_d \tau_{y,d} b^{m_0-1-d}$, and likewise for z .

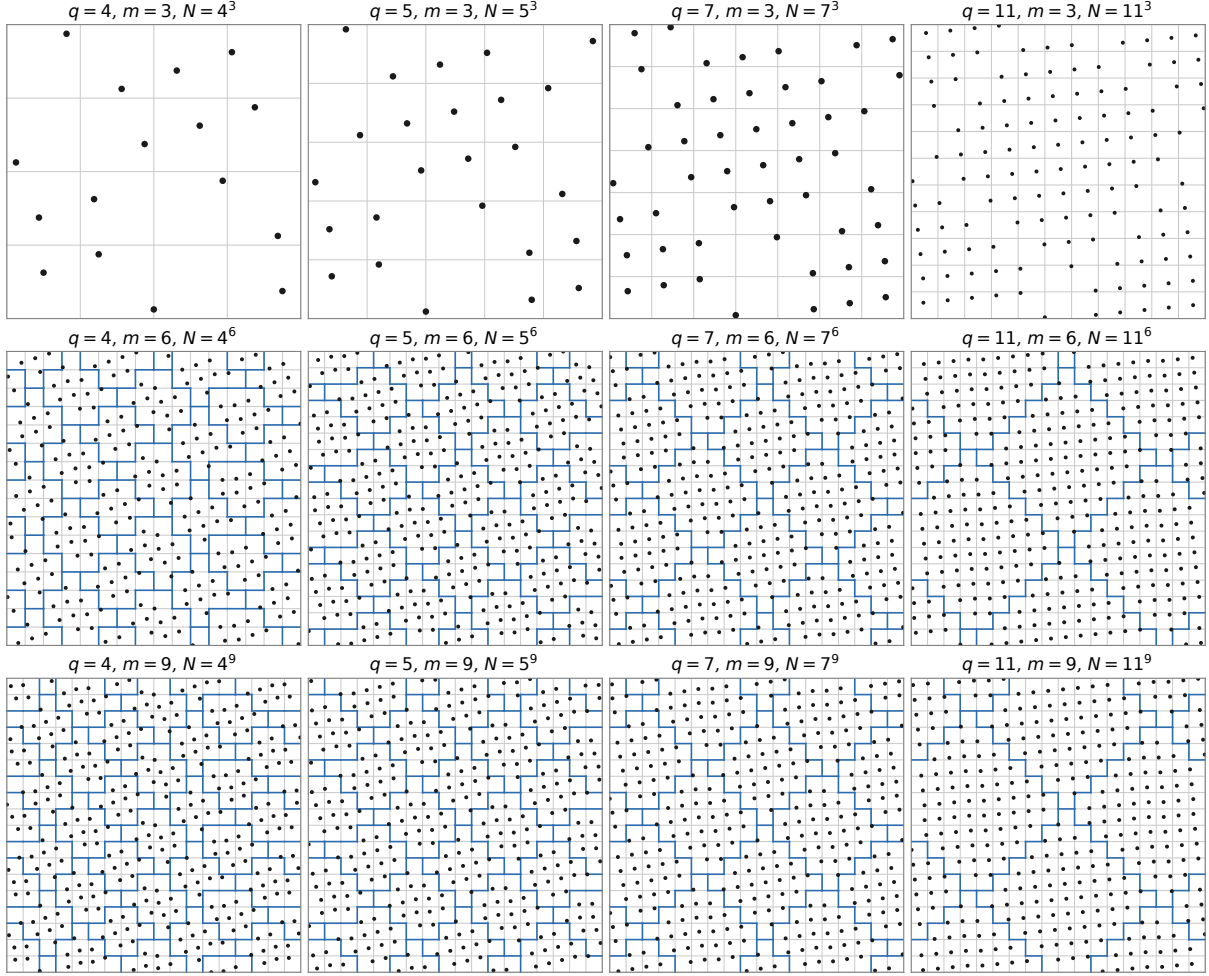


FIGURE 16. One slab of cells of $\mathcal{P}_{k,q}$ for $q = 4, 5, 7, 11$ and $m = 3, 6, 9$: the points with z -cell $n_z = \lfloor q^k/2 \rfloor$ and (x, y) -cells in a $W \times W$ window ($W = q$ for $m = 3$, i.e. the whole slab; $W = 16$ for $q = 4, m = 6$; $W = 18$ otherwise; so 16 to 324 points), xy -projection in cell units (grey: cell boundaries). Blue: slip lines, i.e. cell edges across which the (x, y) part of the step between the two points differs from that of $(I + M/q)e$ by more than half a cell (not drawn for $k = 1$, where Proposition 43 does not apply). The patches of the tilted square lattice are a few cells wide for $q = 4, 5$ and grow with q .

