

LOW-DISCREPANCY QUASI-UNIFORM DIGITAL SEQUENCES IN EVERY DIMENSION

LEONHARD GRUENSCHLOSS

ABSTRACT. A sequence of points in the unit cube is quasi-uniform if its first N points are spread like a grid for every N : no two of them are closer, and no empty ball between them is larger, than a constant times $N^{-1/s}$ in dimension s . Dick, Goda and Suzuki asked for such sequences among the digital sequences of quasi-Monte Carlo integration, and Goda, Hofer and Suzuki asked whether any Halton-type sequence is quasi-uniform. We show that in dimension two and higher no Halton-type sequence, no Sobol' sequence, no classical Niederreiter sequence and no Faure sequence is quasi-uniform, and that linear scrambles of all coordinates but one do not help: a carry in the last digits of one coordinate leaves the leading digits of all others unchanged, giving explicit pairs of points that are far too close. We then show that one fixed linear scramble of a generalized Faure sequence, the same for all numbers of points, repairs this. In it, the digits of all coordinates at one scale are residues of one rational function, each taken at the coordinate's own point of the projective line, so the residue theorem ties the coordinates together and a carry in one coordinate is seen by the others. For every dimension s and every prime base $p > 2^s$ this gives explicit quasi-uniform digital $(0, s)$ -sequences, hence of low discrepancy, whose first $N = p^{sK-1}$ points are at least $(1 - 2p^{-1/s})N^{-1/s}$ apart, for every K ; in dimensions two and three, for every prime $p \geq 5$, a variant keeps its first N points at least $(1 - 2/p)N^{-1/s}$ apart whenever N is a power of p^{s^2} . For such scrambles, exact linear rules that place every point inside its cell as a function of the last few digits of the cell's index can hold at no more than about one in s of the sizes p^{sK} ; with allowed ranges instead of exact rules we certify all of these sizes, with points at least $(1 - O(1/p))N^{-1/s}$ apart for large p . Quasi-uniform digital sequences follow in every prime base $p \geq 3$ in dimension three, and in every prime base in dimension two, base two included. Some steps are computer-assisted.

1. INTRODUCTION

A point set $P \subset [0, 1]^s$ of N points is *quasi-uniform* if its covering radius $h(P)$, the radius of the largest empty ball, and its separation $\delta(P)$, the smallest distance between two of its points, are both of the optimal order $N^{-1/s}$; equivalently, the mesh ratio $h(P)/\delta(P)$ is bounded. For a sequence the condition is asked of every prefix $P_{[N]}$, the first N points, for all N at once. Dick, Goda and Suzuki [10], continuing Part I with Larcher and Pillichshammer [9], asked for digital nets and sequences in a fixed base that are both low-discrepancy and quasi-uniform. Their positive example is the two-dimensional Larcher–Pillichshammer net [27]; for dimension $s \geq 3$ they state the construction as open, for nets and for sequences, and Suzuki [39] recently wrote that no such family is known there. Goda, Hofer and Suzuki proved that the Halton sequences are not quasi-uniform and asked whether any Halton-type sequence is [16, Open Problem 2]. The companion paper [18] answers the question of Dick, Goda and Suzuki for nets in every dimension. This paper answers it for sequences, and settles the question of Goda, Hofer and Suzuki: no Halton-type sequence is quasi-uniform.

Date: Version 1, 2026-10-30. The Lean formalization and the archive of the computations of this version are release v1.0.0 of <https://github.com/lgruen/quasi-uniform-sequences-lean>.

ORCID iD: <https://orcid.org/0009-0004-6476-2191>. Email: leonhard@gruenschloss.org.

The classical sequences fail. The Halton, Faure, Sobol' and Niederreiter sequences are built from polynomial bases: each coordinate reads the index, written as a polynomial over a finite field, in its own base, one block of digits at a time. Their prefixes of q^m points are nets at every scale, so their covering radius is always of the right order. Their separation is not, and the reason is a carry (Figure 2). Take two indices whose difference is a carry in the last digits of one coordinate: in base p the digits $0.a(p-1)\cdots(p-1)$ of one point become $0.(a+1)0\cdots 0$ for the other, and the two points sit on either side of a cell boundary. If the same difference is divisible by a high power of every other base, it leaves the leading digits of all other coordinates unchanged, and the two points are close in every coordinate at once. For polynomial bases such differences exist at infinitely many sizes. In the carrying base b a carry is a run of ones, $1 + b + \cdots + b^{\nu-1} = (b^\nu - 1)/(b - 1)$, and this run is divisible by all the other bases as soon as $b^\nu \equiv 1$ modulo $b - 1$ times their product, which holds for suitable ν . The Frobenius map $f \mapsto f^p$, which is additive in characteristic p , then stretches one such pair into a pair at p times the scale, and the excess of the shared digits over the cell side grows each time. Theorem 6 turns this into explicit close pairs for every digital sequence whose coordinates read the index in pairwise coprime polynomial bases, one of them as a radical inverse.

Table 1 lists the consequences. In dimension $s \geq 2$ no Halton-type sequence is quasi-uniform, which answers Open Problem 2 of [16] with explicit index pairs (Corollary 7); neither is any Faure sequence (Corollary 8), any Sobol' sequence (Corollary 13) or any classical Niederreiter sequence (Corollary 11); and scrambling every coordinate but one does not help (Corollary 14). These statements were not found in the literature we searched (through October 2026); the earlier results are listed in the table. So, among sequences of this kind, a quasi-uniform one has to scramble every coordinate beyond a scalar, and the natural repair is a scramble that lets the coordinates see each other's carries.

Why sequences are harder than nets. The nets of [18] also scramble the generalized Faure sequences, but anew for every number of points. At a full level $N = q^{sK}$ the prefix of a $(0, s)$ -sequence has exactly one point in each cell of side $N^{-1/s}$, so what decides the separation is where each point sits inside its cell relative to its neighbours. To first order this position is given by the *geometric digits*, the first digit of each coordinate below the cell. They are a linear function of the cell digits, the *offset map*. What matters for the separation are its *carry responses*: how the geometric digits change when one cell index steps to the next cell, across a boundary where l of its digits change (a carry of length l). For the Faure sequence the offset map changes with the level: in dimension two one of its coefficients is $(-1)^K(K+1)$ at level K , which runs through all residues modulo p (Example 19). A net can undo this with a scramble chosen for its size. A sequence cannot: a row of its scramble, once used, stays in use at every finer level, so one fixed scramble has to serve all scales. The natural candidates are the *self-similar* scrambles. Let a_c be the point at which coordinate c reads the index (its *place*). Multiplying the index polynomial by $w = \prod_c (z - a_c)$ takes the cell picture one level finer, and for a self-similar scramble it shifts the digits of every coordinate by one place and multiplies them by one fixed scale. Such scrambles have the same offset map at every level (Proposition 22), and then one finite check bounds the separation at every level (Lemma 23). What remains is to choose the infinitely many carry responses, one for each carry length, all of them well. How much of this exact linear rules of bounded depth can do is limited (Theorem 51 below).

The fix: residues. A Taylor coefficient of the index polynomial V at a point a is a residue, $[(z - a)^n]V = \text{Res}_a(V(z - a)^{-n-1}dz)$. More generally, every scramble of a generalized Faure sequence reads digit n of coordinate c as the residue at the place a_c of V times a differential with a pole of order $n+1$ there (Lemma 21). The residues of one rational function at all its poles on the projective line add up to zero. So if all coordinates read their digits from one rational differential, the residue theorem is a linear identity between digits of different coordinates. It

TABLE 1. Classical sequences that are not quasi-uniform (Section 3). All are digital sequences in dimension $s \geq 2$; every result gives explicit close pairs along an explicit sequence of sizes (Theorem 6). “Earlier”: the cases known before, as far as we found.

sequences	scope	earlier	where
polynomial-base digital sequences	pairwise coprime bases $b_c \in \mathbb{F}_q[z]$ of any degrees, every coordinate b_c -adic, one coordinate a radical inverse	–	Thm. 6
Halton-type	every prime p , every $s \geq 2$, any pairwise coprime bases in $\mathbb{F}_p[z]$, monic or not, irreducible or not [16, Def. 2]	Halton sequences and three families of Halton-type sequences [16]	Cor. 7
Faure, unscrambled frames	$(P^0, \dots, P^{s-1})$ in prime base p , every $2 \leq s \leq p$; any distinct places over $\mathbb{F}_q$; separation at most of order $N^{-1/(s-1)}$ along a sequence of N when two places differ by 1	$s = p$ [10]; $s = 2$ and $s = p$ [16]	Cor. 8, Rem. 9
Sobol’	every $s \geq 2$, any admissible direction numbers, with or without the van der Corput coordinate, natural or Gray-code order, every projection to $s' \geq 2$ coordinates	$s = 2$ [14, 40]; the opposite was suggested numerically [37]	Cor. 13
Niederreiter	classical, over every $\mathbb{F}_q$ (natural identification); generalized, when one coordinate is a radical inverse	–	Cor. 11
one coordinate unscrambled	bases as in Thm. 6; one coordinate a radical inverse up to a scalar, all others with any fixed lower-triangular scramble; for a linear base also a diagonal scramble	Faure, $s = p$ (every prime p), first coordinate unscrambled [16, Rem. 3]; (L, P) , (I, LP) in base 2 [10, Thm. 4.2]	Cor. 14
randomizations	digital shifts, Faure–Tezuka index scrambles, reorderings that keep every full level as a set; a fixed Toeplitz scramble of the carrying coordinate with rational multiplier (under a squarefree condition)	Owen scrambling: almost surely not quasi-uniform [39]	Rem. 15, 16

holds at every level and involves no carries: a carry in one coordinate is now seen by the others. In the simplest example, the *brick wall* in dimension two, the identity says that the height of a point inside its cell in coordinate 1 is half the finest cell digit of coordinate 0, at every level: neighbouring columns of points are staggered by half a cell, like the courses of a brick wall (Section 4).

This gives two closed forms (Section 5). In the *staggered residue sequence*, the brick wall in every dimension, one coordinate is staggered by a rank-1 lattice rule in the cell indices of the others; it is certified at every full level for every prime $p > 2^s$, with the constant $(\lfloor p/2^{s-1} \rfloor - 1)/p$, which is the best this one-coordinate bound allows (Corollary 29). The *residue sequence* lets every coordinate read the same differential $V dz$. The residue theorem then relates the last cell digits of all coordinates at the prefixes P_{sK-1} , one digit before each full level. Give one coordinate one cell digit fewer than the others, so that every box of these depths holds one point (a *skeleton*

coordinate in the language of [18]): its next digit is then a fixed linear combination of the finest cell digits of the other coordinates, the *skeleton relation*. As a result the points of P_{sK-1} occupy exactly those *fine cells*, the cubes of side p^{-K} , whose indices lie in the Construction-A lattice $\Lambda_v = \{b \in \mathbb{Z}^s : \sum_c v_c b_c \equiv 0 \pmod{p}\}$ of a *check vector* $v \in (\mathbb{F}_p^*)^s$, one point in each (Theorem 36, Figure 6). This is the picture of the nets of [18]: a lattice image plus a jitter of less than one fine cell, now produced at every $m \equiv -1 \pmod{s}$ by one fixed scramble. With a Korobov check vector the separation there is at least $(\rho - 1)p^{-1/s} > 1 - 2p^{-1/s}$, $\rho = \lfloor p^{1/s} \rfloor$, in every dimension (Corollary 37); with searched check vectors it exceeds 1, the value of the cubic grid, already at moderate primes, because the lattice Λ_v can be close to a denser packing than the grid (the hexagonal lattice has 1.0746 in the plane).

The nets of [18] go further at the full levels: they prescribe all s geometric digits by a fixed linear rule in the last few cell digits, a *design*, and this is how they reach separations $1 - O(1/q)$. A scramble puts one factor in front of the differential at each place, its *local multiplier*. Reading the digits in blocks of s , with s different local multipliers per coordinate, the residue theorem installs such a design at every s -th full level: the *block-periodic residue sequences* have separation $1 - 2/p$ at $N = p^{4K}$ in dimension two and at $N = p^{9K}$ in dimension three, for every prime $p \geq 3$ resp. $p \geq 5$, with a short proof (Theorem 42).

Level families. Each construction is certified at its own family of sizes $N = p^m$, its *level family* (Figure 1): $m \equiv -1$ or $m \equiv 0 \pmod{s}$, or $m \in s^2\mathbb{N}$. Every family with bounded gaps gives a bound for all N (Lemma 2), and hence quasi-uniformity, but the bound loses the factor $p^{-\Delta/s}$, where Δ is the largest gap. So a denser family can win for all N even with a smaller constant at its certified sizes: the residue sequences give LB/p for all N , the block-periodic sequences only LB/p^s .

What more is possible, and what is not. Why not s exact relations at every full level, which would put the design of the nets into every full level of one sequence? Within the scrambles of generalized Faure sequences, and for exact linear relations of bounded depth among the digits, this is impossible: a late enough range of $R + 1$ consecutive levels carries at most $J + R + 1$ independent relations of depth at most J , about one per level (Theorem 51, a residue-theorem argument at a single place). So all s geometric digits can be designed on at most a fraction $1/s$ of the full levels, which the block-periodic sequences attain (Corollary 52); the skeleton relations of the residue sequence and designed geometric digits share one count (Corollary 59); and no designed geometric digit fits at a full level next to skeleton relations (Corollary 58). Section 7 states the scope of each of these statements. To reach every full level with constants tending to 1, Section 8 uses certificates that are not exact relations: it keeps each carry response inside a fixed set of allowed values, a *window*, by choosing the free digits of a self-similar scramble one at a time. Half a cell is, up to $1/p$, the only offset that is equally good for a forward step, a backward step and no step (Lemma 66); staggering one coordinate by half a cell against all the others gives $1 - O(1/p)$ at every full level for large primes, in every dimension (Theorem 68). In a stated scope, windows and the skeleton relations of the residue sequence cannot be selected together (Proposition 73).

Results. All sequences of this paper are explicit linear scrambles of generalized Faure sequences, hence digital $(0, s)$ -sequences, with star discrepancy $O((\log N)^s/N)$ [31]. Each comes with a lower bound on $\text{sep}(P_m) = \delta(P_m)N^{1/s}$ at every m of its level family and is therefore quasi-uniform. Table 2 lists the results; the headlines are these.

- (1) *The classical sequences fail* (Section 3, Table 1), with explicit close pairs.
- (2) *A closed form in every dimension.* For every $s \geq 2$ and every prime $p > 2^s$ the residue sequence with a Korobov check vector is a quasi-uniform digital $(0, s)$ -sequence with $\text{sep}(P_{sK-1}) \geq (\rho - 1)p^{-1/s} > 1 - 2p^{-1/s}$ for every K (Theorem 36, Corollaries 37 and 38),

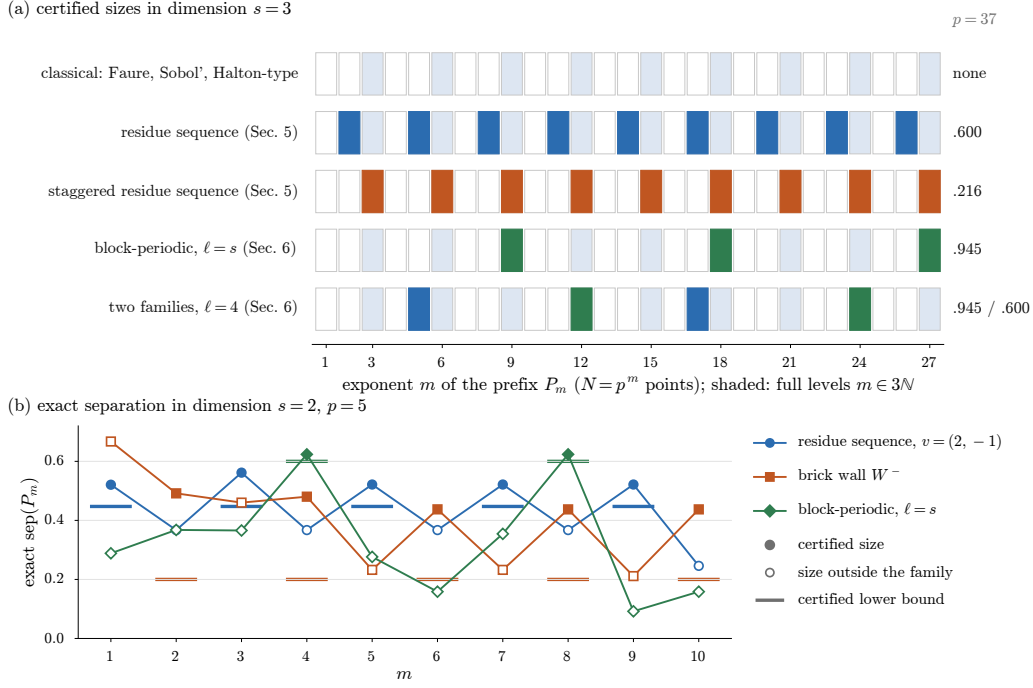


FIGURE 1. Level families. (a) The exponents $m \leq 27$ at which each construction has a certified lower bound on $\text{sep}(P_m)$ in dimension $s = 3$ (filled; shaded columns are the full levels), with the certified constant at $p = 37$: residue sequence, best check vector of Table 7 (Theorem 36); staggered residue sequence with dyadic weights, $8/37$ (Corollary 29); block-periodic residue sequence, $1 - 2/37$ (Theorem 42(b)); block period $\ell = 4$ (Theorem 45): the design at $m \in 12\mathbb{N}$ and skeleton relations at $m = 5, 17, 29, \dots$ (blue). The classical sequences have no certified level; they fail along explicit sequences of levels (Section 3). (b) Exact $\text{sep}(P_m)$, $m = 1, \dots, 10$, in dimension two over $\mathbb{F}_5$: the residue sequence with the Korobov vector $v = (2, -1)$ (certified 0.447 at odd m), the brick wall W^- (certified 0.2 at even m , Theorem 32) and the block-periodic sequence of Theorem 42(a) (certified 0.6 at $m \in 4\mathbb{N}$). Filled markers: sizes in the level family; bars: the certified bounds. Off its family a sequence is not controlled: the block-periodic sequence falls to 0.092 at $m = 9$ and the residue sequence to 0.246 at $m = 10$. Exact computations from the generator matrices.

and the staggered residue sequence has $\text{sep}(P_{sK}) \geq (\lfloor p/2^{s-1} \rfloor - 1)/p$ for every K (Corollary 29). With searched check vectors the constant of the residue sequence reaches 1.024 in dimension two ($p = 1009$) and 1.035 in dimension three ($p = 10007$) (Table 7).

- (3) *Separation $1 - O(1/p)$ from small primes on, at every s -th full level.* The block-periodic residue sequences have $\text{sep}(P_{s^2K}) \geq 1 - 2/p$ for every prime $p \geq 3$ ($s = 2$) and $p \geq 5$ ($s = 3$), and $1 - (a_s^* + 1)/p$ in every dimension $s \geq 4$ for $p \geq 5a_s^* + 4$; with a smaller diagonal of the design, $1 - 4/p$, $1 - 8/p$, $1 - 15/p$, $1 - 60/p$ for $s = 4, \dots, 7$ and every prime $p \geq 11, 23, 37, 191$ (Theorem 42; computer-assisted for these four).
- (4) *Limits of exact relations* (Section 7): about one exact relation of bounded depth per level, in the scope stated there.

TABLE 2. The main results: digital $(0, s)$ -sequences in base q with $\text{sep}(P_m) \geq \text{LB}$, the entry of the fourth column, for every m in the stated level family, hence quasi-uniform; the fifth column is the resulting bound $\delta(P_{[N]})N^{1/s} \geq \cdot$ for every $N \geq 2$ (Lemma 2). Form: *closed*, explicit functions of p (for the window constructions with any admissible choice of the free digits); *table*, a finite certificate. Proof: *proof**, the last step is one exact rational evaluation; *c.a.*, computer-assisted (Section 2.5). $\rho = \lfloor p^{1/s} \rfloor$; $a_4^* = 5$, $a_5^* = 16$. First row: the closed form $(\rho - 1)p^{-1/s}$ is proved; the values for searched check vectors v are exact finite evaluations (c.a.). Not listed: the sequences of Theorem 45 and Corollary 47, which are certified on two level families at once.

s	base	levels m	$\text{sep}(P_m) \geq$	all N	form	proof	where
≥ 2	prime $p > 2^s$	$s\mathbb{N} - 1$	$(\rho - 1)p^{-1/s} > 1 - 2p^{-1/s}$; searched v : 1.024 ($s = 2$), 1.035 ($s = 3$)	LB/p	closed	proof; c.a.	Thm. 36, Cor. 37, Tab. 7
≥ 2	prime $p > 2^s$	$s\mathbb{N}$	$(\lfloor p/2^{s-1} \rfloor - 1)/p$	LB/p	closed	proof	Cor. 29
2	prime $p \geq 3$	$4\mathbb{N}$	$1 - 2/p$	LB/p^2	closed	proof	Thm. 42
3	prime $p \geq 5$	$9\mathbb{N}$	$1 - 2/p$	LB/p^3	closed	proof	Thm. 42
4; 5	prime $p \geq 11$; 23	$16\mathbb{N}$; $25\mathbb{N}$	$1 - 4/p$; $1 - 8/p$	LB/p^s	closed	c.a.	Thm. 42
6; 7	prime $p \geq 37$; 191	$36\mathbb{N}$; $49\mathbb{N}$	$1 - 15/p$; $1 - 60/p$	LB/p^s	closed	c.a.	Thm. 42
≥ 4	prime $p \geq 5a_s^* + 4$	$s^2\mathbb{N}$	$1 - (a_s^* + 1)/p$	LB/p^s	closed	proof	Thm. 42
≥ 3	prime $p \geq p_0(s)$	$s\mathbb{N}$	$1 - C_s''/p$	LB/p	closed	proof	Thm. 68
3	prime $p \geq 1.97 \cdot 10^7$	$3\mathbb{N}$	$1 - 742/p$	LB/p	closed	proof*	Thm. 104
2	prime $p > 3677$	$2\mathbb{N}$	$1 - 17/p$	LB/p	closed	proof + c.a.	Cor. 70
2	2	$2\mathbb{N}$	0.3678	$\text{LB}/2$	closed	c.a.	Thm. 76
3	3; 4	$3\mathbb{N}$	0.05598; 0.11293	LB/q	closed	c.a.	Thms. 80, 81
3	7	$3\mathbb{N}$	1/7	$\text{LB}/7$	table	c.a.	Thm. 95
4	4	$4\mathbb{N}$	0.03013	$\text{LB}/4$	closed	c.a.	Thm. 82
2-5	$\mathbb{F}_8, \dots, \mathbb{F}_{169}$ (Tab. 11)	$s\mathbb{N}$	Table 11	LB/q	closed	c.a.	Prop. 83

- (5) *Every full level.* For every $s \geq 3$ a closed form gives $\text{sep}(P_{sK}) \geq 1 - C_s''/p$ for every prime $p \geq p_0(s)$ (Theorem 68), in dimension three $1 - 742/p$ for every prime $p \geq 1.97 \cdot 10^7$ (Theorem 104); in dimension two, $1 - 17/p$ for every prime $p > 3677$ (Corollary 70).
- (6) *Every base in small dimensions* (Theorem 84, which lists the level families). In dimension two every prime base is covered (base 3 by Theorem 42(a) and, at every full level, by a computer-assisted bound); in base 2 the sequence is a two-sided scramble of the Sobol' sequence with $\text{sep}(P_{2K}) \geq 0.3678$, which answers a question of Dick, Goda and Suzuki [10, Section 4.2]: it is well-separated in their sense [10, Def. 3.8] (Theorem 76). In dimension three every prime base $p \geq 3$ is covered, base 5 at the sizes 5^{9K} only, and base 4; in dimension four every prime $p \geq 7$ and base 4; in dimension five every prime $p \geq 11$; in dimension six every prime $p \geq 17$; in every dimension s every prime $p > 2^s$; and prime-power bases in dimensions two to five (Table 11).

Small bases and practice. In the bases 2, 3 and 4 neither residues nor windows give anything at every full level. There we choose frames whose local roots are lacunary series, such as $\sum_k x^{2^k}$, so that the responses are computed by a small finite automaton and the bound at every level is one finite minimum (Section 9). Section 9 also reads the staggered residue sequence over prime-power fields and collects the coverage by dimension. In practice (Section 10) the residue sequences are

generated like any digital sequence, from closed-form matrices, and they stay certified under digital shifts (Lemma 86). In dimension three their smallest $\text{sep}(P_{[N]})$ over $64 \leq N \leq 2^{23}$ is 0.235 to 0.267 at $p = 13, 17, 23, 31$: six to eighteen times the Owen-scrambled Sobol' sequence and 1.7 to 1.9 times the best plain Faure sequence (Figure 14, Table 13).

Scope. Each bound holds at the sizes of its level family; between them Lemma 2 loses the factor $q^{-\Delta_{\mathcal{M}}/s}$ (in Figure 14, 0.636 at the certified size against 0.020 for all N , with an observed minimum of 0.267). The bounds are lower bounds, often loose at small primes (for $s = 3, p = 11$ the residue sequence has the certified 0.449 against the exact 0.7686 and 0.6144 at $m = 2$ and $m = 5$), and at its first full level the Faure sequence is better than ours. The constants $1 - O(1/p)$ at every full level concern large primes ($p > 3677$ in dimension two, $p \geq 1.97 \cdot 10^7$ in dimension three, $p_0(4) \leq 1.44 \cdot 10^{16}$); at every s -th full level they hold from small primes on. Base 5 in dimension three at every full level, the primes $s \leq p < 2^s$ for $s \geq 4$ at every full level (and, outside the ranges above, at any level family), and the prime-power bases beyond Proposition 83 are open, and we measured separation, not integration error. These caveats are not repeated below.

Related work. Quasi-uniformity of quasi-Monte Carlo point sets was studied systematically in [9, 10]. Sobol' and Shukhman suggested from numerical experiments that the Sobol' sequence keeps its points at distance of order $N^{-1/s}$ [37]; Goda disproved this for $s = 2$ [14], and Corollary 13 disproves it in every dimension $s \geq 2$. The negative results before this paper are those of Table 1: the two-dimensional Sobol' sequence [14], whose mesh ratio grows at least like $N^{1/4}$ [40], the Faure sequence of dimension equal to its base [10], the Halton sequences and three families of Halton-type sequences [16], and Owen-scrambled (t, s) -sequences, almost surely [39]; Suzuki also shows that random linear scrambles of binary digital nets with fixed t have mesh ratio $O_P(\log N)$ under a uniform coincidence condition, which holds for instance for the prefixes of Sobol' sequences [39, Thm. 5.5, Lem. 4.10]. Without digital structure, quasi-uniform sequences exist in every dimension: Kronecker sequences with badly approximable parameters [9, Thm. 3.9], with discrepancy $O(N^{-1+\varepsilon})$ for algebraic parameters [9, Section 3.3], and greedy farthest-point sequences [34, 17], without a discrepancy guarantee; neither is a (t, s) -sequence. Sakai and Goda [35] select quasi-uniform rank-1 and Korobov lattice point sets, one for each N . Goda [15] constructs Kronecker sequences whose two-dimensional projections are quasi-uniform for every N , and nested lattices with this property at $N = p^m$. Among digital nets, the Larcher–Pillichshammer nets are quasi-uniform [27, 10], and [18] gives quasi-uniform digital $(0, m, s)$ -nets in every dimension with separation $1 - O(1/q)$; in both cases there is a separate net for each m . Generalized Faure sequences and their scrambles are classical [12, 30, 41, 42, 33, 28]; Tezuka's generalized Niederreiter sequences [41] define generator rows by Laurent coefficients. Mayor and Niederreiter [29] construct digital sequences from differentials of function fields; in genus 0 their construction contains every scramble of a frame, in the residue form of Lemma 21, and so every sequence of this paper. Niederreiter and Özbudak [32] read all coordinates as residues of one differential and use the residue theorem over all places for a duality. In these works the aim is the quality parameter t . Choosing the scramble so that the residue theorem ties one digit of every coordinate together with constant coefficients at every level of a level family, and using this for the separation, was not found in the literature we searched. In computer graphics, separation is an explicit design goal. Grünscloß, Hanika, Schwede and Keller [19] and Grünscloß and Keller [20] construct $(0, m, 2)$ - and $(0, m, 3)$ -nets with large minimum distance by search and by permutations, a new net for each m . Ahmed and Wonka [1] optimise dyadic nets and prove $\delta\sqrt{N} = 1/\sqrt{2}$ for a Gray-code net of each size 4^k ; these nets are not nested. The progressive multi-jittered sequences of Christensen, Kensler and Kilpatrick [5] and the stochastic (t, s) -sequences of Helmer, Christensen and Kensler [21] are built by randomised best-candidate choices; their

separation is empirical. Bonneel, Coeurjolly and Ostromoukhov [3] construct $(0, s)$ -sequences from Artin–Schreier polynomials; their subject is the quality parameter t , not separation, and their polynomials define Sobol’-type sequences, whereas our Artin–Schreier frames are a choice of places with lacunary local roots (Section 9).

This paper keeps the frames, the cells, the geometric digits, the lattice image and the designs of [18], and answers the question that paper leaves open: whether one fixed scramble can serve all scales. The new ingredients are the failure theorem for polynomial bases, the residue theorem as a design tool for the separation, the count of exact relations, and the windows.

Organisation. Section 2 fixes the objects, the level families and the conventions. Section 3 proves that the classical sequences fail. Section 4 describes the position of a point inside its cell, the residue form of a scramble and the self-similar scrambles. Sections 5 and 6 construct the residue and block-periodic residue sequences, Section 7 counts exact relations, and Section 8 certifies every full level with windows. Section 9 treats the small bases, prime powers and the coverage by dimension, Section 10 implementation, practice, randomisation and Hammersley lifts, and Section 11 open problems. The appendices hold secondary proofs, the base-7 bound in dimension three, the computer-assisted parts with the archive and the Lean status, and the staggered windows at a finite prime with their data.

2. DIGITAL SEQUENCES, FRAMES AND SEPARATION

This section fixes the objects and the conventions. Everything here is classical except for the normalisation of the separation constant and the form of the prefix lemma (Lemma 2): a bound at the prefixes of one family of sizes, with bounded gaps between consecutive sizes, gives a bound for every number of points.

2.1. Digital Nets and Sequences. Let $q = p^r$ be a prime power and $s \geq 1$. Digits live in $\mathbb{F}_q$ and are read through a fixed bijection $\text{enc}: \mathbb{F}_q \rightarrow \{0, \dots, q-1\}$ with $\text{enc}(0) = 0$. For prime q it is the identity on $\{0, \dots, p-1\}$. For a prime power we use the *natural identification* of Niederreiter [31]: fix a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ that contains 1, and read an element with coordinates $(x_0, \dots, x_{r-1}) \in \{0, \dots, p-1\}^r$ as the integer $\sum_i x_i p^i$. For $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ with the basis $(1, \omega)$ this is $0, 1, \omega, \omega^2 \mapsto 0, 1, 2, 3$. We write $\bar{y} := \text{enc}^{-1}(q-1)$ for the top digit ($\bar{y} = -1$ for prime q). A point set lives on the torus $[0, 1)^s = \mathbb{R}^s / \mathbb{Z}^s$.

An *elementary box* in base q is a product $\prod_c I_c$ in which I_c is one of the q^{d_c} intervals $[iq^{-d_c}, (i+1)q^{-d_c})$, $0 \leq i < q^{d_c}$, for integers $d_c \geq 0$. A set of q^m points is a (t, m, s) -net in base q if every elementary box of volume q^{t-m} contains exactly q^t points. An infinite sequence of points in $[0, 1)^s$ is a (t, s) -sequence in base q if for all $k \geq 0$ and $m \geq t$ its points number $kq^m, \dots, (k+1)q^m - 1$ form a (t, m, s) -net [30, 31, 11]. The letter t always denotes this quality parameter. A (t, s) -sequence has star discrepancy $O((\log N)^s/N)$ [31], so every sequence of this paper is a low-discrepancy sequence.

The index. We never write the index of a point as an integer variable. The point is labelled by its *index polynomial* $V(z) = \sum_k V_k z^k \in \mathbb{F}_q[z]$, whose coefficients $V_k \in \mathbb{F}_q$ are the *index digits* (V_0 least significant). The integer index of the point is

$$\iota(V) = \sum_k \text{enc}(V_k) q^k,$$

so the N -th point of the sequence, counted from 0, is the point whose index polynomial has $\iota(V) = N$. A *digital sequence* over $\mathbb{F}_q$ is given by s generator matrices $C_0, \dots, C_{s-1} \in \mathbb{F}_q^{\mathbb{N}_0 \times \mathbb{N}_0}$; digit n of coordinate c of the point $y(V)$ is

$$y_{c,n}(V) = \sum_k C_c[n][k] V_k, \quad y_c(V) = \sum_{n \geq 0} \text{enc}(y_{c,n}(V)) q^{-n-1}.$$

Rows are output digits (row 0 is the most significant digit) and columns are index digits. If the digits of $y_c(V)$ are eventually $\bar{y}$, the point lies on the upper boundary of the elementary box named by its digits; as usual [31, Section 4.1] we assign it to that box, and the separation bounds below allow this (the jitter in (3) may equal q^{-j}). We write $Y_c(x) = \sum_n y_{c,n} x^n$ for the digit series of coordinate c . Coordinates are numbered $c = 0, \dots, s-1$.

The *prefix* $P_m = \{y(V) : \deg V < m\}$ consists of the first q^m points, and $P_{[N]} = \{y(V) : \iota(V) < N\}$ of the first N points for general N . By Niederreiter's criterion [30, Thm. 6.1] (the box criterion of [18]), P_m is a $(0, m, s)$ -net if and only if for every $d = (d_0, \dots, d_{s-1})$ with $\sum_c d_c = m$ the *box matrix*, formed by the first d_c rows of every C_c restricted to the columns $0, \dots, m-1$, is invertible. The points numbered $kq^m, \dots, (k+1)q^m - 1$ form a digital shift of P_m (the index digits from m on are fixed), and a digital shift maps every elementary box onto one of the same shape. Hence a digital sequence is a (t, s) -sequence if and only if every prefix P_m is a (t, m, s) -net.

The prefixes P_{sK} are the *full levels*. At level K the prefix has $N = q^{sK}$ points, and the elementary boxes with K digits in every coordinate, the *cells*, have side $q^{-K} = N^{-1/s}$; a $(0, sK, s)$ -net has exactly one point in each cell. (The companion paper [18] calls the level k .) Not every result of this paper is about full levels: each one names the set of exponents m at which it bounds P_m (Section 2.4).

2.2. Frames and Scrambles. All sequences in this paper are scrambles of one classical family, the generalized Faure sequences of Faure [12], Niederreiter [30] and Tezuka [41, 42]. As in [18] we describe them by *places* on the projective line over $\mathbb{F}_q$. Fix distinct elements $a_0, \dots, a_{s-1} \in \mathbb{F}_q$ (so $s \leq q$), the places of the coordinates. Coordinate c of the unscrambled point reads the Taylor coefficients of the index polynomial at a_c :

$$y_{c,n}(V) = [(z - a_c)^n] V, \quad \text{i.e.} \quad C_c = P_{a_c}, \quad P_a[n][k] = \binom{k}{n} a^{k-n}.$$

The index itself is read at the place ∞ : the prefix P_m is the set of polynomials with a pole of order less than m at ∞ . We call $(a_0, \dots, a_{s-1}; \infty)$ a *frame*. For prime $q = p$ and the *Faure places* $0, 1, \dots, s-1$ this is the Faure sequence $(I, P, P^2, \dots, P^{s-1})$, since $P_a = P_1^a$; in dimension two it is (I, P) , which for $q = 2$ is the two-dimensional Sobol' sequence [38]. Up to a scramble, the frame sequence is the Niederreiter sequence with the linear base polynomials $z - a_c$ [30]. For prime q it is also exactly the Halton-type sequence of Goda, Hofer and Suzuki [16, Def. 2] with the monic linear bases $z - a_c$: the $(z - a_c)$ -adic digits of the index polynomial are its Taylor coefficients at a_c , and their index and digit conventions coincide with ours. For $s \geq 2$ no such sequence is quasi-uniform (Section 3).

In words: read the digits of the index as a polynomial V ; coordinate c is the Taylor expansion of V around its own point a_c . For example, let $q = 3$ and $V = 2 + z$ (integer index $5 = 2 + 1 \cdot 3$). At $a = 0$ the Taylor digits are $(2, 1)$; at $a = 1$, $V = 0 + 1 \cdot (z - 1)$ in $\mathbb{F}_3$, so the digits are $(0, 1)$. A polynomial of degree less than 2 is determined by $(V(0), V(1))$, that is, by its cell: this is the net property for $s = 2$ and one digit per coordinate, and Lemma 1 below is the same statement for every s and every number of digits.

A Taylor coefficient is a residue: $[(z - a)^n] V = \text{Res}_a(V(z - a)^{-n-1} dz)$, where $\text{Res}_a(F dz)$ denotes the coefficient of $(z - a)^{-1}$ in the expansion of F in powers of $z - a$. Section 4 uses this to write every scramble, and Sections 5–7 use it to design them.

A *scramble* of coordinate c is an infinite lower-triangular matrix L_c with nonzero diagonal, fixed once and for all (independent of m). The scrambled sequence has the generator matrices $C_c = L_c P_{a_c}$: digit n of the scrambled coordinate is a linear combination of the unscrambled digits $0, \dots, n$, with a nonzero coefficient on digit n . Dick, Goda and Suzuki, and Goda, Hofer

and Suzuki, number the coordinates from 1, so (L_1, L_2P) in the notation of [10] is (L_0, L_1P_1) here.

Lemma 1 (Frames have $t = 0$). *For distinct places $a_0, \dots, a_{s-1} \in \mathbb{F}_q$ and arbitrary scrambles $L_0, \dots, L_{s-1}$, the digital sequence with generator matrices $C_c = L_c P_{a_c}$ is a $(0, s)$ -sequence in base q .*

Proof. Let $m \geq 1$ and $\sum_c d_c = m$. For the unscrambled frame, the first d_c digits of coordinate c are the coefficients of $V \bmod (z - a_c)^{d_c}$ in the basis $(z - a_c)^n$. By the Chinese remainder theorem the map $V \mapsto (V \bmod (z - a_c)^{d_c})_c$ is a bijection from the polynomials of degree less than m onto $\prod_c \mathbb{F}_q[z]/((z - a_c)^{d_c})$: both sides have q^m elements, and a polynomial of degree less than m divisible by $\prod_c (z - a_c)^{d_c}$ is zero. So every box matrix is invertible. A lower-triangular L_c replaces the first d_c rows of C_c by an invertible combination of themselves, so every box minor is multiplied by $\prod_c \det L_{c,[d_c]} \neq 0$, where $L_{c,[d]}$ is the leading $d \times d$ block (the scrambling identity of [18]). Every prefix is therefore a $(0, m, s)$ -net. $\square$

That scrambling preserves t is classical: for nested random scrambles it is due to Owen [33], and for lower-triangular linear scrambles it underlies the generalized Faure sequences of Tezuka [42] and Matoušek's linear scrambling [28]. So $t = 0$ comes for free; what the scramble changes, and what this paper is about, is the position of each point inside its cell.

2.3. Separation and Quasi-Uniformity. For $\mathbf{y}, \mathbf{y}' \in [0, 1]^s$ let $\|\mathbf{y} - \mathbf{y}'\|_T = \min_{\mathbf{k} \in \mathbb{Z}^s} \|\mathbf{y} - \mathbf{y}' + \mathbf{k}\|$ be the toroidal Euclidean distance. For a finite point set P with $N \geq 2$ points, the *separation* is

$$\delta(P) = \min_{\mathbf{y} \neq \mathbf{y}' \in P} \|\mathbf{y} - \mathbf{y}'\|_T, \quad \text{and} \quad \text{sep}(P) = \delta(P) N^{1/s}$$

is its *separation constant*. A $(0, sK, s)$ -net has one point in each cell of side $N^{-1/s}$, so $\text{sep}(P)$ measures the separation in cell units; $\text{sep}(P) = 1$ for the grid $q^{-K}\mathbb{Z}^s$.

The *covering radius* is $h(P) = \sup_{\mathbf{y} \in [0, 1]^s} \min_{\mathbf{y}' \in P} \|\mathbf{y} - \mathbf{y}'\|$, and $h(P)/\delta(P)$ is the *mesh ratio*. A sequence is *quasi-uniform* if the mesh ratio $h(P_{[N]})/\delta(P_{[N]})$ is bounded over all $N \geq 2$ [9, 10]. Since $h(P) \gtrsim N^{-1/s}$ and $\delta(P) \lesssim N^{-1/s}$ for every N -point set, this is the same as $h(P_{[N]}) \asymp N^{-1/s}$ and $\delta(P_{[N]}) \asymp N^{-1/s}$. We state mesh ratios as h/δ ; the convention of [10] divides by the separation radius $\delta/2$ and gives twice our value.

Which distance. The toroidal distance never exceeds the Euclidean distance in the cube. Our lower bounds on δ are toroidal, so they hold for the Euclidean separation of [9, 10, 16] as well. Our upper bounds on δ (the close pairs of Section 3) bound the Euclidean distance in the cube, so they bound the toroidal separation too. Our bounds on h are for the Euclidean distance in the cube. So every statement transfers to both conventions in the direction in which it is used.

2.4. Level Families. For a $(0, s)$ -sequence the covering radius is never the problem: the prefixes are nets at every scale. The problem is the separation, and it suffices to control it along one family of prefixes. The general principle, that quasi-uniformity along a subsequence of sizes with bounded ratios implies quasi-uniformity along all N , is [9, Lemma 1.3]; we give the toroidal version with explicit constants, for the families of prefixes that occur in this paper.

A *level family* is an infinite set $\mathcal{M} \subseteq \mathbb{N} = \{1, 2, \dots\}$ of exponents m , namely those at which a result certifies a bound on $\text{sep}(P_m)$. Its *largest gap* is

$$\Delta_{\mathcal{M}} := \max(\min \mathcal{M}, \sup\{m' - m : m < m' \text{ consecutive elements of } \mathcal{M}\}).$$

The families of this paper are $\mathcal{M} = s\mathbb{N}$ (all full levels, $\Delta_{\mathcal{M}} = s$), $\mathcal{M} = s\mathbb{N} - 1 = \{s-1, 2s-1, \dots\}$ ($\Delta_{\mathcal{M}} = s$), $\mathcal{M} = s^2\mathbb{N}$ ($\Delta_{\mathcal{M}} = s^2$), and unions of residue classes of these (Section 6).

Lemma 2 (Prefix lemma). *Let $(y(V))$ be a $(0, s)$ -sequence in base q and $\mathcal{M}$ a level family with $\Delta := \Delta_{\mathcal{M}} < \infty$. Suppose that $\text{sep}(P_m) \geq \text{LB}$ for every $m \in \mathcal{M}$, with $\text{LB} > 0$. Then for every $N \geq 2$*

$$\delta(P_{[N]}) \geq \text{LB } q^{-\Delta/s} N^{-1/s}, \quad h(P_{[N]}) \leq \sqrt{s} q N^{-1/s}, \quad \frac{h(P_{[N]})}{\delta(P_{[N]})} \leq \frac{\sqrt{s} q^{1+\Delta/s}}{\text{LB}}.$$

In particular the sequence is quasi-uniform.

Proof. Separation. Let $N \geq 2$ and let m' be the least element of $\mathcal{M}$ with $q^{m'} \geq N$. Then $P_{[N]} \subseteq P_{m'}$, and a subset has at least the separation of the whole set, so $\delta(P_{[N]}) \geq \delta(P_{m'}) \geq \text{LB } q^{-m'/s}$. It remains to show $q^{m'} \leq q^\Delta N$. If $m' = \min \mathcal{M}$, then $q^{m'} \leq q^\Delta \leq q^\Delta N$. Otherwise m' has a predecessor m'' in $\mathcal{M}$; by the choice of m' , $q^{m''} < N$, and $m' - m'' \leq \Delta$, so $q^{m'} \leq q^\Delta q^{m''} < q^\Delta N$.

Covering. Let $m \geq 0$ with $q^m \leq N < q^{m+1}$, and write $m = sK + j$ with $0 \leq j < s$. The first q^m points form the prefix $P_m \subseteq P_{[N]}$, which is a $(0, m, s)$ -net. Split the cube into the elementary boxes with $K + 1$ digits in the first j coordinates and K digits in the others. Each has volume q^{-m} , so it contains a point of P_m , and its diameter is at most $\sqrt{s} q^{-K}$. Every point of $[0, 1]^s$ lies in the closure of one of these boxes, so $h(P_{[N]}) \leq \sqrt{s} q^{-K}$. Finally $q^{-K} = q^{(j-m)/s} < q^{(j+1)/s} N^{-1/s} \leq q N^{-1/s}$, since $j + 1 \leq s$.

The bound on the mesh ratio is the quotient of the two bounds. $\square$

Remark 3 (The cases used). For $\mathcal{M} = s\mathbb{N}$ and $\mathcal{M} = s\mathbb{N} - 1$ the factor is $q^{-\Delta/s} = 1/q$: $\delta(P_{[N]}) \geq (\text{LB}/q) N^{-1/s}$. For $\mathcal{M} = s^2\mathbb{N}$ it is q^{-s} . For $\mathcal{M} = s\mathbb{N}$ comparing the two intermediate bounds directly gives the sharper mesh ratio $h/\delta \leq \sqrt{s} q/\text{LB}$: if $q^{sK} \leq N < q^{s(K+1)}$, the covering argument gives $h \leq \sqrt{s} q^{-K}$ and the separation argument $\delta \geq \text{LB } q^{-K-1}$ (for $K = 0$, $h \leq \sqrt{s}$ and $\delta \geq \text{LB}/q$).

The lemma loses the factor $q^{-\Delta/s}$ only at the prefixes between two elements of $\mathcal{M}$: for consecutive $m'' < m < m'$ in $\mathcal{M}$ the separation argument gives $\text{sep}(P_m) \geq \text{LB } q^{(m-m'')/s}$. A construction certified at a denser family therefore has the better bound for all N , even when its constant at the certified levels is smaller (Sections 6 and 7).

2.5. Conventions. Every result names its level family: the exponents m at which it bounds $\text{sep}(P_m)$, for every element of the family at once. The bound for all N then follows from Lemma 2.

Every result has a written proof. Some proofs end in an exact finite computation: a minimum over an explicitly enumerated finite set, or explicit integer hypotheses checked at each prime of a finite range. We call such a proof *computer-assisted* (c.a.) and state its scope with the result. A proof whose last step is one exact rational evaluation is marked *proof**; the threshold $p_0(s)$ of Section 8 is the infimum of explicit monotone conditions, and an upper estimate of it is certified in this way. Searches only find parameters (multipliers, check vectors, window systems, tables), whose properties are then proved or checked; a value found by a search is a lower bound on an optimum, never a claim of optimality. Exact separations quoted for figures and tables are illustrations. No proof uses a search or an illustration. A statement that a construction fails, or that a kind of certificate cannot do better, is always made with its exact scope (which sequences, which scrambles, which kind of certificate); a finite search is never used as evidence that something does not exist. Appendix C lists the data, the independent re-verification and the parts that are in addition verified in Lean. Table 3 lists the main symbols and terms.

3. WHY THE CLASSICAL SEQUENCES FAIL

The classical low-discrepancy sequences of Halton, Faure, Sobol' and Niederreiter are built from polynomial bases. Each coordinate reads the index polynomial in its own base $b_c(z)$, one

TABLE 3. Notation and terms at a glance. Terms marked [18] are used in the sense of the companion paper on nets.

symbol or term	meaning	defined in
q, p, s	base (prime power $q = p^r$), its characteristic, dimension	§2
$V, \iota(V)$	index polynomial of a point; its integer index	§2
$P_m, P_{[N]}$	first q^m points, first N points	§2
full level, cell	prefix P_{sK} ; elementary cube of side q^{-K}	§2
level family $\mathcal{M}, \Delta_{\mathcal{M}}$	the exponents m with a certified bound on $\text{sep}(P_m)$; its largest gap	§2.4
$\text{sep}(P) = \delta(P)N^{1/s}$	toroidal separation in cell units (1 for the grid)	§2
natural identification	digits of $\mathbb{F}_q$ read as integers through base- p coordinates	§2
frame, places a_c, P_a	coordinate c reads the Taylor digits of V at a_c ; Pascal matrix	§2
scramble L_c	lower-triangular, nonzero diagonal, fixed for all prefixes	§2
b_c -adic coordinate	its first $e_c Q$ digits depend only on $V \bmod b_c^Q$	§3
radical inverse, digit map	digit block Q is π_c of the Q -th b_c -adic digit of V	§3
π_c		
Halton-type sequence	coordinate c reads the b_c -adic digits of V ; pairwise coprime $b_c \in \mathbb{F}_p[z]$ [16]	§3
geometric digit(s) r_c, R_c ; layer	first digit(s) of coordinate c below the cell; layer: their change $D(1)$ under a carry-free step	(3)
lattice image, jitter ε_c	$n + \text{enc}(R)/q^j$; the contribution of the deeper digits ($\leq q^{-j}$)	(3)
offset map	linear map from the cell digits to the geometric digits of P_{sK}	§4
carry length l , carry depth	cell digits changed by a step; coefficient index from the finest digit	§4
carry response $D_i(l)$	change of digit $K + i$ under a carry of length l in one coordinate	§4
own, cross response	$O_c^{(l)}$: moving coordinate; $X_{c \leftarrow c'}^{(l)}$: coordinate c when c' moves	§4
constant response	a response that does not depend on the carry length	§4.3
slip planes	hyperplanes where a geometric digit wraps around modulo q	§4.3
jump of depth l	change of the lattice image across a boundary of carry length $l \geq 2$	§4.3
uniformizer w , local root	$w = \prod_c (z - a_c)$; the root of $w(Z) = x$ at a_c	(5)
z_c		
self-similar scramble, θ, g_c	one multiplier series per coordinate; scale; multipliers	Def. 20
Res_a , principal part	coefficient of $(z - a)^{-1} dz$; the polar terms at a	§2, Lem. 21
local multiplier φ_c	unit series in $z - a_c$; $y_{c,n} = \text{Res}_{a_c}(V\varphi_c(\theta/w)^{n+1} dz)$	Lem. 21
f_j, LB_j	guaranteed gap in one coordinate; digit relaxation with j digits	Lem. 23
exact digit relation	linear identity among the digits of a prefix, of bounded depth	Def. 49
depth J ; admissible range	relation of top index T uses the digits $T - J, \dots, T$; levels $[K_0, K_0 + R]$ of Thm. 51	Def. 49, §7.2
level-independent relation	exact relation with the same coefficients at every level	Prop. 54
skeleton coordinate, digit	at P_{sK-1} : a coordinate with one cell digit fewer; its next digit	§5
skeleton relation, fine cell	$\sum_c v_c y_{c,K-1} = 0$ on P_{sK-1} ; cube of side q^{-K} at P_{sK-1}	§5
check vector v ; Λ_v ; λ_{jit}	$\Lambda_v = \{b \in \mathbb{Z}^s : v \cdot b \equiv 0 \bmod p\}$; $\lambda_{\text{jit}}(\Lambda) = \min_{b \neq 0} \ (b - 1)_+\ _2$	§5
residue sequence $\mathcal{R}_v$	every coordinate reads the differential $V dz$ at its place	Def. 33
staggered res. sequence	geometric digit of $c_\star = \text{rank-1}$ lattice rule in the finest cell digits	Def. 25
$\mathcal{R}_v^\star, c_\star$		
$ x $	centred absolute value of $x \in \mathbb{F}_p$, in $[0, p/2]$	§5.2
brick wall W^-	$\mathcal{R}_v^\star$ for $s = 2$: heights staggered by half a cell between columns	Def. 31
inclusion bound	bound on $\text{sep}(P_{sK})$ from $P_{sK} \subset P_{s(K+1)-1}$	Rem. 40
design, reachable	matrices F_n : geometric digits from the last cell levels [18]	§6
block-periodic residue seq.	local multipliers repeat with period ℓ in the row index	Def. 41
free series ψ_c ; cross $\kappa_{c \leftarrow c'}$	what a self-similar scramble leaves free; $\kappa_{c \leftarrow c'} = -X_{c \leftarrow c'}^{(1)}$	Prop. 62
window W , $\text{LB}(W)$	set of values a response may take; the bound given by the windows	Prop. 64
covering condition	every line of the depth direction meets the window	Prop. 64
selection rule, history	picks an admissible free digit at each depth; the digits chosen before	Prop. 64
correction terms $\chi_{c,d}, \Psi_c$	deeper digits in a corrected skeleton relation; their partial sums	Lem. 71
staggered windows, $\frac{1}{2}$	staggered coordinate offset by half a cell; $\frac{1}{2} = (p+1)/2 \in \mathbb{F}_p$	§8
first-order deficit	the constant C in a bound $1 - C/p$ [18]	§8
$p_0(s)$	threshold of the staggered rule	§8
proof * , c.a.	last step one exact rational evaluation; computer-assisted	§2.5

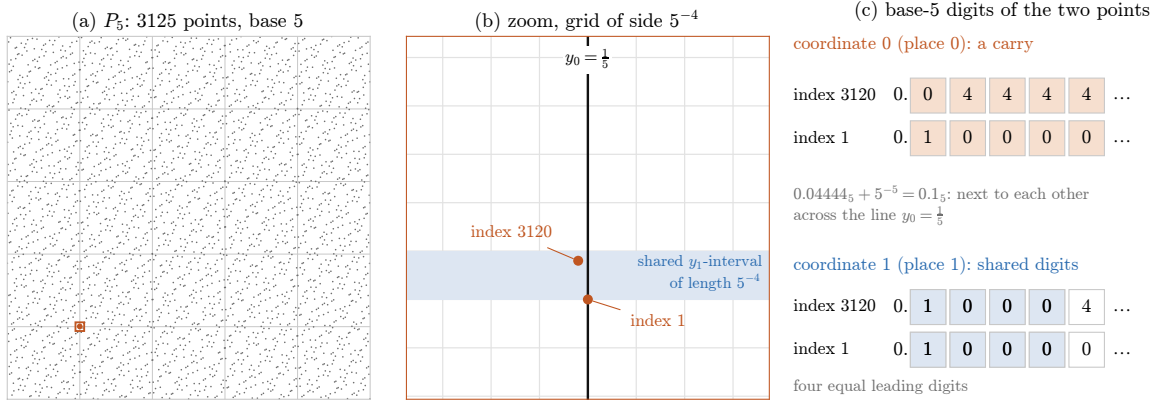


FIGURE 2. A carry that the other coordinate cannot see. The two-dimensional Faure sequence (I, P) in base 5 (the Halton-type sequence with the bases z and $z - 1$), prefix P_5 (3125 points), exact points from the generator matrices. (a) The prefix; the small box marks a closest pair, the points with indices 1 and 3120 (the minimum is attained by several pairs). (b) Zoom with the grid of side 5^{-4} : the two points lie on either side of the line $y_0 = \frac{1}{5}$ and in the same interval of length 5^{-4} of coordinate 1. (c) Their digits. Coordinate 0 is a carry: 0.04444_5 and 0.1_5 differ by 5^{-5} . Coordinate 1 has four equal leading digits. The distance $\sqrt{17} \cdot 5^{-5} = 1.32 \cdot 10^{-3}$ is the separation of P_5 (Euclidean and toroidal; $\text{sep}(P_5) = 0.0738$), and the pair is the one of Remark 9 with $Q = 5$.

block of digits at a time, like a radical inverse. Their prefixes are nets at every scale, so their covering radius is always of the right order $N^{-1/s}$. Dick, Goda and Suzuki asked for quasi-uniform digital sequences [10], and Goda, Hofer and Suzuki asked whether any Halton-type sequence is [16]. For the classical sequences of all four kinds the answer is no, and the reason is one picture.

Take two indices whose difference is a carry in the last digits of one coordinate. In base p the digits $0.a(p-1) \cdots (p-1)$ of one point become $0.(a+1)0 \cdots 0$ for the other: the two points sit on either side of a cell boundary, one unit of the last digit apart. If the same index difference is divisible by a high power of every other base, then it does not change the leading digits of any other coordinate. The two points are close in every coordinate at once, much closer than $N^{-1/s}$ (Figure 2). For polynomial bases such differences exist at infinitely many sizes, because a run of ones in one base is divisible by high powers of all the other bases (Theorem 6).

This section proves this for every digital sequence in polynomial bases with one coordinate a radical inverse (Theorem 6), derives the classical cases (Halton-type, Faure, Niederreiter and Sobol' sequences), and shows which scrambles do not help: as long as one coordinate is still a radical inverse, up to a scalar, the sequence is not quasi-uniform, whatever triangular scrambles the other coordinates receive (Corollary 14). The repair scrambles every coordinate, through residues at the places (Sections 4 and 5).

Throughout this section $s \geq 2$, $q = p^r$, and digits are read through the natural identification enc of Section 2. The distance between two points is the Euclidean distance in the cube; it bounds the toroidal distance from above, so every upper bound on δ below holds for both (Section 2). As in [16], the separation of a prefix is the minimum over pairs of distinct indices.

3.1. Polynomial Bases. Let $b_c \in \mathbb{F}_q[z]$ have degree $e_c \geq 1$; it need not be monic or irreducible. Every $V \in \mathbb{F}_q[z]$ has a unique b_c -adic expansion $V = \sum_{Q \geq 0} a_Q b_c^Q$ with $\deg a_Q < e_c$, obtained by

repeated division by b_c ; the a_Q are the b_c -adic digits of V , and $a_0, \dots, a_{Q-1}$ are determined by $V \bmod b_c^Q$. The map $V \mapsto (a_Q)_Q$ is $\mathbb{F}_q$ -linear.

Definition 4 (b_c -adic coordinates and radical inverses). Coordinate c of a digital sequence over $\mathbb{F}_q$ is b_c -adic if for every $Q \geq 1$ its first $e_c Q$ digits $y_{c,0}(V), \dots, y_{c,e_c Q-1}(V)$ depend only on $V \bmod b_c^Q$; by linearity this means that they vanish for $V \in b_c^Q \mathbb{F}_q[z]$. It is a b_c -adic radical inverse with digit map π_c , where π_c is an $\mathbb{F}_q$ -linear bijection from the polynomials of degree less than e_c onto $\mathbb{F}_q^{e_c}$, if for every V and every $Q \geq 0$ its digit block $(y_{c,Qe_c}(V), \dots, y_{c,(Q+1)e_c-1}(V))$ equals $\pi_c(a_Q)$, where a_Q is the Q -th b_c -adic digit of V .

A radical inverse is b_c -adic. The examples:

- The unscrambled frame of Section 2: coordinate c is a $(z - a_c)$ -adic radical inverse with the identity as digit map, since the $(z - a_c)$ -adic digits of V are its Taylor coefficients at a_c .
- The Halton-type sequences of Goda, Hofer and Suzuki [16, Def. 2], in the sense of Hofer [22]: $q = p$ prime, pairwise coprime $b_0, \dots, b_{s-1} \in \mathbb{F}_p[z]$, and coordinate c reads the b_c -adic digits of the index, each digit a_Q written as the e_c base- p digits given by its coefficients, the coefficient of z^{e_c-1} first. This is a b_c -adic radical inverse with $\pi_c(a) = ([z^{e_c-1}]a, \dots, [z^0]a)$. Their index $n = \sum_i n_i p^i \mapsto \sum_i n_i z^i$ is our V with $\iota(V) = n$.
- A lower-triangular scramble L_c of a b_c -adic coordinate is b_c -adic: its first d digits are combinations of the first d unscrambled digits. A nonzero scalar multiple of a radical inverse with digit map π_c is a radical inverse with digit map $\mu\pi_c$.
- Sobol' and Niederreiter sequences (Lemmas 12 and 10 below).

For a digital sequence the digits of the two points with indices V and $V + D$ differ by the digits of D , coordinate by coordinate. So a coordinate is blind to every index difference D that is divisible by a high power of its base: the leading digits of the two points agree.

3.2. A Close Pair from a Carry. In a prime base the carry looks as follows. Add the digit string $0.011 \dots 1$ to $0.00(p-1) \dots (p-1)$ digit by digit modulo p : the result is $0.010 \dots 0$, which as a real number is exactly one unit of the last digit larger. For a prime power $q = p^r$ the same works with two special digits. Put

$$\bar{y} = \text{enc}^{-1}(q-1), \quad y^\circ = \text{enc}^{-1}(q/p-1),$$

so $\bar{y} = -1$ and $y^\circ = 0$ for prime q . Under the natural identification enc^{-1} is additive on base- p digit vectors. The integers $q/p-1$ and q/p have the base- p digit vectors $(p-1, \dots, p-1, 0)$ and $(0, \dots, 0, 1)$, and $q-1$ and 0 have $(p-1, \dots, p-1)$ and $(0, \dots, 0)$. In both cases the difference is the vector $(1, \dots, 1)$ modulo p , so

$$(1) \quad \text{enc}^{-1}(q/p) - y^\circ = \text{enc}^{-1}(0) - \bar{y} = -\bar{y}.$$

Adding $-\bar{y}$ to every digit of $y^\circ \bar{y} \dots \bar{y}$ therefore gives $\text{enc}^{-1}(q/p) 0 \dots 0$, one unit of the last digit more.

In the lemma below these digits are written as polynomials of degree less than e through the digit map π : g is the carry digit, added at every position of the run, and $\tilde{g}$ and g' write the lower of the two points, just below the cell boundary. The lemma needs three things of the index difference D : in the carrying base it is a run of the carry digit, (i); in every other base it is divisible by a high power, (ii), so those coordinates share their leading digits; and it is small enough for both points to lie in P_m , (iii).

Lemma 5 (A close pair from a carry). *Let coordinate $\hat{c}$ of a digital sequence over $\mathbb{F}_q$ be a b -adic radical inverse with digit map π , where $b = b_{\hat{c}}$ has degree $e = e_{\hat{c}}$, and let every other coordinate*

c be b_c -adic. Let $g, \tilde{g}, g' \in \mathbb{F}_q[z]$ have degree less than e with

$$\pi(g) = -\bar{y}(1, \dots, 1), \quad \pi(\tilde{g}) = (y^\circ, \bar{y}, \dots, \bar{y}), \quad \pi(g') = \bar{y}(1, \dots, 1),$$

and put $S_n = (b^n - 1)/(b - 1) = 1 + b + \dots + b^{n-1}$. Let $D \in \mathbb{F}_q[z] \setminus \{0\}$, let $0 \leq \eta < \lambda$ be integers, $L = e\lambda$, and suppose

- (i) $D \equiv g b^\eta S_{\lambda-\eta} \pmod{b^\lambda}$;
- (ii) for every $c \neq \hat{c}$, $b_c^{j_c}$ divides D for some j_c with $e_c j_c \geq L$;
- (iii) $\deg D < m$.

Then $V_1 = \tilde{g} b^\eta + g' b^{\eta+1} S_{\lambda-\eta-1}$ and $V_2 = V_1 + D$ are indices of points of P_m , and $\|y(V_1) - y(V_2)\| < \sqrt{s+3} q^{-L}$. In particular $\delta(P_m) < \sqrt{s+3} q^{-L}$ and $\text{sep}(P_m) < \sqrt{s+3} q^{m/s-L}$.

Proof. Degrees. $\deg V_1 \leq e(\lambda - 1) + e - 1 < L$. By (ii) for one $c \neq \hat{c}$ (here $s \geq 2$ is used) and $D \neq 0$, $\deg D \geq e_c j_c \geq L$, so $L < m$ by (iii). Hence V_1 and V_2 have degree less than m , and $V_1 \neq V_2$.

Coordinate $\hat{c}$. $V_1 = \tilde{g} b^\eta + \sum_{j=\eta+1}^{\lambda-1} g' b^j$ is its own b -adic expansion: its b -adic digits are $\tilde{g}$ at position η , g' at the positions $\eta + 1, \dots, \lambda - 1$, and 0 elsewhere. By (i) the b -adic digits of D at the positions below λ are those of $g b^\eta S_{\lambda-\eta} = \sum_{j=\eta}^{\lambda-1} g b^j$: 0 below η and g from η on. Applying π blockwise and using linearity, the first L digits of coordinate $\hat{c}$ are

$$V_1 : (0^{e\eta}, y^\circ, \bar{y}^{L-e\eta-1}), \quad V_2 : (0^{e\eta}, y^\circ - \bar{y}, 0^{L-e\eta-1}) = (0^{e\eta}, \text{enc}^{-1}(q/p), 0^{L-e\eta-1})$$

by (1). Read as integers in units of q^{-L} , these prefixes are $A = (q/p - 1)q^{L-e\eta-1} + q^{L-e\eta-1} - 1$ and $(q/p)q^{L-e\eta-1} = A + 1$. A polynomial has finitely many nonzero b -adic digits and $\pi(0) = 0$, so the remaining digits of each point are finitely many and contribute some $\tau_i \in [0, q^{-L})$. Hence $y_{\hat{c}}(V_2) - y_{\hat{c}}(V_1) = q^{-L} + \tau_2 - \tau_1 \in (0, 2q^{-L})$.

Coordinates $c \neq \hat{c}$. $V_2 - V_1 = D$ is divisible by $b_c^{j_c}$, so the first $e_c j_c \geq L$ digits of coordinate c agree, the two values lie in one closed interval of length q^{-L} , and $|y_c(V_2) - y_c(V_1)| \leq q^{-L}$.

Summing the squares, $\|y(V_1) - y(V_2)\|^2 < (4 + s - 1) q^{-2L}$. $\square$

The lemma turns the search for a close pair into polynomial arithmetic: one needs a difference D of small degree that is a run of the carry digit g in base b and is divisible by high powers of all the other bases. What counts is the excess $sL - m$ of the length of the shared digits over the cell side: the lemma gives $\text{sep}(P_m) < \sqrt{s+3} q^{-(sL-m)/s}$. A family of differences along which $sL - m$ grows without bound proves that the sequence is not quasi-uniform.

3.3. The General Theorem. The differences come from one divisibility. In the carrying base b , the run of ones is $S_n = 1 + b + \dots + b^{n-1} = (b^n - 1)/(b - 1)$. Let Θ be the product of the other bases, each raised to a power so that all factors have the same degree, and $R = (1 - b)\Theta$. The polynomial b is a unit modulo R , so some power b^ν is $\equiv 1 \pmod{R}$, and then S_ν is divisible by Θ , that is, by all the other bases. Multiplying by a power of the other bases that is $\equiv 1$ modulo b^ν lengthens their shared digits without touching the carry, and raising to the power $Q = p^w$ (the Frobenius map) stretches carry and shared digits by Q , while the excess grows linearly in Q .

Theorem 6 (Polynomial-base digital sequences are not quasi-uniform). *Let $s \geq 2$ and let a digital sequence over $\mathbb{F}_q$ have pairwise coprime $b_0, \dots, b_{s-1} \in \mathbb{F}_q[z]$ of degrees $e_c \geq 1$ such that every coordinate c is b_c -adic and one coordinate $\hat{c}$ is a $b_{\hat{c}}$ -adic radical inverse (Definition 4). Put $b = b_{\hat{c}}$, $e = e_{\hat{c}}$, $E = \text{lcm}(e_0, \dots, e_{s-1})$ and*

$$\Theta = \prod_{c \neq \hat{c}} b_c^{E/e_c}, \quad R = (1 - b) \Theta.$$

Let $\nu \geq 1$ be such that R divides $b^\nu - 1$ (for example the order of b modulo R), let $k \geq 1$ be a multiple of the order of Θ modulo b^ν with $(E/e)(k+1) \geq \nu$, and put $\eta = (E/e)(k+1) - \nu$. With g as in Lemma 5, define for $Q \in \{1, p, p^2, \dots\}$

$$D_Q = g b^{Q\eta} S_{Q\nu} \Theta^{Qk}, \quad L_Q = QE(k+1), \quad m_Q = Q(sE(k+1) - (s-1)E).$$

Then D_Q satisfies (i)–(iii) of Lemma 5 with $(\eta, \lambda, L, m) = (Q\eta, Q(\eta+\nu), L_Q, m_Q)$. So P_{m_Q} contains the two points with indices V_1 and $V_1 + D_Q$ of the lemma, at distance less than $\sqrt{s+3} q^{-L_Q}$, and

$$\text{sep}(P_{m_Q}) < \sqrt{s+3} q^{-Q(s-1)E/s}, \quad \text{sep}(P_{sK_Q}) < \sqrt{s+3} q^{1-Q(s-1)E/s} \quad (K_Q = \lceil m_Q/s \rceil).$$

Both tend to 0 as $Q \rightarrow \infty$, and the sequence is not quasi-uniform.

Proof. Existence of ν and k . A common factor of b and $1-b$ divides 1, and b is coprime to every b_c with $c \neq \hat{c}$; so b is a unit in the finite ring $\mathbb{F}_q[z]/(R)$ ($\deg R \geq e \geq 1$), and its order is an admissible ν . Likewise Θ is a unit modulo b^ν , and any large multiple of its order serves as k . The integer η is ≥ 0 , and it is an integer because e divides E .

(i). Since k is a multiple of the order of Θ modulo b^ν , $\Theta^k = 1 + b^\nu H$ for a polynomial H . In characteristic p the map $f \mapsto f^Q$ is additive on $\mathbb{F}_q[z]$ for every power Q of p , so

$$\Theta^{Qk} = (1 + b^\nu H)^Q = 1 + b^{Q\nu} H^Q.$$

(Only $1^Q = 1$ is used here. Had we only $\Theta^k \equiv \gamma \pmod{b^\nu}$ with a constant $\gamma \neq 1$, we would get γ^Q , and $\gamma^Q = \gamma$ would require Q to be a power of q .) Hence $D_Q \equiv g b^{Q\eta} S_{Q\nu} \pmod{b^{Q\eta+Q\nu}}$, which is (i) with $\eta \mapsto Q\eta$, $\lambda = Q(\eta + \nu)$ and $\lambda - Q\eta = Q\nu$. Then $L = e\lambda = QE(k+1) = L_Q$.

(ii). R divides $b^\nu - 1$, so R^Q divides $(b^\nu - 1)^Q = b^{Q\nu} - 1 = (b-1)S_{Q\nu}$, by additivity of $f \mapsto f^Q$ again. As $R^Q = (1-b)^Q \Theta^Q$ and $b-1 \neq 0$, cancelling one factor $b-1$ in the factorial ring $\mathbb{F}_q[z]$ gives $(b-1)^{Q-1} \Theta^Q \mid S_{Q\nu}$. So $\Theta^{Q(k+1)}$ divides D_Q , and $b_c^{j_c}$ divides D_Q with $j_c = QE(k+1)/e_c$, that is $e_c j_c = L_Q$, for every $c \neq \hat{c}$.

(iii). $\deg \Theta = (s-1)E$, so

$$\deg D_Q \leq (e-1) + eQ\eta + e(Q\nu - 1) + (s-1)EQk = L_Q - 1 + (s-1)(L_Q - QE) = m_Q - 1.$$

Lemma 5 gives the pair and $\text{sep}(P_{m_Q}) < \sqrt{s+3} q^{m_Q/s - L_Q}$, and $m_Q/s - L_Q = -Q(s-1)E/s$. The pair also lies in the full level $P_{sK_Q} \supseteq P_{m_Q}$, and $K_Q - L_Q \leq m_Q/s + 1 - L_Q$. Finally, N balls of radius $h(P)$ cover the cube, so $h(P) \geq \omega_s^{-1/s} N^{-1/s}$ for every N -point set, ω_s the volume of the unit ball. Along $N = q^{m_Q}$ the mesh ratio is therefore at least $\omega_s^{-1/s} / \text{sep}(P_{m_Q}) \rightarrow \infty$. $\square$

The pair needs nothing about the coordinates $c \neq \hat{c}$ except that they are b_c -adic, and nothing about $\hat{c}$ except its digit map π (through g and V_1). For a fixed choice of bases and of π , the close pairs are the same for every choice of the other coordinates. The levels m_Q can be very large (Table 4), but they are explicit, and nothing is searched. The theorem gives upper bounds on δ along one family of levels; it does not determine the rate at which the separation decays.

In the language of Section 4 (where carry responses are defined), the index difference D_Q moves the point of a cell to the next cell of coordinate $\hat{c}$ with an own response of $+1$ in the last digit and with cross responses that vanish to many digits: the configuration that Remark 24 calls fatal.

3.4. Halton-Type and Faure Sequences. Goda, Hofer and Suzuki proved that the Halton sequences (in integer bases) are not quasi-uniform, and so are three families of Halton-type sequences: dimension two with the bases $z+a, z+a+1$; base two with the bases $z, z+1, z^2+z+1$; and dimension p with the bases $z, z-1, \dots, z-(p-1)$ [16, Thm. 2]. Their Open Problem 2 asks to “prove or disprove that no Halton-type sequence is quasi-uniform” in dimension $d \geq 2$ and,

if none is, to find for arbitrary bases a pair of indices that disproves quasi-uniformity [16, Open Problem 2] (wording of the arXiv version). The following corollary answers it in the affirmative, with explicit pairs.

Corollary 7 (No Halton-type sequence is quasi-uniform). *Let p be prime, $s \geq 2$, and let $b_0, \dots, b_{s-1} \in \mathbb{F}_p[z]$ be pairwise coprime of degrees $e_c \geq 1$, not necessarily monic or irreducible. The Halton-type sequence in these bases [16, Def. 2] is not quasi-uniform. Explicitly, choose any coordinate $\hat{c}$, use the notation of Theorem 6, and put $\Sigma = 1 + z + \dots + z^{e-1}$ and $\Sigma' = 1 + z + \dots + z^{e-2}$ ($\Sigma' = 0$ for $e = 1$). For $Q = 1, p, p^2, \dots$ the indices*

$$V_1 = -\Sigma' b^{Q\eta} - \Sigma b^{Q\eta+1} S_{Q\nu-1}, \quad V_2 = V_1 + \Sigma b^{Q\eta} S_{Q\nu} \Theta^{Qk}$$

satisfy $\iota(V_1), \iota(V_2) < p^{mQ}$, the two points are at Euclidean distance less than $\sqrt{s+3} p^{-LQ}$, and $\delta(P_{mQ}) p^{mQ/s} < \sqrt{s+3} p^{-Q(s-1)E/s}$.

Proof. Every coordinate is a b_c -adic radical inverse with $\pi_c(a) = ([z^{e_c-1}]a, \dots, [z^0]a)$ (Section 3.1), and the sequence is digital over $\mathbb{F}_p$ because the b_c -adic digits depend linearly on the index. For $q = p$ we have $\bar{y} = -1$ and $y^\circ = 0$, so $g = \Sigma$, $\tilde{g} = -\Sigma'$ and $g' = -\Sigma$ in Lemma 5. Theorem 6 applies with any $\hat{c}$. $\square$

The corollary concerns the Halton-type sequences of [16, Def. 2], over prime fields. Theorem 6 holds over $\mathbb{F}_q$ whenever digits are read through the natural identification; the more general Halton-type sequences of Hofer in rational bases [23], to which [16] refer, are not treated here (Section 11). For linear bases the corollary is about the unscrambled frames of Section 2.

Corollary 8 (Faure sequences and unscrambled frames). *For every prime power q , every $2 \leq s \leq q$ and all distinct places $a_0, \dots, a_{s-1} \in \mathbb{F}_q$, the unscrambled frame sequence $(P_{a_0}, \dots, P_{a_{s-1}})$ is not quasi-uniform. In particular, the Faure sequence $(P^0, P^1, \dots, P^{s-1})$ in prime base p is not quasi-uniform for every $2 \leq s \leq p$.*

Proof. Coordinate c is a $(z - a_c)$ -adic radical inverse with the identity as digit map, and distinct linear polynomials are pairwise coprime. Apply Theorem 6. The Faure sequence has the places $0, 1, \dots, s-1$. $\square$

For $s = p$ this is due to Dick, Goda and Suzuki [10], who note that their argument does not decide the Faure sequences with $2 < s < p$; Goda, Hofer and Suzuki treat $s = 2$ and $s = p$ [16]. When two places are one apart, as for the Faure sequence, a direct construction gives the rate of [16].

Remark 9 (A faster rate when two places are one apart). Let $q = p$ be prime, let the unscrambled frame have places $a_{\hat{c}}$ and $a_{c_1} = a_{\hat{c}} + 1$, put $Y = z - a_{\hat{c}}$, $\delta_c = a_c - a_{\hat{c}}$ and $\gamma = \prod_{c \neq \hat{c}} (-\delta_c)$, and for $Q \in \{p, p^2, \dots\}$

$$D = -\gamma^{-1}(Y-1)^{Q-1} \prod_{c \neq \hat{c}, c_1} (Y - \delta_c)^Q, \quad V_1 = -(Y + Y^2 + \dots + Y^{Q-1}), \quad V_2 = V_1 + D.$$

Then $\delta(P_{(s-1)Q}) < \sqrt{p^2 + s + 2} N^{-1/(s-1)}$ with $N = p^{(s-1)Q}$, and $\text{sep}(P_{(s-1)Q}) \rightarrow 0$ like $N^{1/s-1/(s-1)}$. Indeed, since $\delta_c^Q = \delta_c$ in $\mathbb{F}_p$, $(Y-1)D = -\gamma^{-1} \prod_{c \neq \hat{c}} (Y^Q - \delta_c) \equiv -1 \pmod{Y^Q}$, so the first Q Taylor digits of D at $a_{\hat{c}}$ are all 1. The digits of V_1 there are $(0, -1, \dots, -1)$ and those of V_2 are $(1, 0, \dots, 0)$, a carry of length Q , so coordinate $\hat{c}$ differs by less than $2p^{-Q}$ (as in Lemma 5). As $Y - 1 = z - a_{c_1}$, the polynomial D is divisible by $(z - a_{c_1})^{Q-1}$ and by $(z - a_c)^Q$ for the other c : coordinate c_1 shares $Q-1$ leading digits and differs by at most p^{1-Q} , the others share Q digits. Finally $\deg D = (s-1)Q - 1$, $\deg V_1 = Q - 1$, and $(4 + p^2 + s - 2)p^{-2Q}$ bounds the squared distance. Figure 2 shows the case $p = 5$, $s = 2$, places 0 and 1, $Q = 5$: $\iota(V_1) = 5^5 - 5 = 3120$, $\iota(V_2) = 1$; there the pair is the closest pair of P_5 .

3.5. Niederreiter Sequences. Niederreiter's sequences [30] and their generalization by Tezuka [41] (see [11, Ch. 8]) are digital sequences over $\mathbb{F}_q$ with distinct monic irreducible bases $b_c \in \mathbb{F}_q[z]$. For every c , $Q \geq 0$ and $0 \leq i < e_c$ a polynomial $\vartheta_{c,Q,i} \in \mathbb{F}_q[z]$ is given, such that $\vartheta_{c,Q,0}, \dots, \vartheta_{c,Q,e_c-1}$ are linearly independent modulo b_c for every Q , and digit Qe_c+i of coordinate c is

$$y_{c,Qe_c+i}(V) = [z^{-1}] \frac{\vartheta_{c,Q,i}(z) V(z)}{b_c(z)^{Q+1}},$$

the coefficient of z^{-1} in the expansion in powers of z^{-1} . (This is the generator matrix whose row Qe_c+i lists the coefficients of $z^{-1}, z^{-2}, \dots$ of $\vartheta_{c,Q,i}/b_c^{Q+1}$.) The classical sequence has $\vartheta_{c,Q,i} = z^i$. Write $\bar{\vartheta}_{c,i}$ for the remainder of $\vartheta_{c,0,i}$ modulo b_c .

Lemma 10 (Niederreiter coordinates are b_c -adic). *In a generalized Niederreiter sequence every coordinate c is b_c -adic. If $\vartheta_{c,Q,i} \equiv \bar{\vartheta}_{c,i} \pmod{b_c^{Q+1}}$ for all Q and i , then coordinate c is a b_c -adic radical inverse; in particular every coordinate of a classical Niederreiter sequence is.*

Proof. Write $b = b_c$, $e = e_c$, $\vartheta_{c,Q,i} = \sum_{j \geq 0} \vartheta^{(j)} a_j b^j$ and $V = \sum_j a_j b^j$ (b -adic expansions). Then $\vartheta_{c,Q,i} V / b^{Q+1}$ is the sum of the terms $\vartheta^{(j')} a_j b^{j+j'-Q-1}$. A term with $j+j' \geq Q+1$ is a polynomial. A term with $j+j' = Q+1-u$, $u \geq 2$, is $O(z^{-2})$ at infinity, since $\deg(\vartheta^{(j')} a_j) \leq 2e-2 < ue-1$. Neither has a z^{-1} coefficient, so

$$y_{c,Qe_c+i}(V) = \sum_{j=0}^Q [z^{-1}] \frac{\vartheta^{(Q-j)} a_j}{b}.$$

Block Q depends only on $a_0, \dots, a_Q$, that is on $V \bmod b^{Q+1}$: the coordinate is b -adic. Under the congruence, $\vartheta^{(0)} = \bar{\vartheta}_{c,i}$ and $\vartheta^{(j)} = 0$ for $1 \leq j \leq Q$, so block Q is $\pi_c(a_Q)$ with $\pi_c(a) = ([z^{-1}] \bar{\vartheta}_{c,i} a / b)_{i < e}$. The pairing $(f, a) \mapsto [z^{-1}] fa / b$ on polynomials of degree less than e is nondegenerate: for $a \neq 0$ pick f with $fa \equiv z^{e-1} \pmod{b}$ (b is irreducible); then the value is $1/\text{lc}(b) \neq 0$. Since the $\bar{\vartheta}_{c,i}$ form a basis of these polynomials, π_c is a bijection. $\square$

Corollary 11 (Niederreiter sequences). *Every classical Niederreiter sequence over $\mathbb{F}_q$ ($s \geq 2$, natural identification) is not quasi-uniform. So is every generalized Niederreiter sequence in which one coordinate $\hat{c}$ satisfies $\vartheta_{\hat{c},Q,i} \equiv \bar{\vartheta}_{\hat{c},i} \pmod{b_{\hat{c}}^{Q+1}}$ for all Q, i , whatever the polynomials of the other coordinates; the close pairs of Theorem 6 then depend only on the bases and on the $\bar{\vartheta}_{\hat{c},i}$.*

Proof. Lemma 10 and Theorem 6; distinct monic irreducible polynomials are pairwise coprime. $\square$

The corollary uses the natural identification for the output digits. Niederreiter's general definition allows other bijections between $\mathbb{F}_q$ and the digits; with those the identity (1) can fail (over $\mathbb{F}_5$, if the digits 0, 1, 2, 3, 4 stand for the field elements 0, 3, 2, 1, 4, the differences 3, 4, 4, 3 of consecutive digits all differ from the wrap-around difference $0 - 4 = 1$), and we do not treat them. Generalized Niederreiter sequences with no coordinate of the stated form, and the sequences of Niederreiter and Xing, are not treated either.

3.6. Sobol' Sequences. Sobol' sequences [38] are digital sequences in base 2. Coordinate c has a polynomial $b_c = z^e + \alpha_1 z^{e-1} + \dots + \alpha_{e-1} z + 1 \in \mathbb{F}_2[z]$ of degree $e = e_c$ and initial direction numbers $u_1, \dots, u_e$ (written m_k in [38]), which are *admissible*: u_k is odd and $u_k < 2^k$. The further direction numbers follow Sobol's recurrence

$$(2) \quad u_k = 2\alpha_1 u_{k-1} \oplus 2^2 \alpha_2 u_{k-2} \oplus \dots \oplus 2^{e-1} \alpha_{e-1} u_{k-e+1} \oplus 2^e u_{k-e} \oplus u_{k-e} \quad (k > e),$$

where $\oplus$ adds binary expansions digit by digit modulo 2. Column $k - 1$ of C_c holds the binary digits of $2^{-k}u_k$, so $y_c(V) = \bigoplus_k V_{k-1} 2^{-k}u_k$. Sobol' takes distinct primitive polynomials. In the usual implementations the first coordinate is the van der Corput coordinate, $b = z$ and $u_k = 1$ (so $C = I$) [4, 25]; some implementations start with $z + 1$. Points are produced in the natural order or in Gray-code order [2], which permutes $\{0, \dots, 2^m - 1\}$ for every m and therefore has the same prefixes P_m as sets.

Lemma 12 (Sobol' coordinates are radical inverses). *Let coordinate c of a Sobol' sequence have the polynomial b_c of degree e and constant term 1, and admissible initial direction numbers. Then it is a b_c -adic radical inverse whose digit map π_c is upper unitriangular in the bases $1, z, \dots, z^{e-1}$ and digits $0, \dots, e - 1$.*

Proof. (a) Multiplication by b_c shifts the digits by e places: $y_c(b_c V) = 2^{-e}y_c(V)$, in the sense of binary expansions. For $V = z^{k-1}$ we have $b_c z^{k-1} = z^{k+e-1} + \alpha_1 z^{k+e-2} + \dots + \alpha_{e-1} z^k + z^{k-1}$, so

$$\begin{aligned} y_c(b_c z^{k-1}) &= 2^{-k-e}u_{k+e} \oplus \alpha_1 2^{-k-e+1}u_{k+e-1} \oplus \dots \oplus \alpha_{e-1} 2^{-k-1}u_{k+1} \oplus 2^{-k}u_k \\ &= 2^{-k-e}u_k = 2^{-e}y_c(z^{k-1}), \end{aligned}$$

by (2) at the index $k + e$, multiplied by 2^{-k-e} . Both sides are linear in V . (b) For $i < e$ the number $2^{-i-1}u_{i+1}$ has binary digits only at the digit positions $0, \dots, i$ (since $u_{i+1} < 2^{i+1}$), with a 1 at position i (since u_{i+1} is odd). So for $\deg a < e$ the point $y_c(a)$ has digits only at the positions $0, \dots, e - 1$, and $\pi_c(a)$, the vector of these digits, is upper unitriangular in a . (c) For $V = \sum_Q a_Q b_c^Q$, (a) and (b) give $y_c(V) = \bigoplus_Q 2^{-eQ}y_c(a_Q)$, with the terms in disjoint blocks of digits; so block Q is $\pi_c(a_Q)$. $\square$

Only admissibility and the constant term 1 are used; primitivity is not. The lemma is about the ideal sequence with infinitely many binary digits; an implementation with 32 or 64 bits agrees with it on those digits and on indices below 2^{32} or 2^{64} .

Corollary 13 (No Sobol' sequence is quasi-uniform). *Every Sobol' sequence is not quasi-uniform: in every dimension $s \geq 2$, for every choice of admissible initial direction numbers, for any pairwise coprime polynomials with constant term 1 (in particular Sobol's distinct primitive polynomials), with or without the van der Corput coordinate, in natural or in Gray-code order. The same holds for the projection to any $s' \geq 2$ of its coordinates. With the van der Corput coordinate as $\hat{c}$ the close pairs are explicit and do not depend on the direction numbers: let $b_1, \dots, b_{s-1}$ be the other polynomials, $E = \text{lcm } e_c$, $\Theta = \prod_{c \geq 1} b_c^{E/e_c}$, choose $\nu \geq 1$ with $(1+z)\Theta \mid z^\nu - 1$ and j with $2^j \geq \nu$, put $\eta = E(2^j + 1) - \nu$, and for $Q = 2^w$, $w \geq 0$,*

$$D_Q = z^{Q\eta}(1+z+\dots+z^{Q\nu-1})\Theta(z^{2^j Q}), \quad \iota(V_1) = 2^{L_Q} - 2^{Q\eta+1}, \quad \iota(V_2) = \iota(V_1) \text{ XOR } \iota(D_Q),$$

with $L_Q = QE(2^j + 1)$ and $m_Q = Q(sE(2^j + 1) - (s-1)E)$. The two points lie in P_{m_Q} , at distance less than $\sqrt{s+3}2^{-L_Q}$, and $\text{sep}(P_{m_Q}) < \sqrt{s+3}2^{-Q(s-1)E/s}$.

Proof. By Lemma 12 every coordinate with a polynomial of constant term 1 is a radical inverse, and the van der Corput coordinate ($C = I$) is the z -adic radical inverse with $\pi = 1$. Polynomials with constant term 1 are coprime to z , and distinct irreducible polynomials are coprime. A projection is again a digital sequence of the same kind, and a sequence without the van der Corput coordinate is a projection of one with it. Theorem 6 applies with any $\hat{c}$. For the explicit pair take $b = z$, $e = 1$, $\pi = 1$, so $g = g' = 1$, $\tilde{g} = 0$, and $k = 2^j$. Over $\mathbb{F}_2$ we have $\Theta^{2^j} = \Theta(z^{2^j}) \equiv \Theta(0) = 1 \pmod{z^{2^j}}$, hence $\Theta^k \equiv 1 \pmod{z^\nu}$; this is all that the proof of Theorem 6 uses about k , and $E(k+1) \geq \nu$. Then $\Theta^{Qk} = \Theta(z^{2^j Q})$, $S_{Q\nu} = 1 + z + \dots + z^{Q\nu-1}$, and $V_1 = z^{Q\eta+1}S_{Q\nu-1} = \sum_{i=Q\eta+1}^{L_Q-1} z^i$. Addition in $\mathbb{F}_2[z]$ is the XOR of the integer indices. $\square$

TABLE 4. The close pairs of Corollary 13 with the van der Corput coordinate as $\hat{c}$, for the first s Sobol' polynomials in the order of [4, 25]: $z, z+1, z^2+z+1, z^3+z+1, z^3+z^2+1, z^4+z+1, z^4+z^3+1$; ν is the least admissible value, $k = 2^j$ the least power of two $\geq \nu$, and $Q = 1$. For $Q = 2^w$ multiply L, m and $(s-1)E$ by Q . The last column (rounded up) bounds $\text{sep}(P_m)$ at $Q = 1$; at level m_Q the bound is $\sqrt{s+3} 2^{-Q(s-1)E/s}$. The pairs do not depend on the direction numbers. Exact computation, recomputed independently (Appendix C).

s	degrees $e_1, \dots, e_{s-1}$	E	ν	k	L_1	m_1	$(s-1)E$	$\sqrt{s+3} 2^{-(s-1)E/s}$
2	1	1	2	2	3	5	1	1.59
3	1, 2	2	12	16	34	98	4	0.98
4	1, 2, 3	6	168	256	1 542	6 150	18	0.12
5	1, 2, 3, 3	6	168	256	1 542	7 686	24	0.11
6	1, 2, 3, 3, 4	12	1 680	2 048	24 588	147 468	60	$2.93 \cdot 10^{-3}$
7	1, 2, 3, 3, 4, 4	12	1 680	2 048	24 588	172 044	72	$2.54 \cdot 10^{-3}$

The two-dimensional Sobol' sequence (I, P) was known not to be quasi-uniform [14], with a mesh ratio that grows at least like $N^{1/4}$ [40]. Goda, Hofer and Suzuki proved it for the Halton-type sequence with the bases $z, z+1, z^2+z+1$, which they relate to the three-dimensional Sobol' sequence, and state that the question remains open for Sobol' sequences in dimension $d \geq 3$ [16]. Sobol' and Shukhman had suggested, from numerical experiments, that the separation of the Sobol' sequence is of the optimal order $N^{-1/s}$ [37]; Corollary 13 disproves this in every dimension $s \geq 2$ (for $s = 2$ this is [14]). By Lemma 12 the three-dimensional Sobol' sequence differs from that Halton-type sequence only in the digit map of the third coordinate, which the close pairs do not see. Corollaries 7, 8 (for $2 < s < p$), 13 (for $s \geq 3$) and 11 were not found in the literature we searched (through October 2026). The pairs of Table 4 sit at astronomically large levels for $s \geq 4$; they prove the failure, but they are not the closest pairs, and they do not determine how fast $\text{sep}(P_m)$ decays.

3.7. Scrambles That Do Not Help, and What Escapes. A scramble changes the points but keeps the shared leading digits: a lower-triangular scramble of a coordinate makes each of its first d digits a combination of the first d unscrambled digits. So the shared leading digits that D produces in the other coordinates survive any lower-triangular scramble. What a scramble can destroy is the carry, and only in the coordinate that carries it.

Corollary 14 (One coordinate left unscrambled). *Let $s \geq 2$ and let $b_0, \dots, b_{s-1} \in \mathbb{F}_q[z]$ be pairwise coprime. Suppose that coordinate $\hat{c}$ of a digital sequence over $\mathbb{F}_q$ is μ times a $b_{\hat{c}}$ -adic radical inverse, $\mu \in \mathbb{F}_q^*$, and that every other coordinate c is L_c times a b_c -adic coordinate, for arbitrary fixed nonsingular lower-triangular matrices L_c . Then the sequence is not quasi-uniform. In particular, for distinct places $a_c \in \mathbb{F}_q$ the scrambled frame $C_{\hat{c}} = \mu \text{diag}(\beta^n) P_{a_{\hat{c}}}$, $C_c = L_c P_{a_c}$ ($c \neq \hat{c}$) is not quasi-uniform for any $\mu, \beta \in \mathbb{F}_q^*$.*

Proof. L_c times a b_c -adic coordinate is b_c -adic, and μ times a radical inverse with digit map π is a radical inverse with digit map $\mu\pi$ (Section 3.1); Theorem 6 applies. For the frame, write $V = \sum_n [(z-a)^n] V (z-a)^n = \sum_n (\beta^n [(z-a)^n] V) (\beta^{-1}(z-a))^n$ with $a = a_{\hat{c}}$: the digits $\beta^n [(z-a)^n] V$ of coordinate $\hat{c}$ before the factor μ are the $\beta^{-1}(z-a)$ -adic digits of V , a radical inverse in a linear base that is coprime to the other bases. $\square$

So within the polynomial-base sequences (pairwise coprime bases, every coordinate b_c -adic), a quasi-uniform sequence has no coordinate that is a radical inverse up to a scalar; for a coordinate

with a linear base, a diagonal scramble is not enough. The generalized Faure sequences of Tezuka [42] with one scalar scramble are covered, and so are the generalized Niederreiter sequences of Corollary 11 after any lower-triangular scramble of the other coordinates. The sequences of Sections 5–9 scramble every coordinate non-diagonally. For a self-similar scramble (Definition 20) this is a one-line check: $C_c = L_c P_{a_c}$ with $L_c[n][j] = [x^n] g_c(x) (z_c(\theta x) - a_c)^j$, and L_c diagonal would force g_c to be constant and $z_c(\theta x) = a_c + \beta x$, hence $w(a_c + \beta x) = \theta x$, impossible since $w(a_c + \beta x)$ has degree $s \geq 2$ in x .

Remark 15 (Randomizations and reorderings). The following do not restore quasi-uniformity of any sequence covered by Theorem 6. (a) *Digital shifts*, $y_{c,n}(V) \mapsto y_{c,n}(V) + \sigma_{c,n}$ with addition in $\mathbb{F}_q$, in every coordinate: the first L digits of coordinate $\hat{c}$ are a bijective function of $V \bmod b^\lambda$, so there is V_1 of degree less than L whose shifted digits are $(0^{e\eta}, y^\circ, \bar{y}, \dots, \bar{y})$, and the pair $V_1, V_1 + D_Q$ works as before. Only the bound becomes $\leq \sqrt{s+3} q^{-LQ}$, because a shifted coordinate may have infinitely many nonzero digits. (b) *Index scrambles* $C_c \mapsto C_c U$ with one nonsingular upper-triangular U for all coordinates (Faure and Tezuka [13]), and the Gray-code order: every prefix P_m is unchanged as a set. (c) *Reorderings* that keep every full level P_{sK} as a set: by Theorem 6, $\text{sep}(P_{sK_Q}) \rightarrow 0$ along the full levels K_Q , and these prefixes are the same sets in the new order.

Remark 16 (A fixed rational multiplier in the carrying coordinate is not enough). One might try to break the carry with a fixed Toeplitz scramble of the carrying coordinate: read coordinate $\hat{c}$ of a frame over $\mathbb{F}_p$ as the Taylor digits at $a = a_{\hat{c}}$ of $\varrho(Y)V$, where $Y = z - a$ and $\varrho = A/B$ is a rational unit, $A, B \in \mathbb{F}_p[[Y]]$, $A(0)B(0) \neq 0$; the other coordinates get arbitrary lower-triangular scrambles. With $\delta_c = a_c - a$, $E_1 = \prod_{c \neq \hat{c}} (1 - Y/\delta_c)$ and $R_1 = (1 - Y)A$, the sequence is still not quasi-uniform whenever $R_1 E_1$ is squarefree (in particular $a + 1$ is not a place). So, whenever $R_1 E_1$ is squarefree, a fixed rational multiplier of this kind in the Taylor variable does not help (other rational multipliers and irrational ones are not treated here); the scrambles of Section 4 change the variable itself, from $z - a_c$ to the uniformizer w .

Proof. Let ν be the least common multiple of the multiplicative orders of the roots of $R_1 E_1$; then $p \nmid \nu$ and $R_1 E_1 \mid 1 - Y^\nu$. Take powers Q, Q' of p with $Q \equiv 1 \pmod{\nu}$ and $Q' \geq \nu$, put $L = Q(Q' + 1)$ and $H = E_1^{-L}/R_1 \in \mathbb{F}_p[[Y]]$. Over $\mathbb{F}_p$, $E_1^{-L}(Y) = E_1^{-(Q'+1)}(Y^Q)$, and $1/R_1 = ((1 - Y^\nu)/R_1)/(1 - Y^\nu)$ has ν -periodic coefficients. For $(\nu - 1)Q \leq n < \nu Q$ and $i < \nu$ we have $n - iQ \equiv n - i \pmod{\nu}$, so $[Y^n]H = [Y^n](T/R_1)$, where T is $E_1^{-(Q'+1)}$ truncated at degree $\nu - 1$. Since $Q' \geq \nu$, T is the truncation of $1/E_1$, which is the polynomial $(1 - Y^\nu)/E_1$. So $[Y^n]H = [Y^n](1 - Y^\nu)/(E_1 R_1) = 0$, because this is a polynomial of degree less than $(\nu - 1)Q$, and BH vanishes on $[(\nu - 1)Q + \deg B, \nu Q)$.

Let $\eta = L - \nu Q \geq Q$, let T_1 be BH truncated below degree νQ , and $D = E_1^L Y^\eta T_1$. Then $\varrho D \equiv Y^\eta/(1 - Y) \pmod{Y^L}$, so the scrambled digits of D in coordinate $\hat{c}$ are $(0^\eta, 1^{L-\eta})$ on the positions below L ; D is divisible by $(z - a_c)^L$ for $c \neq \hat{c}$; and $\deg D < m := sL - Q + \deg B$. Let V_1 be the polynomial of degree less than L whose scrambled digits at these positions are $(0^\eta, 0, -1, \dots, -1)$, and $V_2 = V_1 + D$. As in the proof of Lemma 5 (with tails in $[0, p^{-L}]$), the two points are at distance at most $\sqrt{s+3} p^{-L}$, so $\text{sep}(P_m) \leq \sqrt{s+3} p^{-(Q-\deg B)/s}$, which tends to 0 along $Q \equiv 1 \pmod{\nu}$. $\square$

Remark 17 (What escapes). Theorem 6 says nothing when every coordinate is scrambled by a lower-triangular matrix that destroys its radical-inverse structure: then the digits of D in coordinate $\hat{c}$ would have to be $L_{\hat{c}}^{-1}$ applied to the carry pattern, which is no longer a run of one digit in base b . Such scrambles can indeed be quasi-uniform: the base-two sequence of Theorem 76 is a lower-triangular scramble of both coordinates of the two-dimensional Sobol'

sequence, with $\text{sep}(P_{2K}) \geq 0.3678$ for every K , and the sequences of Sections 5–9 are scrambles of every coordinate of a frame. For random scrambles the picture is different. A random nested (Owen) scramble makes every (t, s) -sequence almost surely not quasi-uniform [39], and a random linear (matrix) scramble of a binary digital net with fixed t has mesh ratio $O_P(\log N)$ under a uniform coincidence condition, which holds for instance for the prefixes of Sobol' sequences [39, Thm. 5.5, Lem. 4.10]; this bound does not decide whether a randomly linearly scrambled Sobol' sequence is quasi-uniform, and we do not know the answer (Section 11).

4. RESIDUES, SELF-SIMILAR SCRAMBLES AND CARRY RESPONSES

Every prefix of a $(0, s)$ -sequence is a net, so at a full level each cell holds exactly one point (Lemma 1). The separation is decided by where that point sits inside its cell, compared with the points of the neighbouring cells. This section describes that position and how it changes from cell to cell. Section 3 showed what goes wrong for the classical sequences; here we see the same failure at the level of the cells: for the Faure sequence the rule that places the points changes with the level. The fix has two parts. First, every scramble can be read through residues of the index polynomial at the places (Lemma 21). Second, for the self-similar scrambles the rule that places the points is the same at every level (Proposition 22), so one finite check bounds the separation at all levels (Lemma 23). Sections 5–7 use exactly this machinery, and Section 8 adds the free digits and windows. The running example is the brick wall W^- in base 7, a two-dimensional sequence whose neighbouring columns of points are staggered by half a cell, like the courses of a brick wall.

4.1. Geometric Digits and the Lattice Image. Fix a level K and a point of P_{sK} . Its cell is $n = (n_0, \dots, n_{s-1})$, where $n_c = \sum_{i < K} \text{enc}(y_{c,i}) q^{K-1-i}$; digit $i = 0$ is the coarsest and digit $K - 1$ the finest. As in [18], the next digit $r_c := y_{c,K}$, the first digit below the cell, is the *geometric digit*: it locates the point inside its cell up to $1/q$ of the side. The change of the geometric digits under a carry-free step of one cell index is the *geometric layer* of [18]; it is the one-digit carry response $D(1)$ defined in the next subsection. More generally, for a depth $j \geq 1$ let $R_c \in \mathbb{F}_q^j$ be the vector of the j geometric digits $y_{c,K}, \dots, y_{c,K+j-1}$, read as the integer $\text{enc}(R_c) = \sum_{i < j} \text{enc}(y_{c,K+i}) q^{j-1-i} \in [0, q^j)$. In cell units the point is

$$(3) \quad q^K y_c = n_c + \frac{\text{enc}(R_c)}{q^j} + \varepsilon_c, \quad 0 \leq \varepsilon_c \leq q^{-j},$$

where the *jitter* ε_c collects the digits from $K + j$ on. The *lattice image* $n + \text{enc}(R)/q^j$ of [18] (there $j = 1$) is a point of the grid $q^{-j}\mathbb{Z}^s$, the position predicted by the first j geometric digits; the jitter moves the true point by at most one grid unit.

Example 18 (Running example). The brick wall W^- in base $p = 7$ is the staggered residue sequence of Section 5 with $s = 2$, the Faure places $a_0 = 0$, $a_1 = 1$, staggered coordinate 1, scale $\theta = -\frac{1}{4}$ and constants $\mu = (-4, 2)$ (Example 30; its residue form is given after Lemma 21). Its generator matrices are $C_0 = L_0$ and $C_1 = L_1 P_1$, with the leading blocks (entries in $\mathbb{F}_7$)

$$C_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 6 & 2 & 0 & 0 \\ 5 & 2 & 4 & 0 \\ 0 & 1 & 5 & 1 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 4 & 0 & 3 & 6 \\ 3 & 1 & 0 & 0 \\ 6 & 1 & 2 & 0 \end{pmatrix}, \quad L_1 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 4 & 3 & 0 & 0 \\ 3 & 5 & 1 & 0 \\ 6 & 2 & 6 & 5 \end{pmatrix}.$$

Take the index polynomial $V(z) = 3 + z$ (integer index $10 = 3 + 1 \cdot 7$). Its digits are $C_0(3, 1)^\top = (3, 6, 3, 1)$ in coordinate 0 and $C_1(3, 1)^\top = (1, 5, 3, 5)$ in coordinate 1. At level $K = 1$, in the prefix P_2 with its 7×7 cells, the point lies in the cell $n = (3, 1)$, its geometric digits are $(r_0, r_1) = (6, 5)$, and its lattice image is $(3 + \frac{6}{7}, 1 + \frac{5}{7}) = (3.857, 1.714)$. The point itself is at

$7y = (3.921, 1.792)$: the jitter $(0.064, 0.077)$ is less than $\frac{1}{7}$. With $j = 2$ geometric digits the lattice image is $(3 + \frac{45}{49}, 1 + \frac{38}{49}) = (3.918, 1.776)$, within $\frac{1}{49}$ of the point.

4.2. Carries and Carry Responses. The map from the cell digits $(y_{c,i})_{c,i < K}$ to the geometric digits $(y_{c,K+i})_{c,i < j}$ is $\mathbb{F}_q$ -linear, since both are linear functions of V and the cell digits determine V . We call it the *offset map* of P_{sK} . Writing the net as the graph of this map is the graph form of [18] with depths $(K, \dots, K)$. The offset map has two kinds of entries. The *own* entries say how the geometric digits of coordinate c depend on the cell digits of the same coordinate, the *cross* entries how they depend on the cell digits of another coordinate c' . We index them by *carry depth*, counted from the finest digit: own coefficient $n \geq 1$ belongs to cell digit $K - n$, cross coefficient $n \geq 0$ to cell digit $K - 1 - n$. The shift by one between the two is chosen so that a carry of length l (defined next) involves exactly the own coefficients $1, \dots, l$ and the cross coefficients $0, \dots, l - 1$.

Separation is a question about neighbouring cells, and the step from a cell to its neighbour is a carry. Increasing $n_{c'}$ by one changes its l finest digits, where $l - 1$ is the number of trailing digits with code $q - 1$; we call $l \in [1, K]$ the *carry length*. For prime q the step adds 1 to each of these l digits. The toroidal wrap, the step from the last cell $q^K - 1$ to the cell 0, changes all K digits; we count it as a step of carry length K .