APPENDIX F. FORMAL VERIFICATION

Method. The formalization uses Lean 4 [13], toolchain `v4.35.0-rc3`, with the matching Mathlib [44], and forms one Lake project with one statement library: 616 theorem statements in twelve statement files, one for each part of the paper (Table 15). The statement files contain no proofs; besides Mathlib they import only the definition modules of the project, which define the objects (nets from their generator matrices or graph forms, designs and searched data as explicit constants), so that statements and proofs use the same definitions. The proofs are in separate modules, and a solution file proves every statement under its name. Every proof is checked by the Lean kernel. The tool Comparator, with one configuration that lists the 616 theorems, checks that the proved theorems are exactly those of the statement library and use only the permitted axioms, and re-checks the proofs with the Lean kernel and with a second, independent kernel (NanoDa). Both kernels accept all 616 theorems. The only axioms used are `propext`, `Classical.choice` and `Quot.sound`; `native_decide` is not used, and finite certificates are evaluated by `decide` in the kernel. Some proofs were reorganized for formalization (for instance, finite case splits replace the case analyses of Theorem 46 and Proposition 103); the statements are those of the text.

Theorem A as a self-contained entry. Theorem A also forms a separate entry in the format of the Palomar collection of formalizations: a statement file of 438 lines that imports only Mathlib, copies verbatim the 43 definitions that the statement reaches, and states Theorem A together with three theorems that justify the data defined by choice: the columns of Definition 23 are the only family with the properties required there, the positive generator γ_j of Lemma 20 is unique, and the net of Definition 14 exists and does not depend on the choices made in its construction (the reduction modulo q and the solution of the residual problem, Propositions 12 and 13). Its solution derives the four theorems from the library, and Comparator checks the entry separately.

Blueprint. A blueprint, made with `leanblueprint`, presents the results of the paper in its words, with their proofs, links every formalized result to the Lean declarations that prove it, and shows the dependency graph. The developments are in the repository <https://github.com/lgruen/separated-nets-lean>; its release v1.0.0 accompanies this version of the paper and is archived at Zenodo.

What is formalized. Every theorem, proposition, lemma and corollary of the paper, every definition except Definition 3 (which only introduces names), and the proved statements of the remarks listed in Table 15 are formalized, apart from the finite computations listed below.

Cited theorems. Two formalized results use classical theorems that are not in our version of Mathlib; these theorems are not formalized here, and enter as explicit hypotheses. (1) The design U_s (Remark 24): the constant 1 in $a_s \leq e^{(1+o(1))s^2}$ is proved from the prime number theorem $\psi(x) \sim x$ [21, 12]; everything else is unconditional, including $(s-1)\psi(s-2) \leq \log a_s \leq (s-1)\psi(s-2) + s \log 2$ for $s \geq 6$ (a consequence of the bounds $L_s \leq a_s \leq L_s(s^2 + 2^{s-2})$ of Remark 24, as $s^2 + 2^{s-2} \leq 2^s$ for $s \geq 6$) and $\log a_s = \Theta(s^2)$ with explicit constants from Chebyshev's bounds. (2) Proposition 100: parts (i)–(iii) with Hajós's theorem [22] and Keller's property for $s \leq 7$ [49, 1] as hypotheses; part (iv) unconditionally, except that its strict inequalities for $s = 2, 3$ use the optimal packing bounds (Thue's for $s = 2$ [9, Ch. 1], Hales's for $s = 3$ [23]) as hypotheses. Some statements of the text are consequences of cited theorems that are neither formalized nor used as hypotheses: Niederreiter's discrepancy bound [46] (Remark 66); the optimality of the range of q [39, Cor. 2] (after Theorem A and Lemma 10); the bound $s \leq 3$ in base two [46, Cor. 5.11] (Remark 59); the growth $\text{lcm}(1, \dots, s-3) = e^{(1+o(1))s}$ after Proposition 90 (the prime number theorem); and $K(F) \geq s^{1-O(1/\log \log s)}$ (in particular $K(F) \geq s^{1-o(1)}$) after Theorem 92, a consequence of Wigert's divisor bound [25, Thm. 317], whereas the div^* inequality of Theorem 92 itself is formalized.