Let $D_i(l) \in \mathbb{F}_q^{s \times s}$ be the change of the geometric digit $K + i$ of coordinate c (row) when $1 \in \mathbb{F}_q$ is added to each of the l finest cell digits of coordinate c' (column), with $D_i(0) = 0$; this is the *carry response*. For prime q it is exactly the change caused by a step of $n_{c'}$ by $+1$ with carry length l ; for $q = 4$ see Remark 89 in Appendix A. We write $D(l) = D_0(l)$ for the one-digit response, $O_c^{(l)} = D(l)[c][c]$ for the *own response* and $X_{c \leftarrow c'}^{(l)} = D(l)[c][c']$, $c \neq c'$, for the *cross response*. They are partial sums of the coefficients of the offset map: if $O_{c,n}$ and $X_{c \leftarrow c',n}$ are the own and cross coefficients at carry depth n , then

$$O_c^{(l)} = \sum_{n=1}^l O_{c,n} = [x^l] \frac{O_c(x)}{1-x}, \quad X_{c \leftarrow c'}^{(l)} = \sum_{n=0}^{l-1} X_{c \leftarrow c',n} = [x^{l-1}] \frac{X_{c \leftarrow c'}(x)}{1-x},$$

with $O_c(x) = \sum_{n \geq 1} O_{c,n} x^n$ and $X_{c \leftarrow c'}(x) = \sum_{n \geq 0} X_{c \leftarrow c',n} x^n$; here $[x^n] F$ is the coefficient of x^n in a power series F . A priori all of these depend on K .

In the running example at $K = 1$, the right neighbour of the cell $(3, 1)$ is the cell $(4, 1)$, which holds the point with index polynomial $V = 4$; its geometric digits are $(3, 2)$. The step changes (r_0, r_1) by $(3, 2) - (6, 5) = (4, 4)$ modulo 7, which is the column $(O_0^{(1)}, X_{1 \leftarrow 0}^{(1)})$ of $D(1)$.

4.3. Sheared Lattices, Slip Planes and Jumps. Before computing the offset map we describe what it looks like. Consider a patch of cells in which every step is carry-free ($l = 1$) and no geometric digit wraps around modulo q . There the lattice image of the point in cell n is

$$n + \frac{1}{q} \tilde{D}(1) n + \text{const},$$

where the entries of the integer matrix $\tilde{D}(1)$ are the representatives of $D(1)$ realised on the patch. So on such a patch the lattice images form the sheared lattice $(I + \tilde{D}(1)/q)\mathbb{Z}^s$, and the points are this lattice plus the jitter, as in the nets of [18]. Two kinds of defects interrupt it. Where a geometric digit wraps around modulo q , the lattice is offset by one cell; these hyperplanes are the *slip planes* of [18]. And where a cell index crosses a boundary of carry length $l \geq 2$, which happens at every q^{l-1} -th boundary of that coordinate, the lattice image changes by the column $D(l)$ instead of $D(1)$; we call this a *jump of depth l* . (Jumps are not the faults of [18], which are coefficients of its skeleton digits.) They form a hierarchy: depth-one boundaries everywhere, depth-two boundaries every q cells, depth-three boundaries every q^2 cells, and so on up to the

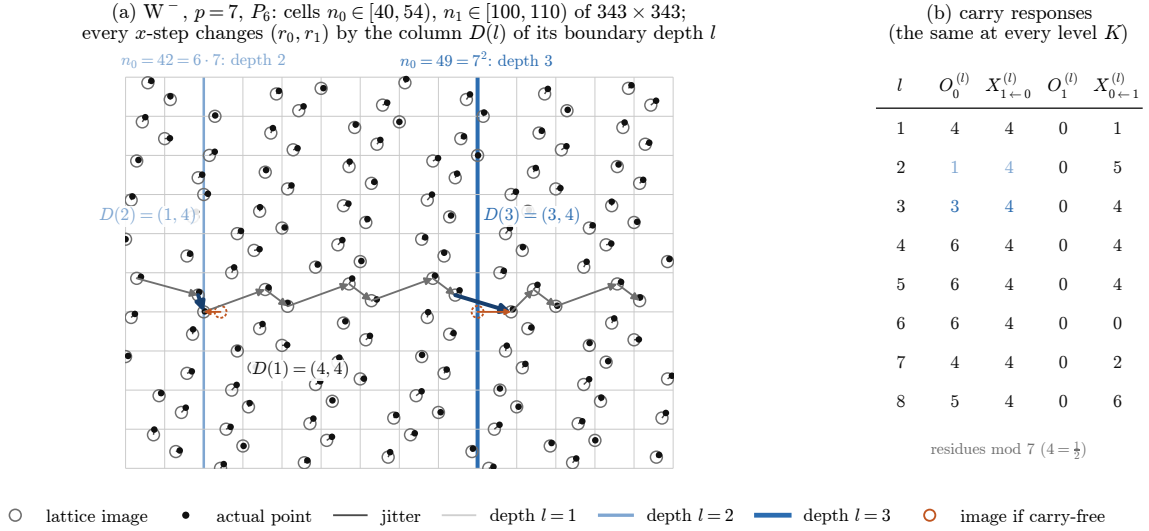


FIGURE 3. Jumps in the running example W^- ($p = 7$). (a) Cells $n_0 \in [40, 54)$, $n_1 \in [100, 110)$ of the 343×343 cells of the prefix P_6 , with lattice images and jitter. Vertical cell boundaries are shaded by their depth (carry length) l : depth 1 everywhere, depth 2 at $n_0 = 42 = 6 \cdot 7$, depth 3 at $n_0 = 49 = 7^2$. Along one row the arrows join the lattice images of horizontal neighbours. Every step changes the geometric digits (r_0, r_1) by the column $D(l)$ of its boundary depth: $D(1) = (4, 4)$ on the plain boundaries, $D(2) = (1, 4)$ at $n_0 = 42$, $D(3) = (3, 4)$ at $n_0 = 49$; the dashed circles show where a carry-free step would have put the lattice image. Between boundaries of depth ≥ 2 the points form one sheared lattice; at each deeper boundary it jumps by an amount that depends only on l . (b) The responses $l = 1, \dots, 8$ of W^- (Table 5): the cross response $X_{1 \leftarrow 0} = 4 = \frac{1}{2}$ and the own response $O_1 = 0$ are constant (the brick wall), while $O_0^{(l)}$ and $X_{0 \leftarrow 1}^{(l)}$ vary with l and are never periodic (Proposition 92). Note $D(2) = (1, 4)$: the own shift $+1$ is fatal on its own (Figure 5(b)); the constant cross response $\frac{1}{2}$ is what keeps the neighbours apart. Exact digits from the generator matrices of Example 18.

toroidal wrap, the jump of depth K (Figure 3). A jump is harmless if it moves the neighbouring point away, and fatal if it moves it onto the point across the boundary.

In Table 5 the jump of depth l is the difference between the columns $D(l)$ and $D(1)$. In W^- two of the four responses are *constant*, that is, they do not depend on the carry length: $X_{1 \leftarrow 0}^{(l)} = 4 = \frac{1}{2}$ and $O_1^{(l)} = 0$ for every l . The other two keep changing with l , so the horizontal positions change at every deeper boundary, while the vertical stagger by half a cell between neighbouring columns stays the same. This is the brick wall; the constant half alone gives a bound at every level (Theorem 32), and the residue form below shows in one line where it comes from.

Refining the level turns every boundary of depth l into one of depth $l + 1$ and inserts new boundaries of depth one. For an arbitrary scramble the responses $D(l)$ are new at every level. For the scrambles introduced below they are the partial sums of one fixed series (Proposition 22); a refinement then only relabels the jumps, and a bound on the one set $\{D(l) : l \geq 1\}$ is a bound at every scale.

TABLE 5. The carry responses of the running example W^- in base 7 for carry lengths $l = 1, \dots, 8$, modulo 7. A horizontal step (coordinate 0 moves) changes (r_0, r_1) by $(O_0^{(l)}, X_{1 \leftarrow 0}^{(l)})$, a vertical step by $(X_{0 \leftarrow 1}^{(l)}, O_1^{(l)})$. The values are the same at every level $K \geq l$ (exact computation from the generator matrices at $K = 8$ and $K = 9$; Proposition 22).

l	1	2	3	4	5	6	7	8
$O_0^{(l)}$ (own, horizontal step)	4	1	3	6	6	6	4	5
$X_{1 \leftarrow 0}^{(l)}$ (cross, horizontal step)	4	4	4	4	4	4	4	4
$O_1^{(l)}$ (own, vertical step)	0	0	0	0	0	0	0	0
$X_{0 \leftarrow 1}^{(l)}$ (cross, vertical step)	1	5	4	4	4	0	2	6

TABLE 6. The Faure sequence (I, P) in base 7 at the levels $K = 1, \dots, 8$. Row 2: the depth-one cross coefficient $(-1)^K(K+1)$ of Example 19 (undefined at $K = 1$). Row 3: the exact separation constant of P_{2K} , computed for $K \leq 4$. For comparison, every response of the running example W^- is the same at all levels (Table 5).

K	1	2	3	4	5	6	7	8
depth-one cross coefficient	–	3	3	5	1	0	6	2
sep(P_{2K})	.8690	.3115	.2463	.0174	–	–	–	–

4.4. The Faure Baseline. The Faure sequence shows what goes wrong without this property: its offset map changes with the level. Section 3 proves that the sequence is not quasi-uniform; the following example shows the failure at the level of carry responses.

Example 19 (The Faure offset map). Let $s = 2$ and consider the Faure sequence (I, P) at level K . Write $V = A_0 + z^K A_1$ with $\deg A_0, \deg A_1 < K$. The cell digits of coordinate 0 are the coefficients of A_0 , those of coordinate 1 the Taylor coefficients $y_{1,i} = [(z-1)^i]V$, $i < K$, and the geometric digit of coordinate 0 is $r_0 = A_1(0)$. Since $z^K A_1 \equiv V - A_0$ modulo $(z-1)^K$ and $\deg A_1 < K$, the polynomial A_1 is the residue of $z^{-K}(V - A_0)$ modulo $(z-1)^K$. Expanding $z^{-K} = \sum_{i \geq 0} \binom{-K}{i} (z-1)^i$ and evaluating at $z = 0$, where $(z-1)^i$ takes the value $(-1)^i$, the coefficient of $y_{1,K-1-n}$ in r_0 is

$$\sum_{i=0}^n \binom{-K}{i} (-1)^{K-1-n+i} = (-1)^{K-1-n} \sum_{i=0}^n \binom{K-1+i}{i} = (-1)^{K-1+n} \binom{K+n}{n}.$$

This is the cross coefficient of coordinate 0 at carry depth n . It depends on K : at depth zero it alternates in sign, and at depth one it is $(-1)^K(K+1)$, which runs through all residues modulo p as K grows.

So the local picture of the Faure sequence changes at every level (Table 6); at level $K = 4$ two of the 7^8 points are only 0.0174 cell units apart. The nets of [18] conjugate the binomial rows to a fixed shape by a change of scramble that depends on m ; a sequence cannot, because that would rewrite rows that are already in use. At level K the new freedom of a scramble is row K of each L_c , and once chosen it shapes the offset map at every later level. The simplest way to obtain a bound at every level is an offset map that is the same at every level.

4.5. Self-Similar Scrambles. The way out is to use the structure that relates the levels: going one level finer is multiplication of the index by one fixed polynomial w . Fix a frame $(a_0, \dots, a_{s-1}; \infty)$ over $\mathbb{F}_q$ and put

$$w = \prod_{c=0}^{s-1} (z - a_c) \in \mathbb{F}_q[z], \quad w_c = \frac{w}{z - a_c} = \prod_{b \neq c} (z - a_b).$$

Since the places are distinct, w has a simple zero at every a_c : it is a *uniformizer* at each place. Let $\deg V < sK$. The first K unscrambled digits of coordinate c are $V \bmod (z - a_c)^K$, and a scramble replaces them by an invertible triangular function of themselves. By the Chinese remainder theorem,

$$\{V : \deg V < sK\} \longleftrightarrow \prod_c \mathbb{F}_q[z]/((z - a_c)^K) \cong \mathbb{F}_q[z]/(w^K)$$

is a bijection. So the cells of P_{sK} are the elements of the ring $\mathbb{F}_q[z]/(w^K)$, the *cell ring*, and the point in a cell is a function of the cell. Every V of degree less than sK has a unique w -adic expansion

$$(4) \quad V = \sum_{k < K} \sum_{b < s} \nu_{k,b} z^b w^k, \quad \nu_b(x) = \sum_{k < K} \nu_{k,b} x^k,$$

by repeated division by w . Passing from level K to level $K+1$ adds one more w -adic digit $(\nu_{K,b})_b$ at the top, and the cell ring $\mathbb{F}_q[z]/(w^{K+1})$ contains $w \cdot \mathbb{F}_q[z]/(w^K) \cong \mathbb{F}_q[z]/(w^K)$: *going one level finer is multiplication by w* . The place ∞ of the index enters only here, through the degree bound $\deg V < sK$.

To compare the places we use one local variable for all of them. Let x stand for w . For every c there is a unique power series $z_c(x) \in a_c + x\mathbb{F}_q[[x]]$ with $w(z_c(x)) = x$, the *local root* at a_c ; it exists because $w'(a_c) = w_c(a_c) \neq 0$, and $z_c(x) = a_c + x/w'(a_c) + O(x^2)$. The s local roots are the s roots of $w(Z) = x$ in $\mathbb{F}_q[[x]]$, so

$$(5) \quad w(Z) - x = \prod_c (Z - z_c(x)).$$

Substituting $z = z_c(x)$ into (4) gives $V(z_c(x)) = \sum_b z_c(x)^b \nu_b(x)$: at every place the w -adic digits of the index become the x -adic digits of a power series.

Every scramble can be written in this local variable, one unit series $g_{c,n}$ per row: $y_{c,n} = [x^n] g_{c,n}(x) V(z_c(\theta x))$, where row n of L_c and the coefficients of $g_{c,n}$ up to x^n determine each other (the Riordan form, Lemma 90 in Appendix A). Multiplication of the index by w multiplies $V(z_c(\theta x))$ by θx , since $w(z_c(\theta x)) = \theta x$. If all rows of L_c share one series, the digit series therefore transform as $Y_c(wV) = \theta x Y_c(V)$: refinement shifts every digit by one place and multiplies it by θ .

Definition 20 (Self-similar scramble). A scramble $(L_0, \dots, L_{s-1})$ of the frame is *self-similar* with *scale* $\theta \in \mathbb{F}_q^*$ and *multipliers* $g_0, \dots, g_{s-1}$ (unit series) if

$$y_{c,n} = [x^n] g_c(x) V(z_c(\theta x)) \quad \text{for all } c, n, V,$$

with one common θ . Equivalently, $Y_c(x) = g_c(x) V(z_c(\theta x))$ for every coordinate, and the generator matrices are $C_c[n][k] = [x^n] g_c(x) z_c(\theta x)^k$: column k of C_c is the series $g_c z_c(\theta x)^k$.

For $\theta = 1$ the prefix P_{sK} , shrunk by the factor q , reappears in the corner box $[0, q^{-1})^s$ of $P_{s(K+1)}$; for general θ the shrunk copy is in addition multiplied digit by digit by θ . In the

running example (Faure frame $w = z^2 - z$, $p = 7$, scale $\theta = -\frac{1}{4} = 5$) the multipliers and scaled local roots begin

$g_0 = 1 + 6x + 5x^2 + x^6 + \dots$, $g_1 = 2 + 4x + 3x^2 + 6x^3 + \dots$, $z_1(\theta x) = 1 + 5x + 3x^2 + 5x^3 + 4x^4 + \dots$, and $z_0(\theta x) = 1 - z_1(\theta x)$. Column 0 of C_1 is g_1 , that is $(2, 4, 3, 6)$, and column 1 is $g_1 z_1 = 2 + 0x + x^2 + x^3 + \dots$, as in Example 18. One series per coordinate generates every row. The Faure sequence (I, P) is not self-similar for any θ : its offset map depends on K , and by Proposition 22 below a self-similar offset map does not.

4.6. Residue Form. The multipliers g_c are series in the common variable x ; for the constructions of the following sections it is better to write them at the places themselves, as functions of z . A residue does this. Recall that $\text{Res}_a(F dz)$ is the coefficient of $(z - a)^{-1}$ in the expansion of F in powers of $z - a$, and that a Taylor digit is a residue, $[(z - a)^k]V = \text{Res}_a(V(z - a)^{-k-1} dz)$ (Section 2). A *polar differential* at a of pole order $n + 1$ is $\sum_{k \leq n} \lambda_k (z - a)^{-k-1} dz$ with $\lambda_n \neq 0$; its terms are the *principal part* of a function at a .

Lemma 21 (Residue form of a scramble). *Let $a_0, \dots, a_{s-1} \in \mathbb{F}_q$ be distinct places and $w = \prod_c (z - a_c)$.*

(a) *For every scramble (L_c) of the frame,*

$$y_{c,n}(V) = \text{Res}_{a_c}(V \eta_{c,n}), \quad \eta_{c,n} = \sum_{k \leq n} L_c[n][k] (z - a_c)^{-k-1} dz,$$

a polar differential at a_c of exact pole order $n + 1$. Conversely, every family of polar differentials $\eta_{c,n}$ at a_c of pole orders $n + 1$ ($n \geq 0$) defines a scramble in this way.

(b) *The scramble is self-similar with scale θ (Definition 20) if and only if there are unit power series φ_c in $z - a_c$, the local multipliers, with*

$$y_{c,n}(V) = \text{Res}_{a_c} \left(V \varphi_c \left(\frac{\theta}{w} \right)^{n+1} dz \right) \quad \text{for all } c, n, V.$$

The multipliers and the local multipliers determine each other by

$$g_c(x) = \theta \varphi_c(z_c(\theta x)) z'_c(\theta x), \quad \varphi_c(z) = \theta^{-1} g_c(w(z)/\theta) w'(z).$$

(c) (Residue theorem.) *Let $F \in \mathbb{F}_q(z)$ be a rational function with no poles outside $\{a_0, \dots, a_{s-1}, \infty\}$, and let $[z^{-1}]F$ be the coefficient of z^{-1} in its expansion in powers of $1/z$ at ∞ . Then*

$$\sum_c \text{Res}_{a_c}(F dz) = [z^{-1}]F.$$

In particular the sum vanishes when $F = O(z^{-2})$ at ∞ , that is, when the degree of the numerator of F is at most the degree of its denominator minus 2.

The proof is in Appendix A.2; part (b) is a change of variable $u = w$ in the residue, and part (c) is partial fractions. In (b) only φ_c up to $(z - a_c)^n$ enters row n , just as row n of a Riordan form depends on g_c up to x^n . Since V is a polynomial, a part of $\eta_{c,n}$ or of $\varphi_c(\theta/w)^{n+1} dz$ that is regular at a_c contributes nothing: a scramble is a family of principal parts, one at each place for each digit. In complex analysis (c) is the statement that the residues of a rational differential on the projective line add up to zero, $\sum_c \text{Res}_{a_c}(F dz) + \text{Res}_\infty(F dz) = 0$; over $\mathbb{F}_q$ we need only the elementary form above.

Function fields. Part (a) is the genus-0 case of the construction of digital sequences from differentials by Mayor and Niederreiter [29]. On the rational function field $\mathbb{F}_q(z)$ take as their expansion place the place ∞ of the index, with local parameter $1/z$, as their divisor $D = -2P_0$, where P_0 is the zero of z , and as their places the points a_c . For row n of coordinate c take

the differential $\omega = -z^{-2}\eta_{c,n}$. It has a pole of order $n+1$ at a_c , at most a double pole at 0 (one of order $n+3$ if $a_c = 0$), no other pole, and it is regular at ∞ , so it is an admissible basis element of their chain $\Omega(D) \subset \Omega(D - P_c) \subset \dots$. By the residue theorem, in its expansion at ∞ the coefficient of $z^{-k-1}d(1/z)$ is $\text{Res}_{a_c}(z^k\eta_{c,n}) = C_c[n][k]$, and every admissible choice there is of this form. So every scramble of a frame, and hence every sequence of this paper, is a sequence of [29] in genus 0, and their Theorem 3.1 gives $t = 0$ (Lemma 1). Niederreiter and Özbudak [32] read all coordinates of a point as residues of one differential, at all places, against powers of a local parameter, and use the residue theorem over all places to prove a duality and bound the quality parameter. In their language a self-similar scramble reads the differential $V dz$ with one local parameter w/θ at every place; their sequences are not of this form, since their index differentials have their pole at a place of degree two. Both papers aim at the quality parameter. What is new here is the choice of the differentials, a common local parameter and simple local multipliers, such that the residue theorem gives relations with one digit of each coordinate and constant coefficients at every level of a level family, and the use of these relations for the separation (Sections 5 and 6).

Why residues. The running example is defined by residues (Example 30):

$$y_{0,n}(V) = -4 \text{Res}_0 \left(\frac{V dz}{(z-1)(w/\theta)^{n+1}} \right), \quad y_{1,n}(V) = 2 \text{Res}_1 \left(\frac{V dz}{(z-1)(w/\theta)^n} \right).$$

In the notation of (b) its local multipliers are $\varphi_0 = -4/(z-1)$ and $\varphi_1 = -8z$, and (b) gives the multipliers g_0, g_1 quoted above. Take $\deg V < 2K$ and $F = V/((z-1)(w/\theta)^K)$. It has poles only at 0, 1 and ∞ , and $F = O(z^{-2})$ at ∞ , so by (c) its residues at 0 and 1 add up to zero. The residue at 0 is $y_{0,K-1}(V)/(-4)$ and the residue at 1 is $y_{1,K}(V)/2$. Hence

$$y_{1,K}(V) = 2 y_{0,K-1}(V)/4 = \frac{1}{2} y_{0,K-1}(V) \quad \text{for every } K \geq 1 \text{ and } \deg V < 2K :$$

the geometric digit of coordinate 1 is half the finest cell digit of coordinate 0, and it does not depend on the cell digits of coordinate 1. A step of n_0 with any carry length, the toroidal wrap included, adds 1 to the finest digit and so moves r_1 by $\frac{1}{2} = 4$; a step of n_1 does not move it. These are the two constant rows of Table 5. The coordinates are read at different places, and the residue theorem ties them together at every level. Sections 5–7 build on this one identity.

4.7. The Same Offset Map at Every Level. For a self-similar scramble the offset map is the same at every level. In words: write the multipliers and the local roots into one $s \times s$ matrix series $\mathcal{A}(x)$; the response to a carry of length l is the l -th partial sum of the single matrix series $I - \mathcal{A}(0)\mathcal{A}(x)^{-1}$, and the level K does not appear, because level $K+1$ is level K with one more digit on top. Precisely, define the *frame matrix* $\mathcal{A}$ and its inverse G ,

$$\mathcal{A}(x)[c][b] = g_c(x) z_c(\theta x)^b \quad (0 \leq c, b < s), \quad G = \mathcal{A}^{-1}, \quad \hat{G} = \frac{G}{1-x},$$

with the coefficients $\mathcal{A}_a = [x^a]\mathcal{A}$, $\hat{G}_a = [x^a]\hat{G}$ and $\mathcal{A}_{>i} = \mathcal{A} - \sum_{a \leq i} \mathcal{A}_a x^a$. The proposition describes all j geometric digits; on a first reading one can take $i = 0$, where $\mathcal{A}_{>0}G = I - \mathcal{A}(0)G$.

Proposition 22 (Multi-digit offset map). *Let the scramble be self-similar with scale θ and multipliers g_c . Then for every $K \geq 1$, $i \geq 0$ and $1 \leq l \leq K$, the carry response is*

$$D_i(l) = [x^{l+i}] \mathcal{A}_{>i}(x) \hat{G}(x) = I - \sum_{a \leq i} \mathcal{A}_a \hat{G}_{l+i-a}.$$

More precisely, the coefficient of cell digit $K-1-d$ of coordinate c' in the geometric digit $K+i$ of coordinate c is $[x^d] x^{-i-1} \mathcal{A}_{>i}G[c][c']$. In particular the offset map does not depend on K , and

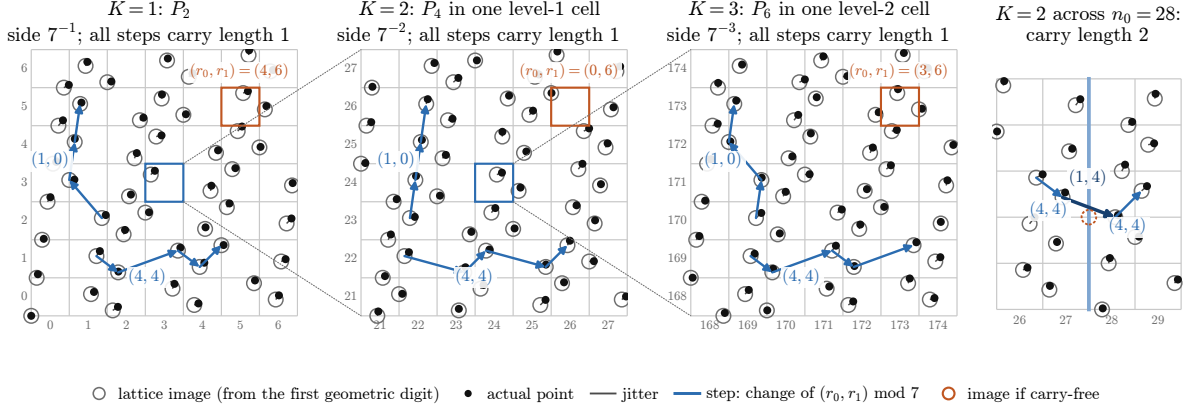


FIGURE 4. Self-similarity of the running example W^- in base 7. First three panels: P_2 with its 7×7 cells; the 49 points of P_4 in the marked cell; the 49 points of P_6 in the marked subcell (cell indices printed along the edges). The panels are not copies of one another; what repeats is the offset map. Inside one parent cell every step has carry length 1, and in every panel a step to the right changes the geometric digits (r_0, r_1) by $(4, 4)$ and a step up by $(1, 0)$ modulo 7 (printed on two arrows). From one panel to the next all first geometric digits shift by $(3, 0)$ modulo 7, as the marked cell shows $((4, 6) \rightarrow (0, 6) \rightarrow (3, 6))$. Right: a step across a boundary of carry length 2 ($n_0 = 27 \rightarrow 28 = 4 \cdot 7$) changes the digits by $D(2) = (1, 4)$ instead of $(4, 4)$; the dashed circle is where a carry-free step would have put the lattice image (Figure 3).

the one-digit offset map is the expansion of the matrix series

$$\mathcal{D}(x) := I - \mathcal{A}(0)G(x), \quad D(l) = [x^l] \frac{\mathcal{D}(x)}{1-x},$$

that is, $O_c(x) = \mathcal{D}(x)[c][c]$ and $X_{c \leftarrow c'}(x) = x^{-1}\mathcal{D}(x)[c][c']$ for $c' \neq c$.

Proof. $\mathcal{A}(0)[c][b] = g_c(0)a_c^b$ is a Vandermonde matrix with nonzero row factors, so G exists. By (4) and $w(z_c(\theta x)) = \theta x$, the digit series are $Y = \mathcal{A}(x)\tilde{\nu}(x)$ with $\tilde{\nu}_b(x) = \nu_b(\theta x)$, a vector of polynomials of degree less than K . The cell digits are $Y \bmod x^K$, so $\tilde{\nu} = (G(Y \bmod x^K)) \bmod x^K$. Change the cell digits by $x^a \mathbf{1}_{c'}$ (one unit at digit a of coordinate c' , where $\mathbf{1}_{c'}$ is the indicator vector of c'). Then $\tilde{\nu}$ changes by $x^a G_{<K-a} \mathbf{1}_{c'}$, and Y by

$$\mathcal{A} x^a G_{<K-a} \mathbf{1}_{c'} = x^a \mathbf{1}_{c'} - x^a \mathcal{A} G_{\geq K-a} \mathbf{1}_{c'},$$

using $\mathcal{A}G = I$. The first term changes only cell digits. The coefficient of x^{K+i} in the second is $-\sum_{b \leq i} \mathcal{A}_b G_{d+1+i-b} \mathbf{1}_{c'}$ with $d = K-1-a$, and this equals $[x^{d+1+i}] \mathcal{A}_{>i} G \mathbf{1}_{c'}$ because $[x^{d+1+i}] \mathcal{A}G = 0$. Summing over the l finest digits $a = K-l, \dots, K-1$, i.e. $d = 0, \dots, l-1$, gives $[x^{l-1}] x^{-i-1} \mathcal{A}_{>i} G / (1-x) = [x^{l+i}] \mathcal{A}_{>i} \hat{G}$, and $[x^{l+i}] \mathcal{A} \hat{G} = 1$ gives the second form. For $i = 0$, $\mathcal{A}_{>0} G = I - \mathcal{A}(0)G$; the own coefficient n sits at $d = n-1$ and the cross coefficient n at $d = n$, which gives the formulas for O_c , $X_{c \leftarrow c'}$ and $D(l)$. $\square$

The proposition holds in every characteristic and for every frame. The torus wrap $l = K$ is not special: it is the coefficient of x^K of the same series.

In the running example the series $\mathcal{D}(x)/(1-x)$ of Proposition 22 reproduces Table 5, and the table is the same at every level; this is what Figure 4 shows in three nested zooms.

The responses of a self-similar scramble cannot all be constant. Two responses of one column (the own and the cross response for $s = 2$, two cross responses for $s \geq 3$) are never both rational series, so they are never both eventually periodic (Proposition 92 in Appendix A); and in dimension two, with the places 0 and 1, no scramble has an offset map that depends only on the finest cell digits, a sheared lattice without jumps, at two consecutive levels $K, K + 1 \geq 2$ (Corollary 53). Apart from a few constant responses, as in the brick wall, the responses keep changing with the carry length. Section 7 counts how many exact relations of this kind a sequence can carry, and Section 8 keeps the remaining responses in fixed sets of allowed values.

4.8. Digit Relaxation. We now turn the offset map into a lower bound on the separation. The picture is that of [18]. Two points in cells that are two or more cells apart in some coordinate are at least one cell side apart. So only neighbouring cells matter, and for neighbours the distance is the cell step plus the change of the lattice image, up to the jitter. The change of the lattice image is given by the offset map, through the carry responses of the coordinates that move.

The bound in one coordinate. A point sits at the fractional position $\text{enc}(R)/q^j$ plus a jitter in its cell; its neighbour one cell to the right sits at $\text{enc}(R \oplus \sigma)/q^j$ plus its own jitter, where σ is the change of the geometric digits given by the offset map. The worst case over the position R is the closest the two can come; from it we subtract one grid unit for the two jitters (Figure 5(a)). For a step $e_c \in \{-1, 0, 1\}$ and a change $\sigma \in \mathbb{F}_q^j$ of the j geometric digits of one coordinate, put

$$f_j(e_c, \sigma) = \frac{1}{q^j} \max\left(0, \min_{R \in \mathbb{F}_q^j} |e_c q^j + \text{enc}(R \oplus \sigma) - \text{enc}(R)| - 1\right),$$

where $\oplus$ is digitwise addition in $\mathbb{F}_q$. It is the smallest possible gap, in cell units, between the two points in that coordinate; we call it the *guaranteed gap*. For $q = 7$ and $j = 1$: a backward shift $\sigma = -3$ of the neighbour gives $f_1(1, -3) = \frac{3}{7}$, while the forward shift $\sigma = +1$ gives $f_1(1, 1) = 0$, since the point at the right edge of its cell and the neighbour at the left edge of the next cell can touch. A coordinate that does not move ($e_c = 0$) is safe when σ is near $\frac{1}{2}$, half a cell (Figure 5(b)).

Lemma 23 (Digit relaxation). *Let P_{sK} be a $(0, sK, s)$ -net in base q with $q^K \geq 4$ and carry responses $D_i(l)$, and let $j \geq 1$. For a step $e \in \{-1, 0, 1\}^s \setminus \{0\}$, carry lengths $l_{c'} \in [1, K]$ and digits $y_{c'} \in \mathbb{F}_q$ for the moving coordinates ($e_{c'} \neq 0$), let $\sigma_c \in \mathbb{F}_q^j$ have the entries*

$$\sigma_{c,i} = \sum_{c': e_{c'} \neq 0} e_{c'} \delta_i(l_{c'}, y_{c'})[c][c'], \quad i < j,$$

with $\delta_i(l, y) = D_i(l)$ for prime q and $\delta_i(l, y)$ as in (8) in general. Then

$$\text{sep}(P_{sK}) \geq \min(1, \text{LB}_j), \quad \text{LB}_j := \min\left(\sum_c f_j(e_c, \sigma_c)^2\right)^{1/2},$$

the minimum over all steps e up to sign, all carry lengths and (for non-prime q) all digits $y_{c'}$ of the moving coordinates.

Proof. Let two points lie in the cells n and n' . Represent $n' - n$ modulo q^K with entries in $(-q^K/2, q^K/2]$. If some entry has absolute value at least 2, the points are at least one cell side apart in that coordinate, which gives the 1. Otherwise $n' = n + e$ on the torus with $e \in \{-1, 0, 1\}^s \setminus \{0\}$, as each cell holds one point; swapping the points we may replace e by $-e$. By (3) the difference in coordinate c , in cell units, is

$$e_c + \frac{\text{enc}(R'_c) - \text{enc}(R_c)}{q^j} + \varepsilon'_c - \varepsilon_c, \quad |\varepsilon'_c - \varepsilon_c| \leq q^{-j}.$$

Its absolute value is at most $2 \leq q^K/2$, so it is the toroidal difference. The offset map is $\mathbb{F}_q$ -linear in the cell digits, and only the cell indices of the moving coordinates change, each by a carry

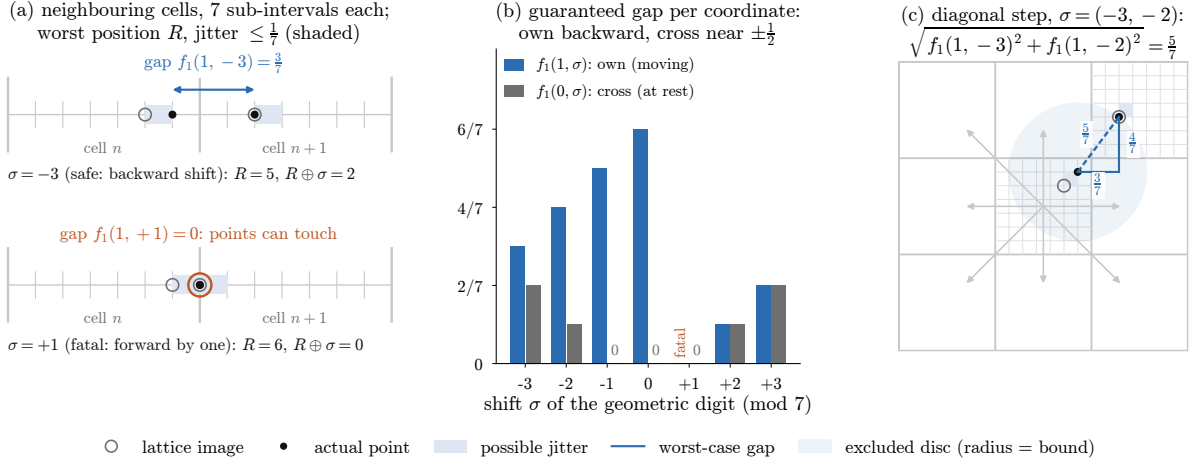


FIGURE 5. The digit relaxation (Lemma 23) for one geometric digit, $q = 7$ (schematic with exact values). (a) Two neighbouring cells, each split into 7 sub-intervals. A point sits at $R/7$ plus a jitter of at most $1/7$ (shaded); its neighbour in the next cell sits at $(R \oplus \sigma)/7$ plus its own jitter. The worst case puts the first point at the right end of its jitter and the neighbour at the left end. For $\sigma = -3$ (a backward shift) the gap is at least $f_1(1, -3) = 3/7$ for every R ; for $\sigma = +1$ (forward by one sub-interval) the point at the right edge of its cell and the neighbour at the left edge of the next cell can touch: $f_1(1, 1) = 0$. (b) The guaranteed gap $f_1(e, \sigma)$ over $\sigma \in \mathbb{F}_7$ for a coordinate that moves to the next cell ($e = 1$, own response) and for one that stays ($e = 0$, cross response). Own responses must point backward; cross responses must stay near $\pm \frac{1}{2}$, half a cell. (c) In the plane the coordinate gaps add in squares: a diagonal step with $\sigma = (-3, -2)$ keeps the neighbour outside the disc of radius $\sqrt{(3/7)^2 + (4/7)^2} = 5/7$ around the point. The bound is the minimum of these numbers over all steps and all carry lengths.

of its own length l'_c , stopping at a digit with some value y_c ; by (8) this gives $R'_c = R_c \oplus \sigma_c$ for a step $+1$, and a step -1 is the reverse of a step $+1$ from the lower cell, which gives $-\sigma_c$. The absolute value is therefore at least $f_j(e_c, \sigma_c)$, and summing the squares over c bounds the distance in cell units. Finally $\delta(P_{sK}) N^{1/s} = \delta(P_{sK}) q^K$ is the distance in cell units. $\square$

The case $j = 1$ is the one-digit relaxation of [18], which under its hypothesis (H2) on the deeper digits in addition gives a coordinate that moves alone no jitter; here the deeper digits are always counted as jitter. Taking the minimum over all carry lengths $l \geq 1$ instead of $l \leq K$ only enlarges the set, so for an offset map that does not depend on K , such as that of a self-similar scramble (Proposition 22), the value LB_j computed from all $l \geq 1$ bounds $\text{sep}(P_{sK})$ for every K with $q^K \geq 4$. The bound minimises each coordinate separately, over the position and the jitter of that coordinate alone. This coordinatewise relaxation is why it is valid without knowing where the points sit, and also why it can be loose: the worst positions in different coordinates need not occur in the same pair of points.

Remark 24 (One digit). For $j = 1$ and prime $q = p$, σ is a single residue and f_1 is explicit:

$$f_1(1, -A) = 1 - \frac{A+1}{p} \quad (0 \leq A < p), \quad f_1(1, 1) = 0, \quad f_1(-1, \sigma) = f_1(1, -\sigma).$$

So a backward shift of the neighbour's geometric digit is harmless, and the forward shift by one unit is fatal: the point at the right edge of its cell and the neighbour at the left edge of the next cell can come arbitrarily close. An own response $+1$ together with vanishing cross responses is the configuration behind the close pairs of Section 3. In dimension two the terms of the bound are $(f_1(1, O_c^{(l)})^2 + f_1(0, X_{1 \leftarrow c}^{(l)})^2)^{1/2}$ for the axis steps of coordinate c , and

$$\left(f_1(1, O_0^{(l_0)} \pm X_{0 \leftarrow 1}^{(l_1)})^2 + f_1(\pm 1, X_{1 \leftarrow 0}^{(l_0)} \pm O_1^{(l_1)})^2\right)^{1/2}$$

for the diagonal $(+)$ and antidiagonal $(-)$ steps. In the running example (Table 5) the horizontal step with $l = 1$ has $\sigma = (4, 4) = (-3, \frac{1}{2})$ and the term $\sqrt{(3/7)^2 + (2/7)^2} = 0.515$; the step with $l = 2$ has the fatal own shift 1 and keeps only its cross term $f_1(0, \frac{1}{2}) = \frac{2}{7} = 0.2857$, which is the bound of Theorem 32 at $p = 7$.

What remains is to choose a self-similar scramble whose infinitely many responses $D(l)$ all stay away from the configurations that bring neighbours together. The residue form makes some of them constant by design (Sections 5–6); the rest are kept in windows (Section 8).

5. RESIDUE SEQUENCES

Section 3 located the failure of the classical sequences in one place: each coordinate reads the index at its own place, and a carry in the last digits of one coordinate is invisible to the leading digits of all the others. Two points on either side of a cell boundary of one coordinate can then agree in every other coordinate. The repair must tie the coordinates together, and it must do so with one fixed scramble, the same for all numbers of points.

Section 4 found the tool. Every scramble reads digit n of coordinate c as a residue of the index polynomial at the place a_c (Lemma 21), and the residues of one rational function at all the places add up to its coefficient at infinity (Lemma 21(c)). If the coordinates read their digits from one common rational differential, this identity is a linear relation between digits of different coordinates, and it holds at every level. For the brick wall it says that the height of a point in coordinate 1 is half the finest cell digit of coordinate 0 (Section 4).

This section turns that observation into two constructions. The *staggered residue sequence* (Section 5.2) uses the identity at the full levels: one coordinate is staggered by a rank-1 lattice rule in the cell indices of the others. This is the brick wall in every dimension, certified at every full level for every prime $p > 2^s$, but with a constant of about 2^{1-s} , because the other coordinates are not controlled inside their cells. The *residue sequence* (Section 5.3) deletes one factor of the differential. The same kind of relation then holds one digit earlier, at the prefixes P_{sK-1} , in all coordinates alike, and these prefixes become exactly the lattice image plus jitter of the nets of [18], with constants that tend to 1 and exceed 1 at moderate primes. Section 6 carries all s geometric digits of the nets at every s -th full level, Section 7 explains why a frame scramble cannot carry more exact relations of bounded depth, and Section 10 compares the residue sequence with the window constructions in practice. Throughout this section p is a prime, the places $a_0, \dots, a_{s-1} \in \mathbb{F}_p$ are distinct (so $p \geq s$), $w = \prod_c (z - a_c)$ and $w_c = w/(z - a_c)$.

5.1. The Residue Theorem as a Design Tool. By Lemma 21(b) a self-similar scramble with scale θ reads digit n of coordinate c as

$$y_{c,n}(V) = \text{Res}_{a_c} \left(V \varphi_c \left(\frac{\theta}{w} \right)^{n+1} dz \right),$$

with a local multiplier φ_c at each place. Take a rational function Φ whose finite poles lie at the places, and suppose that at every place a_c the differential $\Phi(\theta/w)^{T+1} dz$ is a constant multiple of the differential that reads one digit of coordinate c . Then for $\deg V < m$ the residue of

$F = V\Phi(\theta/w)^{T+1}$ at a_c is a multiple of that digit, and by Lemma 21(c) the residues add up to $[z^{-1}]F$, which is 0 as soon as $F = O(z^{-2})$ at ∞ . That is a linear relation among one digit of each coordinate on the prefix P_m , the same at every level T , with no carries anywhere: an *exact digit relation* (Section 7). The residue theorem over all places also gives the duality of Niederreiter and Özbudak [32], where the relations bound the quality parameter (Section 4). Here w/θ is a local parameter at every place at once, so $(\theta/w)^{T+1}$ is a single power of the local parameter at each place, and each relation involves one digit of each coordinate. The design question is which Φ and which local multipliers make this relation useful for the separation. The two simplest choices are $\Phi = 1/(z - a_{c_*})$, which reads digit T of every coordinate except one, c_* , and digit $T + 1$ of c_* (Section 5.2), and $\Phi = 1$, which reads digit T of every coordinate (Section 5.3).

5.2. Staggered Residue Sequences. Fix a coordinate c_* , the *staggered coordinate*, and let $C = \{c \neq c_*\}$ be the others.

Definition 25 (Staggered residue sequence). Let $s \geq 2$, let $\theta, \mu_* \in \mathbb{F}_p^*$, and let $k = (k_c)_{c \in C} \in (\mathbb{F}_p^*)^{s-1}$ be the *weights*; put $\mu_c = -\mu_*/k_c$ for $c \in C$. The *staggered residue sequence* $\mathcal{R}_v^*$ with check vector $v = (v_c)$, $v_c = k_c$ for $c \in C$ and $v_{c_*} = -1$, is the digital sequence over $\mathbb{F}_p$ with the digits

$$y_{c,n}(V) = \mu_c \operatorname{Res}_{a_c} \left(\frac{V dz}{(z - a_{c_*})(w/\theta)^{n+1}} \right) \quad (c \in C), \quad y_{c_*,n}(V) = \mu_* \operatorname{Res}_{a_{c_*}} \left(\frac{V dz}{(z - a_{c_*})(w/\theta)^n} \right).$$

Its generator matrices have the entries (row n , column i , i.e. the coefficient of the index digit V_i)

$$C_c[n][i] = \mu_c \theta^{n+1} [(z - a_c)^n] \frac{z^i}{(z - a_{c_*}) w_c(z)^{n+1}} \quad (c \in C),$$

$$C_{c_*}[n][i] = \mu_* \theta^n [(z - a_{c_*})^n] \frac{z^i}{w_{c_*}(z)^n}.$$

The matrix formula is the residue written out: at a_c the denominator is $(z - a_c)^{n+1}$ times the unit $(z - a_{c_*}) w_c^{n+1}$, so the residue is the coefficient of $(z - a_c)^n$ in V divided by that unit. Each entry is one coefficient of a power series, computed by truncated power-series arithmetic over $\mathbb{F}_p$. In the notation of Lemma 21(b) the local multipliers are

$$\varphi_c = \frac{\mu_c}{z - a_{c_*}} \quad (c \in C), \quad \varphi_{c_*} = \frac{\mu_* w_{c_*}}{\theta},$$

both units at their places, since $w_{c_*}(a_{c_*}) = w'(a_{c_*}) \neq 0$. So $\mathcal{R}_v^*$ is a self-similar scramble, and Proposition 22 applies to it.

Lemma 26 (Staggered residue sequences have $t = 0$). $C_c = L_c P_{a_c}$ with a fixed lower-triangular matrix L_c whose diagonal entries are $L_c[n][n] = \mu_c \theta^{n+1} / ((a_c - a_{c_*}) w'(a_c)^{n+1})$ for $c \in C$ and $L_{c_*}[n][n] = \mu_* \theta^n / w'(a_{c_*})^n$. Hence $\mathcal{R}_v^*$ is a digital $(0, s)$ -sequence over $\mathbb{F}_p$.

Proof. At a_c , $c \in C$, the differential $dz / ((z - a_{c_*})(w/\theta)^{n+1})$ is $(z - a_c)^{-n-1}$ times a unit power series with constant term $\theta^{n+1} / ((a_c - a_{c_*}) w'(a_c)^{n+1})$; at a_{c_*} the differential $dz / ((z - a_{c_*})(w/\theta)^n)$ is $(z - a_{c_*})^{-n-1}$ times a unit with constant term $\theta^n / w'(a_{c_*})^n$. So the digit n of each coordinate is the residue of V against a polar differential of exact pole order $n+1$ at its place, and Lemma 21(a) gives $C_c = L_c P_{a_c}$ with lower-triangular L_c ; its diagonal is the constant term of the unit times μ_c (resp. μ_*). Nothing depends on a level, and Lemma 1 gives $t = 0$. $\square$

Lemma 27 (The staggered digit is a rank-1 lattice rule). *For every $K \geq 1$ and every V with $\deg V < sK$,*

$$y_{c_*,K}(V) = \sum_{c \in C} k_c y_{c,K-1}(V), \quad \text{more generally} \quad y_{c_*,K+i}(V) = \sum_{c \in C} k_c y_{c,K-1+i}(V) \quad (i \geq 0).$$

Proof. Let $F = \theta^K V / ((z - a_{c_\star})w^K)$. Its finite poles are at the places, and its numerator has degree at most $sK - 1$, two less than the degree $sK + 1$ of its denominator; so $F = O(z^{-2})$ at ∞ , and Lemma 21(c) gives $\sum_c \text{Res}_{a_c}(F dz) = 0$. By Definition 25, $\text{Res}_{a_{c_\star}}(F dz) = y_{c_\star, K}(V)/\mu_\star$ and $\text{Res}_{a_c}(F dz) = y_{c, K-1}(V)/\mu_c$ for $c \in C$. Multiplying by $\mu_\star$ and using $-\mu_\star/\mu_c = k_c$ gives the first identity. The second is the first at level $K + i$, since $\deg V < sK \leq s(K + i)$. $\square$

For a prime base the finest cell digit $y_{c, K-1}$ of coordinate c at level K is the cell index n_c modulo p , so the geometric digit of the staggered coordinate is

$$r_{c_\star} \equiv \sum_{c \in C} k_c n_c \pmod{p},$$

a rank-1 lattice rule in the cell indices of the other coordinates. A step of n_c by $+1$ adds 1 to the finest digit whatever the carry length, the toroidal wrap included, so it moves $r_{c_\star}$ by exactly k_c ; a step of $n_{c_\star}$ does not move it. In the language of Section 4: the cross responses $X_{c_\star \leftarrow c}^{(l)} = k_c$ and the own response $O_{c_\star}^{(l)} = 0$ are constant, for every carry length l .

So a step in a coordinate of C offsets the neighbour in coordinate $c_\star$ by a fixed amount, and the theorem below measures how far from 0 these offsets stay. For $x \in \mathbb{F}_p$ we write $|x| \in [0, p/2]$ for its *centred absolute value*, the absolute value of its representative in $(-p/2, p/2)$.

Theorem 28 (Staggered residue sequences). *Let $p \geq 5$ and put*

$$\beta(k) = \min_{e' \in \{-1, 0, 1\}^C \setminus \{0\}} \frac{|k \cdot e'| - 1|}{p}, \quad k \cdot e' = \sum_{c \in C} k_c e'_c \in \mathbb{F}_p.$$

Then $\text{sep}(P_{sK}) \geq \beta(k)$ for every $K \geq 1$. If $\beta(k) > 0$, the sequence is quasi-uniform, with $\delta(P_{[N]}) \geq (\beta(k)/p)N^{-1/s}$ for every $N \geq 2$ and $h/\delta \leq \sqrt{s}p/\beta(k)$.

Proof. We apply the digit relaxation (Lemma 23) with $j = 1$ and keep only the term of coordinate $c_\star$. For a step e with any carry lengths, the change of $r_{c_\star}$ is $\sigma_{c_\star} = k \cdot e'$, where e' is the restriction of e to C (the constant responses above). If $e' = 0$, then $e_{c_\star} = \pm 1$, $\sigma_{c_\star} = 0$, and the term is $f_1(\pm 1, 0) = (p - 1)/p$. If $e' \neq 0$ and $e_{c_\star} = 0$, the term is $f_1(0, \sigma) = (|\sigma| - 1)/p$: the two positions $\text{enc}(R)$ and $\text{enc}(R + \sigma)$ differ by $\hat{\sigma}$ or $p - \hat{\sigma}$, where $\hat{\sigma} \in [1, p - 1]$ represents σ , and the smaller is $|\sigma|$. If $e' \neq 0$ and $e_{c_\star} = \pm 1$, then $f_1(1, \sigma) = (\hat{\sigma} - 1)/p$ and $f_1(-1, \sigma) = (p - \hat{\sigma} - 1)/p$ are both at least $(|\sigma| - 1)/p$. Since $|\sigma| \leq p/2$, the minimum over all steps is $\min(1, \beta(k), (p - 1)/p) = \beta(k)$, and Lemma 23 (with $p^K \geq 5$) gives $\text{sep}(P_{sK}) \geq \beta(k)$. The last statement is Lemma 2 with $\mathcal{M} = s\mathbb{N}$ and Remark 3. $\square$

What the theorem sees. Take integer representatives $\tilde{k}_c$ of the weights and put $\tilde{k}_{c_\star} = 0$. In cell units, the height of the point in cell n in coordinate $c_\star$ is $n_{c_\star} + \text{frac}(\tilde{k} \cdot n/p)$ up to a jitter of $1/p$. Reducing modulo p only subtracts integer multiples of the unit vector $\mathbf{1}_{c_\star}$, so these heights form, globally and at every level, the lattice $(I + \mathbf{1}_{c_\star} \tilde{k}^\top/p)\mathbb{Z}^s$ in the coordinate $c_\star$: a wrap of $r_{c_\star}$ is a translation of this lattice, so there are no slip planes and no jumps in that coordinate. The other $s - 1$ coordinates are not designed. Inside its cell a point can sit anywhere in them, a jitter of a whole cell; two points in neighbouring cells may agree in every coordinate except $c_\star$, and only the gap $(|k \cdot e'| - 1)/p$ in coordinate $c_\star$ is left. That is what $\beta(k)$ measures.

Corollary 29 (Dyadic weights). *Let p be an odd prime, order C as $c_1, \dots, c_{s-1}$ and put $k_{c_i} = 2^{i-s} \in \mathbb{F}_p$. Then*

$$\beta(k) = \frac{\lfloor p/2^{s-1} \rfloor - 1}{p},$$

and no weights $k \in (\mathbb{F}_p^*)^{s-1}$ give a larger value of β . In particular, for every $s \geq 2$ and every prime $p > 2^s$ the staggered residue sequence with dyadic weights is a quasi-uniform digital $(0, s)$ -sequence with $\text{sep}(P_{sK}) \geq (\lfloor p/2^{s-1} \rfloor - 1)/p$ for every $K \geq 1$; and $\beta(k) > 0$ for some k only if $p > 2^s$.

Proof. For $e' \in \{-1, 0, 1\}^{s-1} \setminus \{0\}$ we have $k \cdot e' = A/2^{s-1}$ with the integer $A = \sum_i e'_i 2^{i-1}$, and $0 < |A| \leq 2^{s-1} - 1$ ($A \neq 0$ because the term of the largest i with $e'_i \neq 0$ exceeds the sum of the others in absolute value). Let x be the centred representative of $A/2^{s-1}$. Then $2^{s-1}x - A$ is an integer multiple of p , and it is nonzero, since otherwise 2^{s-1} would divide A . Hence $2^{s-1}|x| \geq p - |A| \geq p - 2^{s-1} + 1$, and as $|x|$ is an integer, $|x| \geq \lceil (p+1)/2^{s-1} \rceil - 1 = \lfloor p/2^{s-1} \rfloor$. So $\beta(k) \geq (\lfloor p/2^{s-1} \rfloor - 1)/p$.

Conversely, let k be any weights and consider the 2^{s-1} subset sums $S_A = \sum_{c \in A} k_c \in \mathbb{F}_p$, $A \subseteq C$. The difference of two of them is $k \cdot e'$ with $e' = \mathbf{1}_A - \mathbf{1}_B \in \{-1, 0, 1\}^C \setminus \{0\}$. If all these differences have centred absolute value at least $d \geq 1$, the 2^{s-1} sums are distinct points of the cycle $\mathbb{Z}/p\mathbb{Z}$ at mutual distance at least d , so $2^{s-1}d \leq p$. Hence $\min_{e'} |k \cdot e'| \leq \lfloor p/2^{s-1} \rfloor$ and $\beta(k) \leq (\lfloor p/2^{s-1} \rfloor - 1)/p$, with equality for the dyadic weights by the first part. Finally $\lfloor p/2^{s-1} \rfloor \geq 2$ if and only if $p \geq 2^s$, that is $p > 2^s$; then $p \geq 5$ and $p \geq s$, and Theorem 28 applies. $\square$

The dyadic weights stagger the coordinate $c_\star$ by multiples of 2^{1-s} of a cell: half a cell for one other coordinate, quarters for two, and so on. Their value tends to 2^{1-s} , and the corollary shows that no other weights do better for *this bound*. The cap is a property of the certificate, not of the sequence: the argument of the second part uses only the steps with $e_{c_\star} = 0$ and carry length 1, so it caps every one-digit relaxation that keeps only the term of a single coordinate. The separation itself is larger. For instance, the exact values of $\text{sep}(P_s)$ ($K = 1$) computed for $s = 4$ and $s = 5$ lie between 0.1985 and 0.4837 (for instance, with the Faure places, $c_\star = s - 1$ and $\theta = 1$, 0.3678 for $s = 4$, $p = 17$, and 0.4837 for $s = 5$, $p = 37$), against $\beta = 1/17$ and $1/37$; whether such values persist for all K is open. For $p = 11, 37$ and 211 in dimension 3, 4 and 5 the corollary gives $1/11, 3/37$ and $12/211$; in dimension three it gives $9/41, 24/101$ and $251/1009$ at $p = 41, 101$ and 1009 .

Example 30 (The brick wall). Let $s = 2$, with the Faure places $a_0 = 0, a_1 = 1$ (so $w = z^2 - z$, $w_0 = z - 1, w_1 = z$), staggered coordinate $c_\star = 1$, scale $\theta = -\frac{1}{4}$ and constants $\mu = (\mu_0, \mu_\star) = (-4, 2)$. The weight is $k_0 = -\mu_\star/\mu_0 = \frac{1}{2}$, the dyadic weight for $s = 2$. The digits are

$$y_{0,n}(V) = -4 \text{Res}_0 \left(\frac{V dz}{(z-1)(w/\theta)^{n+1}} \right), \quad y_{1,n}(V) = 2 \text{Res}_1 \left(\frac{V dz}{(z-1)(w/\theta)^n} \right),$$

and the local multipliers are $\varphi_0 = -4/(z-1)$ and $\varphi_1 = 2z/\theta = -8z$. For $p = 7$ the generator matrices are those of Example 18 (a direct check of the 4×4 blocks). By Lemma 27, $r_1 \equiv \frac{1}{2}n_0 \pmod{p}$: the height of a point in coordinate 1 moves by half a cell from one column of cells to the next and stays fixed along a column, at every level and every carry length. These are the constant responses $X_{1 \leftarrow 0}^{(l)} = \frac{1}{2}$ and $O_1^{(l)} = 0$ of Table 5.

Definition 31 (Brick wall). For an odd prime p , the *brick wall* W^- is the staggered residue sequence of Example 30 over $\mathbb{F}_p$.

In the multiplier form of Definition 20, Lemma 21(b) turns the local multipliers into $g_0 = 2/(\sqrt{1-x}(1+\sqrt{1-x}))$ and $g_1 = (1+\sqrt{1-x})/\sqrt{1-x}$, where $\sqrt{1-x} \in \mathbb{F}_p[[x]]$ has constant term 1 (the scaled local roots are $z_{0,1}(\theta x) = (1 \mp \sqrt{1-x})/2$). In that form the two constant responses need a computation with the frame matrix; the residue form gives them in one line.

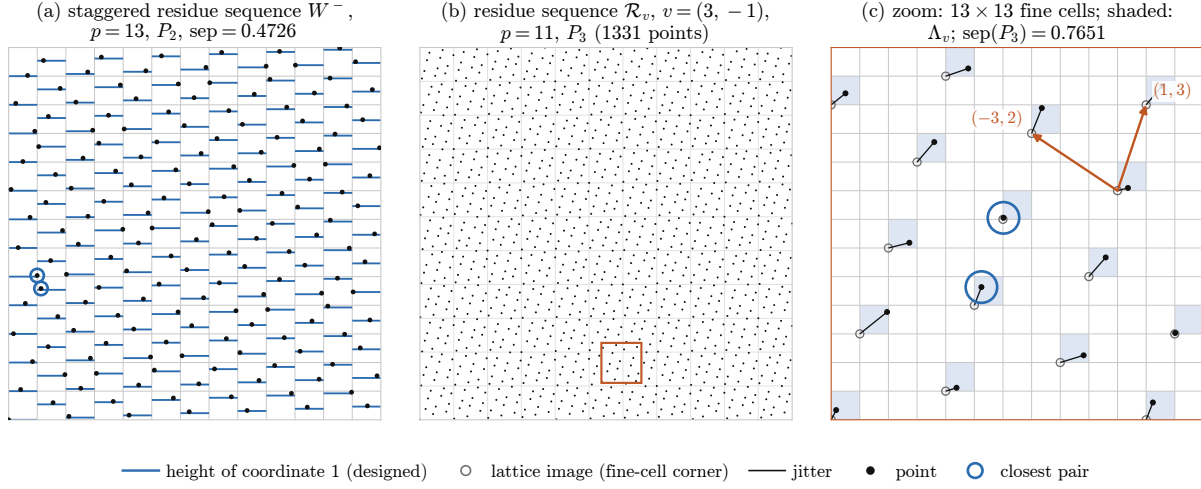


FIGURE 6. The two residue constructions, exact points from the generator matrices. (a) The brick wall W^- (staggered residue sequence, $s = 2$) for $p = 13$, the full level P_2 with its 13×13 cells. In each cell the blue segment is the designed height of the point in coordinate 1, $n_1 + r_1/13$ with $r_1 \equiv \frac{1}{2}n_0$ (Lemma 27): it is constant along a column and moves by half a cell from one column to the next. The horizontal position is not designed. The circled closest pair sits in neighbouring columns at almost the same horizontal position; exact $\text{sep}(P_2) = 0.4726$ (also at $m = 4, 6$), certified bound $5/13 = 0.3846$ (Theorem 32). (b) The residue sequence $\mathcal{R}_v$, $s = 2$, $p = 11$, places $(0, 1)$, $\theta = 1$, $v = (3, -1)$ (the Korobov vector, $\rho = 3$), the prefix P_3 (level $K = 2$, fine cells of side 11^{-2}). (c) Zoom on the marked 13×13 fine cells. The shaded fine cells are those of the lattice $\Lambda_v = \{b : 3b_0 - b_1 \equiv 0 \pmod{11}\}$, spanned by $(1, 3)$ and $(-3, 2)$; each holds exactly one point, and no other fine cell holds one (Theorem 36(i)). The lattice image of a point is the corner of its fine cell, and the jitter moves it by less than one fine cell. Exact $\text{sep}(P_3) = 0.7651$ (0.6238 at $m = 5$ and $m = 7$), certified bound $\lambda_{\text{jit}}(\Lambda_v) p^{-1/2} = 2/\sqrt{11} = 0.6030$ for every P_{2K-1} .

Theorem 32 (Brick wall). *For every prime $p \geq 5$ the brick wall is a digital $(0, 2)$ -sequence over $\mathbb{F}_p$ with*

$$\text{sep}(P_{2K}) \geq \frac{p-3}{2p} \quad \text{for every } K \geq 1,$$

and it is quasi-uniform.

Proof. This is Corollary 29 with $s = 2$: $\lfloor p/2 \rfloor - 1 = (p-3)/2$. □

The proof uses one coordinate and one geometric digit. Coordinate 0 is left to the frame: two points in neighbouring columns of cells can sit at almost the same horizontal position, and then they are only about half a cell apart (Figure 6(a)). To do better in the full levels the horizontal positions must be controlled as well; then, in a self-similar scramble, the half can no longer be kept exactly (Proposition 92) and has to be kept in a window, which is the hexagonal brick wall of Section 8. The next construction instead reads one relation of the same kind in all coordinates alike.

5.3. Residue Sequences. The staggered residue sequence reads its relation at two scales: the coordinates of C at the scale of the cells (their finest cell digit $y_{c,K-1}$), the coordinate $c_\star$ one

digit deeper (its geometric digit $y_{c_*,K}$). That is why the coordinates of C keep a jitter of a whole cell. The remedy is to read the relation at one common scale in all coordinates. Deleting the factor $1/(z - a_{c_*})$ from the differential does exactly this: every coordinate then reads the same differential $V dz$, and the residue theorem relates the digits $y_{c,K-1}$ of all coordinates, at the prefixes P_{sK-1} , one digit before the full level.

Definition 33 (Residue sequence). Let $s \geq 2$, $\theta \in \mathbb{F}_p^*$ and let $v = (v_0, \dots, v_{s-1}) \in (\mathbb{F}_p^*)^s$ be a *check vector*. The *residue sequence* $\mathcal{R}_v$ is the digital sequence over $\mathbb{F}_p$ with the digits

$$y_{c,n}(V) = v_c^{-1} \text{Res}_{a_c} \left(V \left(\frac{\theta}{w} \right)^{n+1} dz \right), \quad C_c[n][i] = v_c^{-1} \theta^{n+1} [(z - a_c)^n] \frac{z^i}{w_c(z)^{n+1}}.$$

Its local multipliers are the constants $\varphi_c = v_c^{-1}$, and by Lemma 21(b) its multipliers are $g_c(x) = \theta z'_c(\theta x)/v_c$: in the common uniformizer w , every coordinate reads the w -adic digits of the differential $V dz$ at its own place, where the classical frame reads those of the function V .

Lemma 34 (Residue sequences have $t = 0$). $C_c = L_c P_{a_c}$ with a fixed lower-triangular L_c , $L_c[n][n] = v_c^{-1} \theta^{n+1}/w'(a_c)^{n+1}$. Hence $\mathcal{R}_v$ is a self-similar digital $(0, s)$ -sequence over $\mathbb{F}_p$.

Proof. At a_c , $(\theta/w)^{n+1} dz$ is $(z - a_c)^{-n-1}$ times a unit with constant term $\theta^{n+1}/w'(a_c)^{n+1}$; Lemma 21(a) and Lemma 1 conclude as in Lemma 26. $\square$

Lemma 35 (The skeleton relation). For every $K \geq 1$,

$$\sum_c v_c y_{c,K-1}(V) = \begin{cases} 0, & \deg V \leq sK - 2, \\ \theta^K [z^{sK-1}] V, & \deg V = sK - 1. \end{cases}$$

Moreover $\sum_c v_c y_{c,K-1+i}(V) = 0$ for every $i \geq 0$ and every V with $\deg V \leq sK - 2$.

Proof. Let $F = \theta^K V/w^K$. Then $v_c y_{c,K-1}(V) = \text{Res}_{a_c}(F dz)$, and by Lemma 21(c) the sum is $[z^{-1}]F$. As $w^K = z^{sK} + \dots$, we have $F = \theta^K [z^{sK-1}] V \cdot z^{-1} + O(z^{-2})$ at ∞ when $\deg V \leq sK - 1$, which gives both cases. The second statement is the first at level $K + i$. $\square$

Skeleton coordinates and fine cells. The prefix P_{sK-1} has $N = p^{sK-1}$ points, one digit fewer than a full level. Choose one coordinate c_0 and give it $K - 1$ cell digits and every other coordinate K ; the boxes with these depths have volume $p^{-(sK-1)}$, so each holds exactly one point (Lemma 34). In the language of [18], c_0 is a *skeleton coordinate*, and its next digit $y_{c_0,K-1}$, the *skeleton digit*, is fixed by Lemma 35: $y_{c_0,K-1} = -v_{c_0}^{-1} \sum_{c \neq c_0} v_c y_{c,K-1}$, a rank-1 lattice rule in the finest cell digits of the other coordinates. Every coordinate can play this role; the relation $\sum_c v_c y_{c,K-1} = 0$ is symmetric, and we call it the *skeleton relation*.

Fine cells and the lattice. Giving every coordinate K digits instead turns the skeleton relation into a statement about cubes. The *fine cells* of P_{sK-1} are the cubes of side p^{-K} , and the fine cell of a point is $\hat{n} = (\hat{n}_c)$, $\hat{n}_c = \sum_{i < K} y_{c,i} p^{K-1-i} \in [0, p^K)$ (this is $\lfloor p^K y_c \rfloor$ unless the digits of y_c end in $p - 1$). The skeleton relation is a relation among the last digits of the fine-cell indices, so it describes a lattice. For a check vector v let

$$\Lambda_v = \left\{ b \in \mathbb{Z}^s : \sum_c v_c b_c \equiv 0 \pmod{p} \right\}, \quad \lambda_{\text{jit}}(\Lambda) = \min_{0 \neq b \in \Lambda} \|(|b| - \mathbf{1})_+\|_2,$$

where $|b|$ and $(\cdot)_+$ are taken coordinatewise. Λ_v is the Construction-A lattice of the linear code with parity-check vector v [8, Ch. 5], of index p in $\mathbb{Z}^s$; $\lambda_{\text{jit}}(\Lambda)$ is the length of its shortest nonzero vector after one unit of jitter is subtracted in every coordinate [18].

Theorem 36 (Residue sequences). Let $s \geq 2$ and let v be a check vector. For every $K \geq 1$, with $N = p^{sK-1}$:

- (i) *the fine cells occupied by the points of P_{sK-1} are exactly the elements of $\Lambda_v \cap [0, p^K)^s$, each holding one point;*
- (ii) $\text{sep}(P_{sK-1}) \geq p^{-1/s} \lambda_{\text{jit}}(\Lambda_v)$.

Proof. (i) The fine cell $\hat{n}$ of a point determines its first K digits in every coordinate, and $\hat{n}_c \equiv y_{c,K-1} \pmod{p}$ (for a prime base the K -th digit is the last base- p digit of $\hat{n}_c$). By Lemma 35, $\sum_c v_c \hat{n}_c \equiv 0 \pmod{p}$, so $\hat{n} \in \Lambda_v$. The fine cell determines the box of depths $(K, \dots, K, K-1, K, \dots, K)$ of any skeleton coordinate, which holds one point, so distinct points lie in distinct fine cells. The p^{sK-1} points therefore occupy p^{sK-1} distinct elements of $\Lambda_v \cap [0, p^K)^s$. This set has exactly p^{sK-1} elements: Λ_v contains $p^K \mathbb{Z}^s$, and it is the union of p^{sK}/p classes modulo p^K , one element of $[0, p^K)^s$ each. So every element is occupied.

(ii) Let two points lie in the fine cells $\hat{n}$ and $\hat{n}'$, and let b_c be the representative of $\hat{n}'_c - \hat{n}_c$ modulo p^K in $(-p^K/2, p^K/2]$. Then $b \equiv \hat{n}' - \hat{n} \pmod{p}$, so $b \in \Lambda_v$, and $b \neq 0$ by (i). In units of the fine-cell side p^{-K} , coordinate c of the two points differs by $b_c + zp^K + \epsilon$ on the torus, with $z \in \mathbb{Z}$ and $|\epsilon| \leq 1$ (each point lies in the closure of its fine cell). For $z \neq 0$ the absolute value is at least $p^K - |b_c| - 1 \geq |b_c| - 1$, and for $z = 0$ it is at least $|b_c| - 1$. So the toroidal distance is at least $p^{-K} \|(|b| - 1)_+\|_2 \geq p^{-K} \lambda_{\text{jit}}(\Lambda_v)$, and $p^{-K} N^{1/s} = p^{-1/s}$. $\square$

The link to the nets: lattice image and jitter. Part (i) says that P_{sK-1} is, in the words of [18], a lattice image plus jitter. The lattice image of a point is the corner $\hat{n} p^{-K}$ of its fine cell; these corners are all of $p^{-K} \Lambda_v$ on the torus, one global lattice with no slip planes and no shifts of the lattice between neighbouring cells of P_{sK-1} (no *faults* in the sense of [18]); and the jitter moves each point by less than one fine cell in every coordinate (Figure 6(b),(c)). This is the net with one skeleton coordinate of [18], whose skeleton digit is a rank-1 lattice rule in the last cell digits of the other coordinates, and part (ii) is its Euclidean bound [18]. There are two differences. First, the nets of [18] are built for one size $m = sK - 1$ at a time, by a scramble chosen for that m ; here one fixed scramble of a frame with finite places gives the lattice image at every $m \equiv -1 \pmod{s}$ at once, because the skeleton relation comes from the residue theorem and does not depend on K . Second, the bound of [18] is stated for $s \geq 3$; the proof above is self-contained and covers $s = 2$ as well. Compared with the staggered residue sequence, the relation is the same kind of rank-1 rule, now read in the last cell digit of every coordinate: the jitter shrinks from a whole cell to one fine cell, and the constant is no longer capped.

Corollary 37 (Korobov check vectors). *Let $p > 2^s$, $\rho = \lfloor p^{1/s} \rfloor$ and $v = (\rho, \rho^2, \dots, \rho^{s-1}, -1)$. Then $\lambda_{\text{jit}}(\Lambda_v) \geq \rho - 1$, so for every $K \geq 1$*

$$\text{sep}(P_{sK-1}) \geq (\rho - 1) p^{-1/s} > \max\left(1 - 2p^{-1/s}, \frac{\rho - 1}{\rho + 1}\right).$$

In particular $\text{sep}(P_{sK-1}) > 1/3$ for every prime $p > 2^s$ and $> 1/2$ for every prime $p > 3^s$.

Proof. We show that every $0 \neq b \in \Lambda_v$ has a coordinate with $|b_c| \geq \rho$ (as in [18]); then $\|(|b| - 1)_+\|_2 \geq \rho - 1$. Suppose $|b_c| \leq \rho - 1$ for all c . The integer $T = \sum_{c < s-1} \rho^{c+1} b_c - b_{s-1}$ is divisible by p , and $|T| \leq (\rho - 1)(1 + \rho + \dots + \rho^{s-1}) = \rho^s - 1 < p$, since $\rho^s \leq p$ and p is not an s -th power. So $T = 0$. Reading $T = 0$ modulo ρ gives $\rho \mid b_{s-1}$, hence $b_{s-1} = 0$; dividing by ρ and repeating gives $b_0 = \dots = b_{s-2} = 0$, a contradiction. Finally $p^{1/s} < \rho + 1$ gives $(\rho - 1)p^{-1/s} > 1 - 2p^{-1/s}$ and $> (\rho - 1)/(\rho + 1)$; and $\rho \geq 2$ if and only if $p > 2^s$, $\rho \geq 3$ if and only if $p > 3^s$. $\square$

The constant 2 in $1 - 2p^{-1/s}$ is the same in every dimension. At small primes the first form is much stronger: for $s = 4$ and $p = 17$ it is 0.492, while $1 - 2 \cdot 17^{-1/4} = 0.0150$.

Corollary 38 (Quasi-uniformity). *Let $\text{LB} = p^{-1/s} \lambda_{\text{jit}}(\Lambda_v) > 0$. Then $\delta(P_{[N]}) \geq (\text{LB}/p) N^{-1/s}$ for every $N \geq 2$, $h/\delta \leq \sqrt{s} p^2/\text{LB}$, and $\mathcal{R}_v$ is quasi-uniform. A check vector with $\lambda_{\text{jit}}(\Lambda_v) > 0$ exists if and only if $p > 2^s$, and then the Korobov vector of Corollary 37 is one.*

Proof. The first part is Lemma 2 with the level family $\mathcal{M} = s\mathbb{N} - 1$, whose largest gap is s (Remark 3). $\lambda_{\text{jit}}(\Lambda_v) = 0$ means that Λ_v contains a nonzero vector $e \in \{-1, 0, 1\}^s$. If $p < 2^s$, two of the 2^s subset sums $\sum_{c \in A} v_c$ agree modulo p , and their difference is such a vector; $p = 2^s$ is impossible. For $p > 2^s$ the Korobov vector has $\lambda_{\text{jit}} \geq p - 1 \geq 1$. $\square$

For the primes $s \leq p < 2^s$ the bound is empty, and whether residue sequences are quasi-uniform there is not addressed here (Section 11). The smallest primes above 2^s are 5, 11, 17, 37, 67, 131 and 257 for $s = 2, \dots, 8$.

Better check vectors. Theorem 36 holds for every check vector, and the Korobov vector [26, 36] is not the best one in the Euclidean norm. (Sakai and Goda [35] also choose Korobov generating vectors for separation, by lattice basis reduction, for lattice point sets.) Scaling v does not change Λ_v , so every check vector can be written as $v = (x, -1)$ with $x \in (\mathbb{F}_p^*)^{s-1}$, and $\lambda_{\text{jit}}(\Lambda_v)^2$ is an integer computed exactly by enumerating the vectors of Λ_v in a box (any vector with a coordinate larger than B in absolute value has $\lambda_{\text{jit}}^2 \geq B^2$). Table 7 lists the best vectors found, exhaustively over all x where that is feasible. Each entry is a proof of the stated bound for the listed v , by Theorem 36 and the exact value of λ_{jit}^2 ; a value found by a random search is only a lower bound on the best possible one. In dimension two the bound exceeds 1 at $p = 1009$, and in dimension three at $p = 10007$. At $s = 4$, $p = 1009$ the vector of the table improves the value 0.813 of the searched skeleton nets of [18]; the same vector serves there. The best values appear to tend to $\sqrt{\gamma_s}$, the square root of the Hermite constant (1.122, 1.189, 1.231 for $s = 3, 4, 5$); this is the open limit discussed in [18], and it would transfer to residue sequences verbatim.

Remark 39 (Exact separations). The exact separations at the certified sizes are above the bound and approach it as K grows (exact computations, illustration only). For $s = 3$, $p = 11$, $v = (9, 4, -1)$: $\text{sep}(P_2) = 0.7686$ and $\text{sep}(P_5) = 0.6144$, against 0.4496; for $s = 3$, $p = 1009$ and the Korobov vector: $\text{sep}(P_2) = 0.9484$ against 0.8973; for $s = 4$, $p = 257$, $v = (4, 16, 64, -1)$: $\text{sep}(P_3) = 0.7638$ against 0.7493. All 27 cases computed respect the bound.

Remark 40 (Full levels). At the full levels the residue sequence has only the *inclusion bound*: $P_{sK} \subset P_{s(K+1)-1}$ and Theorem 36 give $\text{sep}(P_{sK}) \geq \lambda_{\text{jit}}(\Lambda_v)/p$, smaller by the factor $p^{1/s-1}$. At P_{sK} the geometric digits of every point satisfy $\sum_c v_c r_c = 0$ (Lemma 35 at level $K + 1$), which constrains the position of a point inside its cell but not its position relative to the neighbours. The digit relaxation does not do better: its one-digit form applied to the offset map of $\mathcal{R}_v$ gives exactly $\lambda_{\text{jit}}(\Lambda_v)/p$ in all 13 parameter sets computed ($s = 2$ and $s = 3$, primes up to 101, several places and scales; exact computation). This is a statement about that bound, not an upper bound on the separation. The measured full-level separations do decrease with K , for instance from 0.367 ($m = 2, \dots, 8$) to 0.246 ($m = 10$) for $s = 2$, $p = 5$, and from 0.444 ($m = 3$) to 0.172 ($m = 6$) for $s = 3$, $p = 11$ (evidence, not a claim). A self-similar scramble carries only one level-independent exact relation of this kind (Proposition 54), so it cannot have both the skeleton relation of $\mathcal{R}_v$ and the staggered relation of $\mathcal{R}_v^*$; Section 7 makes this precise, and Section 6 certifies a sparser family of full levels with constants close to 1.

5.4. Comparison. The two residue constructions certify different level families: $\mathcal{R}_v^*$ every full level P_{sK} , $\mathcal{R}_v$ every prefix P_{sK-1} . For the number of points that matters in practice, every N , Lemma 2 puts them on the same footing: both families have largest gap s , so $\delta(P_{[N]}) N^{1/s} \geq \text{LB}/p$ in both cases. Table 8 compares them; in this all- N measure the residue sequence has the larger certified constant in every case listed. At every full level, on the other hand, only the window

TABLE 7. Certified bounds $\text{sep}(P_{sK-1}) \geq p^{-1/s} \lambda_{\text{jit}}(\Lambda_v)$ for every $K \geq 1$ (Theorem 36), truncated to three digits, for the check vectors v listed and, in the last column, for the Korobov vector $(\rho, \dots, \rho^{s-1}, -1)$, $\rho = \lfloor p^{1/s} \rfloor$ (Corollary 37; there $\lambda_{\text{jit}} = \rho - 1$ in every row). λ_{jit}^2 is exact. Search: E = exhaustive over all check vectors $(x, -1)$; R = random search over $3 \cdot 10^6$ vectors x , so the value is a lower bound on the best possible one. Computed with an exact enumeration program, each run under one minute (Appendix C).

s	p	best v found	λ_{jit}^2	bound	search	Korobov
2	11	(3, -1)	4	.603	E	.603
	17	(4, -1)	9	.727	E	.727
	37	(6, -1)	25	.821	E	.821
	101	(30, -1)	85	.917	E	.895
	1009	(122, -1)	1060	1.024	E	.944
3	11	(9, 4, -1)	1	.449	E	.449
	17	(6, 2, -1)	1	.388	E	.388
	37	(9, 3, -1)	4	.600	E	.600
	101	(35, 13, -1)	13	.774	E	.644
	1009	(105, 11, -1)	89	.940	E	.897
	10007	(7775, 9087, -1)	498	1.035	R	.928
4	17	(9, 15, 4, -1)	1	.492	E	.492
	37	(14, 4, 2, -1)	1	.405	E	.405
	101	(27, 9, 3, -1)	4	.630	E	.630
	1009	(443, 201, 758, -1)	25	.887	R	.709
5	37	(16, 8, 4, 2, -1)	1	.485	E	.485
	101	(2, 4, 8, 16, -1)	1	.397	R	.397
	1009	(560, 313, 92, 858, -1)	9	.752	R	.501

constructions of Section 8 have constants tending to 1, from large primes on. Section 10 (Table 13) measures the separation of every prefix up to 2^{23} points in dimension three.

6. BLOCK-PERIODIC RESIDUE SEQUENCES

The residue sequences of Section 5 carry one exact relation per level: the staggered residue sequence designs one geometric digit at every full level, the residue sequence one skeleton digit at every prefix P_{sK-1} . The nets of [18] design all s geometric digits of one prefix at once, the whole geometric layer together with its responses at carry depths up to $s - 2$, and that is how they reach separations $1 - O(1/q)$ at the full levels. A frame scramble cannot do this at every full level by exact relations: exact relations of bounded depth can design all s geometric digits on at most a fraction $1/s$ of the levels (Section 7). It can do it on exactly that fraction. The idea is to spread the s relations over s consecutive digits: every coordinate reads its digits in blocks of s , with s different local multipliers, and the residue theorem then installs the complete design of the nets at every s -th full level, $m \in s^2\mathbb{N}$. In dimensions two and three this gives $1 - 2/p$ for every prime $p \geq 3$ resp. $p \geq 5$, with a short proof.

6.1. The Construction. A *design* in the sense of [18] prescribes how the geometric digits depend on the last cell digits: $F_n[i][c]$ is the change of the geometric digit of coordinate i when the cell digit of coordinate c at carry depth n (the finest cell digit is at carry depth 0) increases by one. We use designs $F = (F_0, \dots, F_{s-2})$ of integer $s \times s$ matrices, read modulo p , with partial

TABLE 8. Certified constants for every K at the level families stated, and the resulting bound for every N , $\delta(P_{[N]})N^{1/s} \geq \text{LB}/p$ (Lemma 2), in units of 10^{-3} ; all values truncated. $\mathcal{R}_v^*$: dyadic weights (Corollary 29). $\mathcal{R}_v$: Korobov vector (Corollary 37) and the best vector of Table 7.

s	p	$\text{sep}(P_m) \geq$			all N : $\text{LB}/p, \times 10^{-3}$	
		$\mathcal{R}_v^*$	$\mathcal{R}_v, m \equiv -1$		$\mathcal{R}_v^*$	$\mathcal{R}_v$
		$m \equiv 0$	Korobov	best v		best v
3	37	.216	.600	.600	5.84	16.22
	101	.237	.644	.774	2.35	7.66
	1009	.248	.897	.940	0.24	0.93
4	37	.081	.405	.405	2.19	10.95
	101	.108	.630	.630	1.07	6.24
	1009	.123	.709	.887	0.12	0.87
5	37	.027	.485	.485	0.73	13.12
	101	.049	.397	.397	0.49	3.93
	1009	.061	.501	.752	0.06	0.74

sums $M^{(j)} = F_0 + \dots + F_j$; a carry of length l in coordinate c changes the geometric digits by the column c of $M^{(\min(l, s-1)-1)}$. For places a_c and row constants $v \in (\mathbb{F}_p^*)^s$ put $\tau_{ic} = 1/(a_i - a_c)$ for $i \neq c$. The design is *reachable* if for every column c and every $n \leq s-2$

$$F_n[i][c] = v_i^{-1} \tau_{ic} \gamma_{c,n}(\tau_{ic}) \quad (i \neq c)$$

with a polynomial $\gamma_{c,n} \in \mathbb{F}_p[X]$ of exact degree n ; the diagonal entries are free. This is the reachability condition of [18], with the row constants v_i^{-1} and stated for the individual F_n instead of the partial sums, which is equivalent. Write $u_i = 1/(z - a_i)$.

Definition 41 (Block-periodic residue sequence). Let $p \geq s \geq 2$ be a prime, $a_0, \dots, a_{s-1} \in \mathbb{F}_p$ distinct places, $\theta \in \mathbb{F}_p^*$, $v \in (\mathbb{F}_p^*)^s$ row constants, $F = (F_0, \dots, F_{s-2})$ a reachable design, and $\ell \geq s$ the *block period*; if $\ell > s$, let also $v' \in (\mathbb{F}_p^*)^s$ be a second check vector. Put $\Omega = w^\ell/\theta$. At each place a_c define ℓ *local multipliers* $\varphi_{c,0}, \dots, \varphi_{c,\ell-1}$:

- (a) the *design multipliers* $\varphi_{c,\ell-1-n}$, $0 \leq n \leq s-2$: the rational functions with

$$u_i = -v_i \sum_{n=0}^{s-2} F_n[i][c] \varphi_{c,\ell-1-n} \quad \text{for every } i \neq c;$$

- (b) if $\ell > s$, the *skeleton multipliers* $\varphi_{c,j} = w^{\ell-1-j}/v'_c$, $1 \leq j \leq \ell-s$;

- (c) the *own multiplier* $\varphi_{c,0} = v_c^{-1} \Omega u_c + \Omega \sum_{n=0}^{s-2} F_n[c][c] \varphi_{c,\ell-1-n}$.

The *block-periodic residue sequence* is the digital sequence over $\mathbb{F}_p$ with the digits

$$y_{c,\ell n+j}(V) = \text{Res}_{a_c}(V \varphi_{c,j} \Omega^{-(n+1)} dz), \quad n \geq 0, 0 \leq j < \ell.$$

So the digits of each coordinate come in blocks of ℓ , and multiplying the index by w^ℓ shifts every coordinate by one block; for $\ell = 1$ this is a self-similar scramble. The generator matrices are again one coefficient per entry, $C_c[\ell n+j][i] = [(z - a_c)^{\ell(n+1)-1}] z^i \varphi_{c,j} (z - a_c)^{\ell(n+1)} \Omega^{-n-1}$. The system (a) has a unique solution, and the multipliers have the orders of vanishing needed for $t = 0$; both are shown in the proof below.

Theorem 42 (Block-periodic residue sequences). *Let $\ell = s$ in Definition 41.*

- (i) The sequence is a digital $(0, s)$ -sequence over $\mathbb{F}_p$.
- (ii) For every $K \geq 1$, every coordinate i and every V with $\deg V < s^2 K$,

$$y_{i,sK}(V) = \sum_c \sum_{n=0}^{s-2} F_n[i][c] y_{c,sK-1-n}(V) :$$

at every full level $P_{s^2 K}$ the geometric digits follow the design exactly.

- (iii) $\text{sep}(P_{s^2 K}) \geq \text{LB}(F)$ for every $K \geq 1$, where $\text{LB}(F)$ is the one-digit relaxation of Lemma 23 ($j = 1$) for the carry responses $D(l) = M^{(\min(l, s-1)-1)}$; it is the one-digit relaxation of [18] with a jitter of one unit in every coordinate. The level family is $\mathcal{M} = s^2 \mathbb{N}$.

In particular, for every $K \geq 1$:

- (a) $s = 2$, places $(0, 1)$, $v = (1, 1)$, $F_0 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$: $\text{sep}(P_{4K}) \geq 1 - 2/p$ for every prime $p \geq 3$;
- (b) $s = 3$, places $(0, 2, 1)$, $v = (\frac{1}{2}, \frac{1}{2}, -1)$, $(F_0, F_1) = (M, J)$ with

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

the layer of the three-dimensional nets of [18]: $\text{sep}(P_{9K}) \geq 1 - 2/p$ for every prime $p \geq 5$;

- (c) $s \geq 4$, the design U_s^* of [18] moved to the places $0, 1, \frac{1}{2}, \dots, \frac{1}{s-1}$, with $v = (1, 1, 2, \dots, s-1)$: $\text{sep}(P_{s^2 K}) \geq 1 - (a_s^* + 1)/p$ for every prime $p \geq 5a_s^* + 4$, where a_s^* is the constant of [18] ($a_4^* = 5$, $a_5^* = 16$, $a_6^* = 43$, $a_7^* = 170$). For $s = 4$ at every prime $7 \leq p \leq 109$ and for $s = 5$ at every prime $19 \leq p \leq 109$ the value $\text{LB}(F) = 1 - (a_s^* + 1)/p$ holds as well (computer-assisted). Hence $\text{sep}(P_{16K}) \geq 1 - 6/p$ for every prime $p \geq 7$ and $\text{sep}(P_{25K}) \geq 1 - 17/p$ for every prime $p \geq 19$.
- (d) The diagonal entries of F are free: (i)–(iii) hold for every diagonal. Keep the off-diagonal entries of (c), put $F_0[c][c] = -\delta_c$ and $F_n[c][c] = 0$ for $n \geq 1$, with $\delta = (3, 3, 3, 3), (7, \dots, 7), (3, 12, 13, 14, 13, 13), (41, 44, 59, 57, 56, 6, 32)$ for $s = 4, 5, 6, 7$ (in the order of the places). Then $\text{sep}(P_{s^2 K})$ is at least $1 - 4/p, 1 - 8/p, 1 - 15/p, 1 - 60/p$ for every prime $p \geq 11, 23, 37, 191$, respectively, and $\text{sep}(P_{16K}) \geq \sqrt{3}/7$ at $p = 7$; also $\text{LB}(F) > 0$ for $s = 5$ at $p = 11, 13, 17, 19$, for $s = 6$ at every prime $17 \leq p \leq 31$, and for $s = 7$ at $p = 17, 19, 23$ and every prime $31 \leq p \leq 181$ (computer-assisted).

Proof. (i) Fix c and write $\vartheta_n = \varphi_{c,s-1-n}$ for the design multipliers. At a_c , $u_i = -\sum_{k \geq 0} \tau_{ic}^{k+1} (z - a_c)^k$, so $[(z - a_c)^k] u_i = -\tau_{ic}^{k+1}$. By reachability, (a) reads $u_i = -\sum_n \tau_{ic} \gamma_{c,n}(\tau_{ic}) \vartheta_n$, and its matrix $(-\tau_{ic} \gamma_{c,n}(\tau_{ic}))_{i \neq c, n \leq s-2}$ is invertible: the τ_{ic} are nonzero and distinct, and the $\gamma_{c,n}$ have exact degrees $0, \dots, s-2$, so the matrix is a diagonal matrix times a triangular change of basis times a Vandermonde matrix. So (a) has a unique solution, a combination of the u_i with constant coefficients. Comparing the coefficients of $(z - a_c)^k$, $k \leq s-2$, gives $\tau^k = \sum_n \gamma_{c,n}(\tau) [(z - a_c)^k] \vartheta_n$ at the $s-1$ distinct nodes $\tau = \tau_{ic}$, hence as an identity of polynomials of degree at most $s-2$. Expanding τ^k in the triangular basis $(\gamma_{c,n})$ shows $[(z - a_c)^k] \vartheta_n = 0$ for $k < n$ and $[(z - a_c)^n] \vartheta_n \neq 0$: ϑ_n vanishes to order exactly n at a_c , i.e. $\varphi_{c,j}$ to order exactly $s-1-j$. The own multiplier vanishes to order exactly $s-1$: $v_c^{-1} \Omega u_c = v_c^{-1} w_c w^{s-1} / \theta$ does, and the other terms vanish to order at least s . As Ω vanishes to order exactly s at a_c , the differential $\varphi_{c,j} \Omega^{-n-1} dz$ has a pole of order exactly $s(n+1) - (s-1-j) = sn + j + 1$ there. So digit $sn + j$ is the residue of V against a polar differential of exact order $sn + j + 1$, and Lemma 21(a) and Lemma 1 give $t = 0$.

(ii) By (c) with $\ell = s$, $y_{i,sK}(V) = v_i^{-1} \text{Res}_{a_i}(V u_i \Omega^{-K} dz) + \sum_n F_n[i][i] y_{i,s(K-1)+s-1-n}(V)$. The rational function $V u_i \Omega^{-K}$ has its finite poles at the places, and degree at most $(s^2 K - 1) - 1 - s^2 K = -2$; by Lemma 21(c) its residues add up to 0. At a_c , $c \neq i$, (a) replaces u_i by $-v_i \sum_n F_n[i][c] \varphi_{c,s-1-n}$, so $\text{Res}_{a_c}(V u_i \Omega^{-K} dz) = -v_i \sum_n F_n[i][c] y_{c,s(K-1)+s-1-n}(V)$. Hence

$v_i^{-1} \text{Res}_{a_i}(Vu_i\Omega^{-K}dz) = \sum_{c \neq i} \sum_n F_n[i][c] y_{c,sK-1-n}(V)$, which together with the own terms is the claim.

(iii) At the full level P_{s^2K} each coordinate has sK cell digits, and its geometric digit is $y_{\cdot,sK}$. By (ii) it depends only on the cell digits at carry depths $0, \dots, s-2$, through F ; adding 1 to the l finest cell digits of coordinate c changes it by column c of $M^{(\min(l,s-1)-1)}$, at every level and for every carry length, the wrap included. These responses do not depend on K , so Lemma 23 with $j = 1$ gives $\text{sep}(P_{s^2K}) \geq \text{LB}(F)$ for every K (as $p^{sK} \geq 4$). In $\text{LB}(F)$ a moving coordinate whose change σ_i is backward, $e_i\sigma_i \leq 0$ with $|\sigma_i| < p$, contributes $f_1(e_i, \sigma_i) = c_{|\sigma_i|+1}$, $c_j := 1 - j/p$ (Remark 24); every other coordinate contributes at least 0.

(a) F_1 is absent, so the carry length does not matter, and $\sigma = e_0F_0[\cdot][0] + e_1F_0[\cdot][1]$. The axis steps give $\sigma = \mp(1, 1)$ and $\sigma = \pm(1, -1)$: the moving coordinate is backward with $|\sigma| = 1$, a term $c_2 = 1 - 2/p$. The diagonal steps give $\sigma = \pm(0, -2)$ and $\pm(-2, 0)$, the terms $(c_1^2 + c_3^2)^{1/2} \geq c_2$. So $\text{LB}(F) = 1 - 2/p$ for every prime $p \geq 3$. Reachability needs only nonzero crosses for $s = 2$.

(b) Reachability, by hand over $\mathbb{Q}$: in column $c = 0, 1, 2$ the values $v_iM[i][c]/\tau_{ic}$ ($i \neq c$) are $1, 1; 1, 1; -\frac{1}{2}, -\frac{1}{2}$, so $\gamma_{c,0}$ is constant; the values $v_iJ[i][c]/\tau_{ic}$ are $(-1, 0), (0, -1), (\frac{1}{2}, 0)$ at two distinct nodes, so $\gamma_{c,1}$ has degree exactly 1. All numbers are $0, \pm 1, \pm 2, \pm \frac{1}{2}$, so this holds over $\mathbb{F}_p$ for every prime $p \geq 3$. With $\omega_d = 1$ if the carry length in coordinate d is at least 2 and $\omega_d = 0$ otherwise, the changes are $\sigma_i = -e_i - e_{i+1} + (1 - \omega_{i+2})e_{i+2}$ (indices modulo 3), exactly as for the nets of [18]. The sign analysis there, which uses only this formula, $|\sigma_i| \leq 3 < p$ and at least two cell digits per coordinate, shows: an axis step has $\sigma_i = -e_i$; a step with two moving axes has two backward coordinates with $|\sigma| \leq 1$ and $|\sigma| \leq 2$; a step with three moving axes has either a backward coordinate with $|\sigma| = 3$ and another with $|\sigma| \leq 1$, or a forward coordinate and two backward ones with $|\sigma| \leq 1$ and $|\sigma| \leq 2$, or three backward coordinates with $|\sigma| \leq 2$. With the jitter of one unit also on the axis steps this gives

$$\text{LB}(F) = \min(c_2, (c_2^2 + c_3^2)^{1/2}, (c_2^2 + c_4^2)^{1/2}, \sqrt{3}c_3) = \min(c_2, \sqrt{3}c_3) = c_2 = 1 - \frac{2}{p} \quad (p \geq 5),$$

since $\sqrt{3}(1 - 3/p) \geq 1 - 2/p$ exactly when $p \geq (3\sqrt{3} - 2)/(\sqrt{3} - 1) \approx 4.37$.

(c) *Reachability*. By [18], U_s^* is reachable at the places $\hat{a}_c \in \{\infty, 0, 1, \dots, s-2\}$ with constant row scalars: $M^{(j)}[c][d] = \tilde{w}_{cd} \tilde{g}_{d,j}(\tilde{y}_{cd})$ ($c \neq d, j \leq s-2$), where $\tilde{g}_{d,j}$ has degree j , coefficients in $\mathbb{Z}[1/(s-2)!]$ and a leading coefficient whose prime factors are at most $s-2$, and $\tilde{w}_{cd} = \tilde{y}_{cd} = 1/(\hat{a}_c - \hat{a}_d)$ for finite $\hat{a}_c, \hat{a}_d$, $\tilde{w}_{\infty d} = 1, \tilde{y}_{\infty d} = 0, \tilde{w}_{c\infty} = 1, \tilde{y}_{c\infty} = \hat{a}_c$. Move the places by $x \mapsto 1/(x+1)$, so $a_c = 1/(\hat{a}_c + 1)$ ($a_c = 0$ for $\hat{a}_c = \infty$), and let $\tau_{cd} = 1/(a_c - a_d)$. For finite $\hat{a}_c, \hat{a}_d$, $\tau_{cd} = -(\hat{a}_c + 1)(\hat{a}_d + 1)\tilde{y}_{cd}$, and $(\hat{a}_c + 1)\tilde{y}_{cd} = 1 + (\hat{a}_d + 1)\tilde{y}_{cd}$; hence

$$\tilde{y}_{cd} = A_d(\tau_{cd}) := -\frac{\tau_{cd}}{(\hat{a}_d + 1)^2} - \frac{1}{\hat{a}_d + 1}, \quad \tilde{w}_{cd} = \varrho_c \tau_{cd} \varsigma_d, \quad \varrho_c = -\frac{1}{\hat{a}_c + 1}, \quad \varsigma_d = \frac{1}{\hat{a}_d + 1},$$

an affine function of τ_{cd} whose coefficients depend on the column only. For $\hat{a}_c = \infty$: $\tau_{\infty d} = -(\hat{a}_d + 1)$, $A_d(\tau_{\infty d}) = 0 = \tilde{y}_{\infty d}$ and $\tilde{w}_{\infty d} = 1 = \varrho_{\infty} \tau_{\infty d} \varsigma_d$ with $\varrho_{\infty} = -1$. For $\hat{a}_d = \infty$: $\tau_{c\infty} = \hat{a}_c + 1$, so $\tilde{y}_{c\infty} = A_{\infty}(\tau_{c\infty})$ with $A_{\infty}(X) = X - 1$, and $\tilde{w}_{c\infty} = \varrho_c \tau_{c\infty} \varsigma_{\infty}$ with $\varsigma_{\infty} = -1$. Therefore $M^{(j)}[c][d] = \varrho_c \tau_{cd} \varsigma_d \tilde{g}_{d,j}(A_d(\tau_{cd}))$, a polynomial in τ_{cd} of exact degree j times τ_{cd} , for every prime $p \geq s$ (then $\hat{a}_d + 1 \in \{1, \dots, s-1\}$ and the leading coefficients are units, and the places are distinct). Differences of consecutive partial sums give the individual F_n , so the design is reachable with $v_c^{-1} = -\varrho_c$ after a change of sign of all γ , i.e. $v = (1, 1, 2, \dots, s-1)$ in the order $\hat{a} = (\infty, 0, \dots, s-2)$.

The bound. U_s^* has the diagonal $F_0[c][c] = -\alpha_c$ and zero diagonal at the carry depths $n \geq 1$, and it is diagonally dominant: $\alpha_c \geq \sum_{d \neq c} \max_j |M^{(j)}[c][d]|$, with $a_s^* = \max_c \alpha_c$ [18]. An axis step along c has $\sigma_c = -e_c \alpha_c$, a term $1 - (\alpha_c + 1)/p \geq 1 - (a_s^* + 1)/p$. On a step with at least two moving axes every moving coordinate is backward with $|\sigma_i| \leq 2a_s^* < p$, so the step has at least two terms $c_{2a_s^*+1}$, and $\sqrt{2}(p - 2a_s^* - 1) \geq p - a_s^* - 1$ for $p \geq (3 + \sqrt{2})a_s^* + 1$, in particular for

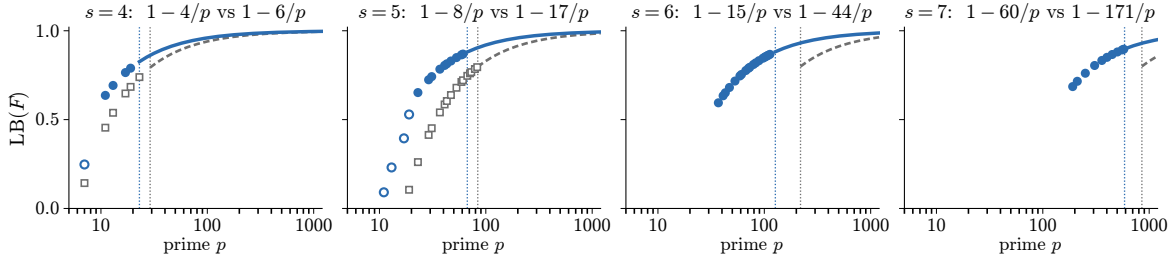


FIGURE 7. $\text{LB}(F)$ of Theorem 42 against p . Grey: U_s^* (dashed: $1 - (a_s^* + 1)/p$, written proof for $p \geq 5a_s^* + 4$; squares: exact values, c.a.). Blue, all c.a.: the free diagonal of (d) (solid: $1 - (A + 1)/p$ past the threshold of Lemma 43; dots: exact values below it; circles: the quoted values at $p = 7, 11 \leq p \leq 19$). Dotted: the thresholds. In Lean for $s = 4, 5, 6$ (from $p = 11, 23, 125$), not for $s = 7$.

$p \geq 5a_s^* + 4$. This is the diagonal dominance argument of [18] with a jitter of one unit on the axis steps. So $\text{LB}(F) \geq 1 - (a_s^* + 1)/p$ for $p \geq (3 + \sqrt{2})a_s^* + 1$ (for $s = 6, 7$ from $p = 191, 757$ on), with equality when a row with $\alpha_c = a_s^*$ has the other entries of its column of F_0 in $\{-1, 0, 1\}$, since its axis step then attains the bound. The coordinate of the place 0 (the place ∞ of [18]) has such a column for every s : at carry depth 0 its column is a multiple of $(\tilde{w}_{c\infty})_c = (1, \dots, 1)$, and U_s^* takes $(1, \dots, 1)$; for $s \leq 10$ it has $\alpha_c = a_s^*$ (exact computation). As the entries of F_0 off the diagonal are nonzero integers, $\alpha_c \geq s - 1$, so $p \geq 5a_s^* + 4$ implies $p \geq s$.

Small primes. $\text{LB}(F)$ is a minimum over finitely many configurations (steps, and carry lengths capped at $s - 1$), and the reachability above holds for every prime $p \geq s$. Its exact value at every prime $7 \leq p \leq 109$ ($s = 4$) and $19 \leq p \leq 109$ ($s = 5$) is $1 - (a_s^* + 1)/p$; with $5a_4^* + 4 = 29$ and $5a_5^* + 4 = 84$ this covers every prime $p \geq 7$ resp. $p \geq 19$ (only the lower bound needs the computation). Part (d) is proved after Lemma 43. $\square$

The free diagonal. The diagonal of U_s^* is chosen for diagonal dominance, which the nets need: on every step every moving coordinate is backward. The sequence never uses the diagonal: reachability and the system (a) involve only the entries $F_n[i][c]$, $i \neq c$, and in the own multiplier (c) the diagonal terms carry the factor Ω . But $\text{LB}(F)$ is set by the worst step, and the axis step along c pays $\alpha_c + 1$. A smaller diagonal softens this step, as long as every other step keeps one short backward coordinate or two backward ones. Figure 7 shows the gain. Here changes are computed in the integers, $\sigma = \sum_c e_c M^{(\min(l_c, s-1)-1)}[\cdot][c]$, and a moving coordinate i is backward if $e_i \sigma_i \leq 0$.

Lemma 43 (Backward coordinates). *Let F be a design with partial sums $M^{(j)}$, let $A \geq 0$ be an integer, and let $S = \max_i \sum_c \max_j |M^{(j)}[i][c]|$. Suppose that every step e , with every choice of carry lengths, has a backward moving coordinate with $|\sigma_i| \leq A$ or two backward moving coordinates. Then $\text{LB}(F) \geq 1 - (A + 1)/p$ for every prime $p > S$ with $(p - A - 1)^2 \leq 2(p - S - 1)^2$.*

Proof. For $p > S$ every change has $|\sigma_i| \leq S < p$, so a backward coordinate contributes $c_{|\sigma_i|+1}$ (proof of Theorem 42(iii)). The term of the step is at least c_{A+1} in the first case and at least $\sqrt{2}c_{S+1} \geq c_{A+1}$ in the second. $\square$

The hypothesis does not depend on p and is a finite check. Diagonal dominance is the case in which every moving coordinate is backward; for U_s^* ($A = a_s^*$, $S \leq 2a_s^*$) the lemma gives the range $p \geq (3 + \sqrt{2})a_s^* + 1$ above.

TABLE 9. The block-periodic residue sequences of Theorem 42 ($\mathcal{M} = s^2\mathbb{N}$). Places and row constants: $(0, 1)$, $(1, 1)$ for $s = 2$; $(0, 2, 1)$, $(\frac{1}{2}, \frac{1}{2}, -1)$ for $s = 3$; $(0, 1, \frac{1}{2}, \dots, \frac{1}{s-1})$, $(1, 1, 2, \dots, s-1)$ for $s \geq 4$. “ U_s^* , δ ”: U_s^* off the diagonal, $F_0[c][c] = -\delta_c$. “proof”: written proof; “c.a.”: computer-assisted (exact $\text{LB}(F)$, and for (d) Lemma 43); each for every prime in the range; in parentheses, further primes with $\text{LB}(F) > 0$.

s	design	$\text{LB}(F)$	proof	c.a.
2	$F_0 = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$	$1 - 2/p$	$p \geq 3$	–
3	(M, J) , Thm. 42(b)	$1 - 2/p$	$p \geq 5$	–
4	U_4^* (above)	$1 - 6/p$	$p \geq 29$	$7 \leq p \leq 109$
5	U_5^*	$1 - 17/p$	$p \geq 84$	$19 \leq p \leq 109$
≥ 4	U_s^*	$1 - (a_s^* + 1)/p$	$p \geq 5a_s^* + 4$	–
4	U_4^* , $\delta = (3, 3, 3, 3)$	$1 - 4/p$	–	$p \geq 11$ (7)
5	U_5^* , $\delta = (7, 7, 7, 7, 7)$	$1 - 8/p$	–	$p \geq 23$ (11–19)
6	U_6^* , $\delta = (3, 12, 13, 14, 13, 13)$	$1 - 15/p$	–	$p \geq 37$ (17–31)
7	U_7^* , $\delta = (41, 44, 59, 57, 56, 6, 32)$	$1 - 60/p$	–	$p \geq 191$ (17–23, 31–181)

Proof of Theorem 42(d). Reachability is that of (c). The hypothesis of Lemma 43 holds with $A = 3, 7, 14, 59$ and $S = 8, 23, 46, 211$ (exhaustive check, computer-assisted), which gives $\text{LB}(F) \geq 1 - (A + 1)/p$ for every prime $p \geq 23, 67, 127, 587$. Below these primes $\text{LB}(F)$ was evaluated exactly at every prime of the stated ranges (computer-assisted; for $s = 5$ it is $1/11, 3/13, 3\sqrt{5}/17, \sqrt{101}/19$ at $p = 11, \dots, 19$), and Theorem 42(iii) applies. For $s = 4, 5$ the bound is attained by the axis step at the place 0 (its column of F_0 is $(1, \dots, 1)$ off the diagonal, and $\delta_0 = A$), for $s = 6$ by the axis step at the place $\frac{1}{3}$ with carry length 4. $\square$

How far can the diagonal go? With the off-diagonal entries of U_s^* fixed, the least A in Lemma 43 gives $\lim_{p \rightarrow \infty} p(1 - \text{LB}(F)) = A + 1$ (a step whose only backward coordinate has $|\sigma_i| = A$ has the term $1 - (A + 1)/p + O(p^{-2})$). An axis step forces $0 \leq \delta_c \leq A$, and an exhaustive search over $\delta \in [0, A]^s$ finds no diagonal with $A \leq 2, 6, 13$ for $s = 4, 5, 6$ (computer-assisted): in this sense 4, 8, 15 are optimal. For $s = 7$, 60 is the best found, against $a_7^* + 1 = 171$.