Checked by scripts, not in Lean. By decision, finite computations whose printed values no formalized result needs are checked by the scripts of Appendix G, and, where Section 14 says so, by a second implementation, not in Lean:

- Theorem 64(1), both at the resolutions below the certificate resolution L (the exact minimum distances of the explicitly shifted nets) and beyond it (the certificate v_L^* of the shifted net, which the formal statement of (1) beyond L takes as a hypothesis), and the entries .4699 and .2586 of column (2) of Table 5. Lean proves parts (2) and (3) for every $m \geq 1$, with their constants, the nets of the theorem (seeds, chains and $t = 0$ at every resolution) and the certificates v_L° , checked in the kernel, and the lift theory (Definition 60, Lemmas 61, 62 and 63) in general;
- the values $a_4^*, \dots, a_{10}^*$ of Table 3 and the base thresholds derived from them after Theorem A, and the running time of the algorithm of Definition 23;
- the thresholds and scans of Tables 6 and 7, including the bound $\delta N^{1/s} \geq 0.8$ of Proposition 84(2) and the thresholds stated after Proposition 81; the deficits, finite maxima and $t = 0$ completions that Propositions 81 and 84 state are formalized;
- the values labelled *computed* (Section 14), among them the lines and spectral values of Remark 16, the resolutions at which v_L° vanishes (Remark 65), the comparison of $\mathcal{W}_p^*$ with $\mathcal{W}_p$ (Remark 107) and the shifts of Remark 108 that break the lock.

Conventions fixed in the formal statements. Where the text states a value up to sign, some formal statements fix the sign. For Lemma 111 the sign is +1 for V in the monomial basis, with the rows taken coordinate by coordinate and the points ordered $v_0, u_0, v_1, u_1, \dots, P$ before Q ; this exact value is formally verified.

APPENDIX G. COMPUTATIONS

The computed values printed in the paper, none of which is used in a proof, the finite certificates of Theorem 64, Theorem 120 and Propositions 40 and 118, and the figures are reproduced by the programs in the folder `scripts/` of the accompanying software deposit (Python 3, run with `uv`, and C++). A driver script builds and runs all of them in a few minutes on one laptop (the certificates of Theorem 64 use several cores if available); it fails if a value differs from the one printed here or a regenerated figure differs from the published one. The README of the folder lists, for each program, what it reproduces:

- the base-2 $(0, m, 3)$ -net of [20, Sec. 2], built from its generator matrices and, independently, by a re-implementation of the C routine printed in [20], with the $(0, m, 3)$ property by box counting and the exact toroidal minimum distance: $\delta N^{1/3} = .750, .649, .486, .433, .472, .466, .424, .447, .375, .265, .186$ for $m = 3, \dots, 13$ (Section 1);
- the two-dimensional nets of Remark 6 for $m = 4, 6, 8, 10$: the $(0, m, 2)$ property; for (iii), all slides along their lines that keep $t = 0$ and their distances from lattice slides ($m = 4, 6, 8$), and, for even $8 \leq m \leq 20$, the $(0, m, 2)$ property and the exact minimum distances, in the tiling metric, of the re-scrambled nets and of the nets themselves;
- the enumeration of one-per-cube lattices in $\frac{1}{e}\mathbb{Z}^3$, $e \leq 11$, and the affinity check of Remark 101;
- the exact minimum distances of Table 12, by a toroidal neighbour-cell scan of nets rebuilt from Definition 41, with the other values of this table;
- the computed values after Proposition 103 (Figure 12(c));
- the evaluations of proved formulas in Table 4;
- Table 3 (a_s^* and the largest entries computed from Definition 23, $5a_s^* + 4$, the bound of Theorem A, a_s of U_s) and the values derived from it in the Introduction and in Table 6;