For $s = 4$ the design of Theorem 42(c) is, in the order of the places $0, 1, \frac{1}{2}, \frac{1}{3}$ and with $v = (1, 1, 2, 3)$,

$$F_0 = \begin{pmatrix} -5 & 2 & 1 & 2 \\ 1 & -3 & -1 & -1 \\ 1 & 2 & -5 & -2 \\ 1 & 1 & 1 & -3 \end{pmatrix}, \quad F_1 = \begin{pmatrix} 0 & -3 & -1 & -1 \\ -2 & 0 & 2 & 1 \\ -1 & -1 & 0 & 3 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad F_2 = \begin{pmatrix} 0 & 2 & 0 & -1 \\ 2 & 0 & -2 & 0 \\ 0 & -1 & 0 & -2 \\ -1 & 0 & -1 & 0 \end{pmatrix};$$

the largest diagonal entry is $a_4^* = 5$, and the design of (d) replaces the diagonal of F_0 by -3 . Table 9 collects the data. Figure 8 shows the case $s = 2, p = 7$ inside and outside the family.

Remark 44 (Exact separations and the levels in between). Exact values (illustration only) are close to the certified ones: for $s = 2$, $\text{sep}(P_4) = 0.5730$, $\text{sep}(P_8) = \text{sep}(P_{12}) = 0.3862$ and $\text{sep}(P_{16}) = 0.3610$ at $p = 3$ (bound $1/3$); 0.6237 at $m = 4, 8$ for $p = 5$ (bound 0.6); $0.8383, 0.8604, 0.8909, 0.9016, 0.9177$ at $m = 4$ for $p = 11, 13, 17, 19, 23$; for $s = 3$, $\text{sep}(P_9) = 0.6211$ at $p = 5$ ($\theta = 1$; bound 0.6) and 0.7378 at $p = 7$ (bound 0.7143); at $p = 3$, where the bound of (b) is 0, $\text{sep}(P_9) = 0.4381$. Outside the family the separation is not controlled: for $s = 2, p = 5$ the levels $m = 2, 3, 5, 6, 7, 9, 10$ have $0.368, 0.366, 0.276, 0.159, 0.354, 0.092, 0.159$ (evidence, not a claim).

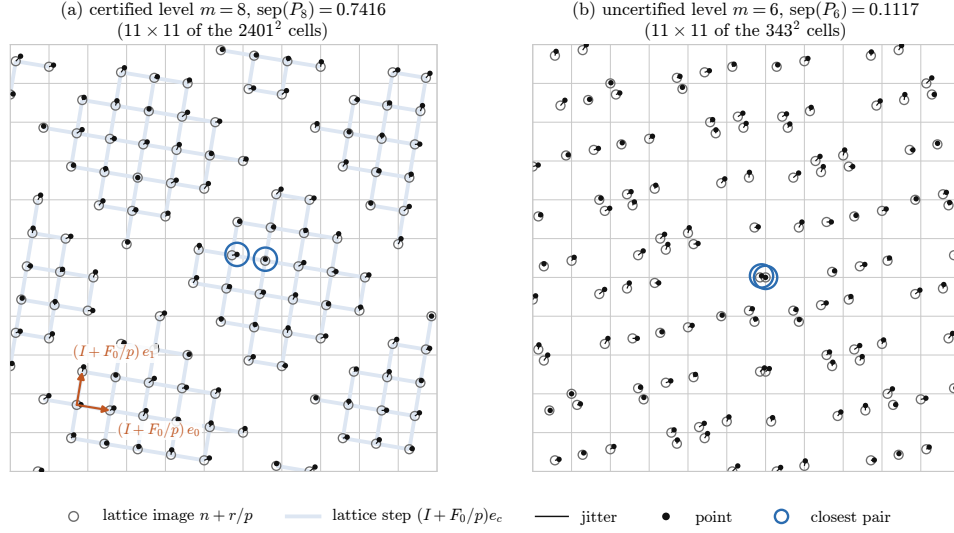


FIGURE 8. The block-periodic residue sequence of Theorem 42(a), $s = 2$, $p = 7$, places $(0, 1)$, $\theta = 1$ (exact points). (a) The full level $m = 8$ (2401×2401 cells), 11 $\times$ 11 cells around the closest pair: each point (dot) lies within one unit of the last digit of its lattice image $n + r/p$ (open circle); where no geometric digit wraps, neighbouring lattice images differ by a column of $I + F_0/p$ (light segments): patches of $\mathbb{Z}^2$ rotated by $\arctan(1/6)$, scaled by $\sqrt{37}/7 \approx 0.87$, separated by slip planes. Exact $\text{sep}(P_8) = 0.7416$ (0.7613 at $m = 4$), certified bound $1 - 2/7 = 0.7143$. (b) The full level $m = 6$, which is not in the family $4\mathbb{N}$: its geometric digits are not designed, and the closest pair is only 0.1117 cell units apart (exact).

All N . The family $s^2\mathbb{N}$ has largest gap s^2 , so Lemma 2 gives $\delta(P_{[N]})N^{1/s} \geq \text{LB}(F)p^{-s}$ for every $N \geq 2$ and the mesh ratio $h/\delta \leq \sqrt{s}p^{s+1}/\text{LB}(F)$: these sequences are quasi-uniform, the strongest of our constructions at their certified sizes, but for all N weaker than the residue sequences of Section 5, whose bound LB/p is larger whenever $p > 2^s$ (for $s = 2$, $p = 5$: 0.024 against 0.089).

The lost $1/p$. The nets of [18] with the layer (M, J) reach $1 - 1/q$ at every full level for $q \geq 8$. The difference is the axis step: in the nets the deeper digits of a coordinate do not depend on its own cell, so an axis step has no jitter in the moving coordinate; here it has, and $1 - 1/p$ becomes $1 - 2/p$. Whether free data in the scramble can restore $1 - 1/p$ is open.

6.2. Two Level Families from One Scramble. With a block period $\ell > s$ the scramble has $\ell - s$ local multipliers left over. Giving them to a second check vector adds skeleton relations of the residue sequence at most levels in between.

Theorem 45 (Two level families from one scramble). *Let $\ell > s$ in Definition 41, with the second check vector v' . Then:*

- (i) *the sequence is a digital $(0, s)$ -sequence over $\mathbb{F}_p$;*
- (ii) *for every $K \geq 1$ and $\deg V < s\ell K$, $y_{i,\ell K}(V) = \sum_c \sum_{n=0}^{s-2} F_n[i][c] y_{c,\ell K-1-n}(V)$, and $\text{sep}(P_{s\ell K}) \geq \text{LB}(F)$;*
- (iii) *for every $T \equiv 1, \dots, \ell - s \pmod{\ell}$ and $\deg V \leq s(T + 1) - 2$, $\sum_c v'_c y_{c,T}(V) = 0$, and $\text{sep}(P_{s(T+1)-1}) \geq p^{-1/s} \lambda_{\text{jit}}(\Lambda_{v'})$.*

So one scramble is certified on the design levels $m \in s\ell\mathbb{N}$, with the constants of Theorem 42, and on the skeleton levels $m = s(T+1) - 1$, $T \equiv 1, \dots, \ell - s \pmod{\ell}$, with those of Theorem 36: a fraction $1/\ell$ of the full levels and a fraction $(\ell - s)/\ell$ of the levels $m \equiv -1 \pmod{s}$. For instance $s = 2$, $\ell = 4$: design levels $8\mathbb{N}$, skeleton levels $3, 5, 11, 13, 19, 21, \dots$; $s = 2$, $\ell = 3$: $6\mathbb{N}$ and $3, 9, 15, \dots$; $s = 3$, $\ell = 4$: $12\mathbb{N}$ and $5, 17, 29, \dots$.

Proof. (i) As in Theorem 42(i), with Ω of order ℓ : the design multipliers vanish to the orders $0, \dots, s-2$, the skeleton multipliers $w^{\ell-1-j}/v'_c$ to the orders $\ell-1-j \in \{s-1, \dots, \ell-2\}$, and the own multiplier to the order $\ell-1$. So $\varphi_{c,j}$ vanishes to order exactly $\ell-1-j$ for every j , digit $\ell n + j$ is the residue against a polar differential of exact order $\ell n + j + 1$, and Lemma 1 applies. (ii) The proof of Theorem 42(ii),(iii) is unchanged: it uses only (a), (c) and $\deg(Vu_i\Omega^{-K}) \leq -2$, which holds for $\deg V < s\ell K$; at $P_{s\ell K}$ the geometric digit is digit ℓK . (iii) Write $T = \ell n + j$ with $1 \leq j \leq \ell - s$. Then $v'_c y_{c,T}(V) = \text{Res}_{ac}(Vw^{\ell-1-j}\Omega^{-n-1}dz) = \theta^{n+1} \text{Res}_{ac}(Vw^{-T-1}dz)$, and by Lemma 21(c) these add up to 0 when $\deg V \leq s(T+1) - 2$. This is the skeleton relation of Lemma 35 at level $T+1$ with the check vector v' . The proof of Theorem 36 uses only $t = 0$ and this relation, so it gives the bound. $\square$

The trade-off is set by ℓ : $\ell = s$ is Theorem 42; as ℓ grows, almost all levels $m \equiv -1$ are certified with the constants of the residue sequence, and the full design appears on a sparser family. Exact computations agree with both bounds, e.g. for $s = 2$, $\ell = 4$, $p = 5$, $v' = (2, 4)$: $\text{sep}(P_m) = 0.5999, 0.6264, 0.4995$ at the skeleton levels $m = 3, 5, 11$ (bound 0.4472) and 0.6787 at the design level $m = 8$ (bound 0.6). For all N the largest gap between certified levels is still of order s^2 (exactly $s^2 - s + 1$, for every $\ell > s$), so Lemma 2 gives no improvement over the residue sequence.

6.3. A Skeleton Relation Implied by the Design. Even with $\ell = s$ the design can carry a skeleton relation at the level just after the design level, provided its diagonal is chosen for it.

Proposition 46 (A skeleton relation implied by the design). *In Definition 41 (any $\ell \geq s$), let $\bar{v} \in (\mathbb{F}_p^*)^s$ satisfy*

$$\bar{v}_i = \xi v_i/w'(a_i) \quad \text{for one } \xi \in \mathbb{F}_p^*, \quad \text{and} \quad \bar{v}^\top F_n \equiv 0 \pmod{p} \quad \text{for every } n \leq s-2.$$

Then $\sum_i \bar{v}_i y_{i,\ell K}(V) = 0$ for every $K \geq 0$ and every V with $\deg V \leq s(\ell K + 1) - 2$: the skeleton relation with check vector $\bar{v}$ holds at the level $m = s(\ell K + 1) - 1$, in addition to the design at $m = s\ell K$. Consequently $\text{sep}(P_{s(\ell K + 1) - 1}) \geq p^{-1/s} \lambda_{\text{jit}}(\Lambda_{\bar{v}})$ for every $K \geq 0$.

Proof. Keep the coefficient at infinity in the proof of Theorem 42(ii): by Lemma 21(c), for every V ,

$$y_{i,\ell K}(V) = \sum_c \sum_{n=0}^{s-2} F_n[i][c] y_{c,\ell K-1-n}(V) + v_i^{-1} [z^{-1}](Vu_i\Omega^{-K})$$

(for $K = 0$ the sum is empty). Multiply by $\bar{v}_i$ and sum over i . The double sum vanishes because $\bar{v}^\top F_n \equiv 0$. By partial fractions $\sum_i u_i/w'(a_i) = 1/w$, so the rest is $\xi[z^{-1}](V\Omega^{-K}/w) = \xi\theta^K[z^{-1}](V/w^{\ell K+1})$, which is 0 for $\deg V \leq s(\ell K + 1) - 2$. The bound follows as in Theorem 36. $\square$

The condition $\bar{v}^\top F_n \equiv 0$ can always be met by the free diagonal, choosing $F_n[c][c]$ with $\bar{v}_c F_n[c][c] = -\sum_{i \neq c} \bar{v}_i F_n[i][c]$. But it has a price. It says that every column of every F_n , read as an integer vector of centred residues, lies in $\Lambda_{\bar{v}}$. Hence

$$\lambda_{\text{jit}}(\Lambda_{\bar{v}}) \leq \min\{\|(|F_n[\cdot][c]| - \mathbf{1})_+\|_2 : n \leq s-2, F_n[\cdot][c] \neq 0\},$$

so a good implied skeleton relation (with $\lambda_{\text{jit}}(\Lambda_{\bar{v}})$ of order $p^{1/s}$) forces an entry of order $p^{1/s}$ in every nonzero column of the design, far from the entries ± 1 of the nets. (For example a column $(-2, -1)$ forces $\lambda_{\text{jit}} \leq 1$.) In dimension two the price can be paid exactly at the primes one more than a square.

Corollary 47 (Primes of the form $u^2 + 1$). *Let $p = u^2 + 1$ be a prime (u even: $p = 5, 17, 37, 101, 197, 257, 401, \dots$), $s = \ell = 2$, places $(0, 1)$, $v = (-u, -1)$ and $F_0 = \begin{pmatrix} -1 & u \\ -u & -1 \end{pmatrix}$. Then for every $K \geq 1$*

$$\begin{aligned} \text{sep}(P_{4K}) &\geq \frac{\sqrt{(u-2)^2 + (u^2 - u - 1)^2}}{p} \geq 1 - \frac{\sqrt{p-1} + 2}{p}, \\ \text{sep}(P_{4K+1}) &\geq \frac{u-1}{\sqrt{p}} = \frac{\sqrt{p-1} - 1}{\sqrt{p}}. \end{aligned}$$

The fine cells occupied by P_{4K+1} form the square lattice $\mathbb{Z}(1, u) + \mathbb{Z}(u, -1)$.

Proof. For $s = 2$ reachability only asks for nonzero crosses. With $w = z^2 - z$, $w'(0) = -1$, $w'(1) = 1$, the vector $\bar{v} = (u, -1)$ satisfies $\bar{v}_i = v_i/w'(a_i)$, and $\bar{v}^\top F_0 = (-u + u, u^2 + 1) \equiv 0$. *Design levels.* The carry length does not matter, and the four steps give $\sigma = (-1, -u)$, $(u, -1)$, $(u-1, -u-1)$ and $(-u-1, 1-u)$. The axis steps have the terms $((p-2)^2 + (u-1)^2)^{1/2}/p \geq (p-2)/p$. On the diagonal steps the two coordinates contribute $(u-2)/p$ and $(p-u-2)/p = (u^2 - u - 1)/p$, and $(p-2)^2 - (p-u-2)^2 - (u-2)^2 = 2pu - 2u^2 - 4 > 0$, so the diagonal term is the minimum; it is at least $(p-u-2)/p$. *Skeleton levels.* By Proposition 46 the skeleton relation with $\bar{v}$ holds at $m = 4K + 1$. The lattice $\Lambda_{\bar{v}} = \{b : ub_0 \equiv b_1\}$ contains $(1, u)$ and $(u, -1)$, whose determinant is $-p$, so they span it, and $|m(1, u) + n(u, -1)|^2 = (m^2 + n^2)p$. The four vectors $\pm(1, u)$, $\pm(u, -1)$ have $\|(|b| - 1)_+\|_2 = u - 1$, and every other nonzero vector has length at least $\sqrt{2p}$, hence $\|(|b| - 1)_+\|_2 \geq \sqrt{2p} - \sqrt{2} \geq u - 1$. So $\lambda_{\text{jit}}(\Lambda_{\bar{v}}) = u - 1$, and Theorem 36 applies. $\square$

At the skeleton levels $\bar{v} = (u, -1)$ is the Korobov vector of Corollary 37 ($\rho = u$), so the bound is the Korobov bound $(\rho - 1)p^{-1/2}$ of the residue sequence; it is about $1 - p^{-1/2}$, against the general lower form $1 - 2p^{-1/2}$, because the fine-cell lattice is an exact square. It is the best over all check vectors at $p = 5, 17, 37, 197$, not at $p = 101, 257, 401$, where other check vectors have a larger λ_{jit}^2 (85, 241, 369 against 81, 225, 361; exact computation). At the design levels the constant is $1 - O(p^{-1/2})$, below the $1 - 2/p$ of Theorem 42(a): the price of the implied relation. Exact computations agree: $\text{LB}(F) = 0.6576, 0.7912, 0.8847$ at $p = 17, 37, 101$, against $\text{sep}(P_4) = 0.6597, 0.8072, 0.8885$; at the skeleton level $m = 5$, $\text{sep}(P_5) = 0.6406, 0.7988, 0.9094$ at $p = 5, 17, 37$, against $0.4472, 0.7276, 0.8220$.

Remark 48 (Meeting the density bound). For $s = 2$ and $\ell \geq 3$, adding the skeleton multipliers of Theorem 45 to the design of Corollary 47 certifies the design at $m \in 2\ell\mathbb{N}$ and the skeleton relation at the levels $m = 2N + 1$ with $N \not\equiv -1 \pmod{\ell}$, i.e. at a fraction $(\ell - 1)/\ell$ of the levels $m \equiv 1 \pmod{2}$ (Theorem 45(iii) and Proposition 46). The two densities add up to 1, the largest value that exact relations of bounded depth allow (Corollary 59). The bound for all N does not improve on that of the residue sequence: the largest gap between certified levels is 3, against 2 for the residue sequence.

7. HOW MANY EXACT RELATIONS A SEQUENCE CAN CARRY

The nets of [18] reach separations $1 - O(1/q)$ at the full levels by designing the whole geometric layer: at one prefix, every geometric digit is a prescribed linear function of the last few cell digits. These are s exact linear identities among the digits of the points, and the nets choose them anew for every size. Sections 5 and 6 install such identities in one fixed scramble, by the residue

theorem. The staggered residue sequence carries one at every full level, the residue sequence one at every prefix P_{sK-1} (its skeleton relation), the block-periodic residue sequences carry s of them at every s -th full level, and the sequences of Theorem 45 and Corollary 47 share the levels between two families. In every case this is about one identity per level. Why not s at every full level? That would put the designed lattice of the nets into every full level of one sequence, with constants $1 - O(1/p)$ at every full level and the best bound for all N (Lemma 2).

This section shows that, for exact relations of bounded depth, about one per level is the limit. The reason is a shortage of digits. Without a depth bound every full level carries s exact relations, namely the offset map itself: each geometric digit is a linear function of all the cell digits. A relation of depth at most J at level T uses, in a given coordinate, only the digits $T - J, \dots, T$, and the residue theorem shows that relations at different levels cannot share these digits: each relation needs a digit position of its own. A range of $R + 1$ consecutive levels offers $J + R + 1$ digit positions in one coordinate, so it carries at most $J + R + 1$ independent relations, about one per level (Theorem 51 and Figure 9).

Scope. All results of this section are negative, and each holds in exactly this scope. The sequences are the lower-triangular scrambles $C_c = L_c P_{a_c}$ of a frame of s distinct places in $\mathbb{F}_q$, the class of Lemma 1; it contains every sequence of Sections 4–6 and every generalized Faure sequence. The certificates are exact linear identities among the digits, of bounded depth (Definition 49), whose coefficients may depend on the level. Every statement names its range of levels. Linearity is no restriction for a designed digit: if a geometric digit is a function of the last J cell digits at all, it is a linear one, because the offset map is linear and the cell digits are free. Exactness is a restriction. The windows of Section 8 keep responses in sets of allowed values instead of fixing them; they are not exact relations, and they do certify every full level. Digital sequences that are not frame scrambles (for instance Niederreiter sequences with bases of degree at least two, or sequences with $t > 0$) are not covered either.

7.1. Exact Digit Relations. Fix a frame $(a_0, \dots, a_{s-1}; \infty)$ over $\mathbb{F}_q$ with distinct places, $s \geq 2$, and a scramble (L_c) ; put $w = \prod_c (z - a_c)$. By Lemma 21(a) digit n of coordinate c is $y_{c,n}(V) = \text{Res}_{a_c}(V \eta_{c,n})$ with a polar differential $\eta_{c,n}$ at a_c of exact pole order $n + 1$; so $\eta_{c,0}, \dots, \eta_{c,T}$ are a basis of the polar differentials at a_c of pole order at most $T + 1$. For a rational function F we write $\text{pp}_a(F dz)$ for the principal part of $F dz$ at a : the terms $(z - a)^{-k} dz$, $k \geq 1$, of its expansion.

Definition 49 (Exact digit relation). Let $T \geq 0$ and $m \geq sT$. An *exact digit relation of top index T on P_m* is a family of coefficients $f_{c,n} \in \mathbb{F}_q$ ($0 \leq c < s$, $0 \leq n \leq T$), not all zero, with

$$\sum_c \sum_{n \leq T} f_{c,n} y_{c,n}(V) = 0 \quad \text{for every } V \text{ with } \deg V < m.$$

It has *depth at most J at coordinate c* if $f_{c,n} = 0$ for $n < T - J$, and *depth at most J* if this holds at every coordinate.

A relation on P_m is also a relation on every smaller prefix $P_{m'}$, $sT \leq m' \leq m$, so the relations of top index T on P_{sT} contain all others; they form a vector space. The examples of this paper:

- (1) A *designed geometric digit* at the full level P_{sT} : $y_{i,T} = \sum_c \sum_{n=T-J}^{T-1} f_{c,n} y_{c,n}$, a relation of top index T and depth at most J . A design in the sense of [18] is one such relation for each of the s coordinates; Theorem 42(ii) gives them at $T = sK$ with depth $s - 1$.
- (2) The relation of the staggered residue sequence, $y_{c_*,T} = \sum_{c \neq c_*} k_c y_{c,T-1}$ on P_{sT} (Lemma 27): top index T , depth 1.
- (3) The skeleton relation $\sum_c v_c y_{c,T} = 0$ on $P_{s(T+1)-1}$ (Lemma 35 at level $T + 1$): top index T , depth 0.

- (4) The offset map: at every level T , each geometric digit $y_{i,T}$ is a linear function of all cell digits of P_{sT} . These are s relations of top index T on P_{sT} , of depth T .

Example (4) shows that relations as such are not scarce; the depth bound is what makes them scarce. The next lemma, the one tool of this section, translates a relation into a single polynomial.

Lemma 50 (The polynomial of a relation). *Let $(f_{c,n})$ be an exact digit relation of top index T on P_m , $m \geq sT$. There is a unique polynomial $A \neq 0$ of degree at most $s(T+1) - m - 1 \leq s-1$ with*

$$\sum_{n \leq T} f_{c,n} \eta_{c,n} = \text{pp}_{a_c}(A w^{-T-1} dz) \quad \text{for every } c.$$

The map from relations to polynomials is linear and injective, and $f_{c,T} \neq 0$ exactly for the coordinates c with $A(a_c) \neq 0$. Conversely, every nonzero polynomial of degree at most $s(T+1) - m - 1$ is the polynomial of exactly one relation of top index T on P_m . Hence these relations form a space of dimension $s(T+1) - m$ (if $m \leq s(T+1)$): s on the full level P_{sT} , and 1 on $P_{s(T+1)-1}$.

Proof. Put $\eta_c = \sum_n f_{c,n} \eta_{c,n}$, a polar differential at a_c of pole order at most $T+1$, and $\eta = \sum_c \eta_c = \Xi dz$. The rational function Ξ has poles only at the places, of order at most $T+1$, and vanishes at ∞ ; so $\Xi = A/w^{T+1}$ with a polynomial A of degree less than $s(T+1)$. Since $\eta_{c'}$ is regular at a_c for $c' \neq c$, η_c is the principal part of Ξdz at a_c . For a polynomial V , the differential $V\eta_c$ has the same residue at a_c as $V\Xi dz$, so by Lemma 21(c)

$$\sum_c \sum_n f_{c,n} y_{c,n}(V) = \sum_c \text{Res}_{a_c}(V\Xi dz) = [z^{-1}](V\Xi).$$

This vanishes for all V of degree less than m if and only if the coefficients of $z^{-1}, \dots, z^{-m}$ in the expansion of Ξ at ∞ vanish, that is, if and only if $A = 0$ or $s(T+1) - \deg A \geq m+1$. If $A = 0$, then every $\eta_c = \text{pp}_{a_c}(\Xi dz) = 0$, and all $f_{c,n} = 0$ because the $\eta_{c,n}$ are linearly independent; so $A \neq 0$ and $\deg A \leq s(T+1) - m - 1$. Uniqueness and linearity are clear, since $A = \Xi w^{T+1}$, and injectivity is the argument just given. The pole order of $\text{pp}_{a_c}(A w^{-T-1} dz)$ is $T+1$ exactly when $A(a_c) \neq 0$, which is the statement about $f_{c,T}$. Conversely, given A , write $\text{pp}_{a_c}(A w^{-T-1} dz)$ in the basis $\eta_{c,0}, \dots, \eta_{c,T}$; the computation above, read backwards, shows that the coefficients form a relation on P_m . $\square$

So on a full level there are exactly the s relations of the offset map, and on $P_{s(T+1)-1}$ exactly one: in the language of Section 5.3, the skeleton digit of a skeleton coordinate is always a linear function of the other digits, and the residue sequence is the case in which this function has depth zero (Lemma 56 below makes this precise). The numerator A also tells which digits a relation involves. A designed geometric digit of coordinate i has $f_{c,T} = 0$ for $c \neq i$, so A vanishes at the $s-1$ places a_c , $c \neq i$: A is a multiple of $w_i = w/(z - a_i)$. The staggered relation (2) has A a multiple of $w_{c_\star}$, and the skeleton relation (3) has a constant A .

7.2. Counting Exact Digit Relations. We call a range of levels $[K_0, K_0 + R]$ *admissible for depth J* if

$$K_0 \geq J \quad \text{and} \quad K_0 > (s-1)R + s - 2.$$

Every subrange $[K_0, K_0 + R']$, $R' \leq R$, of an admissible range is admissible, and for fixed J every level $K_0 \geq \max(J, s-1)$ starts an admissible range of length about $K_0/(s-1)$.

Theorem 51 (Counting exact digit relations). *Let $[K_0, K_0 + R]$ be admissible for depth J , and fix a coordinate c . For every level $T \in [K_0, K_0 + R]$ let r_T be the dimension of a space of exact*

digit relations of top index T on P_{sT} whose depth at coordinate c is at most J (the depth at the other coordinates is arbitrary, and the coefficients may depend on T). Then

$$\sum_{T=K_0}^{K_0+R} r_T \leq J + R + 1.$$

More precisely, $\sum_T r_T$ is at most the number of digit positions n of coordinate c at which at least one of these relations has a nonzero coefficient.

Proof. Choose a basis of each of the spaces and let $\mathcal{N}_c$ be the set of digit positions n of coordinate c used by some basis relation; $\mathcal{N}_c \subseteq [K_0 - J, K_0 + R]$, so $|\mathcal{N}_c| \leq J + R + 1$. The place- c part $\sum_n f_{c,n} \eta_{c,n}$ of each basis relation lies in the span of $\{\eta_{c,n} : n \in \mathcal{N}_c\}$, which has dimension $|\mathcal{N}_c|$. It suffices to show that the place- c parts of all $\sum_T r_T$ basis relations are linearly independent.

Suppose a linear combination of them vanishes. Group it by levels: the part at level T is a relation of top index T on P_{sT} or zero, with a polynomial A_T of degree at most $s-1$ (Lemma 50; $A_T = 0$ if the part is zero), and the vanishing says that $\sum_T \text{pp}_{a_c}(A_T w^{-T-1} dz) = 0$. Put $T^* = K_0 + R$. Then

$$\sum_T A_T w^{-T-1} = w^{-T^*-1} B, \quad B = \sum_T A_T w^{T^*-T}, \quad \deg B \leq sR + s - 1,$$

and $w^{-T^*-1} B$ has no principal part at a_c . As w is $z - a_c$ times a unit at a_c , this means that $(z - a_c)^{T^*+1}$ divides B . But $T^* + 1 = K_0 + R + 1 > sR + s - 1 \geq \deg B$ by admissibility, so $B = 0$. Since $\deg A_T < s = \deg w$, the expansion $B = \sum_T A_T w^{T^*-T}$ is the w -adic expansion of B , which is unique; hence every $A_T = 0$, and by Lemma 50 every level part is the zero relation. The basis relations at each level are independent, so all coefficients of the combination vanish. $\square$

The proof uses one place only, and nothing about the scramble beyond its residue form; it holds over every $\mathbb{F}_q$. The admissibility condition cannot be dropped. For $s = 2$ and $J = 1$, take the range $[1, 2]$, which has $K_0 = 1 \geq J$ but violates $K_0 > (s-1)R + s - 2 = 1$. At level 1 every frame scramble has two relations of depth at most 1, the offset map of P_2 , since a single cell digit per coordinate is all there is. At level 2 the block-periodic residue sequence of Theorem 42(a) designs both geometric digits of P_4 with depth 1. That is $4 > J + R + 1 = 3$ relations. So for $s = 2$ and $J = 1$ the threshold $K_0 \geq 2$ is sharp.

Corollary 52 (Designed geometric digits). *Let $J \geq 0$, and consider a scramble of a frame of $s \geq 2$ distinct places over $\mathbb{F}_q$.*

- (a) *Let E be the set of levels T at which all s geometric digits of P_{sT} are designed by exact relations of depth at most J . Then $|E \cap [K_0, K_0 + R]| \leq (J + R + 1)/s$ for every admissible range, and $\limsup_{X \rightarrow \infty} |E \cap [1, X]|/X \leq 1/s$. Theorem 42 attains the density $1/s$.*
- (b) *Two geometric digits, of coordinates $i \neq i'$, are not both designed with depth at most J at all the levels $K_0, \dots, K_0 + J$, if $K_0 > (s-1)J + s - 2$.*
- (c) *A relation of the form $y_{c_\star, T} = \sum_{c \neq c_\star} k_c y_{c, T-1}$ on P_{sT} (as for the staggered residue sequence) and a skeleton relation $\sum_c v_c y_{c, T} = 0$ on $P_{s(T+1)-1}$ (as for the residue sequence), with any coefficients, do not both hold at two consecutive levels $T = K_0, K_0 + 1$ with $K_0 \geq 2s - 2$.*

Proof. (a) The s design relations at a level $T \in E$ are independent, since the relation of coordinate i has the coefficient 1 at $y_{i, T}$ and 0 at $y_{i', T}$, $i' \neq i$. Theorem 51 gives $s|E \cap [K_0, K_0 + R]| \leq J + R + 1$. For the density, cover the levels from $T_1 = \max(J, 4s)$ to X by consecutive admissible ranges $[T_k, T_k + R_k]$ with $R_k = \lfloor (T_k - s + 1)/(s - 1) \rfloor$ and $T_{k+1} = T_k + R_k + 1$, the last one cut at X . Then $(s-1)R_k \leq T_k - s + 1$ gives admissibility, and $T_k \geq 4s$ gives $R_k + 1 \geq T_k/(2s - 2)$,

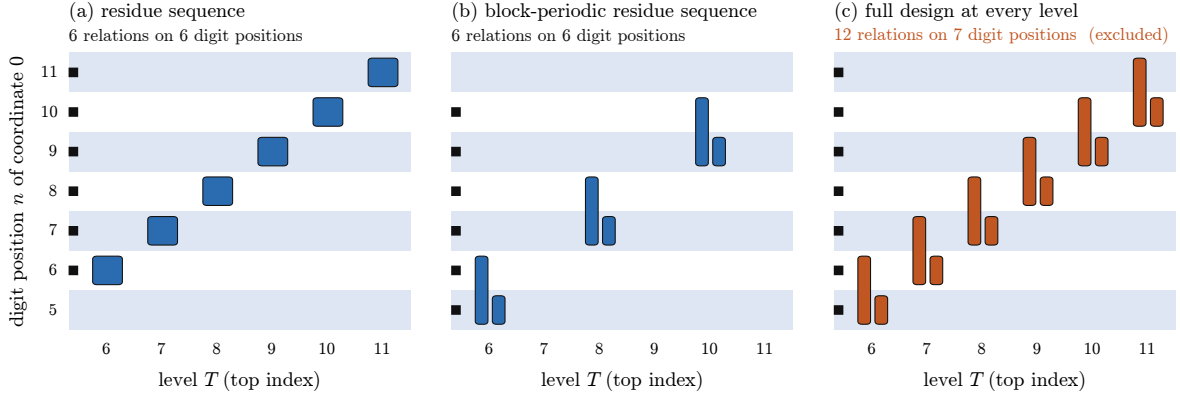


FIGURE 9. Why exact relations are scarce (Theorem 51), for $s = 2$ and the range of levels $T = 6, \dots, 11$, which is admissible for depth $J = 1$. Each column is a level T ; each row is a digit position n of coordinate 0. A relation of top index T is drawn as a bar in column T covering the digit positions at which it has nonzero coefficients in coordinate 0 (depth $J = 1$: positions $T - 1$ and T). The parts in coordinate 0 of all relations of the range are linearly independent (proof of Theorem 51), so there are at most as many bars as rows touched (black squares). (a) The residue sequence: one skeleton relation per level, at position T (Lemma 35). (b) The block-periodic residue sequence of Theorem 42(a): both geometric digits designed at the even levels (Theorem 42(ii)); the relation of coordinate 0 uses the positions $T - 1$ and T , that of coordinate 1 only $T - 1$; no relation at the odd levels. (c) Both geometric digits designed with depth 1 at every level would need twelve bars on seven rows; Corollary 52(b) excludes it.

so the ranges grow geometrically and there are $O(s \log X)$ of them. Summing the bound over the ranges, $|E \cap [1, X]| \leq T_1 + (X + J \cdot O(s \log X))/s$, and the density statement follows. Theorem 42 designs all geometric digits at the levels $T \in s\mathbb{N}$. (b) The two design relations at each level are independent (as in (a)), so the range $[K_0, K_0 + J]$, which is admissible, would carry $2(J+1) > 2J+1$ relations. (c) Both relations have top index T and depth at most 1, and they are independent: the first has a polynomial A that is a nonzero multiple of $w_{c_\star}$, of degree $s - 1 \geq 1$, and the second a constant one (Lemma 50 and the remark after it). The range $[K_0, K_0 + 1]$ is admissible for $J = 1$ when $K_0 > 2s - 3$, and would carry $4 > 3$ relations. $\square$

The case $s = 2$, $J = 1$ of the one-place form is the obstruction stated in Section 4: no scramble of the frame $(0, 1; \infty)$ in dimension two has a sheared lattice without jumps at two consecutive levels $K, K + 1 \geq 2$. We state it as a corollary; Appendix A.3 gives a direct proof, which needs even less: only that coordinate 0 is lower triangular and that P_{2K} and P_{2K+2} are nets.

Corollary 53 (No lattice offset map). *Let $s = 2$, $a_0 = 0$, $a_1 = 1$, $K \geq 2$, and let (L_0, L_1) be any scramble over any $\mathbb{F}_q$. The following three conditions do not hold together: the cross part of the offset map of coordinate 0 depends only on the finest cell digit of coordinate 1 at level K ; it does so at level $K + 1$; and the own part of the offset map of coordinate 1 depends only on the finest cell digit of coordinate 1 at level K . In particular no scramble of this frame has an offset map that depends only on the finest cell digits (a sheared lattice without jumps) at two consecutive levels $K, K + 1 \geq 2$.*

Proof. The three conditions are relations of top indices K , $K+1$ and K , on P_{2K} , P_{2K+2} and P_{2K} : $y_{0,K} = X y_{1,K-1} + (\text{cell digits of coordinate } 0)$, $y_{0,K+1} = X' y_{1,K} + (\text{cell digits of coordinate } 0)$, and $y_{1,K} = O y_{1,K-1} + (\text{cell digits of coordinate } 0)$. The two relations at level K are independent (one has the coefficient 1 at $y_{0,K}$ and 0 at $y_{1,K}$, the other the reverse). In coordinate 1 the three relations use only the digit positions $K-1$ and K , and the range $[K, K+1]$ is admissible for depth 1 because $K \geq 2$. The refined form of Theorem 51 at coordinate 1 gives $3 \leq 2$, a contradiction. A finest-digit offset map at the levels K and $K+1$ satisfies all three conditions. $\square$

7.3. Self-Similar and Block-Periodic Scrambles. For a self-similar scramble the offset map is the same at every level (Proposition 22), so a relation is most useful when its coefficients do not depend on the level. Theorem 51 then allows at most one such relation, and the residue form says which one.

Proposition 54 (A self-similar scramble carries one exact relation). *Let the scramble be self-similar with scale θ and local multipliers φ_c (Lemma 21(b)), and let $J \geq 0$. Call a family $\vartheta_{c,i} \in \mathbb{F}_q$ ($0 \leq c < s$, $0 \leq i \leq J$), not all zero, a level-independent relation if there is $T_0 \geq J$ with*

$$\sum_c \sum_{i=0}^J \vartheta_{c,i} y_{c,T-i}(V) = 0 \quad \text{for every } T \geq T_0 \text{ and every } V \text{ with } \deg V < sT,$$

a relation among the geometric digit $y_{c,T}$ and the last J cell digits at every full level from T_0 on. Put $\vartheta_c(x) = \sum_i \vartheta_{c,i} x^i$.

- (i) For every level-independent relation there is a polynomial $A \neq 0$ of degree at most $s-1$ with $\varphi_c \cdot \vartheta_c(w/\theta) = A$ as power series at every place a_c . The level-independent relations form a space of dimension at most one.
- (ii) If the relation holds on the larger prefixes P_{sT+i} for every $T \geq T_0$, with $1 \leq i \leq s-1$, then $\deg A \leq s-1-i$. On the prefixes $P_{s(T+1)-1}$ ($i = s-1$), A is a constant.
- (iii) Let $q = p$ be prime. The scramble satisfies $y_{c*,T} = \sum_{c \neq c_*} k_c y_{c,T-1}$ on P_{sT} for every $T \geq T_0$ if and only if every $k_c \neq 0$ and it is a staggered residue sequence $\mathcal{R}_v^*$ with these weights (Definition 25). It satisfies a skeleton relation $\sum_c v_c y_{c,T} = 0$ on $P_{s(T+1)-1}$ for every $T \geq T_0$ if and only if it is a residue sequence $\mathcal{R}_{v'}$ with scale θ and a check vector v' proportional to v (Definition 33). No self-similar scramble has both relations.

Proof. (i) At level T , $y_{c,T-i}(V) = \text{Res}_{a_c}(V \varphi_c(\theta/w)^{T-i+1} dz)$ and $(\theta/w)^{T-i+1} = (w/\theta)^i (\theta/w)^{T+1}$, so the place- c part of the relation is $\text{pp}_{a_c}(\theta^{T+1} \varphi_c \vartheta_c(w/\theta) w^{-T-1} dz)$. By Lemma 50 it equals $\text{pp}_{a_c}(A_T w^{-T-1} dz)$ with a nonzero polynomial A_T of degree at most $s-1$. Two functions $H_1 w^{-T-1}$, $H_2 w^{-T-1}$ with H_1, H_2 regular at a_c have the same principal part there if and only if $H_1 \equiv H_2 \pmod{(z-a_c)^{T+1}}$. So $\tilde{A}_T := \theta^{-T-1} A_T$ satisfies $\tilde{A}_T \equiv \varphi_c \vartheta_c(w/\theta) \pmod{(z-a_c)^{T+1}}$ at every place. Then $\tilde{A}_T \equiv \tilde{A}_{T+1}$ modulo every $(z-a_c)^{T+1}$, hence modulo w^{T+1} ; both have degree less than $s(T+1)$, so $\tilde{A}_T = \tilde{A}_{T+1}$. Call this polynomial A . It is congruent to $\varphi_c \vartheta_c(w/\theta)$ modulo every power of $z-a_c$, hence equal to it as a power series, and $A \neq 0$.

Let ϑ' be a second level-independent relation, with polynomial A' . If $A' = \lambda A$, then $\varphi_c(\vartheta'_c - \lambda \vartheta_c)(w/\theta) = 0$ at every place; as φ_c is a unit and w/θ is $z-a_c$ times a unit, $\vartheta'_c = \lambda \vartheta_c$, and the two relations are proportional. Otherwise A/A' is a non-constant rational function whose numerator and denominator have degree at most $s-1$. No ϑ'_c is zero, since then A' would vanish as a power series at a_c . In the Laurent series at a_c , $A/A' = \varrho_c(w)$ with $\varrho_c(x) = \vartheta_c(x/\theta)/\vartheta'_c(x/\theta) \in \mathbb{F}_q(x)$. This is an identity of rational functions in z , and $x \mapsto w$ is an injective map of fields $\mathbb{F}_q(x) \rightarrow \mathbb{F}_q(z)$, so all ϱ_c are one non-constant $\varrho = P_1/P_2$ in lowest terms. Then $P_1(w)$ and $P_2(w)$ are coprime (a common root β would make $w(\beta)$ a common root of P_1 and P_2), so $A/A' = P_1(w)/P_2(w)$ has numerator or denominator of degree $s \max(\deg P_1, \deg P_2) \geq s$. That contradicts the degree bound $s-1$.

(ii) On P_{sT+i} , Lemma 50 gives $\deg A_T \leq s(T+1) - (sT+i) - 1 = s-1-i$.
 (iii) If $y_{c_\star, T} = \sum_c k_c y_{c, T-1}$, then $\vartheta_{c_\star} = 1$ and $\vartheta_c(x) = -k_c x$ for $c \neq c_\star$. By (i), $A = -k_c \varphi_c w / \theta$ at a_c , so $k_c \neq 0$ (else A would vanish at a_c as a power series) and $A(a_c) = 0$ for every $c \neq c_\star$. As $\deg A \leq s-1$, $A = \lambda w_{c_\star}$ with $\lambda \neq 0$. Hence $\varphi_c = -(\lambda \theta / k_c) / (z - a_{c_\star})$ for $c \neq c_\star$ and $\varphi_{c_\star} = \lambda w_{c_\star}$: these are the local multipliers of $\mathcal{R}_v^\star$ with $\mu_\star = \lambda \theta$ and $\mu_c = -\mu_\star / k_c$ (Section 5.2). If $\sum_c v_c y_{c, T} = 0$ on $P_{s(T+1)-1}$, then $\vartheta_c = v_c$ and, by (ii), $A = \alpha$ is a nonzero constant; so every $v_c \neq 0$ and $\varphi_c = \alpha / v_c$, the local multipliers of $\mathcal{R}_{v/\alpha}$. Conversely both sequences have their relations (Lemmas 27 and 35). Finally, the skeleton relation on $P_{s(T+1)-1}$ holds in particular on P_{sT} , and its polynomial is constant, while the staggered relation has the non-constant polynomial $\lambda w_{c_\star}$; two independent level-independent relations contradict (i). $\square$

Scope. The proposition counts relations whose most significant digit is the geometric digit (or, in (ii), the digit $y_{c, T}$ read on P_{sT+i}). Identities among deeper digits are not extra relations: the residue sequence satisfies $\sum_c v_c y_{c, T+i} = 0$ on P_{sT} for every $i \geq 0$ (Lemma 35), infinitely many independent identities, but for $i \geq 1$ each is the skeleton relation of a later level restricted to a smaller prefix; in the sense of Definition 49 it has top index $T+i$ and lives on a prefix smaller than $P_{s(T+i)}$. Part (iii) explains the two constructions of Section 5: each is the only self-similar scramble with its relation, and the remark on full levels after Theorem 36 is the last statement of (iii). Part (ii) also bounds the nets that a self-similar sequence can imitate. The prefix $P_{s(T+1)-j}$ has j skeleton coordinates, and the nets of [18] with j skeleton coordinates prescribe j skeleton digits; a self-similar scramble supplies at most one relation of bounded depth with coefficients independent of the level, so for $j \geq 2$ it cannot supply them in this way.

The block-periodic scrambles of Section 6 escape the count of Proposition 54 by reading their digits in blocks. In general, a *block-periodic scramble of period ℓ* has digits $y_{c, \ell n+j}(V) = \text{Res}_{a_c}(V \varphi_{c,j} \Omega^{-n-1} dz)$, $0 \leq j < \ell$, with $\Omega = w^\ell / \theta$ and power series $\varphi_{c,j}$ at a_c that vanish to order exactly $\ell-1-j$; Definition 41 is an instance, and $\ell=1$ is a self-similar scramble. The digit $\ell n+j$ is then the residue against a polar differential of exact order $\ell n+j+1$, so this is a scramble of the frame. Its structure repeats with period ℓ in the level, and a relation is level-independent of class j if its coefficients $\vartheta_{c,i}$ of $y_{c, T-i}$ ($i \leq J$) are the same for all $T \equiv j \pmod{\ell}$, $T \geq T_0$, on P_{sT} .

Proposition 55 (A block-periodic scramble carries ℓ exact relations). *For a block-periodic scramble of period ℓ and every $J \geq 0$, the level-independent relations of all classes $j = 0, \dots, \ell-1$ together span a space of dimension at most ℓ : if d_j is the dimension of the space of level-independent relations of class j , then $d_0 + \dots + d_{\ell-1} \leq \ell$.*

Proof. Fix a class j and a relation of that class, and let $T = \ell n + j \geq T_0$. Each digit $y_{c, T-i}$ is read by $\varphi_{c,j'} \Omega^{-n'-1} dz$ with $T-i = \ell n' + j'$, and $\Omega^{-n'-1} = \Omega^{n-n'} \Omega^{-n-1}$, where j' and $n-n'$ depend only on i and j . So the place- c part of the relation is $\text{pp}_{a_c}(h_c \Omega^{-n-1} dz)$ with

$$h_c = \sum_{j' < \ell} \varphi_{c,j'} P_{c,j'}(\Omega),$$

where the polynomials $P_{c,j'}$ collect the coefficients $\vartheta_{c,i}$ and do not depend on n . The orders of vanishing of the terms $\varphi_{c,j'} P_{c,j'}(\Omega)$ at a_c are $\equiv \ell-1-j' \pmod{\ell}$, pairwise different, so h_c determines the $P_{c,j'}$, and $h_c = 0$ only for the zero relation. By Lemma 50 the place- c part is also $\text{pp}_{a_c}(A_T w^{-T-1} dz)$ with $\deg A_T \leq s-1$. Since $\Omega^{-n-1} = \theta^{n+1} w^{-T-1} w^{-(\ell-1-j)}$, comparing the two forms as in the proof of Proposition 54 gives $h_c \equiv \hat{A}_n \pmod{(z-a_c)^{\ell(n+1)}}$ at every place, with the polynomial $\hat{A}_n = \theta^{-n-1} A_T w^{\ell-1-j}$ of degree less than $s(\ell-j) \leq s\ell$. As there, $\hat{A}_n$ does not depend on n , and $h_c = \hat{A}$ as power series at every place for one polynomial

$$\hat{A} = A w^{\ell-1-j}, \quad \deg A \leq s-1.$$

The map from relations (of all classes) to these polynomials $\hat{A}$ is linear and injective: within a class by the remark on h_c , and across classes because $\sum_j A^{(j)} w^{\ell-1-j} = 0$ with $\deg A^{(j)} < s$ forces every $A^{(j)} = 0$, by the uniqueness of the w -adic expansion.

Suppose there were $r > \ell$ independent relations, with polynomials $\hat{A}^{(1)}, \dots, \hat{A}^{(r)}$, linearly independent over $\mathbb{F}_q$ and of degree less than $s\ell$. At one place a_c write $\hat{A}^{(k)} = \sum_{j'} \varphi_{c,j'} P_{c,j'}^{(k)}(\Omega)$. The $r \times \ell$ matrix $(P_{c,j'}^{(k)}(x))$ over $\mathbb{F}_q(x)$ has rank at most $\ell < r$, so there are polynomials $\varrho_1(x), \dots, \varrho_r(x)$, not all zero, with $\sum_k \varrho_k P_{c,j'}^{(k)} = 0$ for every j' . Then the polynomial $\sum_k \varrho_k(\Omega) \hat{A}^{(k)}$ vanishes as a power series at a_c , hence is zero. Writing $\varrho_k = \sum_i \varrho_{k,i} x^i$, it is $\sum_i \Omega^i \sum_k \varrho_{k,i} \hat{A}^{(k)}$, and since $\deg \Omega = s\ell$ and each $\sum_k \varrho_{k,i} \hat{A}^{(k)}$ has degree less than $s\ell$, the uniqueness of the Ω -adic expansion gives $\sum_k \varrho_{k,i} \hat{A}^{(k)} = 0$ for every i , hence all $\varrho_{k,i} = 0$, a contradiction. $\square$

So a block period ℓ buys ℓ level-independent relations per ℓ levels, again about one per level, in agreement with Theorem 51. A full designed layer at one class uses s of them, which is why Theorem 42 needs $\ell \geq s$ and takes $\ell = s$. The bound is attained by the constructions of Section 6: exact computation of the relation spaces class by class gives $2 + 0$ and $3 + 0 + 0$ for Theorem 42 with $s = 2$ and $s = 3$, and $2 + 1 + 1 + 0$, $3 + 1 + 0 + 0$, $2 + 1 + 0$ for Theorem 45 with $(s, \ell) = (2, 4)$, $(3, 4)$, $(2, 3)$.

7.4. Skeleton Relations and Designs. The residue sequence is certified at every prefix P_{sK-1} with constants that tend to 1, the block-periodic sequences at every s -th full level with $1 - O(1/p)$. One would like both in one sequence. The skeleton relation turns out to be rigid: it fixes the rows of the generator matrices, and then no design fits next to it.

Write $\hat{y}_{c,n}(V) = \text{Res}_{a_c}(V w^{-n-1} dz)$ for the *residue digits*; for $q = p$ they are the digits of the residue sequence $\mathcal{R}_v$ with $\theta = 1$ and $v = (1, \dots, 1)$.

Lemma 56 (An exact skeleton relation fixes the row). *Let $n \geq 0$ and $v \in \mathbb{F}_q^s \setminus \{0\}$ with $\sum_c v_c y_{c,n}(V) = 0$ for every V with $\deg V \leq s(n+1) - 2$. Then every $v_c \neq 0$, and there is $\xi \in \mathbb{F}_q^*$ with*

$$y_{c,n} = \frac{\xi}{v_c} \hat{y}_{c,n} \quad \text{for every } c :$$

row n of every generator matrix is the row of the residue digits, up to one nonzero scalar per coordinate.

Proof. The relation has top index n , depth 0, and holds on $P_{s(n+1)-1}$. By Lemma 50 its polynomial is a nonzero constant ξ , so $v_c \eta_{c,n} = \xi \text{pp}_{a_c}(w^{-n-1} dz)$ for every c . The right side has exact pole order $n+1$, as w is $z - a_c$ times a unit, so $v_c \neq 0$, and $y_{c,n}(V) = \text{Res}_{a_c}(V \eta_{c,n}) = (\xi/v_c) \text{Res}_{a_c}(V w^{-n-1} dz)$ because the regular part of $w^{-n-1} dz$ contributes nothing. $\square$

Row 0 is always of this form ($y_{c,0} = L_c[0][0] V(a_c)$ and $\hat{y}_{c,0} = V(a_c)/w'(a_c)$), and the skeleton relation on P_{s-1} holds for every frame scramble, with $v_c = 1/(L_c[0][0] w'(a_c))$, because $\sum_c V(a_c)/w'(a_c) = 0$ for $\deg V \leq s - 2$. From row 1 on the lemma is a real restriction.