part of the paper	results	statement file; proof modules
Sec. 2	Lems. 1, 2, 4; Rem. 5; Def. 7	Prelim (19); F* , DShift
Sec. 3	Lems. 8, 10, 11, 18; Props. 9, 12, 13, 17; Def. 14, Cor. 15; Rem. 16	Frames (50); F* , Proj* , Obs*
Sec. 4	Thm. A, Prop. 19, Lems. 20, 21, 22, Def. 23; the design U_s of Rem. 24 (assuming PNT)	ThmA (66); ThmA* , SU* ; Theorem A also Headline
Sec. 5	Lems. 25, 26, 29, 31, 38; Prop. 27, Cors. 28, 39; Defs. 34, 30, 36; Thms. 33, 35; Prop. 40; mathematical claims of Rem. 32	Skeleton (67); Sk* , S1* , S2* , T3*
Sec. 6	Def. 41, Thms. 42, 45, 46, Prop. 43, Rem. 44; Def. 47, Thms. 48, 49, Lem. 50, Props. 51, 52; Def. 53, Prop. 54, Thm. 56, Rem. 55; Cor. 57, Rem. 58	Dim3 (67; Def. 41 in Frames); Main* , Net* , Sep* , Col* , D3* , KN*
Sec. 7	Def. 60, Lems. 61, 62, 63; Thm. 64(2), (3), and (1) beyond L given its certificate; Rem. 65; the proved statements of Rem. 59	Base23 (21); B23*
Sec. 8	Lem. 67, Props. 68, 73; Cors. 69, 71; Rems. 70, 72	DGS (64); *Shift* , DGS*
Secs. 9–11	Def. 74, Props. 75, 77, Lem. 76, Cors. 78, 79, Props. 81, 83, 84; Rem. 82; the proved statements of Rem. 80; Prop. 85, Def. 86, Thms. 87, 88; Lems. 89, 91, Prop. 90, Thm. 92; Lem. 93, Cor. 94, Thm. 95	Deficit (75); Deficit* , Obs* , Ceil , D4D2* , K1* , Lstar* , Col*
Sec. 12	Lems. 96, 98, Cor. 97; Prop. 100 (assuming Hajós, Keller for $s \leq 7$, packing bounds)	WhyLat (14); WL*
Secs. 13.1–13.3	Prop. 102, Table 8; Prop. 103; Props. 104, 106, Lem. 105, Rems. 107, 108	Large (81); S1E* , SkCert* ; QUNetsM3/TC* , QUNetsM3/W*
Secs. 13.4–13.7	Prop. 109; Def. 110, Lems. 111, 112, Prop. 113 and the remark after it; Lem. 114, Prop. 115, Thm. 116, Prop. 122; Lem. 117, Prop. 118, Rem. 119, Thm. 120	Split (78); Split* , HL* , Half* , Q5* , TD* , Acct*
App. C	Defs. 126, 130, Prop. 131, Props. 129, 128, Lem. 127, Rem. 132; Table 10	Appendix (14); PP* , KN*

TABLE 15. Formal verification: for each part of the paper, the statement file of the Lean library that states its results (in **QUNets/Statements/**, with the number of its theorems; 616 in all) and the principal proof modules (in **Z3Net/** unless stated; ***** stands for any part of a name). Several results are also used, or restated, in other files. “Assuming X ” means that the result uses the classical theorems X , which are not in Mathlib, as explicit hypotheses (PNT, the prime number theorem; Appendix F). **Headline** is the self-contained entry for Theorem A.

- the certified deficits, $\sigma_{\max}(F)$, q_{tail} and thresholds of Table 6 (K and thresholds for $s \leq 6$; $\sigma_{\max}$ and q_{tail} for $s \leq 8$) and the finite parts of Proposition 81, by the exact relaxation of Lemma 4 on the designs of Appendix A; and the K_1 , thresholds and sizes of Table 7 (the per-prime $t = 0$ completions of Proposition 84 are not rerun by these scripts; they were reproduced by independent implementations and are checked in the Lean kernel, Section 14);
- the certificates of Theorem 64 (Table 5): the chains replayed from the seeds, $t = 0$ at every resolution, the integers v_L^* of Lemma 62 with the proviso $g_L \leq b^{L/3} - Wb^{-2L/3}$, the exact minima between the seed and the certificate resolutions, and the small- m nets, by the checker of the deposit (with OpenMP about half a minute on ten cores); for part (3), the integers v_L° , the exact minima over all digital shifts at the resolutions up to L and

of the small- m nets (Lemma 63), and the freezing of the chains, by a second checker (a few seconds);

- the column nets of Section 6.5: Theorem 48 on random column point sets against an exact brute-force distance, the closed forms of Theorem 49 against two exact kernels at every $q \leq 241$ coprime to 6 (composites included), the box minors, all digital shifts at small q against Proposition 52, the class maximum of the digital column nets against Theorem 95, the comparison with $\mathcal{T}_p$ after Proposition 103, and the comparison nets with a common second digit of Figure 10(c);
- the rank-one nets of Section 13.3, Proposition 104: the box minors of $\mathcal{W}_p$, Lemma 105 by enumeration of all cells at small p , the numerical steps of the proof of Proposition 104 in exact arithmetic (the rules of part (2) against the lemma, Table 9 and the tangent-line constants, and, independently, the full quadratic of every option in each of the 24 classes of p modulo 48), the relaxation at every prime $53 \leq p \leq 3000$, the pair of part (3), the exact minimum distances of $\mathcal{W}_p$ at every prime $5 \leq p \leq 199$ and at 307, 353 (the finite part of (4)), the comparison with $\mathcal{T}_p$, the layer with a geometric digit shared by two coordinates at $p = 307$ and its value in the limit model, and the digital shifts of Remark 108;
- for Proposition 106 and Remark 107: the constants and every numerical fact of the proof in exact arithmetic, the value $F(\psi^*) = \mu^{*2}$ from all options, the identity $F_p(u) = F(u/p)$ and $\max_u F_p(u) < \mu^{*2}$ over all u at small primes, the box minors and the bound with K for $\mathcal{W}_p^*$, the thresholds, and the exact minimum distances of $\mathcal{W}_p$ and $\mathcal{W}_p^*$ at the primes $p \leq 1009$ where they differ (recomputed by the scripts at 193, 241, 337; at the other five primes the values come from two separate distance programs that agree, and are not rerun by the driver);
- the certificates of Proposition 118 (the 126 box minors, the exact scans of Lemma 117 and of Proposition 115(1) with their monotone tails, the finite check of the limit), the constants of Remark 119 and Remark 121, the exact minimum distances of $\mathcal{Q}_p^*$ for $7 \leq p \leq 61$, and the enumerations of Theorem 120 and of the text after it;
- the data printed in Proposition 40, Remark 101 and Tables 11, 13, 14, compared with their sources entry by entry, with the finite checks in the proof of Proposition 40, the layer of Remark 119 and the identity and estimates in the proof of Proposition 103;
- every printed decimal bound, recomputed in exact arithmetic and checked to be truncated or rounded as stated in Section 2.5 (this check also reads the integers T_p of Table 10 from the formalization);
- the figures, including those of Part I (Figures 4, 9, 3, 6) and of the accounting (Figures 10, 15, 13), each regenerated by its script, which also asserts the properties stated in its caption.

REFERENCES

- [1] J. Brakensiek, M. Heule, J. Mackey, D. Narváez, *The resolution of Keller's conjecture*, J. Automat. Reason. 66 (2022) 277–300, doi:10.1007/s10817-022-09623-5; conference version in: IJCAR 2020, Lecture Notes in Comput. Sci. 12166, Springer, 2020, 48–65, doi:10.1007/978-3-030-51074-9_4; arXiv:1910.03740.
- [2] E. S. Barnes, N. J. A. Sloane, *New lattice packings of spheres*, Canad. J. Math. 35 (1983) 117–130, doi:10.4153/cjm-1983-008-1.
- [3] H. Cohn, N. Elkies, *New upper bounds on sphere packings I*, Ann. of Math. 157 (2003) 689–714, doi:10.4007/annals.2003.157.689; arXiv:math/0110009.
- [4] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, M. Viazovska, *The sphere packing problem in dimension 24*, Ann. of Math. 185 (2017) 1017–1033, doi:10.4007/annals.2017.185.3.8; arXiv:1603.06518.
- [5] R. R. Coveyou, R. D. MacPherson, *Fourier analysis of uniform random number generators*, J. ACM 14 (1967) 100–119, doi:10.1145/321371.321379.