Corollary 57 (Residue rows with level-dependent scalars). *A scramble of the frame satisfies, for every $n \geq n_0$, a skeleton relation $\sum_c u_{c,n} y_{c,n}(V) = 0$ on $P_{s(n+1)-1}$ with some $u_n \in \mathbb{F}_q^s \setminus \{0\}$, if and only if for every $n \geq n_0$ there are $\mu_{c,n} \in \mathbb{F}_q^*$ with $y_{c,n} = \mu_{c,n} \hat{y}_{c,n}$ for all c ; then u_n is proportional to $(1/\mu_{c,n})_c$. For $q = p$, the self-similar scrambles with this property are exactly the residue sequences $\mathcal{R}_v$ (any scale θ and check vector v).*

Proof. One direction is Lemma 56 at each $n \geq n_0$. Conversely, if $y_{c,n} = \mu_{c,n} \hat{y}_{c,n}$, then $\sum_c \mu_{c,n}^{-1} y_{c,n}(V) = \sum_c \text{Res}_{a_c}(V w^{-n-1} dz) = [z^{-1}](V/w^{n+1})$, which vanishes for $\deg V \leq s(n+1) - 2$ (Lemma 21(c)). A self-similar row $y_{c,n} = \text{Res}_{a_c}(V \varphi_c(\theta/w)^{n+1} dz)$ equals $\mu_{c,n} \hat{y}_{c,n}$ for all V if and

only if $\theta^{n+1}\varphi_c \equiv \mu_{c,n} \pmod{(z - a_c)^{n+1}}$; for all $n \geq n_0$ this forces φ_c to be a constant, $\varphi_c = v_c^{-1}$, which is the residue sequence (Definition 33); and $\mathcal{R}_v$ has the skeleton relation at every level (Lemma 35). $\square$

So a scramble with the skeleton relation at every $m \equiv -1 \pmod{s}$ has no freedom left except one vector u_n per level: its direction is the check vector of the skeleton relation at that level (and should be a good one, with $\lambda_{\text{jit}}(\Lambda_{u_n})$ large), its scale is free. The residue sequence is the self-similar member, with u_n proportional to v for every n . Next to such rows there is no room for a design.

Corollary 58 (No designed relation next to skeleton relations). *Let $J \geq 0$ and $K \geq \max(s - 1, sJ)$, and suppose that the skeleton relations $\sum_c u_{c,n} y_{c,n} = 0$ on $P_{s(n+1)-1}$ hold at the $J + 1$ levels $n = K - J, \dots, K$. Then every exact digit relation of top index K and depth at most J on P_{sK} is a multiple of $\sum_c u_{c,K} y_{c,K} = 0$. In particular the full level P_{sK} has no designed geometric digit of depth at most J , and no designed layer.*

Proof. By Lemma 56, $\eta_{c,n}$ is a nonzero multiple of $\text{pp}_{a_c}(w^{-n-1}dz)$ for $K - J \leq n \leq K$. Let a relation have polynomial A (Lemma 50, $\deg A \leq s - 1$). Its place- c part $\text{pp}_{a_c}(Aw^{-K-1}dz)$ then lies in the span of $\text{pp}_{a_c}(w^{-n-1}dz)$, $K - J \leq n \leq K$. Fix a place a_c and expand A in powers of the uniformizer: $A = \sum_{k \geq 0} \nu_k w^k$ as power series at a_c , $\nu_k \in \mathbb{F}_q$. Then $\text{pp}_{a_c}(Aw^{-K-1}dz) = \sum_{k \leq K} \nu_k \text{pp}_{a_c}(w^{k-K-1}dz)$, and these principal parts have the exact pole orders $K + 1 - k$, so they are independent; hence $\nu_k = 0$ for $J < k \leq K$. Put $P(X) = \sum_{k \leq J} \nu_k X^k$. The polynomial $A - P(w)$ has degree at most $\max(s - 1, sJ)$ and a zero of order at least $K + 1$ at a_c ; since $K + 1 > \max(s - 1, sJ)$, $A = P(w)$. As $\deg A < s$, P is constant, and A is a constant ν . So the place- c part is $\nu \text{pp}_{a_c}(w^{-K-1}dz)$, which is $\nu \xi_K^{-1} u_{c,K} \eta_{c,K}$ by Lemma 56 at $n = K$ (with its constant ξ_K), at every place. So $f_{c,n} = 0$ for $n < K$ and $f_{c,K} = \nu \xi_K^{-1} u_{c,K}$. A designed geometric digit of coordinate i has $f_{c,K} = 0$ for $c \neq i$, which forces $\nu = 0$, since every $u_{c,K} \neq 0$. $\square$

The relation $\sum_c u_{c,K} y_{c,K} = 0$ that survives is the skeleton relation of level K restricted to P_{sK} : it puts the geometric digits of each point on a hyperplane, which says where the point sits inside its cell, not where it sits relative to its neighbours (Remark 40). The corollary is a local argument and does not use Theorem 51. Its hypothesis $K \geq \max(s - 1, sJ)$ cannot be weakened to $K \geq J + 1$ in general: for $s = 4$, the places 0, 1, 2, 3 over $\mathbb{F}_{11}$, $J = 3$ and $K = 4$, the relations of top index 4 and depth at most 3 on P_{16} among the residue digits form a space of dimension 2 (exact computation by two independent methods). At every $K \geq 5$ the dimension is 1 there (exact computation for $5 \leq K \leq 11$, the corollary for $K \geq 12$), and for $p = 13$ and $p = 17$ it is 1 already at $K = 4$: the failure depends on the prime.

Combined with Theorem 51, the skeleton relations and the designs share one count.

Corollary 59 (Density bound for exact relations). *Let $J \geq 0$, and for a scramble of a frame let E be the set of levels T at which all s geometric digits of P_{sT} are designed by exact relations of depth at most J , and S the set of levels T at which $P_{s(T+1)-1}$ satisfies a skeleton relation $\sum_c u_{c,T} y_{c,T} = 0$ (with any $u_T \neq 0$). Then for every admissible range $I = [K_0, K_0 + R]$,*

$$|S \cap I| + (s - 1)|E \cap I| \leq J + R + 1, \quad \text{and} \quad \limsup_{X \rightarrow \infty} \frac{|S \cap [1, X]| + (s - 1)|E \cap [1, X]|}{X} \leq 1.$$

In particular $d_S + (s - 1)d_E \leq 1$ whenever the densities d_S of S and d_E of E exist, and a skeleton relation at every level of an admissible range leaves room for at most $J/(s - 1)$ design levels in it.

Proof. A level of E carries s independent relations of top index T (proof of Corollary 52(a)), and a level of S carries one, of depth 0; a relation on $P_{s(T+1)-1}$ is also one on P_{sT} . So $|S \cap I| +$

$(s-1)|E \cap I| \leq |(S \setminus E) \cap I| + s|E \cap I| \leq \sum_{T \in I} r_T \leq J + R + 1$ by Theorem 51. The density statement follows with the covering of the proof of Corollary 52(a). $\square$

The bound is attained: the residue sequence has $d_S = 1$, and for $s = 2$ the sequences of Remark 48 have $d_E = 1/\ell$ and $d_S = (\ell - 1)/\ell$. Theorem 42 has $d_E = 1/s$, $d_S = 0$, and Theorem 45 has $(s-1)/\ell + (\ell-s)/\ell = (\ell-1)/\ell$: one relation per block of ℓ levels is left unused.

Remark 60 (Levels certified by exact relations). Call a prefix P_m , $m = s(T+1) - j$ with $1 \leq j \leq s$, *certified by exact relations* if its certificate uses j independent exact digit relations of top index T on P_m , of depth at most J ; by Lemma 50 P_m has exactly j relations of top index T , and the certificate asks all of them to have bounded depth. For $j = 1$ this is the skeleton relation, for $j = s$ a design at the full level P_{sT} , and for $1 < j < s$ the j skeleton digits of the nets of [18] with j skeleton coordinates. If several prefixes with the same T are certified, the one with the largest j alone uses at least as many independent relations of top index T as there are such prefixes. Hence in an admissible range at most $J + R + 1$ of the $s(R+1)$ exponents $sK_0 \leq m < s(K_0 + R + 1)$ are certified (Theorem 51). If all gaps between consecutive certified exponents there were at most $s-1$, at least $s(R+1)/(s-1) - 1$ of them would be certified, more than $J + R + 1$ as soon as $R + 1 > (s-1)(J+1)$. Admissible ranges with $R + 1 > (s-1)(J+1)$ start at every level of order $(s-1)^2(J+1)$ and beyond, so gaps of at least s between certified exponents occur arbitrarily far out: no certificate by exact relations of bounded depth covers every prefix, and in Lemma 2 such certificates give at best the factor q^{-1} for all N , which the residue sequence already attains. This concerns the exponent of the bound for all N , not its constant. Gaps of at most s need a certified exponent at every level, and at a cost of about one relation per level this forces, at all but at most J levels of every admissible range, a relation of depth at most J on $P_{s(T+1)-1}$, whose polynomial is constant: a skeleton relation, with correction terms if its depth is positive. With depth 0 these are the rows of Corollary 57, and their certificate, Theorem 36 with a check vector per level, gives at best the constant of the residue sequence; with corrections the certificate is Theorem 72, whose bound is smaller. A sharper analysis of these sequences than these certificates is not excluded.

Remark 61 (An exhaustive search). Can the scrambles of Corollary 57, which keep the skeleton relation at every $m \equiv -1 \pmod{2}$ with the best check directions, be certified at the full levels better than by the inclusion bound $\lambda_{\text{jit}}(\Lambda)/p$ of Remark 40? Their full-level responses are explicit in the vectors u_n , so for $s = 2$ and $p = 11, 13, 17$ we enumerated all of them by an exhaustive branch-and-bound search: every sequence $u_0, \dots, u_{K_{\max}}$ in which $u_1, \dots, u_{K_{\max}-1}$ have the largest possible $\lambda_{\text{jit}}(\Lambda_{u_n})$ (u_0 and $u_{K_{\max}}$ arbitrary), maximising the smallest one-digit relaxation (Lemma 23, $j = 1$) of the actual responses over the full levels $K \leq K_{\max}$. For $K_{\max} = 10, 8$ and 11 respectively the maximum equals the inclusion bound $0.1818, 0.1720, 0.1765$ of the best check direction. This is an exhaustive result in exactly this scope: $s = 2$, these three primes, these $K_{\max}$, the best check directions, and the one-digit relaxation. The actual separations of these sequences can be larger than the certificate, and nothing is claimed for other primes, other dimensions, weaker check directions or multi-digit certificates.

7.5. What Is Excluded, and What Is Open. In summary: in the class of lower-triangular scrambles of a frame of s distinct finite places over $\mathbb{F}_q$, exact digit relations of bounded depth are limited to about one per level in every admissible range of levels (Theorem 51). Consequently, all s geometric digits can be designed on at most a fraction $1/s$ of the full levels (Corollary 52; attained by Theorem 42); skeleton relations and designs together obey $d_S + (s-1)d_E \leq 1$ (Corollary 59; attained); a self-similar scramble carries one level-independent relation and a block-periodic one ℓ (Propositions 54 and 55); an exact skeleton relation fixes the row it lives in (Lemma 56), and no design of depth at most J fits at a full level next to $J+1$ such relations

(Corollary 58); and certificates by such relations leave gaps of at least s between certified sizes (Remark 60). In particular, no sequence in this class is certified by exact relations of bounded depth both at every prefix P_{sK-1} by skeleton relations and at every full level by designs. Outside this scope these questions are open: windows, which are not exact and do certify every full level (Section 8; whether windows can be combined with skeleton relations is the subject of Section 8.5); certificates that use several digits or the exact positions instead of the one-digit relaxation; choices of free digits that look at later digits; relations of unbounded depth; and digital sequences that are not scrambles of such a frame (places of higher degree, $t > 0$). No digital sequence is known to us that is certified both at every $m \equiv -1 \pmod{s}$ with the constants of Theorem 36 and at every full level with $1 - O(1/p)$. For exact designed relations of bounded depth next to exact skeleton relations this is excluded (Corollary 58); for windows chosen together with a corrected skeleton relation in a self-similar scramble, Proposition 73 excludes it in the scope stated there; in general it is open.

8. EVERY FULL LEVEL: WINDOWS AND THE HALF-CELL STAGGER

The staggered residue sequence certifies every full level P_{sK} for every prime $p > 2^s$, but with a constant of about 2^{1-s} (Corollary 29); the block-periodic residue sequences reach $1 - 2/p$ in dimensions two and three for every prime $p \geq 3$ resp. $p \geq 5$, but only at every s -th full level (Theorem 42), which costs the factor p^{-s} instead of p^{-1} in the bound for every N (Lemma 2). For exact relations this is no accident: all s geometric digits can be designed by exact relations of bounded depth on at most a fraction $1/s$ of the full levels (Corollary 52).

This section certifies every full level by inequalities instead. The free digits of a self-similar scramble, chosen one at a time, keep each carry response inside a fixed set of allowed values, a *window*, without fixing it (Section 8.1); windows are not exact relations, and Theorem 51 does not apply to them. Which windows are cheap? A response read by a coordinate that steps forward is harmless just behind 0 and fatal just in front of it; read by a coordinate that does not move, it must stay away from 0 on both sides. Half a cell is the one response that costs the same for every kind of step: up to $1/p$, the neighbour is half a cell away in that coordinate whether the coordinate steps forward, steps back or stays (Lemma 66). Staggering one coordinate by half a cell against all the others gives $1 - O(1/p)$ at every full level, in every dimension, for large primes (Theorem 68), and $1 - 17/p$ in dimension two for $p > 3677$ (Corollary 70).

So the gain over Theorem 42 is every full level instead of every s -th one, and the gain over the residue sequence (Theorem 36) is a constant tending to 1 at the full levels themselves. The thresholds are large ($1 - 742/p$ for $p \geq 1.97 \cdot 10^7$ in dimension three), so this is a statement about every full level, not a practical recommendation (Section 10). Section 8.5 shows, in a stated scope, that windows and skeleton relations cannot be selected together. All proofs of this section are in Appendix A.4, the finite-prime details in Appendix D.

8.1. Free Digits and Windows. Fix a frame $(a_0, \dots, a_{s-1}; \infty)$ over $\mathbb{F}_q$ and a scale θ . For $s = 2$ put $\hat{\omega}_c(z) = z - a_{1-c}$, and for $s \geq 3$ put $\hat{\omega}_c = 1$.

Proposition 62 (Responses of self-similar scrambles). *Let $s \geq 2$ and consider a self-similar scramble with scale θ and local multipliers φ_c (Lemma 21(b)).*

- (a) *There are unique $\lambda_c \in \mathbb{F}_q^*$ and unit power series ψ_c with $\psi_c(0) = 1$ such that $\theta \varphi_c(z) \hat{\omega}_c(z) = \lambda_c / \psi_c(w(z))$ as power series at a_c . Every $\lambda_c \in \mathbb{F}_q^*$ and every unit series ψ_c with $\psi_c(0) = 1$ occur, each for exactly one local multiplier. The multiplier of Definition 20 is $g_c(x) = \lambda_c / (\psi_c(\hat{\omega}_c(z_c)) w'(z_c))$, with ψ_c at θx and $z_c = z_c(\theta x)$.*
- (b) *The offset map is the same at every level, for every number of geometric digits.*

- (c) Let $s \geq 3$. With the own kernel $\hat{w}_{c'} = w_{c'}/w'(a_{c'})$ and the cross kernel $\check{w}_{cc'} = (a_{c'} - a_c)/(z - a_c)$, both expanded in w at $a_{c'}$ (so that their value at $w = 0$ is 1),

$$O_{c'}(x) = 1 - [\hat{w}_{c'} \psi_{c'}](\theta x), \quad X_{c \leftarrow c'}(x) = -\kappa_{c \leftarrow c'} [\check{w}_{cc'} \psi_{c'}](\theta x),$$

$$\kappa_{c \leftarrow c'} = \frac{\theta \lambda_c}{\lambda_{c'} w'(a_c) (a_{c'} - a_c)}.$$

- (d) Let $s = 2$, with the places $a_0 = 0, a_1 = 1$. Then $X_{0 \leftarrow 1}(x) = -\kappa_{0 \leftarrow 1} \psi_1(\theta x)$ and $O_1(x) = 1 - z_1(\theta x)^2 \psi_1(\theta x)$ with $\kappa_{0 \leftarrow 1} = \theta \lambda_0 / \lambda_1$, symmetrically for column 0 with ψ_0 and $\kappa_{1 \leftarrow 0} = \theta \lambda_1 / \lambda_0$; in particular $\kappa_{0 \leftarrow 1} \kappa_{1 \leftarrow 0} = \theta^2$.

So column c' of the offset map is one free unit series $\psi_{c'}$ times a fixed vector of kernels, and only the *depth-zero crosses* $\kappa_{c \leftarrow c'} = -X_{c \leftarrow c'}^{(1)}$ are fixed, by the constants λ_c . (The brick wall is $\psi_0 = 1, \psi_1 = 1/z_1^2, \lambda = (1, 2)$.) From now on $q = p \geq 5$ is prime, and at depth $l \geq 1$ we collect column c' in $\mathbf{u}_l = (O_{c'}^{(l)}, (X_{c \leftarrow c'}^{(l+1)})_{c \neq c'}) \in \mathbb{F}_p^s$.

Proposition 63 (Depth direction). *Let $s \geq 3$, or $s = 2$ with the places 0, 1. For every column c' and every depth $l \geq 1$,*

$$\mathbf{u}_l = \beta_l + \bar{\psi}_l \alpha_{c'}, \quad \alpha_{c'} = (1, (\kappa_{c \leftarrow c'})_{c \neq c'}), \quad \bar{\psi}_l = -\theta^l \psi_{c', l},$$

where the offset β_l depends only on $\psi_{c', 0}, \dots, \psi_{c', l-1}$. The coefficients $\psi_{c', l}, l \geq 1$, are free: every choice is realized by a self-similar scramble, and row n of $L_{c'}$ depends only on $\psi_{c', 0}, \dots, \psi_{c', n}$.

So the free digit at depth l moves $\mathbf{u}_l$ along the line $\beta_l + \mathbb{F}_p \alpha_{c'}$, and the earlier choices (the *history*) decide which line. A *window* is a set $W_{c \leftarrow c'} \subseteq \mathbb{F}_p$ of allowed values for every entry (row c affected, column c' carrying), with the *own window* $W_o^{(c')} := W_{c' \leftarrow c'}$ and the *column window* $W^{(c')} := W_o^{(c')} \times \prod_{c \neq c'} W_{c \leftarrow c'}$. The windows define the *window bound*

$$\text{LB}(W)^2 := \min_e \sum_c \min_{\sigma \in S_c(e)} f_1(e_c, \sigma)^2, \quad S_c(e) := \sum_{c': e_{c'} \neq 0} e_{c'} W_{c \leftarrow c'} \quad (\text{sumset}),$$

the minimum over all steps $e \in \{-1, 0, 1\}^s \setminus \{0\}$ up to sign: the digit relaxation (Lemma 23, $j = 1$) for responses known only to lie in their windows. A digit $\psi \in \mathbb{F}_p$ is *admissible* at depth l for column c' if $\beta_l - \theta^l \psi \alpha_{c'} \in W^{(c')}$, and a *selection rule* assigns to each column, depth and history an admissible digit. We write LB_K^{act} for the value LB_1 of Lemma 23 computed from the actual responses $D(l), l \leq K$.

Proposition 64 (Choosing within windows). *Let $s \geq 3$ and any frame, or $s = 2$ and the places 0, 1; fix θ and the constants λ_c . Suppose that for every column c'*

- (i) $-\kappa_{c \leftarrow c'} \in W_{c \leftarrow c'}$ for all $c \neq c'$, and
- (ii) every line $\beta + \mathbb{F}_p \alpha_{c'}, \beta \in \mathbb{F}_p^s$, meets $W^{(c')}$ (the covering condition).

Then (a) at every depth and for every history admissible digits exist; (b) every selection rule defines a self-similar scramble and a digital $(0, s)$ -sequence over $\mathbb{F}_p$; (c) all responses lie in their windows, $O_c^{(l)} \in W_o^{(c)}$ and $X_{c \leftarrow c'}^{(l)} \in W_{c \leftarrow c'}$ for every $l \geq 1$; (d) for every $K \geq 1$, $\text{sep}(P_{sK}) \geq \min(1, \text{LB}_K^{\text{act}}) \geq \min(1, \text{LB}(W))$.

The bound depends only on the windows, not on the selection rule (Appendix D.4 fixes one). Covering costs volume:

Lemma 65 (Volume bound). *Let $W \subseteq \mathbb{F}_q^s$ and $\alpha \in \mathbb{F}_q^s \setminus \{0\}$. If every line $\beta + \mathbb{F}_q \alpha$ meets W , then $|W| \geq q^{s-1}$. In particular a column window satisfying (ii) of Proposition 64 fills at least the fraction $1/p$ of $\mathbb{F}_p^s$.*

So one of the s entries of a column window has at least $p^{1-1/s}$ elements (Figure 17); the cross responses of a column never move in lockstep (Proposition 93 in Appendix A.3), so this cannot be escaped. What a wide window costs depends on where it lies. For $\Phi \in \mathbb{R}/\mathbb{Z}$ let $\text{frac}(\Phi) \in [0, 1)$ be its representative and $\|\Phi\|$ its distance to 0, and put

$$\bar{f}(+1, \Phi) = 1 - \text{frac}(-\Phi), \quad \bar{f}(-1, \Phi) = \bar{f}(+1, -\Phi), \quad \bar{f}(0, \Phi) = \|\Phi\|.$$

So $\bar{f}(+1, \Phi) = \text{frac}(\Phi)$ for $\Phi \neq 0$, and $\bar{f}(\pm 1, 0) = 1$.

Lemma 66 (Cost of a response). *Let p be prime, $\sigma \in \mathbb{F}_p$ and $\Phi = \sigma/p \in \mathbb{R}/\mathbb{Z}$. Then $f_1(e, \sigma) = \max(0, \bar{f}(e, \Phi) - 1/p)$ for $e \in \{-1, 0, 1\}$. The three functions $\bar{f}(+1, \cdot)$, $\bar{f}(-1, \cdot)$, $\bar{f}(0, \cdot)$ agree at exactly one point, $\Phi = \frac{1}{2}$, where all three equal $\frac{1}{2}$.*

An own response, read by a coordinate that moves forward, is cheap just behind 0 and fatal just in front of it; a response read by a coordinate that does not move must stay away from 0 on both sides (Figure 16 in Appendix D). Reading every entry of a column window at full cost would lose about $p^{-1/s}$ by Lemma 65. A window can be wide without being read: bounding every step by its first moving coordinate leaves some crosses unread; this ordering of the coordinates gave a closed form at every full level with separation $1 - O(p^{-1/s})$ from moderate primes on in an earlier version of this work, and it is not needed here. Or a window can be read without its width mattering: near $\frac{1}{2}$, which costs the same, up to $1/p$, for a forward step, a backward step and no step.

8.2. Staggered Windows. In the limit $p \rightarrow \infty$ windows become closed sets $W_{c \leftarrow c'} \subseteq \mathbb{R}/\mathbb{Z}$ of responses in cell units, and by Lemma 66 the window bound becomes the *continuum bound* $c^*(W)^2 := \min_e \sum_c \inf_{\Phi \in S_c(e)} \bar{f}(e_c, \Phi)^2$.

Fix a staggered coordinate $c_\star$ and let $C = \{c \neq c_\star\}$. (The staggered residue sequence of Section 5.2 shares this idea of one coordinate staggered by the others, but it is a different construction: there the stagger is an exact relation and the coordinates of C are not controlled inside their cells; here every response is kept in a window.) For $a, \varepsilon > 0$ the *staggered windows* are: in column $i \in C$, own $\{-a\}$, cross into $c_\star$ $W_{\star \leftarrow i} = \frac{1}{2} + [-\varepsilon, \varepsilon]$ (the *half-cell offset*), crosses into the other coordinates of C $[-\varepsilon, \varepsilon]$; in column $c_\star$, own $\{0\}$ and crosses $[-\varepsilon, \varepsilon]$. A step in a coordinate $i \in C$ offsets $c_\star$ by half a cell and moves the neighbour back by a in coordinate i , which shortens the spacing in i to $1 - a$.

Theorem 67 (Staggered windows). *Let $s \geq 2$ and $a, \varepsilon > 0$ with $(s-1)\varepsilon < a \leq 1 - \varepsilon$ and $(1 - a - \varepsilon)^2 + (\frac{1}{2} - \varepsilon)^2 \geq 1$. Then the staggered windows have $c^*(W) \geq 1$. Such an a exists for every $0 < \varepsilon < \varepsilon_s$, where*

$$\varepsilon_s = \frac{2s + 1 - \sqrt{3s^2 + 4s}}{2(s^2 + 1)} \approx \frac{2 - \sqrt{3}}{2s} \approx \frac{0.134}{s}$$

is the smaller root of $(1 - s\varepsilon)^2 + (\frac{1}{2} - \varepsilon)^2 = 1$ (for instance $\varepsilon_3 = (7 - \sqrt{39})/20 = 0.0377$).

The binding steps are the axis step of $c_\star$ and the steps that move one coordinate of C together with $c_\star$; in a step that moves two coordinates of C the half-cell offsets cancel, but two gaps of 0.73 already exceed distance 1. So only the own responses need small windows. At $\varepsilon = 0$ the points form columns along $c_\star$ on a square grid of spacing $1 - a$ in the coordinates of C , with heights alternating by half a cell; at $a = 1 - \sqrt{3}/2$ this is body-centred tetragonal in dimension three (Figure 18 in Appendix D.2) and the hexagonal brick wall in dimension two (Section 8.4).

8.3. Every Full Level at Large Primes. At a finite prime the windows become integer intervals of width about εp and the half becomes $\frac{1}{2} = (p+1)/2$; the fixed crosses $\kappa_{c \leftarrow c'}$ must lie in their windows and every column must cover. On the Faure places every $\kappa_{c \leftarrow c'}$ is taken as one odd integer, a fixed fraction of p , times a fixed rational; the half is the one factor 2 that survives in the row of c_* (Lemma 101 in Appendix D.2), so no congruence condition on p is needed, and the coverings follow from a mixed-radix hierarchy of step sizes (Lemmas 98 and 100, Appendix D). The only loss of order $1/p$ is the own window of c_* , whose size is bounded independently of p (Lemma 99). This explicit construction is the *staggered rule* (Definition 102, Appendix D.2).

Theorem 68 (Separation $1 - O(1/p)$ at every full level). *For every $s \geq 3$ there are a staggered rule on the Faure places $(0, 1, \dots, s-1)$, an effectively computable $p_0(s)$ and a constant C_s'' such that for every prime $p \geq p_0(s)$ the staggered rule gives a quasi-uniform digital $(0, s)$ -sequence over $\mathbb{F}_p$ with*

$$\text{sep}(P_{sK}) \geq 1 - \frac{C_s''}{p} \quad \text{for every } K \geq 1.$$

There is no congruence condition on p .

The proof is in Appendix D.2; C_s'' is the *first-order deficit*, as in [18]. For $s = 3$ one explicit rule gives $\text{sep}(P_{3K}) \geq 1 - 742/p$ for every prime $p \geq 1.97 \cdot 10^7$ (Theorem 104 in Appendix D.2, proof*), and $1 - 779/p$ for every prime $p \geq 3 \cdot 10^6$ (Remark 105, c.a.). For $s = 4$ and $s = 5$ the rules of Table 16 give $p_0 = 1.44 \cdot 10^{16}$, $C_4'' = 32\,044$ and $p_0 = 1.98 \cdot 10^{21}$, $C_5'' = 2.73 \cdot 10^9$ (proof*).

Where this stands. Among the constructions of this paper certified at every full level, the staggered windows (Theorems 68 and 69) are the ones with constants $1 - O(1/p)$; their thresholds are large, and lowering them is open (Section 11).

8.4. Dimension Two: the Hexagonal Brick Wall. For $s = 2$ the staggered windows have $C = \{0\}$ and $c_* = 1$: the brick wall with its half kept in a window, and the columns compressed to the hexagonal row spacing $\sqrt{3}/2$ (Figure 10). Proposition 62(d) takes the place of (c), and the only constraint on the crosses is $\kappa_{1 \leftarrow 0} \kappa_{0 \leftarrow 1} = \theta^2$. Let $b, e \geq 1$ be integers, $\nu = 2b + 1$, $k = 2\nu e^2$ and $\theta = \nu e$, and choose the constants λ_c with $\kappa_{1 \leftarrow 0} = -\nu/2$ and $\kappa_{0 \leftarrow 1} = -k$; the product is $\nu k/2 = \theta^2$, and the half comes from the factor 2 in k . With $M_A := \lceil (p-3)/\nu \rceil + 3$ and $M_B := \lceil (p-1)/k \rceil - 1$ the windows are

$$W_0^{(0)} = [-(k+M_A-1), -k], \quad W_{1 \leftarrow 0} = \frac{1}{2} + [-b, b], \quad W_0^{(1)} = [-(M_B-1), 0], \quad W_{0 \leftarrow 1} = [-k, k].$$

Theorem 69 (Hexagonal brick wall). *If $2k + M_A < p$ and $\eta := (p-1-2b-2M_B)/(2p) > 0$, then every selection rule gives a digital $(0, 2)$ -sequence over $\mathbb{F}_p$ with $\text{sep}(P_{2K}) \geq \min(1, \text{LB}^{\text{HB}})$ for every $K \geq 1$, where*

$$(\text{LB}^{\text{HB}})^2 = \min \left(\left(1 - \frac{k+M_A}{p}\right)^2 + \left(\frac{p-3-2b}{2p}\right)^2, \left(1 - \frac{M_B}{p}\right)^2, \left(1 - \frac{2k+M_A}{p}\right)^2 + \eta^2 \right).$$

Corollary 70 (Separation $1 - 17/p$). *For every prime $p > 3677$, the hexagonal brick wall with $e = 1$ and $b = \lfloor p/68 \rfloor$ satisfies $\text{sep}(P_{2K}) \geq 1 - 17/p$ for every $K \geq 1$, and is quasi-uniform.*

The proofs are in Appendix A.5; the corollary is a hand estimate for $p \geq 10^4$ and an exact evaluation at the 715 primes $3677 < p < 10^4$ (c.a.). The threshold is small because every column has a single cross. At $p = 401$ with $(b, e) = (5, 1)$ Theorem 69 certifies 0.9054; the exact value at the first level is $\text{sep}(P_2) = 0.9922$. For comparison, the brick wall of Theorem 32 has the bound $(p-3)/(2p)$, and Theorem 42 gives $1 - 2/p$ at $m \in 4\mathbb{N}$ for every prime $p \geq 3$.

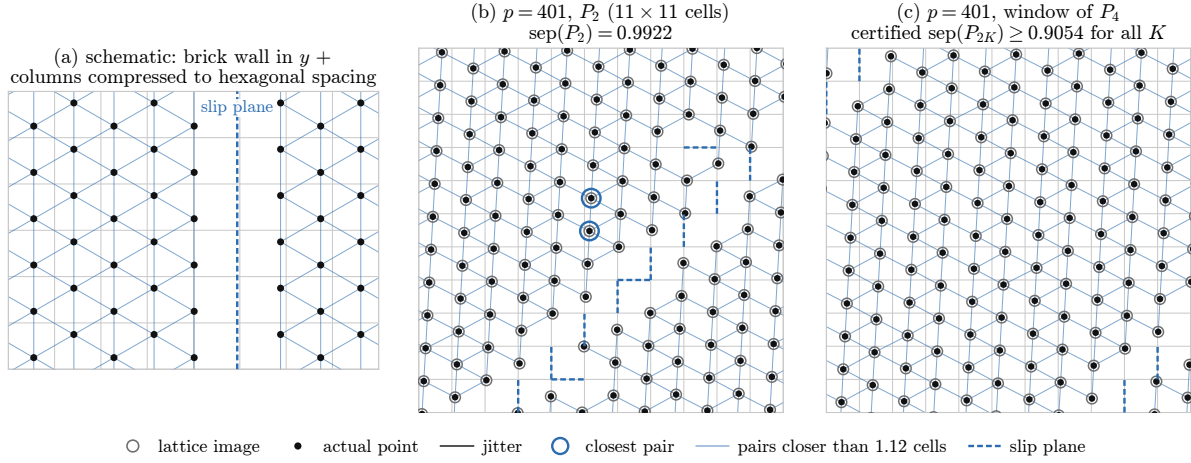


FIGURE 10. The hexagonal brick wall (Theorem 69), exact points from the generator matrices. (a) Schematic: the heights move by half a cell from one column of cells to the next, as in the brick wall, and the columns are compressed to the hexagonal spacing $\sqrt{3}/2$, so that all neighbour gaps are about 1; where the horizontal offset wraps around there is a slip plane. (b) $p = 401$, $(b, e) = (5, 1)$, the full level P_2 , 11×11 cells around the closest pair; thin lines join pairs closer than 1.12 cells. Exact $\text{sep}(P_2) = 0.9922$. (c) A window of the full level P_4 of the same sequence. Certified $\text{sep}(P_{2K}) \geq 0.9054$ for every K .

8.5. Windows and Skeleton Relations. The residue sequence certifies every prefix P_{sK-1} with constants tending to 1, and windows certify every full level with $1 - O(1/p)$. Can one sequence do both? For exact relations of bounded depth Corollary 58 excludes it. For windows the residue theorem still constrains the answer: every self-similar scramble satisfies a skeleton relation with correction terms, and the corrections move together with the full-level responses.

Lemma 71 (Every self-similar scramble satisfies a corrected skeleton relation). *Consider a self-similar scramble with scale θ and local multipliers φ_c . Put $v_c := 1/\varphi_c(a_c)$ and define the correction coefficients $\chi_{c,d} \in \mathbb{F}_q$ by the expansion of $1/\varphi_c$ in powers of the uniformizer at a_c ,*

$$\frac{1}{\varphi_c} = v_c \sum_{d \geq 0} \chi_{c,d} \left(\frac{w}{\theta} \right)^d, \quad \chi_{c,0} = 1.$$

Then for every $K \geq 1$ and every V with $\deg V \leq sK - 2$,

$$\sum_c v_c \left[y_{c,K-1}(V) + \sum_{d=1}^{K-1} \chi_{c,d} y_{c,K-1-d}(V) \right] = 0.$$

The residue sequence is the case of constant local multipliers, where all $\chi_{c,d}$ vanish and the relation is the skeleton relation of Lemma 35. For $s \geq 3$, Proposition 62(a) gives $v_c = \theta/\lambda_c$ and $\chi_{c,d} = \theta^d \psi_{c,d}$: the correction coefficients are the free digits of Proposition 63, up to the factor θ^d . With the *correction partial sums* $\Psi_c(j) := \sum_{d=1}^j \chi_{c,d}$ ($\Psi_c(0) = 0$), the relation certifies the prefixes P_{sK-1} as follows. For $B \geq 0$ let

$$\lambda_{\text{jit},B}(\Lambda) := \min_{0 \neq b \in \Lambda} \|(|b| - (1+B)\mathbf{1})_+\|_2 \geq \lambda_{\text{jit}}(\Lambda) - B\sqrt{s}.$$

Theorem 72 (Skeleton relations with bounded corrections). *Let $(y(V))$ be a digital $(0, s)$ -sequence over $\mathbb{F}_p$ and $K \geq 1$, and suppose that every point of P_{sK-1} satisfies the relation of Lemma 71 for some $v \in (\mathbb{F}_p^*)^s$ and $\chi_{c,d} \in \mathbb{F}_p$ (not necessarily coming from a self-similar scramble), where the centred representatives of the partial sums $\Psi_c(j) = \sum_{d=1}^j \chi_{c,d}$ lie in $[0, B]$ for $1 \leq j \leq K-1$. Then $\text{sep}(P_{sK-1}) \geq p^{-1/s} \lambda_{\text{jit}, B}(\Lambda_v)$.*

So bounded corrections cost an additive $B\sqrt{s}$ fine cells, not a factor; [18] calls the analogous coefficients of its skeleton digits faults. The sign condition $\Psi_c \geq 0$ is used in the proof, and it matters: for $s = 2$ and $p = 11, 17, 29, 37$, scrambles with corrections -1 have exact separations 0.02–0.08 at the first prefixes P_{2K-1} , where corrections $+1$ give 0.38–0.76, all above the bound of the theorem (exact computations, illustration only).

Proposition 73 (Windows and corrected skeleton relations cannot be selected together). *Consider a self-similar scramble over $\mathbb{F}_p$ with the notation of Lemma 71.*

- (i) *For every full level K , every step e and carry lengths l_c of the moving coordinates, the changes σ_c of the geometric digits satisfy $\sum_c v_c \sigma_c = -\sum_c e_c v_c \Psi_c(l_c)$.*
- (ii) *For every column c and depth l , the sum $O_c^{(l)} + \Psi_c(l)$ depends only on $v_c, \chi_{c,1}, \dots, \chi_{c,l-1}$, on θ and on the local multipliers of the other coordinates. So changing the correction coefficients $\chi_{c,d}$, $d \geq l$, moves the own response $O_c^{(l)}$ and the correction partial sum $\Psi_c(l)$ by equal and opposite amounts, and leaves the cross responses $X_{c' \leftarrow c}^{(l)}$ unchanged.*
- (iii) *Let W be product windows and $B \geq 0$, and suppose that every column c satisfies the joint covering condition $W_o^{(c)} + [0, B] = \mathbb{F}_p$: every line $\{(\xi - t, t) : t \in \mathbb{F}_p\}$, $\xi \in \mathbb{F}_p$, meets $W_o^{(c)} \times [0, B]$. Then $\text{LB}(W) \leq \sqrt{s} B/p$. If moreover Theorem 72 with this B certifies a positive bound for some Λ_v , then $B < p^{1/s} - 1$ and $\text{LB}(W) < \sqrt{s} (p^{1/s} - 1)/p$.*

By (ii), the free digit at depth l moves $(O_c^{(l)}, \Psi_c(l))$ along a line of direction $(1, -1)$, so a selection rule that keeps the column response in $W^{(c)}$ and $\Psi_c(l)$ in $[0, B]$ for every history, the analogue of condition (ii) of Proposition 64, needs the joint covering condition of (iii). (Not every line is reached by a history: at depth 1, and at depth 2 when $w''(a_c) = 0$, the sum takes one value only; so the covering of every line is a hypothesis, as in Proposition 64.) Such a joint selection certifies at the full levels at most the order of the inclusion bound $\lambda_{\text{jit}}(\Lambda_v)/p$ of the residue sequence (Remark 40), whatever B . *Scope:* Proposition 73(iii) concerns self-similar scrambles of one frame, full levels certified by the window bound of product windows with the covering of every line, and prefixes P_{sK-1} certified by Theorem 72 with a correction window maintained by the same covering. It does not exclude certificates from the actual responses along one specific choice of digits (covering only the lines that are actually reached, a choice that looks at later digits), non-product column windows, windows on several geometric digits, other certificates for the prefixes P_{sK-1} , or scrambles that are not self-similar (Section 11).

9. SMALL BASES AND COVERAGE BY DIMENSION

The constructions of Sections 5–8 need room in the base. A residue sequence needs a check vector with $\lambda_{\text{jit}}(\Lambda_v) > 0$, which exists only for $p > 2^s$ (Corollary 38); the staggered residue sequence has a positive bound only for $p > 2^s$ (Corollary 29); the block-periodic sequences start at $p = 3, 5, 7, 19$ for $s = 2, 3, 4, 5$ (Theorem 42); window constructions need several residues per window. In the bases 2, 3 and 4 none of them gives anything at every full level: base 2 is too small for all of them, and in base 3 the brick-wall bound $(p-3)/(2p)$ is 0.

This section takes a different route for the smallest bases. Instead of choosing responses, it chooses frames and multipliers for which the map $l \mapsto D_i(l)$ is computed by a small finite

automaton reading the base- q digits of l . The set of all responses is then finite and known exactly, and the digit relaxation at every level is one finite minimum. This gives closed forms in base 2 in dimension two (Theorem 76, which answers a question of Dick, Goda and Suzuki), base 3 in dimensions two and three, and base 4 in dimensions three and four. The price is that nothing is chosen digit by digit, and the constants fall quickly with the dimension. Section 9.4 reads the staggered residue sequence over prime-power fields, and Section 9.5 collects, dimension by dimension, which bases are covered and for which level family.

9.1. Lacunary Roots and Exact Response Sets. The responses are coefficients of power series built from the local roots (Proposition 22), so their structure is that of the roots (Figure 11(a)). In the Faure frame of an odd base the root $1 + u$, $u + u^2 = x$, has the signed Catalan numbers as coefficients, with no visible pattern. In characteristic two the same equation $u^2 + u = x$ is solved by the lacunary series $u = \sum_k x^{2^k}$, whose coefficients can be read off the binary digits of the exponent. Every algebraic power series over $\mathbb{F}_q$ is q -automatic by Christol's theorem [6, 7], so automata exist for every algebraic scramble; what a usable bound needs is that they are explicit and small. We use two families of frames whose roots are lacunary. In both, the places form one orbit of a group of affine maps $z \mapsto \alpha z + \beta$ that fix w and ∞ , so every place looks like every other.

Artin-Schreier frames. Let $H \subseteq \mathbb{F}_q$ be an additive subgroup with $|H| = s$ and let the places be the elements of H . Then $w = \wp_H(z) = \prod_{h \in H} (z - h) = \sum_i \wp_{H,i} z^{p^i}$ is an additive polynomial, with $\wp_{H,0} \neq 0$, and the translations by H fix it. For $H = \mathbb{F}_p$ these are the places $0, \dots, p-1$ of the Faure sequence in dimension $s = p$.

Kummer frames. Let $s = q - 1$ and let the places be the unit group, $a_c = \zeta^c$ for a generator ζ of $\mathbb{F}_q^*$, with $w = z^{q-1} - 1$; the multiplications by ζ fix it. For $q = 3$ the places are ± 1 , and $y = 2z - 1$ carries the Faure places $\{0, 1\}$ onto these ($y^2 - 1 = 4(z^2 - z)$ in $\mathbb{F}_3$).

Lemma 74 (Lacunary roots). *Let q be a power of the prime p .*

- (a) *In the Artin-Schreier frame of H the local roots are $z_c = a_c + U$, where $U \in x\mathbb{F}_q[[x]]$ is the solution of $\wp_H(U) = x$. It is supported on the powers of p and satisfies $U(x) = U(x^q) - \wp_H^b(x)$, where $\wp_H^b$ is the additive polynomial with $\wp_H^b(\wp_H(z)) = z^q - z$. For $H = \mathbb{F}_q$, $U = -\sum_{k \geq 0} x^{q^k}$.*
- (b) *In the Kummer frame the local roots are $z_c = a_c \tau$, where $\tau^{q-1} = 1 + x$, $\tau(0) = 1$, and*

$$\tau^{-1} = \prod_{i \geq 0} (1 + x^{q^i}), \quad \tau^{-1}(x) = (1 + x) \tau^{-1}(x^q);$$

$[x^n] \tau^{-1} = 1$ if every base- q digit of n is 0 or 1, and 0 otherwise.

In both cases the root has degree s over $\mathbb{F}_q(x)$.

Proof. (a) $\wp_H(a_c + U) = \wp_H(U) = x$, so $a_c + U$ is the local root at a_c . The recursion $U = \wp_{H,0}^{-1}(x - \sum_{i \geq 1} \wp_{H,i} U^{p^i})$ preserves support in the powers of p . Since $\wp_H^b \circ \wp_H$ is monic of degree q and vanishes on $\mathbb{F}_q$, it is $z^q - z$; hence $U^q - U = \wp_H^b(x)$, and $U^q = U(x^q)$. (b) $T = \prod_i (1 + x^{q^i})$ satisfies $T(x)^q = T(x^q) = T(x)/(1 + x)$, so $\tau = T^{-1}$ solves $\tau^{q-1} = 1 + x$, and $(a_c \tau)^{q-1} = \tau^{q-1}$. Expanding the product, x^n occurs once for each way of writing n as a sum of distinct powers of q . The degree: $\wp_H(Z) - x$ is linear in x , and $Z^{q-1} - (1 + x)$ is Eisenstein at $1 + x$. $\square$

Both relations are *Mahler equations*: the root at x is an affine function of the root at x^q , additive for translations and multiplicative for rotations. We take $\theta = 1$ and multipliers that are rational functions of the root, $g_c \in \mathbb{F}_q(x)(U)$ resp. $\mathbb{F}_q(x)(\tau)$. A scramble of these frames is *symmetric* if all coordinates use the same multiplier $g_c = g$; then $V(z) \mapsto V(z + h)$ (resp. $V(\zeta z)$) permutes the coordinates of every point and preserves every prefix.

To read a coefficient digit by digit we use the *Cartier operators* $\mathcal{C}_r(\sum_n c_n x^n) = \sum_n c_{qn+r} x^n$, $0 \leq r < q$. They satisfy $\mathcal{C}_r(A(x^q)F) = A\mathcal{C}_r F$ and

$$(6) \quad [x^l]F = [x^0] \mathcal{C}_{l_k} \cdots \mathcal{C}_{l_1} \mathcal{C}_{l_0} F \quad \text{for } l = \sum_{i \leq k} l_i q^i.$$

For example, $q = 3$ and $F = \tau^{-1}$: by Lemma 74(b), $\mathcal{C}_r \tau^{-1} = \mathcal{C}_r(1+x) \cdot \tau^{-1} = [r \leq 1] \tau^{-1}$, so reading the digits of n visits two states, τ^{-1} and 0, and a digit 2 kills the coefficient (Figure 11(c)). The responses behave in the same way. By Proposition 22, $D_i(l) = [x^l] \mathcal{H}_i$ with

$$\mathcal{H}_i := x^{-i} \mathcal{A}_{>i} \hat{G} = \frac{x^{-i} (I - \mathcal{A}_{\leq i} G)}{1 - x}, \quad \mathcal{A}_{\leq i} = \sum_{a \leq i} \mathcal{A}_a x^a.$$

Proposition 75 (Exact response sets). *Let a self-similar scramble have a frame matrix $\mathcal{A}(x)$ with entries in $\mathbb{F}_q(x)(\vartheta)$, where $\vartheta \in \mathbb{F}_q[[x]]$ has degree s' over $\mathbb{F}_q(x)$ and $\vartheta(x) = A(x)\vartheta(x^q) + B(x)$ with $A, B \in \mathbb{F}_q[x]$. Fix $j \geq 1$ and let $\vec{\mathcal{H}}$ be the vector of the series $\mathcal{H}_i$ and $x\mathcal{H}_i$, $i < j$. There is a finite set $\mathcal{S}$ of such vectors, containing $\vec{\mathcal{H}}$ and stable under every $\mathcal{C}_r$, with*

$$(D_i(l), D_i(l-1))_{i < j} = [x^0] \mathcal{C}_{l_k} \cdots \mathcal{C}_{l_0} \vec{\mathcal{H}} \quad (l \geq 1).$$

So the set $\{(D_i(l), D_i(l-1))_{i < j} : l \geq 1\}$ is exactly the set of values $[x^0]S$ over the states $S \in \mathcal{S}$ reached from $\vec{\mathcal{H}}$ by a digit word with a nonzero digit, and a finite breadth-first search computes it.

The proof (Appendix A.6) writes every series over one common denominator and shows that the Cartier operators keep the degrees of the numerators bounded.

The proposition applies to the Artin–Schreier frames with $\vartheta = U$, $A = 1$, $B = -\wp_H^b$, and to the Kummer frames with $\vartheta = \tau^{-1}$, $A = 1 + x$, $B = 0$ (Lemma 74). The pairs $(D_i(l), D_i(l-1))$ are what Lemma 23 needs for $q = 4$, through (8). With all $l \geq 1$ in place of $l \leq K$, Lemma 23 then gives one bound for every level with $q^K \geq 4$. The point of the proposition is exactness, not finiteness (which Christol’s theorem gives): a screen over carry lengths up to some bound can miss binding responses. For the base-3 sequence of Remark 78, the last of its 84 response tuples first appears at $l = 2469$.

9.2. Dimension Two. In base two every digital $(0, 2)$ -sequence is, up to a reordering inside each prefix, a scramble $(L_0, L_1 P_1)$ of the Sobol’ sequence [24]. Dick, Goda and Suzuki prove that neither one-sided choice, (L, P_1) or $(P_0, L P_1)$, is well separated, and ask whether a two-sided pair is [10, Section 4.2]; random linear scrambles of binary digital nets with fixed t have mesh ratio $O_P(\log N)$ under a uniform coincidence condition, which the Sobol’ prefixes satisfy [39, Thm. 5.5, Lem. 4.10]. The one-sided failure is an instance of Corollary 14: a coordinate that is left a radical inverse up to a scalar forces close pairs. The following explicit pair, which scrambles both coordinates, answers the question positively.

Theorem 76 (Base 2). *Let $u = \sum_{k \geq 0} x^{2^k} \in \mathbb{F}_2[[x]]$, so that $u^2 + u = x$, and let the digital sequence over $\mathbb{F}_2$ have the digits*

$$y_{0,n}(V) = [x^n] (1+x)(1+u) V(u), \quad y_{1,n}(V) = [x^n] \frac{u}{x} V(1+u),$$

that is, $C_0 = L_0$ and $C_1 = L_1 P_1$ with $L_0[n][k] = [x^n] (1+x)(1+u) u^k$ and $L_1[n][k] = [x^{n+1}] u^{k+1}$. It is a $(0, 2)$ -sequence in base 2, and for every $K \geq 1$

$$\text{sep}(P_{2K}) \geq \frac{\sqrt{2269618}}{4096} = 0.36780 \dots$$

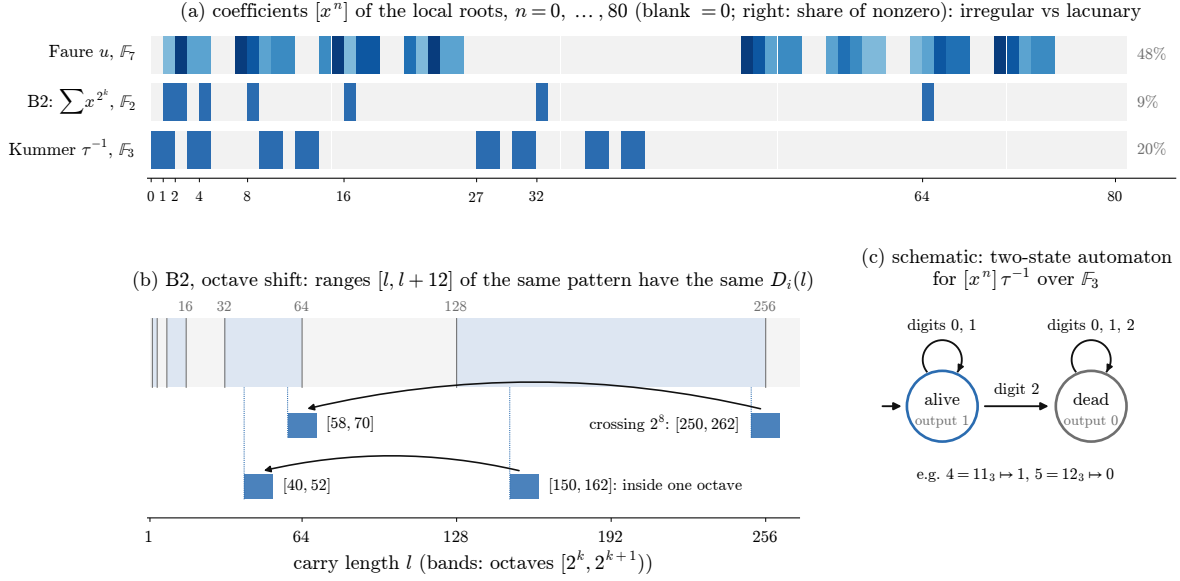


FIGURE 11. Finite carry patterns. (a) Coefficients $[x^n]$, $n \leq 80$, of three local roots (blank = 0): the Faure root u , $u + u^2 = x$, over $\mathbb{F}_7$ (signed Catalan numbers modulo 7), the base-2 root $u = \sum_k x^{2^k}$, and the Kummer root τ^{-1} over $\mathbb{F}_3$, whose coefficient is 1 exactly when n has no base-3 digit 2. All three are automatic by Christol's theorem; only the lacunary ones have a digit rule small enough for an explicit bound. (b) Long carries repeat short ones for the base-2 sequence (Lemma 77, $j = 12$): the responses depend only on the parity of l and the bits $[\log_2 n] \bmod 2$ on $[l, l + 12]$. A range crossing a power of two, $[250, 262] \ni 256$, has the partner $l - 3 \cdot 2^{k-1} = 58$, which crosses 64 at the same relative position; a range inside one octave, $[150, 162]$, has a partner $[40, 52]$ in an octave of the same parity. (c) The two-state automaton that reads the base-3 digits of n and outputs $[x^n] \tau^{-1}$ over $\mathbb{F}_3$.

Consequently $\delta(P_{[N]}) \geq 0.1839 N^{-1/2}$ for every $N \geq 2$, $h/\delta \leq 7.7$ along all N (15.4 in the convention of [10]), and every prefix P_m is k_m -separated in the sense of [10] (their κ_m) with $k_m = \lceil m/2 \rceil + 3$. In particular the sequence is quasi-uniform.

This is the Faure frame in base 2 ($w = z^2 + z$, roots $z_0 = u$, $z_1 = 1 + u$, $\theta = 1$) with $g_0 = (1 + x)(1 + u)$ and $g_1 = u/x = 1/(1 + u)$, an algebraic but not symmetric scramble of the Artin-Schreier frame $H = \mathbb{F}_2$. The multipliers are chosen so that one row of the inverse frame matrix is rational and the other lacunary:

$$(7) \quad \mathcal{A} = \begin{pmatrix} g_0 & g_0 u \\ g_1 & g_1(1 + u) \end{pmatrix}, \quad G = \mathcal{A}^{-1} = \begin{pmatrix} \frac{1}{1+x} & x \\ \frac{u}{x(1+x)} & 1 + u \end{pmatrix}.$$

The one-digit responses are $O_0^{(l)} = l \bmod 2$, $X_{0 \leftarrow 1}^{(l)} = 1$, $O_1^{(l)} = [\log_2 l] \bmod 2$ and $X_{1 \leftarrow 0}^{(l)} = \sum_{n < l} [\log_2(n + 2)] \bmod 2$. In base two the automaton of Proposition 75 can be replaced by a hand argument: long carries repeat the patterns of short ones.

Lemma 77 (Long carries repeat short ones). *For the sequence of Theorem 76 and $j \leq 12$, the tuples $(D_i(l))_{i < j}$, $l \geq 1$, take the same values as for $1 \leq l \leq 63$; for $j = 12$ there are 35 of them.*

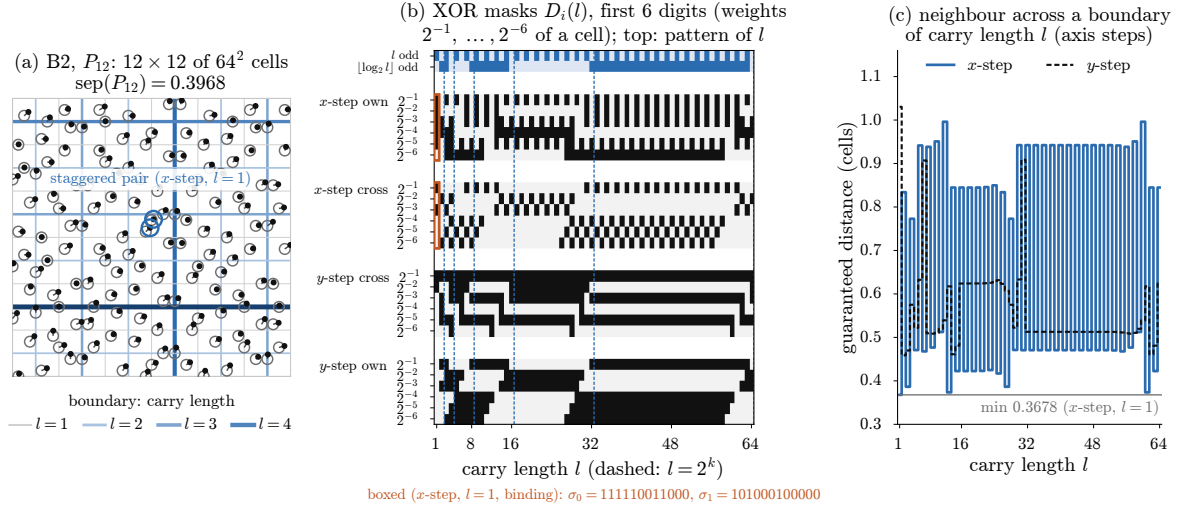


FIGURE 12. XOR staggering in base 2 (Theorem 76). (a) 12×12 of the 64×64 cells of P_{12} , with lattice images and jitter; cell boundaries shaded by carry length. The closest pair is a horizontal neighbour pair across a boundary of carry length 1, staggered vertically by the cross mask. (b) The masks $D_i(l)$ XORed onto the first six geometric digits (rows, worth $2^{-1}, \dots, 2^{-6}$ of a cell) for $l \leq 64$; the strips on top give the pattern of l (Lemma 77). Boxed: the binding case, a horizontal step with $l = 1$, with the 12-digit masks $\sigma_0 = 111110011000$ (own) and $\sigma_1 = 101000100000$ (cross). (c) The guaranteed distance across a boundary of carry length l (Lemma 23, $j = 12$); the minimum 0.3678 is the horizontal step with $l = 1$. Exact $\text{sep}(P_{12}) = 0.3968$.

The proof (Appendix A.6) reads the entries of $\hat{G}$ off the binary digits and maps every carry length $l \geq 64$ to a smaller one with the same responses.

Proof of Theorem 76. The sequence is a self-similar scramble of the Faure frame, so it is a $(0, 2)$ -sequence (Lemma 1) whose offset map is the same at every level (Proposition 22). By Lemma 77, Lemma 23 with $j = 12$ is a minimum over $35 + 35 + 2 \cdot 35^2$ cases (axis steps with one carry length, diagonal and antidiagonal steps with two). This exact computation (computer-assisted) gives $\text{LB}_{12} = \sqrt{2269618}/4096$, attained at the horizontal step with $l = 1$: the own change $\sigma_0 = 111110011000$ and the cross change $\sigma_1 = 101000100000$ give $f_{12}(1, \sigma_0) = 103/4096$ and $f_{12}(0, \sigma_1) = 1503/4096$. This covers $K \geq 2$; for $K = 1$, $\text{sep}(P_2) = 0.6334$. Lemma 2 with $q = 2$ and Remark 3 give $\delta(P_{[N]}) \geq (\text{LB}_{12}/2)N^{-1/2}$ and $h/\delta \leq 2\sqrt{2}/\text{LB}_{12} < 7.7$. Finally two points in a square of side 2^{-k_m} are less than $\sqrt{2} \cdot 2^{-k_m}$ apart, and $\sqrt{2} \cdot 2^{-\lceil m/2 \rceil - 3} < 0.1839 \cdot 2^{-m/2} \leq \delta(P_m)$. $\square$

Since $k_m \leq m/2 + 4$ and δ is measured on the torus, the sequence is well-separated, and toroidally well-separated, in the sense of [10, Def. 3.8], which is the property asked for in [10, Section 4.2].

Why it works. The offset map of a base-two sequence does not shift points by small real amounts: what is fixed per carry length is an $\mathbb{F}_2$ -mask XORed onto the geometric digits (Figure 12(b)). At the most common boundary, $l = 1$ in coordinate 0, the own mask can pull the neighbour almost onto the vertical line through the point. But the cross mask has a leading 1: the vertical offsets differ in their first digit, by $\pm \frac{1}{2}$ of a cell, corrected by the lower digits by at

most $\frac{1}{8} + \frac{1}{128}$ plus the jitter, so the two points stay at least $1503/4096 > 0.366$ of a cell apart vertically. Likewise every step of coordinate 1 flips the leading horizontal digit ($X_{0 \leftarrow 1}^{(l)} = 1$). This is the brick wall of Example 30 in XOR form: where the own mask could close the gap, the cross mask forces a stagger of about half a cell. The true separation is somewhat larger: $\text{sep}(P_m) = 0.3968$ for every even m from 12 to 26, against 0.0442 for the Sobol' sequence at $m = 12$ and 0.0007 at $m = 24$ (exact). The generator data, as a drop-in table of 32-bit direction numbers with a reference implementation, are in the archive (Appendix C.2).

Remark 78 (Base 3). In base three the Faure frame is the Kummer frame $\{\pm 1\}$, with the lacunary root $\tau = \sqrt{1+x}$ of Lemma 74(b), and Proposition 75 handles it as well. Take the roots $z_0 = \tau - 1$, $z_1 = 2 - \tau$ of $z^2 - z = x$, $\theta = 1$ and the multipliers $g_0 = -(1+x)(1-x+\tau)/(1-x)$, $g_1 = -(1+\tau)/\tau$. This self-similar scramble (L_0P_0, L_1P_1) of the Faure sequence in base 3 is a $(0, 2)$ -sequence (Lemma 1), and Proposition 75 with $\vartheta = \tau^{-1}$, $A = 1+x$, $B = 0$, $j = 6$ (a search of 190 states) gives exactly 84 response tuples; Lemma 23 over all steps and pairs of tuples gives $\text{LB}_6 = 0.266926$, attained at an antidiagonal step (computer-assisted). With $\text{sep}(P_2) = 0.5828$ this gives $\text{sep}(P_{2K}) \geq 0.2669$ for every $K \geq 1$: base three in dimension two at every full level, where Theorem 42(a) gives $\text{sep}(P_{4K}) \geq 1/3$ on the sparser level family $4\mathbb{N}$. The unscrambled Faure sequence in base 3 is not quasi-uniform [16] (Corollary 8); its separation falls to 0.016 at $m = 9$, while that of this scramble stays at 0.298 or more for even $m \leq 14$ (exact).

Corollary 79 (Every prime base, dimension two). *For every prime p there is an explicit closed-form scramble (L_0P_0, L_1P_1) of the Faure sequence in base p that is a quasi-uniform $(0, 2)$ -sequence with a bound at every full level: Theorem 76 for $p = 2$, Remark 78 for $p = 3$ and the brick wall (Theorem 32) for $p \geq 5$, with $\text{sep}(P_{2K}) \geq 0.3678$, 0.2669 and $(p-3)/(2p)$, respectively, for every K .*

For large primes the hexagonal brick wall improves the constant at every full level to $1 - 17/p$ (Corollary 70, $p > 3677$), and for every prime $p \geq 3$ the block-periodic residue sequence reaches $1 - 2/p$ at every level $m \in 4\mathbb{N}$ (Theorem 42(a)).

9.3. Dimensions Three and Four, Small Bases. The same method works with symmetric scrambles of the Artin–Schreier frames $H = \mathbb{F}_3$ and $H = \mathbb{F}_4$ and of the Kummer frame $\mathbb{F}_4^*$. In each case the multiplier is a short rational function of the root, found by an exhaustive screen over small families of such functions; the proofs are identical, and their finite parts are collected in Table 10.

Theorem 80 (Base 3, dimension 3). *Let $U = -\sum_{k \geq 0} x^{3^k} \in \mathbb{F}_3[[x]]$, so that $U^3 - U = x$, and $g = (1+x-U)/(1-x)$. The digital sequence over $\mathbb{F}_3$ with the digits $y_{c,n}(V) = [x^n] g(x) V(c+U(x))$, $c \in \mathbb{F}_3$, is a scramble of the Faure sequence (P_0, P_1, P_2) in base 3 and a $(0, 3)$ -sequence, and $\text{sep}(P_{3K}) \geq 0.05598$ for every $K \geq 1$. Consequently $\delta(P_{[N]}) \geq 0.0186 N^{-1/3}$ for all $N \geq 2$ and $h/\delta < 93$.*

Theorem 81 (Base 4, dimension 3). *Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, let $\tau^{-1} = \prod_{i \geq 0} (1 + x^{4^i}) \in \mathbb{F}_4[[x]]$, so that $\tau^3 = 1 + x$, and*

$$g = \frac{\omega^2(\tau + \omega)}{\tau + \omega^2} = 1 + x + \omega x^2 + \omega^2 x^3 + \omega^2 x^5 + \dots$$

The digital sequence over $\mathbb{F}_4$ with the digits $y_{c,n}(V) = [x^n] g(x) V(\omega^c \tau(x))$, $c = 0, 1, 2$, is a $(0, 3)$ -sequence in base 4, and $\text{sep}(P_{3K}) \geq 0.11293$ for every $K \geq 1$. Consequently $\delta(P_{[N]}) \geq 0.0282 N^{-1/3}$ for all $N \geq 2$ and $h/\delta < 61.4$. With the binary code of $\mathbb{F}_4$ it is a binary digital sequence, generated by XOR like the Sobol' sequence.

TABLE 10. The finite parts of the small-base theorems: depth j , number of distinct responses (per moving coordinate; in brackets the change columns after the $\mathbb{F}_4$ carry correction), bound LB_j for every level, the step attaining it (up to the symmetry of the frame), and the exact separation at the largest level we computed. All entries are exact computations; the responses are exact sets by Proposition 75 (Lemma 77 for base 2). Level family: all full levels, $\mathcal{M} = s\mathbb{N}$.

result	base, s	frame	j	responses	LB_j	minimising step; exact sep(P_m)
76	2, 2	Faure ($H = \mathbb{F}_2$)	12	35 tuples	0.367804	(1, 0), $l = 1$; 0.3968 ($m \leq 26$)
78	3, 2	Faure ($\mathbb{F}_3^*$)	6	84 tuples	0.266926	antidiagonal; 0.298 ($m = 14$)
80	3, 3	$H = \mathbb{F}_3$	8	85	0.055983	(1, -1, -1); 0.129 ($m = 15$)
81	4, 3	$\mathbb{F}_4^*$	8	32 (67)	0.112930	(0, 1, 1); 0.168 ($m = 12$)
82	4, 4	$H = \mathbb{F}_4$	5	64 (120)	0.030131	all four move; 0.101 ($m = 12$)

Theorem 82 (Base 4, dimension 4). *Let $U = \sum_{k \geq 0} x^{4^k} \in \mathbb{F}_4[[x]]$, so that $U^4 + U = x$, and $g = 1 + \omega U + U^2$. The digital sequence over $\mathbb{F}_4$ with the digits $y_{c,n}(V) = [x^n] g(x) V(c + U(x))$, $c \in \mathbb{F}_4$, is a $(0, 4)$ -sequence in base 4 and a binary digital sequence, and $\text{sep}(P_{4K}) \geq 0.03013$ for every $K \geq 1$. Consequently $\delta(P_{[N]}) \geq 0.0075 N^{-1/4}$ for all $N \geq 2$ and $h/\delta < 266$.*

Proof of Theorems 80, 81 and 82. By Lemma 74 the frames are the Artin–Schreier frames $H = \mathbb{F}_3$ ($w = z^3 - z$) and $H = \mathbb{F}_4$ ($w = z^4 + z$) with roots $c + U$, and the Kummer frame $\mathbb{F}_4^*$ ($w = z^3 - 1$) with roots $\omega^c \tau$; the multiplier is the same rational function of the root in every coordinate. (For Theorem 81, coordinate c reads $V(z) \omega^2(z - a_{c+1})/(z - a_{c+2})$ at $a_c = \omega^c$, indices modulo 3: the multiplier has its zero and its pole at the two other places.) So $t = 0$ by Lemma 1, and Proposition 75 gives the exact response sets of Table 10, with the carry correction (8) for $q = 4$. Lemma 23 over all steps and all combinations of response columns gives the values LB_j of the table (computer-assisted). For $q = 4$ this covers every $K \geq 1$; for $q = 3$ it covers $K \geq 2$, and $\text{sep}(P_3) = 0.4887$. Lemma 2 gives the rest. With $\mathbb{F}_4 = \mathbb{F}_2 \oplus \mathbb{F}_2 \omega$, multiplication by an element of $\mathbb{F}_4$ is an $\mathbb{F}_2$ -linear 2×2 block and addition is XOR of the codes, which gives the binary form. $\square$

Dick, Goda and Suzuki prove that the Faure sequence in base 3 is not quasi-uniform [10], and Goda, Hofer and Suzuki extend this to scrambles $(P_0, L_1 P_1, L_2 P_2)$ that leave the first coordinate unscrambled, and likewise in every prime base p in dimension p [16, Rem. 3] (Corollary 14 contains both). Theorem 80 scrambles all three coordinates (g is not constant), so it is outside the scope of these results and consistent with them.

The certified bounds in dimensions three and four are far below the exact separations of Table 10 because the binding steps involve long carries that the computable prefixes do not contain; explicit close pairs of points bracket the true infimum closely (Appendix C.4, which also explains why these bases work, Remark 97).

Base seven. At $p = 7$ in dimension three the residue sequences give nothing ($7 < 2^3$), and the block-periodic residue sequence covers only the levels $m \in 9\mathbb{N}$ (Theorem 42(b), $1 - 2/7$). Every full level is covered by a bound of a different kind, in which the admissible own response depends on the current cross responses of its column; it is given in Appendix B (Theorem 95: $\text{sep}(P_{3K}) \geq 1/7$ for every K , computer-assisted).

9.4. Prime-Power Bases. Apart from $q = 4$, the constructions above live over prime fields. The staggered residue sequence does not need this: its two lemmas use only the residue theorem, which holds over every field. What changes over $\mathbb{F}_q$, $q = p^r$ with $r \geq 2$, is the carry. Adding 1 to the integer cell index changes the finest digit by an element $\Delta(y)$ that depends on the digit (Remark 89), not by the constant 1, so the rank-1 rule of the staggered coordinate is read with

several possible increments. The resulting bound is a small finite minimum, and it depends on how the digits of $\mathbb{F}_q$ are encoded as integers.

Write $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$ for a monic irreducible f of degree r , and encode $\sum_{i < r} c_i x^i$ ($0 \leq c_i < p$) as the integer $\sum_i c_i p^i$ (the power-basis encoding of f , a natural identification in the sense of Section 2). With this encoding $\Delta(y)$ is one of the r elements $1, 1+x, \dots, 1+x+\dots+x^{r-1}$, according to the number of trailing digits $p-1$ of the code of y ; let $\mathcal{D}_f$ be this set. For weights $k \in (\mathbb{F}_q^*)^{s-1}$ put

$$\beta_q(k) = \min_{e \in \{-1, 0, 1\}^s \setminus \{0\}} f_1\left(e_{c_\star}, \sum_{c \in C} e_c k_c \Delta_c\right),$$

the minimum over all steps $e \in \{-1, 0, 1\}^s \setminus \{0\}$ and all $\Delta_c \in \mathcal{D}_f$ for the moving coordinates $c \in C$, with f_1 the one-digit function of Lemma 23 for this encoding.

Proposition 83 (Prime-power bases). *Let (s, q, f, k) be a row of Table 11. Read Definition 25 over $\mathbb{F}_q$ (any s distinct places in $\mathbb{F}_q$, any $\theta, \mu_\star \in \mathbb{F}_q^*$, the weights k), with the power-basis encoding of f . The result is a digital $(0, s)$ -sequence over $\mathbb{F}_q$ with*

$$\text{sep}(P_{sK}) \geq \beta_q(k) \quad \text{for every } K \geq 1,$$

with the value of the table; it is quasi-uniform, with $\delta(P_{[N]}) \geq (\beta_q(k)/q) N^{-1/s}$ for every $N \geq 2$. The evaluation of $\beta_q(k)$ is computer-assisted.

Proof. The proofs of Lemmas 26 and 27 use Lemma 21 and Lemma 1, which hold over every finite field; so the sequence is a digital $(0, s)$ -sequence over $\mathbb{F}_q$, and $y_{c_\star, K} = \sum_{c \in C} k_c y_{c, K-1}$ on P_{sK} for every K . In the language of Section 4 the responses of the staggered coordinate are constant, $D(l)[c_\star][c] = k_c$ and $D(l)[c_\star][c_\star] = 0$ for every $l \geq 1$. By (8) a step of coordinate c with carry length l , stopping at the digit y , therefore changes $r_{c_\star}$ by $\Delta(\bar{y})k_c$ if $l \geq 2$ (the wrap included) and by $\Delta(y)k_c$ if $l = 1$; in both cases by $\Delta_c k_c$ with $\Delta_c \in \mathcal{D}_f$. Lemma 23 with $j = 1$, keeping only the term of coordinate $c_\star$, gives $\text{sep}(P_{sK}) \geq \min(1, \beta_q(k)) = \beta_q(k)$ for every K with $q^K \geq 4$, which is every $K \geq 1$ since $q \geq 8$. The value $\beta_q(k)$ is a minimum over at most $3^s r^{s-1}$ terms, each a minimum over the q positions of enc differences, evaluated exactly (computer-assisted). The last statement is Lemma 2 with $\mathcal{M} = s\mathbb{N}$. $\square$

The bound uses one coordinate and one digit, as in Corollary 29, and it is small; the exact separations are several times larger (last column of Table 11; for $s = 3$ the smallest $\text{sep}(P_{[N]})$ over all N up to 10^7 is between 0.0144 ($q = 32$) and 0.1484 ($q = 49$), above β_q/q in every case). The proof uses the encoding only through the set $\mathcal{D}_f$ of increments $\Delta(y)$, so it holds for every bijection enc with $\mathcal{D}_f$ replaced by its set of increments. A zero is a zero of this bound, not a statement about the base: for $q = 8, 9$ in dimension three $\beta_q = 0$ for every digit code and every weight, for $q = 16, 27$ for every $\mathbb{F}_p$ -linear code; in dimension four $\beta_q = 0$ for $q = 16, 25, 27, 32, 64, 81$, and in dimension five for $q = 49$, for every power-basis encoding and every weight (exact computations). Other constructions and certificates with more digits are untried there.

9.5. Coverage by Dimension. Which bases admit a quasi-uniform digital $(0, s)$ -sequence with a certified bound, and on which level family? The answer collects the results of Sections 5–9. The level family matters: every family of this paper gives quasi-uniformity, but a denser family gives the better bound for every N (Lemma 2), and the full levels $\mathcal{M} = s\mathbb{N}$ are the classical choice. Table 12 and Figure 13 give the details.

Theorem 84 (Coverage). *In each of the following cases there is an explicit digital $(0, s)$ -sequence over $\mathbb{F}_q$ with a positive lower bound on $\text{sep}(P_m)$ for every m in the stated level family $\mathcal{M}$, and hence, by Lemma 2, a quasi-uniform one.*

TABLE 11. Proposition 83: the staggered residue sequence over $\mathbb{F}_q$, $q = p^r$, with the power-basis encoding of the monic irreducible f ; weights k by their codes; β_q is certified for every K ($\mathcal{M} = s\mathbb{N}$). For $s \leq 3$, f and k give the best value over all f and k (exhaustive); for $s = 4, 5$ they were found by search. Last column: exact $\text{sep}(P_3)$ for the places 0, 1, 2 (codes), $c_\star = 2$, $\theta = 1$. β_q depends on the encoding: for $q = 25$, $s = 2$ it ranges from $5/25$ ($x^2 + 2$) to $8/25$ ($x^2 + 3$), and for $q = 32$, $s = 3$ it is positive for 2 of the 6 irreducible quintics.

$s = 2$									
q	f	k	β_q	s	q	f	k	β_q	$\text{sep}(P_3)$
8	$x^3 + x + 1$	(2)	1/8	3	25	$x^2 + x + 2$	(9, 12)	2/25	0.1961
9	$x^2 + 1$	(3)	1/9		32	$x^5 + x^3 + x^2 + x + 1$	(12, 2)	1/32	0.1814
16	$x^4 + x + 1$	(2)	1/16		49	$x^2 + 1$	(21, 7)	5/49	0.3565
25	$x^2 + 3$	(10)	8/25		64	$x^6 + x + 1$	(42, 23)	2/64	0.1781
27	$x^3 + x^2 + 2x + 1$	(15)	5/27		81	$x^4 + 2x^3 + x^2 + x + 2$	(3, 9)	2/81	0.1848
32	$x^5 + x^3 + x^2 + x + 1$	(23)	7/32		121	$x^2 + 2x + 5$	(22, 54)	20/121	0.2719
49	$x^2 + 2x + 2$	(21)	19/49		125	$x^3 + 4x^2 + 4$	(45, 66)	14/125	0.2323
64	$x^6 + x^4 + x^3 + x + 1$	(45)	13/64		128	as for $s = 2$	(56, 95)	7/128	0.1767
81	$x^4 + x^2 + x + 1$	(31)	17/81	169	$x^2 + 4x + 9$	(51, 89)	35/169	0.2320	
121	$x^2 + 9$	(55)	53/121	4	49	$x^2 + 1$	(7, 16, 19)	1/49	–
125	$x^3 + 3x + 3$	(51)	44/125		121	$x^2 + x + 8$	(21, 31, 49)	7/121	–
128	$x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$	(95)	31/128		125	$x^3 + x + 1$	(2, 5, 10)	1/125	–
				5	121	$x^2 + 1$	(13, 28, 36, 47)	1/121	–
					169	$x^2 + 2$	(17, 58, 63, 83)	2/169	–

- (a) $s = 2$: every prime p , with $\mathcal{M} = 2\mathbb{N}$; the prime powers $q = 8, 9, 16, 25, 27, 32, 49, 64, 81, 121, 125, 128$, with $\mathcal{M} = 2\mathbb{N}$.
- (b) $s = 3$: $q = 3, q = 4, q = 7$ and every prime $p \geq 11$, with $\mathcal{M} = 3\mathbb{N}$; every prime $p \geq 5$, with $\mathcal{M} = 9\mathbb{N}$; the prime powers $q = 25, 32, 49, 64, 81, 121, 125, 128, 169$, with $\mathcal{M} = 3\mathbb{N}$. In particular every prime base $p \geq 3$ is covered; $p = 5$ only with $\mathcal{M} = 9\mathbb{N}$.
- (c) $s = 4$: $q = 4, 49, 121, 125$ and every prime $p \geq 17$, with $\mathcal{M} = 4\mathbb{N}$; every prime $p \geq 7$, with $\mathcal{M} = 16\mathbb{N}$.
- (d) $s = 5$: $q = 121, 169$ and every prime $p \geq 37$, with $\mathcal{M} = 5\mathbb{N}$; every prime $p \geq 11$, with $\mathcal{M} = 25\mathbb{N}$.
- (e) $s = 6$: every prime $p \geq 17$, with $\mathcal{M} = 36\mathbb{N}$; $s = 7$: $p = 17, 19, 23$ and every prime $p \geq 31$, with $\mathcal{M} = 49\mathbb{N}$.
- (f) every $s \geq 2$: every prime $p > 2^s$, with $\mathcal{M} = s\mathbb{N}$ and, by a second sequence, with $\mathcal{M} = s\mathbb{N} - 1$; both are closed forms with written proofs.

Proof. Each case is a cited result; Table 12 lists the construction, the bound and the kind of proof for each. (f) Corollary 29 (staggered residue sequence, $\mathcal{M} = s\mathbb{N}$) and Corollary 37 with Corollary 38 (residue sequence, $\mathcal{M} = s\mathbb{N} - 1$), both for every prime $p > 2^s$. (a) $p = 2$: Theorem 76; $p = 3$: Remark 78 (computer-assisted), and Theorem 42(a) with $\mathcal{M} = 4\mathbb{N}$ (proof); $p \geq 5$: Theorem 32. The prime powers: Proposition 83. (b) $q = 3$: Theorem 80; $q = 4$: Theorem 81; $q = 7$: Theorem 95; $p \geq 11$: case (f), since $11 > 2^3$. $\mathcal{M} = 9\mathbb{N}$: Theorem 42(b), for every prime $p \geq 5$. The prime powers: Proposition 83. (c) $q = 4$: Theorem 82; $q = 49, 121, 125$: Proposition 83; $p \geq 17$: case (f). $\mathcal{M} = 16\mathbb{N}$: Theorem 42(c) (written proof for $p \geq 29$, exact evaluation for $7 \leq p \leq 109$). (d) $q = 121, 169$: Proposition 83; $p \geq 37$: case (f), since 37 is the least prime above 2^5 . $\mathcal{M} = 25\mathbb{N}$: Theorem 42(d), computer-assisted (the written proof of (c) covers $p \geq 84$). (e) Theorem 42(d), computer-assisted. $\square$

TABLE 12. Coverage by dimension (Theorem 84): base, construction, level family $\mathcal{M}$ (the exponents m with a certified bound on $\text{sep}(P_m)$), the bound, and the kind of proof (“c.a.”: computer-assisted, with the scope stated in the cited result). The bound for every N is $\text{LB } q^{-\Delta_{\mathcal{M}}/s}$ with $\Delta_{\mathcal{M}} = s$ for $\mathcal{M} = s\mathbb{N}$ and $s\mathbb{N} - 1$ and $\Delta_{\mathcal{M}} = s^2$ for $\mathcal{M} = s^2\mathbb{N}$ (Lemma 2). $\rho = \lfloor p^{1/s} \rfloor$. For $s = 4, 5$ the written proof of Theorem 42(c) gives $1 - 6/p$ and $1 - 17/p$ from $p = 29$ and 84 on. Constructions certified at every full level with constants tending to 1 from large primes on (staggered windows, Section 8) are not repeated here.

s	base	construction	$\mathcal{M}$	$\text{sep}(P_m) \geq$	proof
2	$q = 2$	Thm. 76	$2\mathbb{N}$	0.3678	c.a.
	$q = 3$	Rem. 78	$2\mathbb{N}$	0.2669	c.a.
	$p \geq 5$	brick wall, Thm. 32	$2\mathbb{N}$	$(p-3)/(2p)$	proof
	$p \geq 5$	residue seq., Cor. 37	$2\mathbb{N} - 1$	$(\rho-1)p^{-1/2}$	proof
	$p \geq 3$	block-periodic, Thm. 42(a)	$4\mathbb{N}$	$1 - 2/p$	proof
	$q = 8, \dots, 128$	Prop. 83	$2\mathbb{N}$	Tab. 11	c.a.
3	$q = 3$	Thm. 80	$3\mathbb{N}$	0.05598	c.a.
	$q = 4$	Thm. 81	$3\mathbb{N}$	0.11293	c.a.
	$p = 7$	Thm. 95	$3\mathbb{N}$	$1/7$	c.a.
	$p \geq 11$	stagg. residue, Cor. 29	$3\mathbb{N}$	$(\lfloor p/4 \rfloor - 1)/p$	proof
	$p \geq 11$	residue seq., Cor. 37	$3\mathbb{N} - 1$	$(\rho-1)p^{-1/3}$	proof
	$p \geq 5$	block-periodic, Thm. 42(b)	$9\mathbb{N}$	$1 - 2/p$	proof
	$q = 25, \dots, 169$	Prop. 83	$3\mathbb{N}$	Tab. 11	c.a.
4	$q = 4$	Thm. 82	$4\mathbb{N}$	0.03013	c.a.
	$p \geq 17$	stagg. residue, Cor. 29	$4\mathbb{N}$	$(\lfloor p/8 \rfloor - 1)/p$	proof
	$p \geq 17$	residue seq., Cor. 37	$4\mathbb{N} - 1$	$(\rho-1)p^{-1/4}$	proof
	$p \geq 7$	block-periodic, Thm. 42	$16\mathbb{N}$	$1 - 4/p$ ($p \geq 11$)	c.a.
	$q = 49, 121, 125$	Prop. 83	$4\mathbb{N}$	Tab. 11	c.a.
5	$p \geq 37$	stagg. residue, Cor. 29	$5\mathbb{N}$	$(\lfloor p/16 \rfloor - 1)/p$	proof
	$p \geq 37$	residue seq., Cor. 37	$5\mathbb{N} - 1$	$(\rho-1)p^{-1/5}$	proof
	$p \geq 11$	block-periodic, Thm. 42	$25\mathbb{N}$	$1 - 8/p$ ($p \geq 23$)	c.a.
	$q = 121, 169$	Prop. 83	$5\mathbb{N}$	Tab. 11	c.a.
6; 7	see (e)	block-periodic, Thm. 42	$36\mathbb{N}; 49\mathbb{N}$	Tab. 9	c.a.
s	$p > 2^s$	stagg. residue, Cor. 29	$s\mathbb{N}$	$(\lfloor p/2^{s-1} \rfloor - 1)/p$	proof
	$p > 2^s$	residue seq., Cor. 37	$s\mathbb{N} - 1$	$(\rho-1)p^{-1/s}$	proof
	$p \geq 5a_s^* + 4$	block-periodic, Thm. 42(c)	$s^2\mathbb{N}$	$1 - (a_s^* + 1)/p$	proof ($s \geq 4$)

What is not covered. Bases $q < s$ are impossible: a $(0, s)$ -sequence in base q exists only for $s \leq q$ [31]. Among the possible bases the following are not covered by this paper, and we do not claim that they cannot be: the prime powers that are not in Table 11, except $q = 4$ for $s = 3, 4$ (for $q = 8, 9, 16, 27$ in dimension three the bound of Proposition 83 is 0, for every encoding resp. every $\mathbb{F}_p$ -linear one); base 5 in dimension three at every full level (Remark 85); and for $s \geq 4$ the primes $s \leq p < 2^s$ at every full level. On the levels $s^2\mathbb{N}$ these primes are covered from $p = 7, 11, 17$ on for $s = 4, 5, 6$, for $s = 7$ at $p = 17, 19, 23$ and $p \geq 31$, and for $s \geq 8$ where the proof range $p \geq 5a_s^* + 4$ of Theorem 42(c) starts below 2^s (not for $s = 8, 9, 10$). Whether residue sequences are quasi-uniform for $s \leq p < 2^s$ is not addressed (Section 11).

Remark 85 (Base five in dimension three). For $p = 5$ and $s = 3$, Theorem 42(b) gives $\text{sep}(P_{9K}) \geq 3/5$ for every K (exact $\text{sep}(P_9) = 0.6211$), and hence $\delta(P_{[N]}) \geq (3/5)5^{-3}N^{-1/3}$ for every N . A certificate at every full level is open. What was tried: (i) the ordered windows

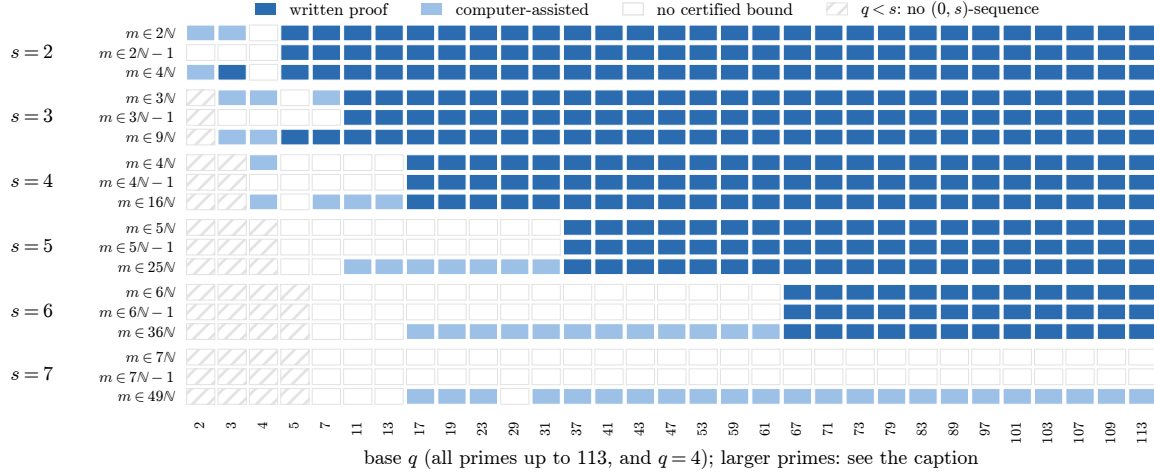


FIGURE 13. Coverage for $s = 2, \dots, 7$ (Theorem 84). Each row is a level family: all full levels $s\mathbb{N}$, the prefixes $s\mathbb{N}-1$ one digit before them, and every s -th full level $s^2\mathbb{N}$ (which is contained in $s\mathbb{N}$, so every base covered in the first row is covered in the third). Dark: a written proof covers this base; light: computer-assisted only (the small-base theorems of this section, Theorem 95, the exact evaluations of Theorem 42(c) below its proof range, and Theorem 42(d)); hatched: no $(0, s)$ -sequence exists in base $q < s$. Every prime above 113 is covered as in the last column, except for $s = 7$, where the full levels are covered from $p = 131$ on. Base 5 in dimension three is certified only on $9\mathbb{N}$.

of an earlier version of this work (shown there to give no positive bound at $p = 5$); (ii) the symmetric frames of this section have no three-dimensional instance over $\mathbb{F}_5$, since three places cannot form one orbit of a subgroup of the affine group of $\mathbb{F}_5$, whose order 20 is prime to 3; (iii) the staggered residue sequences have $\beta(k) \leq 0$ at $p = 5$ (Corollary 29), and among all their parameters up to the affine symmetries of $\mathbb{F}_5$ (128 choices of c_* , θ and the weights) the best keeps $\text{sep}(P_{3K}) \geq 0.30$ for $K \leq 4$ (exact), but at deeper levels there are explicit close pairs: $\text{sep}(P_{216}) \leq 0.0047$ for the choice that is best at $K \leq 4$, and $\text{sep}(P_{300}) \leq 2.9 \cdot 10^{-6}$ for another (exact computations of the two points; whether any of them is quasi-uniform is open); (iv) for one-digit certificates that cover every possible cross response (the graph rule of Appendix B and window coverings), and for several classes of two-digit certificates (ordered product windows as in (i) on 192 relaxed instances, two further window classes on single instances, a frame-independent two-digit graph rule), a SAT solver reported that no positive bound exists in the instances solved; no independently checked certificate of these results was produced, so they are evidence about these classes only. General two-digit windows, certificates with more digits, and other constructions remain unexplored.

10. PRACTICE

The sequences of this paper are digital sequences with fixed generator matrices, generated like the Sobol' and Faure sequences. This section says what they cost, how they compare at the numbers of points one can actually use, how to randomise them without losing the bound, and what their Hammersley lifts give as nets.

10.1. Implementation and Cost. A point is a matrix-vector product over $\mathbb{F}_q$ in each coordinate. For the residue sequences of Section 5 the matrices are closed forms: each entry is one

TABLE 13. The worst normalised separation $\mathcal{J} = \min_{64 \leq N \leq 2^{23}} \delta(P_{[N]})N^{1/3}$ in dimension three (exact, toroidal), and the certified bounds (truncated). Top: residue sequences $\mathcal{R}_v$ (Definition 33; data: places, θ , v), each the best of 600 candidates scanned for $\mathcal{J}$; their certified bound holds at $N = p^{3K-1}$ for every K (Theorem 36), at the full levels only the inclusion bound $\lambda_{\text{jit}}(\Lambda_v)/p$ is certified (Remark 40), and for every N the bound is LB/p (Corollary 38). Bottom: alternatives; random linear scrambles are $C_c = L_c P_{a_c}$ with random lower-triangular L_c .

sequence	p data	$\mathcal{J}$	certified $\text{sep}(\cdot) \geq$		
			P_{3K-1}	P_{3K}	$P_{[N]}$, all N
residue sequence	13 (2, 9, 10), 12, (5, 3, 6)	0.248	0.425	0.076	0.032
	17 (2, 9, 6), 12, (4, 10, 16)	0.235	0.388	0.058	0.022
	23 (18, 22, 15), 5, (4, 14, 20)	0.251	0.497	0.061	0.021
	31 (8, 0, 16), 9, (10, 30, 7)	0.267	0.636	0.064	0.020
Faure (best: $p = 11$)	7–31	0.059–0.140	–	–	–
random linear scrambles	31 median / best of 150	0.117 / 0.217	–	–	–
Sobol’ / Owen-scrambled	2 3 seeds (Owen)	0.035 / 0.015–0.039	–	–	–

coefficient of a power series over $\mathbb{F}_p$,

$$C_c[n][i] = v_c^{-1} \theta^{n+1} [(z - a_c)^n] \frac{z^i}{w_c(z)^{n+1}},$$

computed once by truncated power-series arithmetic; a sequence is given by its places, its scale θ and its check vector v . In base 2 a digit vector is a machine word and the product is an XOR of columns. The sequence of Theorem 76 is therefore the Sobol’ algorithm with a different table: the archive (Appendix C.2) lists 32-bit direction numbers that replace the first two dimensions of a Sobol’ table, Gray-code order permutes points only inside blocks of length 2^m and keeps every bound, and the cost is that of the Sobol’ sequence. The sequences of Theorems 81 and 82 over $\mathbb{F}_4$ are binary sequences as well. In a prime base p one stores the multiples of every generator column; a point costs $\lceil \log_p N \rceil$ table lookups and additions per coordinate and one reduction modulo p per digit, whatever the matrices. With random access to the first 2^{23} points, a straightforward implementation takes 31 and 43 nanoseconds per three-dimensional point in base 31 and base 13, against 4 to 8 for an XOR sequence (one core of an Apple M4; informal timing, unoptimised code), small next to evaluating an integrand such as a light path. One table serves every number of points.

10.2. What the Bounds Give at Reachable Sizes. In dimension three there is exactly one full level below 2^{23} for $17 \leq p \leq 203$, and the residue sequences are certified one digit before each full level, at $N = p^2$ and $N = p^5$; for $p = 31$ only $N = p^2$ lies below 2^{23} . What matters in practice is $\text{sep}(P_{[N]})$ at every N . Table 13 and Figure 14 report its exact minimum

$$\mathcal{J} := \min_{64 \leq N \leq 2^{23}} \text{sep}(P_{[N]})$$

for four residue sequences and for the usual alternatives.

Against what is used by default the gain is large: $\mathcal{J} = 0.235$ to 0.267 , six to eighteen times the Owen-scrambled Sobol’ sequence, whose $\text{sep}(P_{[N]})$ keeps decaying (Figure 14), and 1.7 to 1.9 times the best plain Faure sequence. Each residue candidate is scored on the full range: per prime 600 candidates, half with check vectors from the 20 best classes by λ_{jit} , a tenth with

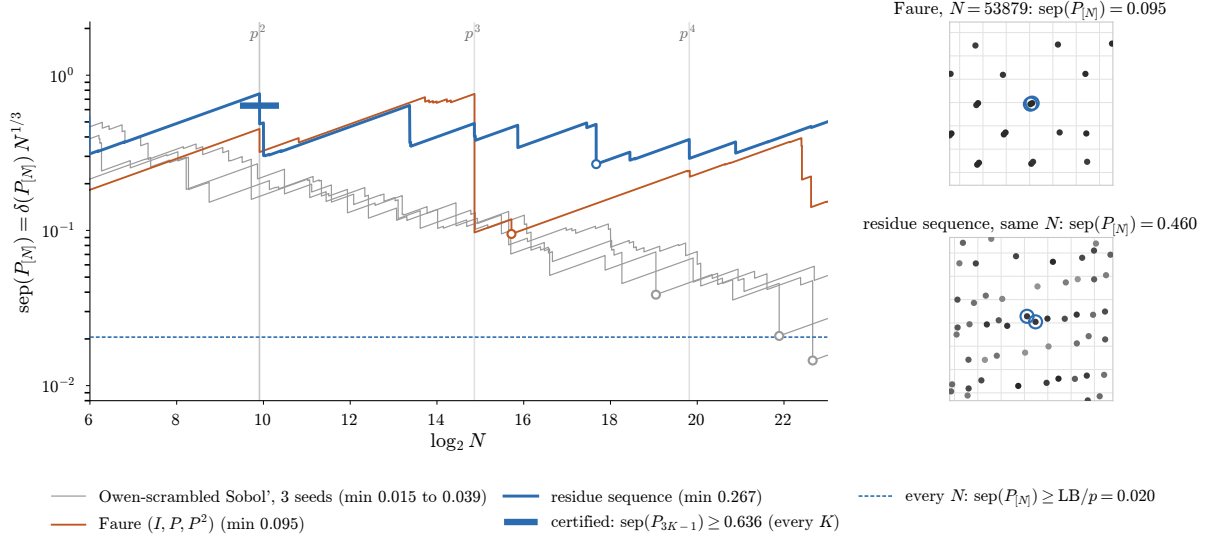


FIGURE 14. Exact $\text{sep}(P_{[N]}) = \delta(P_{[N]}) N^{1/3}$ for every $N \leq 2^{23}$ in dimension three, $p = 31$. Blue: the residue sequence of Table 13 (places $(8, 0, 16)$, $\theta = 9$, $v = (10, 30, 7)$); its certified bound $\text{sep}(P_{3K-1}) \geq 0.636$ for every K (bar at $N = p^2$; the next certified size p^5 lies beyond 2^{23}), and $\text{sep}(P_{[N]}) \geq 0.020$ for every N (dashed; Corollary 38). Orange: Faure (I, P, P^2) . Grey: Owen-scrambled Sobol', three seeds. Open dots: the minimum over $64 \leq N \leq 2^{23}$: 0.267 at $N = 208\,652$, 0.095 at $N = 53\,879$, and 0.015–0.039. Right: a slab one mean spacing $N^{-1/3}$ thick around the closest pair at $N = 53\,879$, where the Faure sequence is worst, 7×7 mean spacings, grey level = depth in the slab: the new Faure points land next to old ones (21 points in the slab instead of about 49), the residue sequence stays spread (53 points, $\text{sep}(P_{[N]}) = 0.460$). At its first full level $N = p^3$ the Faure sequence is better (0.757 against 0.489). Minimum distance only; no integration test.

Korobov vectors, the rest with random check vectors with $\lambda_{\text{jit}} > 0$, each with random places, scale and scaling of v . In scans of this kind the best residue sequences also matched or beat the best ordered window systems of an earlier version of this work (certified at every full level there) by 7 to 12% in $\mathcal{J}$ (a tie at equal search effort at $p = 13$); those systems are in the data archive. Against a searched scramble without a certified bound the gain is of the same size: the best of 150 random linear scrambles at $p = 31$ reaches 0.217.

Where the minimum is attained is telling: at $p = 13, 17, 23$ it is just after a certified size or a multiple of one, at $N = 13^5 + 59$, $2 \cdot 17^5 + 44$ and $23^5 + 415$, when the first points of the next, uncertified, block of p^5 points arrive. What moved $\mathcal{J}$ was the choice of places, scale and check vector; the larger certified constant raised the median of the scan a little at $p = 31$ and not at $p = 23$. The other residue constructions were scanned as well (exact, illustration): the best certified staggered residue sequences reach $\mathcal{J} = 0.191, 0.209, 0.212, 0.246$, and the block-periodic sequence of Theorem 42, whose certified sizes p^{9K} all lie beyond 2^{23} at these primes, reaches only 0.062 to 0.146 in this range. The generator matrices of the four residue sequences are archived (Appendix C). In dimension two the same picture holds for the sequence of Theorem 76: over $N \leq 2^{22}$, the range of our Owen runs, its smallest $\delta(P_{[N]})\sqrt{N}$ is above 0.2 (proved: 0.1839), against a median of 0.009 over 8 seeds of the Owen-scrambled Sobol' sequence.

10.3. Randomisation. Randomised quasi-Monte Carlo and rendering need many independent copies of a sampler and unbiased estimates. Owen scrambling redraws every digit below the stratum independently; it makes every (t, s) -sequence almost surely non-quasi-uniform [39], and it would undo the constructions of this paper. Digital shifts keep the certified bounds. A shift translates the digit vectors, the same translation for every point; it neither repairs a classical sequence (Remark 15) nor destroys the certificates here.

Lemma 86 (Digital shifts). *Let q be prime, or $q = 2^r$ with an $\mathbb{F}_2$ -linear code enc. Let $(y(V))$ be a digital $(0, s)$ -sequence over $\mathbb{F}_q$ and $\varsigma = (\varsigma_{c,n})$ any array of digits in $\mathbb{F}_q$. The sequence with the digits $y_{c,n}(V) + \varsigma_{c,n}$ is a $(0, s)$ -sequence, and:*

- (a) *every bound $\text{sep}(P_{sK}) \geq \min(1, \text{LB}_j)$ that Lemma 23 gives for the unshifted sequence holds for the shifted prefix P_{sK} , and so does every lower bound for LB_j , such as the one-digit form ($j = 1$) of Theorem 42(iii) and its one-coordinate form in Theorem 28;*
- (b) *if $q = p$ is prime and the unshifted sequence is a residue sequence $\mathcal{R}_v$, then for every $K \geq 1$ the fine cells occupied by the shifted prefix P_{sK-1} are the elements $\hat{n}$ of $[0, p^K)^s$ with $\sum_c v_c \hat{n}_c \equiv \sum_c v_c \varsigma_{c,K-1} \pmod{p}$, each holding one point, and $\text{sep}(P_{sK-1}) \geq p^{-1/s} \lambda_{\text{jit}}(\Lambda_v)$.*

In particular the bounds of Theorems 28, 42, 76, 80, 81, 82 and 95, of Remark 78, and of the window constructions (all obtained from Lemma 23), and of Theorem 36 hold for every digitally shifted copy, at the same levels; and if the unshifted bounds hold for every K with $q^K \geq 4$, the bounds of Lemma 2 hold for the shifted sequence for every $N > q^{s(K_0-1)}$, where K_0 is the least K with $q^K \geq 4$; for $q \geq 4$, and for (b), this is every $N \geq 2$.

Proof. A shift maps every elementary box onto one of the same shape, so nets go to nets.

(a) At level K a point with cell digits n and geometric digits R becomes one with cell digits $n + \varsigma_{\text{cell}}$ and geometric digits $R + \varsigma_{\text{geo}}$, so the shifted offset map is affine with the same linear part. Let the shifted index of coordinate c' step by $+1$ with carry length l , stopping at a digit y' . The digits below change from $\bar{y}$ to 0 and that digit from y' to $y' + \Delta(y')$; since the shift is additive, the unshifted digits change by the same amounts. This is the carry pattern of (8) with the digit y' , so the geometric digits change by the expression of Lemma 23 with $y_{c'} = y'$; the wrap is $l = K$, $y' = \bar{y}$. Lemma 23 minimises over all digits $y_{c'}$, all carry lengths and all positions R , among which are the shifted ones.

(b) For a prime base the last base- p digit of the fine-cell index $\hat{n}_c$ of a point of the shifted prefix is $y_{c,K-1}(V) + \varsigma_{c,K-1}$. By Lemma 35, $\sum_c v_c y_{c,K-1}(V) = 0$ for $\deg V \leq sK - 2$, so $\sum_c v_c \hat{n}_c \equiv \sum_c v_c \varsigma_{c,K-1} \pmod{p}$. The shifted prefix is a $(0, sK - 1, s)$ -net, so, as in the proof of Theorem 36(i), distinct points lie in distinct fine cells; there are p^{sK-1} points and exactly p^{sK-1} fine cells with this residue, so every such cell is occupied. For two points in the fine cells $\hat{n}$ and $\hat{n}'$ let b be the representative of $\hat{n}' - \hat{n}$ modulo p^K in $(-p^K/2, p^K/2]^s$. The shift cancels in the difference of the last digits, so $\sum_c v_c b_c \equiv 0 \pmod{p}$, that is $b \in \Lambda_v$, and $b \neq 0$. The rest is the proof of Theorem 36(ii), which uses only $b \in \Lambda_v \setminus \{0\}$ and the fact that each point lies in the closure of its fine cell.

The last statement is Lemma 2, applied to the shifted sequence, a $(0, s)$ -sequence, with $\mathcal{M} = \{sK : q^K \geq 4\}$ in (a) and $\mathcal{M} = s\mathbb{N} - 1$ in (b). $\square$

Part (a) does not cover Theorem 72, whose correction terms are not of the form of Lemma 23; we have not checked whether its bound survives a shift. In practice: XOR one random word per coordinate into every point in base 2 and over $\mathbb{F}_4$; add one random digit vector modulo p in a prime base. The shift must be additive in $\mathbb{F}_q$: digitwise addition modulo 4 of the codes is not an $\mathbb{F}_4$ -shift, and a non-affine permutation of a geometric digit, which still preserves the net property, can break the offset map (it brought the brick wall at $p = 5$ down to $\text{sep}(P_6) = 0.068$,

below its certified bound 0.2). The lemma keeps the certified bound, not the exact separation, and a typical shift comes close to the bound, which is the worst case over the positions R (for Theorem 76, twelve random shifts all gave $\min_{4 \leq m \leq 20, m \text{ even}} \text{sep}(P_m) \in [0.3680, 0.3681]$, against 0.3678). A uniformly random digital shift makes each point uniformly distributed (up to the digits used) and gives unbiased estimators [11], with the bound of every copy certified.

10.4. Hammersley Lifts. Hammersley's construction adds the index as a coordinate: the *Hammersley lift* $\hat{P}_m = \{(\iota(V)p^{-m}, y(V)) : \deg V < m\} \subset [0, 1)^{s+1}$ of a (t, s) -sequence is a $(t, m, s+1)$ -net [31, Lemma 4.22]. The frame nets of [18] (such as $\mathcal{P}_{k,q}$) have this shape, with the index read at the place ∞ , but with a scramble that depends on m , the index coordinate included. We measure $\delta(\hat{P}_m)N^{1/(s+1)}$, toroidal in all $s+1$ coordinates, as [18] does. A *slab* is the set of points whose first coordinate lies in one interval $[ap^{-K_0}, (a+1)p^{-K_0})$: an aligned block of p^{m-K_0} indices.

Proposition 87 (What the lift inherits). *Let $(y(V))$ be a digital $(0, s)$ -sequence over $\mathbb{F}_p$, $m \geq 1$ and $0 \leq K_0 \leq m$. (i) $\hat{P}_m$ is a digital $(0, m, s+1)$ -net. (ii) In its last s coordinates every slab is a digitally shifted copy of P_{m-K_0} , so every bound that Lemma 86 transfers to shifted copies holds inside each slab. In particular, at the primes where the theorems hold, two points of one slab are at distance at least $\text{LB}'N^{-1/(s+1)}$, where LB' is the bound of Theorem 28 for the staggered residue sequence $(\frac{p-3}{2p})$ for the brick wall at $m = (s+1)K$, $K_0 = K$; $p^{-1/(s+1)}\lambda_{\text{jit}}(\Lambda_v)$ for the residue sequence at $m = (s+1)K - 1$, $K_0 = K$; and $\text{LB}(F)$ for the block-periodic sequence at $m = s(s+1)K$, $K_0 = sK$.*

Proof. (ii) A slab consists of the indices $V = U + z^{m-K_0}A$, A fixed, $\deg U < m - K_0$; by linearity $y(V) = y(U) + y(z^{m-K_0}A)$, a shift of P_{m-K_0} . The three cases are Lemma 86(a) (one-coordinate form) for P_{sK} , (b) for P_{sK-1} and (a) (one-digit form) for P_{s^2K} , rescaled to $N = p^m$ points in dimension $s+1$. (i) A box with d_0 digits in the first coordinate and $\sum_c d_c = m$ is contained in one slab with $K_0 = d_0$, a shifted $(0, m - d_0, s)$ -net by (ii); a shift maps boxes to boxes of the same shape, so the box holds one point. The net is digital: the first coordinate has the matrix that reverses the m index digits, the others the generator matrices restricted to the columns $0, \dots, m-1$. $\square$

What the lift loses. The sequence keeps points of order $N^{-1/s}$ apart inside an aligned block of N indices; the lift needs the larger distance $N^{-1/(s+1)}$ between any two points whose indices differ by at most about $N^{s/(s+1)}$, aligned or not. Two indices on either side of a long carry share an aligned block only at a much higher level, where the sequence guarantees much less; for special carry lengths their index polynomials differ by a polynomial that vanishes to high order at the places, as in Theorem 6. The index coordinate, which no scramble touches, plays the unscrambled coordinate of Corollary 14. Let μ_n be the group of n -th roots of unity in $\mathbb{F}_p$.