- [6] R. L. Cook, *Stochastic sampling in computer graphics*, ACM Trans. Graph. 5 (1986) 51–72, doi:10.1145/7529.8927.
- [7] L. Clozel, H. Oh, E. Ullmo, *Hecke operators and equidistribution of Hecke points*, Invent. Math. 144 (2001) 327–351, doi:10.1007/s002220100126.
- [8] R. Cranley, T. N. L. Patterson, *Randomization of number theoretic methods for multiple integration*, SIAM J. Numer. Anal. 13 (1976) 904–914, doi:10.1137/0713071.
- [9] J. H. Conway, N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Springer, 1999.
- [10] J. Dick, T. Goda, G. Larcher, F. Pillichshammer, K. Suzuki, *On the quasi-uniformity properties of quasi-Monte Carlo point sets and sequences, Part I: lattices and Kronecker sequences*, Math. Comp. (2026), doi:10.1090/mcom/4264; arXiv:2502.06202 (theorem numbers cited from arXiv v2).
- [11] J. Dick, T. Goda, K. Suzuki, *On the quasi-uniformity properties of quasi-Monte Carlo point sets and sequences, Part II: digital nets and sequences*, Math. Comp. (2026), doi:10.1090/mcom/4263; arXiv:2501.18226 (theorem numbers cited from arXiv v2).
- [12] C.-J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Ann. Soc. Sci. Bruxelles 20 B (1896) 183–256.
- [13] L. de Moura, S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction – CADE 28, Lecture Notes in Comput. Sci. 12699, Springer, 2021, 625–635, doi:10.1007/978-3-030-79876-5_37.
- [14] J. Dick, F. Pillichshammer, *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge Univ. Press, 2010.
- [15] A. Eskin, H. Oh, *Ergodic theoretic proof of equidistribution of Hecke points*, Ergodic Theory Dynam. Systems 26 (2006) 163–167, doi:10.1017/s0143385705000428; arXiv:math/0409507.
- [16] H. Faure, *Discrépance de suites associées à un système de numération (en dimension s)*, Acta Arith. 41 (1982) 337–351, doi:10.4064/aa-41-4-337-351.
- [17] H. Faure, C. Lemieux, *Generalized Halton sequences in 2008: a comparative study*, ACM Trans. Model. Comput. Simul. 19 (2009), Art. 15, 1–31, doi:10.1145/1596519.1596520.
- [18] T. Goda, R. Hofer, K. Suzuki, *Disproving the quasi-uniformity of the Halton sequences and of some Halton-type sequences*, J. Complexity 95 (2026) 102047, doi:10.1016/j.jco.2026.102047; arXiv:2511.21153 (theorem numbers cited from arXiv v2).
- [19] L. Grünschoß, J. Hanika, R. Schwede, A. Keller, *(t, m, s) -nets and maximized minimum distance*, in: A. Keller, S. Heinrich, H. Niederreiter (eds.), Monte Carlo and Quasi-Monte Carlo Methods 2006, Springer, 2008, 397–412, doi:10.1007/978-3-540-74496-2_23.
- [20] L. Grünschoß, A. Keller, *(t, m, s) -nets and maximized minimum distance, Part II*, in: P. L’Ecuyer, A. B. Owen (eds.), Monte Carlo and Quasi-Monte Carlo Methods 2008, Springer, 2009, 395–409, doi:10.1007/978-3-642-04107-5_25.
- [21] J. Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques*, Bull. Soc. Math. France 24 (1896) 199–220, doi:10.24033/bsmf.545.
- [22] G. Hajós, *Über einfache und mehrfache Bedeckung des n -dimensionalen Raumes mit einem Würfelgitter*, Math. Z. 47 (1942) 427–467, doi:10.1007/bf01180974.
- [23] T. C. Hales, *A proof of the Kepler conjecture*, Ann. of Math. 162 (2005) 1065–1185, doi:10.4007/annals.2005.162.1065.
- [24] J. M. Hammersley, *Monte Carlo methods for solving multivariable problems*, Ann. New York Acad. Sci. 86 (1960) 844–874, doi:10.1111/j.1749-6632.1960.tb42846.x.
- [25] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., revised by D. R. Heath-Brown and J. H. Silverman, Oxford Univ. Press, 2008.
- [26] X. He, *Rotated sphere packing designs*, J. Amer. Statist. Assoc. 112 (2017) 1612–1622, doi:10.1080/01621459.2016.1222289.
- [27] X. He, *Interleaved lattice-based maximin distance designs*, Biometrika 106 (2019) 453–464, doi:10.1093/biomet/asv069; arXiv:1807.02289.
- [28] X. He, *Lattice-based designs with quasi-optimal separation distance on all projections*, Biometrika 108 (2021) 443–454, doi:10.1093/biomet/asaa057; arXiv:1709.02062.
- [29] M. Hall, L. J. Paige, *Complete mappings of finite groups*, Pacific J. Math. 5 (1955) 541–549, doi:10.2140/pjm.1955.5.541.
- [30] R. Hofer, K. Suzuki, *A complete classification of digital $(0, m, 3)$ -nets and digital $(0, 2)$ -sequences in base 2*, Unif. Distrib. Theory 14 (2019) 43–52, doi:10.2478/udt-2019-0004; arXiv:1807.04383.
- [31] R. Kannan, A. Bachem, *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM J. Comput. 8 (1979) 499–507, doi:10.1137/0208040.

- [32] D. E. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 3rd ed., Addison-Wesley, 1997.
- [33] W. Kositwattananarerk, F. Oggier, *Connections between Construction D and related constructions of lattices*, Des. Codes Cryptogr. 73 (2014) 441–455, doi:10.1007/s10623-014-9939-3; arXiv:1308.6175.
- [34] N. M. Korobov, *The approximate computation of multiple integrals*, Dokl. Akad. Nauk SSSR 124 (1959) 1207–1210.
- [35] R. Kritzing, *Dispersion of digital $(0, m, 2)$ -nets*, Monatsh. Math. 195 (2021) 155–171, doi:10.1007/s00605-021-01525-9; arXiv:2004.14760.
- [36] H. W. Lenstra, Jr., *Euclidean number fields of large degree*, Invent. Math. 38 (1976/77) 237–254, doi:10.1007/bf01403131.
- [37] C. Lemieux, *Tractability using periodized generalized Faure sequences*, J. Complexity 31 (2015) 42–56, doi:10.1016/j.jco.2014.08.001.
- [38] C. Lemieux, H. Faure, *New perspectives on $(0, s)$ -sequences*, in: P. L’Ecuyer, A. B. Owen (eds.), Monte Carlo and Quasi-Monte Carlo Methods 2008, Springer, 2009, 113–130, doi:10.1007/978-3-642-04107-5_7.
- [39] G. Larcher, H. Niederreiter, W. Ch. Schmid, *Digital nets and sequences constructed over finite rings and their application to quasi-Monte Carlo integration*, Monatsh. Math. 121 (1996) 231–253, doi:10.1007/bf01298952.
- [40] G. Larcher, F. Pillichshammer, *Walsh series analysis of the L_2 -discrepancy of symmetrized point sets*, Monatsh. Math. 132 (2001) 1–18, doi:10.1007/s006050170054.
- [41] J. C. Lagarias, P. W. Shor, *Keller’s cube-tiling conjecture is false in high dimensions*, Bull. Amer. Math. Soc. (N.S.) 27 (1992) 279–283, doi:10.1090/s0273-0979-1992-00318-x; arXiv:math/9210222.
- [42] J. Mackey, *A cube tiling of dimension eight with no facesharing*, Discrete Comput. Geom. 28 (2002) 275–279, doi:10.1007/s00454-002-2801-9.
- [43] J. Matoušek, *On the L_2 -discrepancy for anchored boxes*, J. Complexity 14 (1998) 527–556, doi:10.1006/jcom.1998.0489.
- [44] The mathlib Community, *The Lean mathematical library*, in: Proc. 9th ACM SIGPLAN Int. Conf. on Certified Programs and Proofs (CPP 2020), ACM, 2020, 367–381, doi:10.1145/3372885.3373824.
- [45] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.
- [46] H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. 104 (1987) 273–337, doi:10.1007/bf01294651.
- [47] A. B. Owen, *Randomly permuted (t, m, s) -nets and (t, s) -sequences*, in: H. Niederreiter, P. J.-S. Shiue (eds.), Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, Lecture Notes in Statist. 106, Springer, 1995, 299–317, doi:10.1007/978-1-4612-2552-2_19.
- [48] L. J. Paige, *Complete mappings of finite groups*, Pacific J. Math. 1 (1951) 111–116, doi:10.2140/pjm.1951.1.111.
- [49] O. Perron, *Über lückenlose Ausfüllung des n -dimensionalen Raumes durch kongruente Würfel*, Math. Z. 46 (1940) 1–26, doi:10.1007/bf01181421; II, Math. Z. 46 (1940) 161–180, doi:10.1007/bf01181436.
- [50] L. Panek, M. Firer, M. M. S. Alves, *Symmetry groups of Rosenbloom–Tsfasman spaces*, Discrete Math. 309 (2009) 763–771, doi:10.1016/j.disc.2008.01.013.
- [51] R. M. Roth, G. Seroussi, *On generator matrices of MDS codes (Corresp.)*, IEEE Trans. Inform. Theory 31 (1985) 826–830, doi:10.1109/tit.1985.1057113.
- [52] M. Yu. Rosenbloom, M. A. Tsfasman, *Codes for the m -metric*, Probl. Inf. Transm. 33 (1997) 45–52.
- [53] L. Rudolph, *The even-order Grönschloß–Keller permutation nets are $(0, m, 2)$ -nets*, preprint, Zenodo, version 1.0.0, 2026, doi:10.5281/zenodo.22264675.
- [54] N. Sakai, T. Goda, *Space-filling lattice designs for computer experiments*, arXiv:2602.15390 (2026).
- [55] I. H. Sloan, S. Joe, *Lattice Methods for Multiple Integration*, Oxford Univ. Press, 1994.
- [56] M. M. Skrikanov, *Coding theory and uniform distributions*, Algebra i Analiz 13 (2001) 191–239; English transl. St. Petersburg Math. J. 13 (2002) 301–337; arXiv:math/9909163 (theorem numbers cited from the arXiv version).
- [57] I. M. Sobol’, *On the distribution of points in a cube and the approximate evaluation of integrals*, Zh. Vychisl. Mat. Mat. Fiz. 7 (1967) 784–802; English transl. USSR Comput. Math. Math. Phys. 7 (1967) 86–112, doi:10.1016/0041-5553(67)90144-9.
- [58] I. M. Sobol’, B. V. Shukhman, *Quasi-random points keep their distance*, Math. Comput. Simulation 75 (2007) 80–86, doi:10.1016/j.matcom.2006.09.004.
- [59] K. Suzuki, *Exact ℓ^∞ -separation radius of Sobol’ sequences in dimension 2*, arXiv:2508.14803 (2025).
- [60] K. Suzuki, *Separation properties of scrambled digital nets and related random point sets*, arXiv:2607.29063 (2026).

- [61] S. Tezuka, *Polynomial arithmetic analogue of Halton sequences*, ACM Trans. Model. Comput. Simul. 3 (1993) 99–107, doi:10.1145/169702.169694.
- [62] S. Tezuka, *Uniform Random Numbers: Theory and Practice*, Kluwer, 1995.
- [63] R. Tavildar, P. Viswanath, *Approximately universal codes over slow-fading channels*, IEEE Trans. Inform. Theory 52 (2006) 3233–3258, doi:10.1109/tit.2006.876226; arXiv:cs/0512017.
- [64] E. R. van Dam, B. Hushlage, D. den Hertog, H. Melissen, *Maximin Latin hypercube designs in two dimensions*, Oper. Res. 55 (2007) 158–169, doi:10.1287/opre.1060.0317.
- [65] E. R. van Dam, G. Rennen, B. Hushlage, *Bounds for maximin Latin hypercube designs*, Oper. Res. 57 (2009) 595–608, doi:10.1287/opre.1080.0604.
- [66] P. O. Vontobel, A. Ganesan, *On universally decodable matrices for space-time coding*, Des. Codes Cryptogr. 41 (2006) 325–342, doi:10.1007/s10623-006-9019-4; arXiv:cs/0601075.
- [67] M. S. Viazovska, *The sphere packing problem in dimension 8*, Ann. of Math. 185 (2017) 991–1015, doi:10.4007/annals.2017.185.3.7.