Proposition 88 (Close pairs across a carry of the index). *Let $n \geq 1$, and let $C_c = L_c P_{a_c}$, $c < s$, be a scrambled frame over $\mathbb{F}_p$ with arbitrary fixed nonsingular lower-triangular L_c and places $A = \{a_c\} \subseteq \{0\} \cup \mu_n$. Let $r, k \geq 0$ with $k + np^r \leq m$. Then*

$$\delta(\hat{P}_m)^2 \leq p^{2(k-m)} + [0 \in A]p^{-2k} + [1 \in A]p^{-2(p^r-1)} + |A \setminus \{0, 1\}|p^{-2p^r}.$$

In particular, with $\gamma = \sqrt{s + p^2}$, if $A = \{0\} \cup \mu_{s-1}$ or $A = \mu_s$, then for $m = sp^r$:

$$\delta(\hat{P}_m)N^{1/(s+1)} \leq \gamma p^{-p^r/(s+1)}, \quad \text{i.e.} \quad \delta(\hat{P}_m) \leq \gamma N^{-1/s};$$

for these place sets and every fixed scramble the lifts are not a well-separated family of nets.

Proof. Put $\ell = np^r - 1$, $i = (p^\ell - 1)p^k$, $j = p^{k+\ell} < p^m$; then $j - i = p^k$, $V_i = -(z^k + \dots + z^{k+\ell-1})$, $V_j = z^{k+\ell}$ and $D = V_j - V_i = z^k(z^{np^r} - 1)/(z - 1)$. In characteristic p , $z^{np^r} - 1 = (z^n - 1)^{p^r} = (z - 1)^{p^r} H^{p^r}$ with $H = 1 + z + \dots + z^{n-1}$, so $D = z^k(z - 1)^{p^r-1} H^{p^r}$; as $H(\zeta) = (\zeta^n - 1)/(\zeta - 1) = 0$

for $\zeta \in \mu_n \setminus \{1\}$, D vanishes to order k at 0, to order at least $p^r - 1$ at 1 and at least p^r at the other $\zeta \in \mu_n$. Coordinate c changes by $L_c P_{a_c} D$; the Taylor coefficients $P_{a_c} D$ vanish below the order of D at a_c , and L_c is lower triangular. So the two points share the first k digits of a coordinate with $a_c = 0$, the first $p^r - 1$ digits of one with $a_c = 1$ and the first p^r digits of the others, and the index coordinates differ by p^k/N ; summing squares gives the bound. For $m = sp^r$ we have $N^{1/s} = p^{p^r}$; multiply the bound by $N^{2/s}$. For $A = \{0\} \cup \mu_{s-1}$ take $n = s - 1$, $k = p^r$: the terms become $p^{-2(s-2)p^r} \leq 1$, 1 , p^2 and $s - 2$ times 1. For $A = \mu_s$ take $n = s$, $k = 0$: $p^{-2(s-1)p^r} \leq 1$, 0 , p^2 and $s - 1$ times 1. In both cases $\delta(\hat{P}_m)^2 N^{2/s} \leq s + p^2$, and $N^{1/(s+1)} = N^{1/s} p^{-p^r/(s+1)}$. $\square$

The proof covers every pair with $V_j - V_i = D$ and index distance p^k/N , also when the carry runs out of the top digit ($j \equiv i + p^k \pmod{p^m}$, across the torus boundary of the index coordinate), and every digitally shifted copy. In plain words, $\delta \leq \gamma N^{-1/s}$ says that at these sizes the lift, N points in dimension $s + 1$, is no better separated than a good set of N points in dimension s . The bound is far from sharp, and below 1 only in windows around $m = sp^r$, geometrically far apart; inside them it decays fast: 0.355 at $p = 5$, $m = 10$; below 10^{-3} at $p = 13$, $24 \leq m \leq 27$; $7.7 \cdot 10^{-6}$ at $p = 5$, $m = 50$ (Figure 15(c)). These place sets, the only ones of the proposition with a bound tending to 0, cover, whatever the scramble, the two-dimensional sequences with the places 0, 1 (Theorems 32, 28 and 36 with these places, 42(a), 45 with $s = 2$ and these places, 69, 76, Remark 78, so all of Corollary 79), and in dimension three the places 0, ± 1 (Theorem 80, Theorem 95 with these places) and $\mu_3 \subset \mathbb{F}_7$ (the archived instance of Theorem 95). They do not cover the places 0, 1, 2 for $p \geq 5$, other place sets, or the sequences over $\mathbb{F}_4$ of Theorems 81 and 82 (base-4 carries do not give D); whether their lifts are well separated is open.

Comparison (exact, illustration; computed range only). We computed the lifts of four sequences with the places 0, 1: Faure, the brick wall (Definition 31, $\theta = -\frac{1}{4}$), the residue sequence with a Korobov vector (Corollary 37, $\theta = 1$) and the block-periodic sequence of Theorem 42(a) ($\theta = 1$). At $m = 3$ ($p = 5, \dots, 19$) and $m = 6$ ($p \leq 17$) they give 0.04 to 0.71, against 0.73 to 0.97 for the nets of [18] (column nets, $\mathcal{P}_{2,q}$); at $p = 5$ the last three fall to 0.07–0.14 at $m = 9, 10$ (Faure to 0.02), where [18] certifies 0.632 resp. 0.630. Their exact closest pairs there are pairs of the proposition ($\ell = 4$; $k = 4$, or $k = 5$ for the residue and block-periodic lifts at $m = 10$; three across the torus boundary), and in 20 of the 21 cases computed for these three sequences at $m \in \{6, 9, 10\}$ the minimum comes from neighbouring slabs. In dimension four ($m = 4$, places (0, 1, 2) or (0, 2, 1), $p \leq 13$) the lifts give 0.18–0.65, against at least 0.8 for [18] at $p = 11, 13$ (at $p = 5, 7$ its certified values do not decide). So the lifts are nets for free, but for separation the frame nets of [18], scrambled for each m , are the right tool.

10.5. Limitations. A sequence in base p is stratified in base p , not in base 2: renderers that rely on dyadic strata at power-of-two sample counts should use base 2 or 4 (Theorems 76, 81, 82). Within one base, $\text{sep}(P_{[N]})$ fluctuates with the position of N between the powers of p , more so for large p ; for the residue sequences the certified sizes are p^{sK-1} , and the smallest values come just after them. The discrepancy is $O((\log N)^s/N)$ with a constant that grows with p [31], but separation and integration error are different quantities, and a comparison with Owen-scrambled Sobol' on rendering integrands and smooth test functions is the obvious next experiment. The guarantees concern the geometry of the point sets: they matter where clumping at an unknown, open-ended number of samples must be excluded, as in progressive sampling, in stippling and object placement, and in quasi-uniform designs for kernel interpolation, where the mesh ratio of Lemma 2 enters directly.

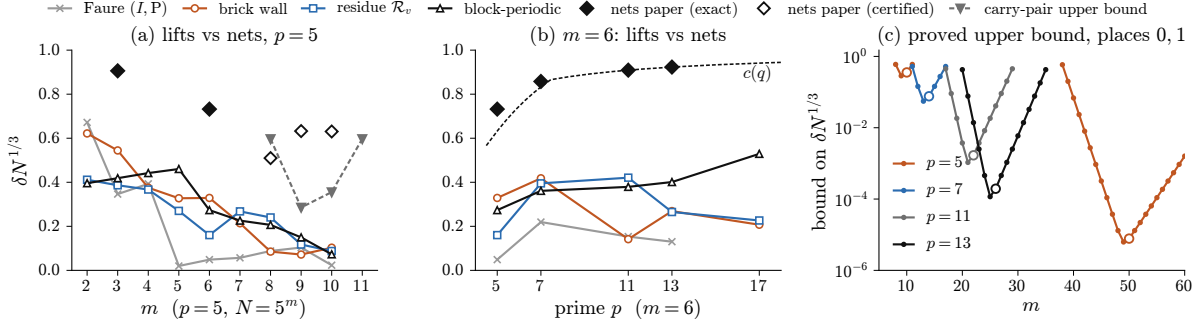


FIGURE 15. Lifts (places 0,1) against the nets of [18], $\delta N^{1/3}$. (a) $p = 5$; diamonds: exact (filled) and certified (open) values of [18]; triangles: the bound of Proposition 88. (b) $m = 6$; dashed: $c(q)$ of [18]. (c) The bound of Proposition 88 where below 1: each V-shaped curve is one r (best k at each m), small only near $m = 2p^r$; circles: $\sqrt{2+p^2} p^{-p^r/3}$ at $m = 2p^r$. The minima tend to 0.

11. OPEN PROBLEMS

- (1) *One sequence certified at both kinds of levels.* No digital sequence is known to us that is certified both at every $m \equiv -1 \pmod{s}$ with the constants of Theorem 36 and at every full level with $1 - O(1/p)$. For exact designed relations of bounded depth next to exact skeleton relations this is excluded (Corollary 58), and more generally exact relations of bounded depth leave room for about one relation per level (Theorem 51); for windows chosen together with a corrected skeleton relation in a self-similar scramble, Proposition 73 excludes it in the scope stated there (product windows, covering of every line, the correction window of Theorem 72). Open are selection rules that look at later digits, windows that are not products or that use several digits, certificates other than the one-digit relaxation, scrambles that are not self-similar, and digital sequences that are not scrambles of a frame of finite places.
- (2) *Every full level with constants tending to 1 at all primes.* At every full level the constants $1 - O(1/p)$ are certified only from large primes on: $1 - 17/p$ for $p > 3677$ in dimension two (Corollary 70), and $1 - C_s''/p$ from $p_0(s)$ on in dimension $s \geq 3$, with $p_0(3) \leq 1.97 \cdot 10^7$ and $p_0(4) \leq 1.44 \cdot 10^{16}$ (Theorems 68 and 104), because one hierarchy of step sizes serves all columns. The block-periodic residue sequences reach $1 - 2/p$ from $p = 3$ ($s = 2$) and $p = 5$ ($s = 3$) on, but only at every s -th full level, and lose one $1/p$ against the $1 - 1/p$ of the nets of [18], as the deeper digits of a coordinate depend on its own cell. Possible routes: windows on the free multipliers of block-periodic scrambles with period $\ell > s$, to certify the full levels between the design levels; coverings of lattice type for the staggered windows, to lower $p_0(s)$.
- (3) *Base five in dimension three at every full level.* Base 5 is covered only on the level family 9N (Theorem 42(b)); Remark 85 lists what was tried for every full level: symmetric frames have no three-dimensional instance over $\mathbb{F}_5$, the staggered residue sequences have explicit close pairs at deep levels, and several one- and two-digit certificate classes were reported unsatisfiable by a SAT solver in the instances solved (evidence about those classes only). General two-digit windows, history-dependent bounds with several digits (as in Appendix B), and non-symmetric algebraic frames remain unexplored.

- (4) *Random linear scrambles of Sobol'.* Every Sobol' sequence fails (Corollary 13), and so does every scramble that leaves one coordinate a radical inverse up to a scalar (Corollary 14); a fixed two-sided linear scramble of the two-dimensional Sobol' sequence is quasi-uniform (Theorem 76). Whether a random linear matrix scramble of the Sobol' sequence is quasi-uniform, almost surely or with positive probability, is open: the bound $O_P(\log N)$ for the mesh ratio of randomly linearly scrambled binary nets that satisfy a uniform coincidence condition, as the Sobol' prefixes do [39, Thm. 5.5, Lem. 4.10], does not decide it. How fast the separation of the Sobol' and Niederreiter sequences decays in dimension $s \geq 3$ is open as well: Section 3 gives explicit close pairs along one sequence of sizes, and the rate $N^{-1/(s-1)}$ only for the Faure sequence (Remark 9).
- (5) *The limit of the residue-sequence constant.* The best certified constant $\max_v p^{-1/s} \lambda_{\text{jit}}(\Lambda_v)$ of the residue sequences (Table 7) appears to tend to $\sqrt{\gamma_s}$, the square root of the Hermite constant; this is the open limit of the skeleton nets of [18], and an answer there transfers verbatim. The upper bound $\lambda_{\text{jit}}(\Lambda_v) \leq \sqrt{\gamma_s} p^{1/s}$ is immediate, since Λ_v has index p . A route for the lower bound that we have not verified: the lattices Λ_v are the sublattices of index p of $\mathbb{Z}^s$ (those whose check vector has no zero entry), and an equidistribution statement for these sublattices, rescaled to covolume 1, in the space of lattices as $p \rightarrow \infty$ could give the limit, since the jitter correction costs at most $\sqrt{s} p^{-1/s}$; we have neither checked whether such a statement is available in the form needed nor worked out the details.
- (6) *Implied skeleton relations in dimension $s \geq 3$.* In dimension two a design can imply a skeleton relation at the level after the design level (Proposition 46, Corollary 47), and with the skeleton multipliers of Theorem 45 the two families meet the density bound of Corollary 59 (Remark 48). For $s \geq 3$ the conditions of Proposition 46 can be met algebraically by the free diagonal, but the remark after it forces an entry of order $p^{1/s}$ in every nonzero column of the design for a good skeleton constant, and then the design constant is no longer $1 - O(1/p)$. No example for $s \geq 3$ has been constructed; a search over places, check vectors and crosses has not been run.
- (7) *The true full-level separation of the staggered residue sequence.* The certified bound $(\lfloor p/2^{s-1} \rfloor - 1)/p \approx 2^{1-s}$ of Corollary 29 is a property of the one-coordinate certificate, not of the sequence: for $s = 4$ and $s = 5$ the exact separations of the first full level P_s in the cases computed lie between 0.1985 and 0.4837 (Section 5.2). Whether $\inf_K \text{sep}(P_{sK})$ stays of order 1 for $s \geq 4$, or decays to the order 2^{1-s} of the bound, is open; a certificate that uses all coordinates would be needed.
- (8) *Small primes and prime powers.* The primes $s \leq p < 2^s$ in dimension $s \geq 4$ are not covered at every full level (on $s^2\mathbb{N}$, Theorem 42 covers them from $p = 7, 11, 17$ on for $s = 4, 5, 6$), and whether residue sequences are quasi-uniform there is not addressed. The staggered residue sequences keep separations well away from 0 at the first levels below 2^s (for instance 0.48 to 0.52 for $K \leq 7$ at $s = 2, p = 3$; exact), but the close pairs found at deep levels for $s = 3, p = 5$ (Remark 85) show how little such data say. Prime powers beyond Proposition 83, the residue sequence over $\mathbb{F}_q$ (the proof of Theorem 36 uses that q is prime), and the more general Halton-type sequences of Hofer in rational bases [23], to which [16] refer (outside the definition treated in Corollary 7), are open.
- (9) *Quality at reachable sizes, integration, and base two.* The certified bounds are loose at small primes, the Faure sequence is better at its first full level, and in the scans of Section 10 the choice of places, scale and check vector moved $\mathcal{J}$ more than the certified constant did. Criteria that target the first levels while keeping a certified bound, and a measured study of integration error, are open. A $(0, s)$ -sequence in base 2 needs $s \leq 2$;

the binary sequences of Theorems 81 and 82 are quasi-uniform in dimensions three and four, with certified bounds at the sparse levels $N = 2^{6K}$ and 2^{8K} and small constants. Binary sequences with certified bounds at denser levels, or with constants comparable to those of large prime bases, are open.

Use of AI systems. The constructions, proofs and Lean formalization were produced by an AI system (Anthropic Claude Opus 5.5) 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; the computer-assisted parts are exact finite computations whose scope is stated with each result. AI systems are not listed as authors; responsibility for this work rests with the author.

APPENDIX A. STRUCTURE PROOFS

This appendix collects proofs that would interrupt the main text. Sections A.1 and A.2 support Section 4: the carry rule for $q = 4$ (Remark 89), the Riordan form (Lemma 90) and the proof of the residue form (Lemma 21). Section A.3 collects facts about responses used in Sections 4 and 7. Section A.4 proves Proposition 62, Section A.5 the results on the hexagonal brick wall (Theorem 69, Corollary 70), and Section A.6 two results of Section 9 (Proposition 75, Lemma 77). The staggered windows at a finite prime are in Appendix D.

A.1. Carries in Base Four.

Remark 89 (Carries for $q = 4$). For a digit $y \in \mathbb{F}_q$ let $\Delta(y) := \text{enc}^{-1}((\text{enc}(y) + 1) \bmod q) - y \in \mathbb{F}_q^*$ be the change in $\mathbb{F}_q$ when its code goes up by one, and let $\bar{y} = \text{enc}^{-1}(q - 1)$ be the top digit. A step of carry length l adds $\Delta(\bar{y})$ to each of the $l - 1$ finest digits and $\Delta(y)$ to digit $K - l$, where y is the value of that digit; for $\mathbb{F}_4$, $\Delta(0) = \Delta(\omega) = 1$ and $\Delta(1) = \Delta(\omega^2) = \omega^2$. By linearity such a step changes the geometric digit $K + i$ of coordinate c by

$$(8) \quad \delta_i(l, y)[c][c'] := \Delta(\bar{y}) D_i(l - 1)[c][c'] + \Delta(y)(D_i(l) - D_i(l - 1))[c][c'],$$

which is $D_i(l)[c][c']$ for prime q and $\omega^2 D_i(l)$ or $D_i(l) + \omega D_i(l - 1)$ for $\mathbb{F}_4$.

A.2. Riordan Form and Residue Form. The Riordan form writes each row of a scramble as one series in the common local variable x ; the self-similar scrambles are those with one series for all rows.

Lemma 90 (Riordan form). *Let $\theta \in \mathbb{F}_q^*$. For every scramble L_c there are unit power series $g_{c,n} \in \mathbb{F}_q[[x]]$, $n \geq 0$, such that for every V*

$$y_{c,n}(V) = [x^n] g_{c,n}(x) V(z_c(\theta x)).$$

Row n of L_c determines and is determined by the coefficients of $g_{c,n}$ up to x^n .

Proof. Write $V(z) = \sum_k [(z - a_c)^k] V(z - a_c)^k$. Since $z_c(\theta x) - a_c = \theta x/w'(a_c) + O(x^2)$ is x times a unit, $[x^n] g(x)(z_c(\theta x) - a_c)^k$ vanishes for $k > n$, equals $g(0)(\theta/w'(a_c))^n \neq 0$ for $k = n$, and for $k < n$ depends only on g up to x^{n-k} , with the coefficient of x^{n-k} entering through the factor $(\theta/w'(a_c))^k \neq 0$. So the map from the coefficients of g up to x^n to row n is triangular with nonzero diagonal, hence a bijection onto the rows with nonzero diagonal entry. $\square$

For the residue form we compute residues in a different local variable. The following change of variable is classical; we include the short proof because it must hold in every characteristic.

Lemma 91 (Change of variable in a residue). *Let Z and u be formal variables and $Z = u\mu(u)$ with a unit series $\mu \in \mathbb{F}_q[[u]]$. For every Laurent series $F \in \mathbb{F}_q((Z))$,*

$$\text{Res}_Z(F(Z) dZ) = \text{Res}_u(F(Z(u)) Z'(u) du),$$

where $\text{Res}_Z(F dZ)$ is the coefficient of Z^{-1} in F , and $Z'(u)$ is the formal derivative.

Proof. Both sides are linear in F . For $k \geq 0$ the series $Z^k Z'$ has no negative powers of u , so on both sides only the finitely many coefficients of Z^k , $k < 0$, in F matter, and it suffices to take $F = Z^k$, $k \in \mathbb{Z}$, where the left side is 1 for $k = -1$ and 0 otherwise. For $k = -1$ the right side is the residue of $Z'/Z = 1/u + \mu'/\mu$, and μ'/μ is a power series, so it is 1. Let $k \neq -1$. Write $\mu = \mu_0 + \mu_1 u + \mu_2 u^2 + \dots$. The coefficient of u^{-1} in $Z^k Z' = u^k \mu^k (\mu + u\mu')$ is a polynomial with integer coefficients in $\mu_0^{-1}, \mu_0, \mu_1, \mu_2, \dots$ (finitely many of them), the same polynomial over every field. Over a field of characteristic zero, with the μ_i independent indeterminates, $Z^k Z' = \frac{d}{du}(Z^{k+1}/(k+1))$ is a derivative, whose coefficient of u^{-1} is zero. So the polynomial is zero, and the right side vanishes over $\mathbb{F}_q$ as well. $\square$

Proof of Lemma 21. (a) Since $\text{Res}_a(V(z-a)^{-k-1} dz) = [(z-a)^k]V$, the right side equals $\sum_{k \leq n} L_c[n][k] [(z-a_c)^k]V$, which is digit n of the scrambled coordinate c (Section 2). The coefficient of $(z-a_c)^{-n-1}$ in $\eta_{c,n}$ is $L_c[n][n] \neq 0$. Conversely, a family of polar differentials $\eta_{c,n} = \sum_{k \leq n} \lambda_{n,k} (z-a_c)^{-k-1} dz$ with $\lambda_{n,n} \neq 0$ defines the lower-triangular matrix $L_c[n][k] = \lambda_{n,k}$ with nonzero diagonal, and the same computation gives $y_{c,n}(V) = \text{Res}_{a_c}(V \eta_{c,n})$.

(b) Fix c and expand at a_c in $Z = z - a_c$. Since $w = w'(a_c)Z + O(Z^2)$ with $w'(a_c) \neq 0$, the series $u = w$ is Z times a unit, and its inverse is $Z = z_c(u) - a_c$, because $w(z_c(u)) = u$. Let φ_c be a unit series in Z . By Lemma 91, with $dz = dZ$,

$$\text{Res}_{a_c}\left(V \varphi_c \left(\frac{\theta}{w}\right)^{n+1} dz\right) = \theta^{n+1} \text{Res}_u\left(V(z_c(u)) \varphi_c(z_c(u)) u^{-n-1} z'_c(u) du\right) = \theta^{n+1} [u^n] H(u),$$

with $H(u) = V(z_c(u)) \varphi_c(z_c(u)) z'_c(u)$. Substituting $u = \theta x$ turns $[u^n]H(u)$ into $\theta^{-n} [x^n] H(\theta x)$, so the residue equals

$$[x^n] \theta \varphi_c(z_c(\theta x)) z'_c(\theta x) V(z_c(\theta x)) = [x^n] g_c(x) V(z_c(\theta x)),$$

with g_c as stated. It is a unit series, since $\varphi_c(a_c) \neq 0$ and $z'_c(0) = 1/w'(a_c) \neq 0$. So a family of local multipliers gives a self-similar scramble with scale θ and multipliers g_c . Conversely, let g_c be a unit series in x and put $\varphi_c(z) := \theta^{-1} g_c(w(z)/\theta) w'(z)$; since $w(z)/\theta$ has no constant term at a_c , this is a power series in Z , and a unit because $g_c(0)w'(a_c) \neq 0$. Differentiating $w(z_c(u)) = u$ gives $w'(z_c(u)) z'_c(u) = 1$, hence

$$\theta \varphi_c(z_c(\theta x)) z'_c(\theta x) = g_c(x) w'(z_c(\theta x)) z'_c(\theta x) = g_c(x).$$

So every self-similar scramble has a residue form, and the two maps $\varphi_c \mapsto g_c$ and $g_c \mapsto \varphi_c$ are mutually inverse: the second composed with the first gives $\varphi_c(z_c(w(z))) = \varphi_c(z)$, because z_c is the compositional inverse of w at a_c on both sides. The scale θ is the same on both sides.

(c) Write $F = G + \sum_c \sum_{k \geq 1} \alpha_{c,k} (z-a_c)^{-k}$ with a polynomial G and finitely many $\alpha_{c,k} \in \mathbb{F}_q$ (partial fractions; the denominator of F is a product of powers of the $z-a_c$). At a_c the polynomial G and the terms $(z-a_b)^{-k}$, $b \neq c$, are regular, and $(z-a_c)^{-k}$ has residue 1 for $k = 1$ and 0 for $k \geq 2$; so $\text{Res}_{a_c}(F dz) = \alpha_{c,1}$. At ∞ , G contributes no power z^{-1} , and $(z-a_c)^{-k} = z^{-k} (1-a_c/z)^{-k}$ contributes to z^{-1} only for $k = 1$, with coefficient 1. Hence $[z^{-1}]F = \sum_c \alpha_{c,1} = \sum_c \text{Res}_{a_c}(F dz)$. If $F = O(z^{-2})$ at ∞ , then $[z^{-1}]F = 0$. $\square$

A.3. Responses of Self-Similar Scrambles. This subsection supports Sections 4 and 7: two responses of one column of a self-similar scramble are never both periodic (Proposition 92), the cross responses of every digital $(0, s)$ -sequence have full rank (Proposition 93), and Corollary 53 has a direct proof.

Proposition 92 (No periodic responses). *Let $s \geq 2$, let the frame be arbitrary, and let the scramble be self-similar over $\mathbb{F}_q$. In every column c' , at most one of the s series $O_{c'}$ and $X_{c \leftarrow c'}$ ($c \neq c'$) is rational. In particular the own response $O_{c'}^{(l)}$ and a cross response $X_{c \leftarrow c'}^{(l)}$ of one column, as functions of the carry length l , are never both eventually periodic, and neither are two cross responses $X_{c_1 \leftarrow c'}^{(l)}$, $X_{c_2 \leftarrow c'}^{(l)}$. For $s = 2$: O_1 and $X_{0 \leftarrow 1}$ are not both rational, and neither are O_0 and $X_{1 \leftarrow 0}$.*

Proof. Write $y = \theta x$ and $z_c = z_c(y)$. No local root is rational. The polynomial $w(Z) - y$ has degree one in y and is primitive in $\mathbb{F}_q[Z][y]$, so it is irreducible in $\mathbb{F}_q[y, Z]$; it is monic of degree $s \geq 2$ in Z , so by Gauss's lemma it is irreducible in $\mathbb{F}_q(y)[Z]$ and has no root in $\mathbb{F}_q(y)$. Since $z_c \in \mathbb{F}_q[[y]]$ is a root, $z_c \notin \mathbb{F}_q(y)$.

The responses. By Proposition 22, $O_{c'} = \mathcal{D}[c']$ and $X_{c \leftarrow c'} = x^{-1} \mathcal{D}[c][c']$ with $\mathcal{D} = I - \mathcal{A}(0)G$. Write $\mathcal{A} = \text{diag}(g_c) \text{Vdm}$ with $\text{Vdm}[c][b] = z_c^b$. Column c' of Vdm^{-1} holds the coefficients of the Lagrange polynomial $\ell_{c'}(Z) = \prod_{c'' \neq c'} (Z - z_{c''}) / (z_{c'} - z_{c''})$, and $\mathcal{A}(0)[c][b] = g_c(0) a_c^b$, so $(\mathcal{A}(0)G)[c][c'] = g_c(0) \ell_{c'}(a_c) / g_{c'}(x)$. By (5) with y in place of x , $\prod_{c'' \neq c'} (Z - z_{c''}) = (w(Z) - y) / (Z - z_{c'})$; at $Z = z_{c'}$ this is $w'(z_{c'})$, and at $Z = a_c$ it is $-y / (a_c - z_{c'})$, since $w(a_c) = 0$. (The series $a_c - z_{c'}$ is nonzero: its constant term is $a_c - a_{c'}$ for $c \neq c'$, and for $c = c'$ its coefficient of y is $-1/w'(a_{c'})$.) Hence

$$(\mathcal{A}(0)G)[c][c'] = -\frac{g_c(0)}{g_{c'}(x) w'(z_{c'})} \cdot \frac{y}{a_c - z_{c'}},$$

so $X_{c \leftarrow c'} = \theta g_c(0) / (g_{c'}(x) w'(z_{c'}) (a_c - z_{c'})) \neq 0$ for $c \neq c'$, and $1 - O_{c'} = (\mathcal{A}(0)G)[c']$. Taking quotients,

$$\frac{1 - O_{c'}}{x X_{c \leftarrow c'}} = -\frac{g_{c'}(0)}{g_c(0)} \cdot \frac{a_c - z_{c'}}{a_{c'} - z_{c'}}, \quad \frac{X_{c_1 \leftarrow c'}}{X_{c_2 \leftarrow c'}} = \frac{g_{c_1}(0)}{g_{c_2}(0)} \cdot \frac{a_{c_2} - z_{c'}}{a_{c_1} - z_{c'}}.$$

In both cases the right side is a nonzero constant times $\Xi = (b_1 - z_{c'}) / (b_2 - z_{c'})$ for two distinct places $b_1 \neq b_2$. If the two series on the left were rational in x , then Ξ would be rational in y , $\Xi \neq 1$, and $z_{c'} = (b_1 - b_2 \Xi) / (1 - \Xi)$ would be rational, a contradiction. Finally, if the responses $O_{c'}^{(l)} = [x^l] O_{c'} / (1 - x)$ are eventually periodic in l , their generating function is rational, and so is $O_{c'}$; the same holds for the cross responses. $\square$

For $s = 2$, and for two cross series in dimension $s \geq 3$, this is the statement used in Section 4; the case of an own and a cross series in dimension $s \geq 3$ comes with the same proof. It is why, apart from a few constant responses as in the brick wall, the responses of a self-similar scramble keep changing with the carry length, and why Section 8 keeps them in windows instead.

For an arbitrary digital sequence the offset map of P_{sK} is defined as in Section 4: the cell digits determine the index, so every geometric digit is a linear function of the cell digits. If the cross responses of a column moved in lockstep, $X_{c_2 \leftarrow c'} = \xi X_{c_1 \leftarrow c'}$, the vector $\mathbf{u}_l$ of Proposition 63 would stay in a hyperplane and a smaller window would do; this never happens.

Proposition 93 (Rank of the cross responses). *Let $(C_0, \dots, C_{s-1})$ be a digital $(0, s)$ -sequence over $\mathbb{F}_q$, $s \geq 2$, and $K \geq s - 1$. For a coordinate c' , let $X_{c'}$ be the $(s - 1) \times K$ matrix whose row $c \neq c'$ holds the coefficients of the cell digits $y_{c',0}, \dots, y_{c',K-1}$ in the geometric digit $r_c = y_{c,K}$ of P_{sK} . Then the minor of $X_{c'}$ on the $s - 1$ finest digits $y_{c',K-s+1}, \dots, y_{c',K-1}$ is nonzero; in particular $X_{c'}$ has rank $s - 1$.*

Proof. Let $\mathbf{B}$ be the box matrix of the composition $(K, \dots, K)$: the first K rows of every C_c , restricted to the columns $0, \dots, sK - 1$. It is invertible because P_{sK} is a $(0, sK, s)$ -net. Its rows are indexed by pairs (c, i) , $i < K$, and the vector of cell digits is $\mathbf{y} = \mathbf{B}\mathbf{V}$ for the vector $\mathbf{V} = (V_0, \dots, V_{sK-1})$ of index digits. Let $\mathbf{R}$ be the $(s-1) \times sK$ matrix of the rows $C_c[K]$, $c \neq c'$, on the same columns. Then $r_c = (\mathbf{R}\mathbf{V})_c = (\mathbf{R}\mathbf{B}^{-1}\mathbf{y})_c$ for $c \neq c'$, so the rows of $X_{c'}$ are the columns (c', i) of $\mathbf{R}\mathbf{B}^{-1}$. For a set S of $s-1$ row indices of $\mathbf{B}$, let $\mathbf{B}_{S \leftarrow \mathbf{R}}$ be $\mathbf{B}$ with the rows in S replaced by the rows of $\mathbf{R}$. Then $\mathbf{B}_{S \leftarrow \mathbf{R}} = E\mathbf{B}$, where E is the identity with the rows in S replaced by the rows of $\mathbf{R}\mathbf{B}^{-1}$, and expanding $\det E$ along the rows outside S shows that the minor of $\mathbf{R}\mathbf{B}^{-1}$ on the columns S is $\pm \det \mathbf{B}_{S \leftarrow \mathbf{R}} / \det \mathbf{B}$. Take $S = \{(c', K-s+1), \dots, (c', K-1)\}$. Up to the order of the rows, $\mathbf{B}_{S \leftarrow \mathbf{R}}$ consists of the first $K+1$ rows of every C_c , $c \neq c'$, and the first $K-s+1$ rows of $C_{c'}$, on the columns below sK : the box matrix of the composition $(K+1, \dots, K+1, K-s+1)$ of sK , which is invertible since $t = 0$. $\square$

Direct proof of Corollary 53. Since $a_0 = 0$, $C_0 = L_0$ is lower triangular with nonzero diagonal, and P_{2K} , P_{2K+2} are nets (Lemma 1), so the offset maps at the levels K and $K+1$ are defined on the index polynomials of degree less than $2K$ and $2K+2$. Suppose the three conditions hold, and write X and X' for the coefficients of $y_{1,K-1}$ in $y_{0,K}$ at level K and of $y_{1,K}$ in $y_{0,K+1}$ at level $K+1$, the only cross coefficients left. Take $V = z^K$. Its digits in coordinate 0 are $y_{0,i} = C_0[i][K] = 0$ for $i < K$ and $y_{0,K} = C_0[K][K] \neq 0$. The own part of $y_{0,K}$ vanishes, so $C_0[K][K] = X y_{1,K-1}(z^K)$, and $X \neq 0$. Take $V = z^{K+1}$, of degree less than $2K$ because $K \geq 2$. Now $y_{0,i} = 0$ for $i \leq K$, so the level- K offset map of coordinate 0 gives $0 = X y_{1,K-1}(z^{K+1})$, hence $y_{1,K-1}(z^{K+1}) = 0$. The own part of the offset map of coordinate 1 involves only $y_{1,K-1}$, and its cross part only the cell digits of coordinate 0, which all vanish; so $y_{1,K}(z^{K+1}) = 0$. Finally the offset map of coordinate 0 at level $K+1$ gives $C_0[K+1][K+1] = y_{0,K+1}(z^{K+1}) = X' y_{1,K}(z^{K+1}) = 0$, a contradiction. $\square$

The direct proof uses only that coordinate 0 is lower triangular and that P_{2K} and P_{2K+2} are nets, so it holds for every two-dimensional digital sequence with these two properties; the proof in Section 7 uses the frame, and the same argument works verbatim for any two distinct places $a_0 \neq a_1$ in place of 0, 1.

A.4. Proofs for Section 8. This subsection contains the proofs of the results on free digits, windows and the half-cell stagger (Sections 8.1 and 8.2) and of the results on windows and skeleton relations (Section 8.5).

Proof of Proposition 62. (a) By Lemma 21(b) the local multiplier φ_c is a unit power series at a_c , and so is $\theta\varphi_c\hat{\omega}_c$, because $\hat{\omega}_c(a_c) = a_c - a_{1-c} \neq 0$ for $s = 2$. Since $w = (z - a_c)w_c(z)$ with $w_c(a_c) = w'(a_c) \neq 0$, every power series in $z - a_c$ is a power series in w ; write $\theta\varphi_c\hat{\omega}_c = \Omega_c(w)$ with a unit series Ω_c , and put $\lambda_c = \Omega_c(0)$ and $\psi_c = \lambda_c/\Omega_c$. Conversely, for any $\lambda_c \in \mathbb{F}_q^*$ and unit series ψ_c with $\psi_c(0) = 1$, $\varphi_c := \lambda_c/(\theta\hat{\omega}_c\psi_c(w))$ is a unit power series at a_c . By Lemma 21(b), $g_c(x) = \theta\varphi_c(z_c(\theta x))z'_c(\theta x)$, and $z'_c = 1/w'(z_c)$ (differentiate $w(z_c(u)) = u$); at $z = z_c(\theta x)$ we have $w(z) = \theta x$, which gives the formula for g_c .

(b) This is Proposition 22.

(c) By Proposition 22, $O_{c'} = \mathcal{D}[c'][c']$ and $X_{c \leftarrow c'} = x^{-1}\mathcal{D}[c][c']$ with $\mathcal{D} = I - \mathcal{A}(0)G$. Write $y = \theta x$ and $\mathcal{A} = \text{diag}(g_c) \text{Vdm}$ with $\text{Vdm}[c][b] = z_c(y)^b$. As in the proof of Proposition 92,

$$(\mathcal{A}(0)G)[c][c'] = \frac{g_c(0)}{g_{c'}(x)} \cdot \frac{y}{(z_{c'}(y) - a_c)w'(z_{c'}(y))}.$$

By (a) with $\hat{\omega} = 1$, $g_{c'}(x)w'(z_{c'}(y)) = \lambda_{c'}/\psi_{c'}(y)$ and $g_c(0) = \lambda_c/w'(a_c)$. For $c = c'$, $y = w(z_{c'}(y)) = (z_{c'}(y) - a_{c'})w_{c'}(z_{c'}(y))$, so $y/(z_{c'}(y) - a_{c'}) = w'(a_{c'})\hat{w}_{c'}(z_{c'}(y))$ and $(\mathcal{A}(0)G)[c'][c'] = [\hat{w}_{c'}\psi_{c'}](y)$, which gives $O_{c'}$. For $c \neq c'$, $y/(z_{c'}(y) - a_c) = y\check{w}_{cc'}(z_{c'}(y))/(a_{c'} - a_c)$; dividing by

$x = y/\theta$ gives $X_{c \leftarrow c'}$ with the stated $\kappa_{c \leftarrow c'}$. The kernels are evaluated at the point $z_{c'}(y)$ of the local root, that is, as series in w at $a_{c'}$ evaluated at $w = y$.

(d) The displayed formula for $(\mathcal{A}(0)G)[c][c']$ does not use $s \geq 3$. In the frame $(0, 1; \infty)$, $w = z^2 - z$, $w' = 2z - 1$, and $z_0 + z_1 = 1$, $z_0 z_1 = -y$. Column 1: $\hat{w}_1 = z$, so (a) gives $g_1(x)w'(z_1) = \lambda_1/(\psi_1(y)z_1)$, $g_1(0) = \lambda_1$ and $g_0(0) = \lambda_0/(\hat{w}_0(0)w'(0)) = \lambda_0$. With $y/(z_1 - 1) = z_1$ and $y/(z_1 - 0) = z_1 - 1$ the formula gives $(\mathcal{A}(0)G)[1][1] = z_1^2 \psi_1(y)$ and $(\mathcal{A}(0)G)[0][1] = (\lambda_0/\lambda_1) y \psi_1(y)$, hence O_1 and $X_{0 \leftarrow 1}$ with $\kappa_{0 \leftarrow 1} = \theta \lambda_0/\lambda_1$. Column 0 is the same computation with $\hat{w}_0 = z - 1$, $y/(z_0 - 0) = z_0 - 1 = -z_1$ and $y/(z_0 - 1) = z_0$: $(\mathcal{A}(0)G)[0][0] = (z_0 - 1)^2 \psi_0(y) = z_1^2 \psi_0(y)$ and $(\mathcal{A}(0)G)[1][0] = (\lambda_1/\lambda_0) y \psi_0(y)$. The product $\kappa_{0 \leftarrow 1} \kappa_{1 \leftarrow 0} = \theta^2$ is immediate. $\square$

Proof of Proposition 63. Both kernels of column c' take the value 1 at $w = 0$ (Proposition 62(c); for $s = 2$ the kernels of (d) are z_1^2 and 1). So $\psi_{c',l}$ enters the coefficient of x^n of $O_{c'}$ and of $X_{c \leftarrow c'}$ only for $n \geq l$, and at $n = l$ with the coefficients $-\theta^l$ and $-\kappa_{c \leftarrow c'} \theta^l$. The partial sum $O_{c'}^{(l)}$ contains the own coefficients up to x^l , and $X_{c \leftarrow c'}^{(l+1)}$ the cross coefficients up to x^l . Freeness is Proposition 62(a): the coefficient of x^n of $g_{c'}$ depends only on $\psi_{c',0}, \dots, \psi_{c',n}$, and by Lemma 90 so does row n of $L_{c'}$. $\square$

Proof of Proposition 64. (a) By (ii) the line $\beta_l + \mathbb{F}_p \alpha_{c'}$ contains a point $\beta_l + t \alpha_{c'}$ of $W^{(c')}$, which gives the admissible digit $\psi = -t/\theta^l$. (b) By Proposition 63 the chosen digits define one unit series ψ_c per coordinate, hence a self-similar scramble; Lemma 1 applies. (c) The offset map is the same at every level (Proposition 62(b)); $X^{(1)} = -\kappa$ lies in its window by (i), and the admissible choice at depth l puts $\mathbf{u}_l$ into $W^{(c')}$. (d) Lemma 23 with $j = 1$ gives the first inequality. For a step e with carry lengths $l_{c'}$, the change of the geometric digit of coordinate c is $\sum_{c'} e_{c'} D(l_{c'})[c][c']$, which lies in $S_c(e)$ by (c); hence $\text{LB}_K^{\text{act}} \geq \text{LB}(W)$. $\square$

Proof of Lemma 65. The q^{s-1} lines of direction α partition $\mathbb{F}_q^s$, and each of them contains a point of W . $\square$

Proof of Lemma 66. Let $\hat{\sigma} \in [0, p)$ represent σ . As R runs through $\mathbb{F}_p$, $\text{enc}(R \oplus \sigma) - \text{enc}(R)$ takes the value $\hat{\sigma}$, and also $\hat{\sigma} - p$ if $\hat{\sigma} \geq 1$ (when the neighbour's digit wraps around). For $e = 1$ the minimum of $|p + \text{enc}(R \oplus \sigma) - \text{enc}(R)|$ is $\hat{\sigma} = p \text{frac}(\Phi)$ if $\hat{\sigma} \geq 1$ and p if $\hat{\sigma} = 0$, that is $p \bar{f}(+1, \Phi)$; for $e = 0$ it is $p \|\Phi\|$; $e = -1$ is $e = 1$ with $-\sigma$. Subtracting the jitter $1/p$ gives the formula. If $\bar{f}(+1, \Phi) = \bar{f}(-1, \Phi)$, then $\text{frac}(\Phi) = \text{frac}(-\Phi)$, so $\Phi \in \{0, \frac{1}{2}\}$; at 0, $\bar{f}(\pm 1, 0) = 1 \neq 0 = \bar{f}(0, 0)$. $\square$

Proof of Theorem 67. Fix a step e , let $E = \text{supp } e$ and $k = |E \cap C|$. (i) A moving coordinate $i \in C$ receives its own response and one cross from each other moving column, so $e_i \Phi_i \in [-a - (|E| - 1)\varepsilon, -a + (|E| - 1)\varepsilon] \subset (-1, 0)$, because $a > (s - 1)\varepsilon$ and $a + (s - 1)\varepsilon < 2a < 1$ (by (ii)); hence $\bar{f}(e_i, \Phi_i) \geq 1 - a - (|E| - 1)\varepsilon$. (ii) $k \geq 2$: since $1 - a - \varepsilon \geq 0$, the hypothesis gives $1 - a - \varepsilon \geq \sqrt{1 - (\frac{1}{2} - \varepsilon)^2} > \sqrt{3}/2$, so $a < 0.134$, $a + (s - 1)\varepsilon < 2a < 0.268$, and two moving coordinates of C give $\sum_c \bar{f}(e_c, \Phi_c)^2 > 2 \cdot 0.732^2 > 1$. (iii) $E = \{c_\star\}$: $\bar{f}(\pm 1, 0) = 1$. (iv) $E = \{i\}$: $\bar{f}(e_i, \Phi_i) = 1 - a$, and $c_\star$ does not move and receives $\pm(\frac{1}{2} + [-\varepsilon, \varepsilon])$, at distance at least $\frac{1}{2} - \varepsilon$ from 0; the sum is at least $(1 - a)^2 + (\frac{1}{2} - \varepsilon)^2 \geq 1$. (v) $E = \{i, c_\star\}$: $\bar{f}(e_i, \Phi_i) \geq 1 - a - \varepsilon$ by (i), and $e_\star \Phi_\star \in \pm(\frac{1}{2} + [-\varepsilon, \varepsilon])$, where $\bar{f}(+1, \cdot) \geq \frac{1}{2} - \varepsilon$; the sum is at least $(1 - a - \varepsilon)^2 + (\frac{1}{2} - \varepsilon)^2 \geq 1$. For the second statement: $\varepsilon \mapsto (1 - s\varepsilon)^2 + (\frac{1}{2} - \varepsilon)^2$ decreases on $[0, \varepsilon_s]$ and equals 1 at ε_s , so for $\varepsilon < \varepsilon_s$ it exceeds 1 at $a = (s - 1)\varepsilon$, and by continuity some $a > (s - 1)\varepsilon$ still works. $\square$

Windows and skeleton relations.

Proof of Lemma 71. By Lemma 21(b), $v_c \chi_{c,d} y_{c,K-1-d}(V) = \theta^K \text{Res}_{a_c}(V \varphi_c \cdot v_c \chi_{c,d}(w/\theta)^d \cdot w^{-K} dz)$. Summing over $d < K$ replaces $v_c \chi_{c,d}(w/\theta)^d$ by the truncation of $1/\varphi_c$ below w^K . The

rest of $1/\varphi_c$ is $O(w^K)$, and times $\varphi_c w^{-K}$ it is regular at a_c ; so the sum equals $\theta^K \text{Res}_{a_c}(V w^{-K} dz)$. By Lemma 21(c) the sum over c is $\theta^K [z^{-1}](V/w^K)$, which is 0 for $\deg V \leq sK - 2$. $\square$

Proof of Theorem 72. As in the proof of Theorem 36, distinct points of P_{sK-1} lie in distinct fine cells $\hat{n}$, and $\hat{n}_c = \sum_{i < K} y_{c,i} p^{K-1-i}$. Let two points lie in the fine cells $\hat{n}$, $\hat{n}'$, and let a_c be the representative of $\hat{n}'_c - \hat{n}_c$ modulo p^K in $(-p^K/2, p^K/2]$. As there, the toroidal distance in coordinate c is at least $(|a_c| - 1)_+ p^{-K}$. If some $|a_c| \geq p$, the distance is at least $(p - 1)p^{-K} \geq p^{-K} \lambda_{\text{jit},B}(\Lambda_v)$, since $p\mathbf{1}_c \in \Lambda_v$. Otherwise write $\hat{n}_c = pu_c + y_{c,K-1}$ with the coarse index u_c . Adding a_c with $|a_c| < p$ changes u_c modulo p^{K-1} by some $\epsilon_c \in \{-1, 0, 1\}$, and $\epsilon_c \neq 0$ only if $\epsilon_c = \text{sgn}(a_c)$. A change of u_c by ± 1 is a carry of some length $j_c \in [1, K-1]$ (the toroidal wrap is $j_c = K-1$), which changes each of the digits $y_{c,K-1-d}$, $1 \leq d \leq j_c$, by ϵ_c and leaves the coarser digits unchanged; put $j_c = 0$ if $\epsilon_c = 0$. The digit $y_{c,K-1}$ changes by a_c modulo p . Subtracting the relation for the two points gives $\sum_c v_c(a_c + \epsilon_c \Psi_c(j_c)) \equiv 0$. Let $f_c \in \epsilon_c[0, B]$ be the integer ϵ_c times the centred representative of $\Psi_c(j_c)$, and $b := a + f$. Then $b \in \Lambda_v$. Each f_c is 0 or has the sign of a_c , so $|b_c| = |a_c| + |f_c| \leq |a_c| + B$, and $b = 0$ would force $a = 0$, which is excluded. Hence the distance is at least $p^{-K} \|(|a| - \mathbf{1})_+\|_2 \geq p^{-K} \|(|b| - (1+B)\mathbf{1})_+\|_2 \geq p^{-K} \lambda_{\text{jit},B}(\Lambda_v)$, and $p^{-K} N^{1/s} = p^{-1/s}$. The inequality $\lambda_{\text{jit},B} \geq \lambda_{\text{jit}} - B\sqrt{s}$ holds because $(|b| - \mathbf{1})_+ \leq (|b| - (1+B)\mathbf{1})_+ + B\mathbf{1}$ coordinatewise. $\square$

Proof of Proposition 73. (i) Lemma 71 at level $K+1$ holds on $P_{s(K+1)-1} \supseteq P_{sK}$. For the two points of the step, $y_{c,K}$ changes by σ_c , the cell digits $y_{c,K-d}$, $1 \leq d \leq l_c$, change by e_c (a carry of length l adds 1 to each of the l finest digits modulo p), and the coarser digits do not change. Subtracting the relation for the two points gives the identity.

(ii) Let $\epsilon \in \mathbb{F}_p$ and $j \geq l$, and replace φ_c by $\varphi_c(1 + \epsilon w^j)$; the other coordinates are unchanged. By Lemma 21(b) the new digits are $y'_{c,n} = y_{c,n} + \epsilon \theta^j y_{c,n-j}$ for $n \geq j$ and $y'_{c,n} = y_{c,n}$ for $n < j$. The offset map at level K is linear in the cell digits, and a response is its value on the change of the cell digits: for a carry of length l in coordinate c this change is $+1$ in each digit $y_{c,n}$, $K-l \leq n \leq K-1$, and 0 in every other cell digit. Take two index polynomials whose new cell digits differ in this way. By induction on n their old cell digits differ in the same way, because the correction $\epsilon \theta^j y_{c,n-j}$ involves only digits with $n-j < K-l$. The geometric digits of the other coordinates are unchanged functions of V , so by linearity every $X_{c' \leftarrow c}^{(l)}$ is unchanged. The own geometric digit $y'_{c,K}$ changes by $O_c^{(l)} + \epsilon \theta^j \Delta y_{c,K-j}$, where $\Delta y_{c,K-j}$ is 1 if $j = l$ and 0 if $j > l$. On the other side $1/\varphi'_c = (1/\varphi_c)(1 - \epsilon w^j + O(w^{j+1}))$ leaves v_c and $\chi_{c,d}$, $d < j$, unchanged and changes $\chi_{c,j}$ by $-\epsilon \theta^j$, so $\Psi_c(l)$ changes by $-\epsilon \theta^l$ if $j = l$ and not at all if $j > l$. In both cases the sum $O_c^{(l)} + \Psi_c(l)$ is unchanged. Any local multiplier with the same $v_c, \chi_{c,1}, \dots, \chi_{c,l-1}$ is φ_c times a unit $1 + O(w^l)$, a product of such factors, and the responses up to depth l depend on finitely many of them (only $\varphi_c \bmod (z - a_c)^{K+1}$ enters level K , remark after Lemma 21).

(iii) By the covering condition, for every column c the set $W_o^{(c)} + [0, B]$ contains $B+1$. Take the step $e = (1, \dots, 1)$ and any $\xi_c \in \sum_{c' \neq c} W_{c \leftarrow c'}$. Then $\omega + \xi_c + t = B+1$ for some $\omega \in W_o^{(c)}$ and $t \in [0, B]$, so $S_c(e) \ni \sigma_c := \omega + \xi_c = B+1 - t \in [1, B+1]$, and $f_1(1, \sigma_c) = (\sigma_c - 1)/p \leq B/p$ (Remark 24). Summing over c gives $\text{LB}(W)^2 \leq sB^2/p^2$. For the second statement, Λ_v has index p in $\mathbb{Z}^s$, so by Minkowski's theorem it contains $b \neq 0$ with $\|b\|_\infty \leq p^{1/s}$; if $B+1 \geq p^{1/s}$ then $(|b| - (1+B)\mathbf{1})_+ = 0$ and $\lambda_{\text{jit},B}(\Lambda_v) = 0$. $\square$

A.5. The Hexagonal Brick Wall.

Proof of Theorem 69. The fixed depth-zero crosses lie in their windows: $-\kappa_{1 \leftarrow 0} = \nu/2 \equiv \frac{1}{2} + b$ and $-\kappa_{0 \leftarrow 1} = k$. Column 1 needs only a fast row: Lemma 98 with one row, step k and arc $[-k, k]$ gives $N_1 = 1 + \lceil (p - 2k - 1)/k \rceil = M_B$. Column 0 is a doubled column, but a parity argument halves the cost of Lemma 100: multiplied by -2 , the condition $\sigma + o\kappa_{1 \leftarrow 0} \in \frac{1}{2} + [-b, b]$ becomes

$o\nu + 2\xi \equiv 2\sigma - 1$ for some $|\xi| \leq b$; the even numbers 2ξ form a complete residue system modulo the odd number ν , so as o runs over M_A consecutive integers, $o\nu + 2\xi$ takes every value in an interval of $\nu M_A - 3\nu + 3 \geq p$ consecutive integers. So Proposition 64 applies. The hypotheses give (D) and (N) of Lemma 99 ($p - 1 - 2b - 2M_B$ is even and positive), whose two numbers for $s = 2$ (where T_2 is absent) are the last two terms, and the first term bounds the axis step of coordinate 0 as in the case $E = \{i\}$ of its proof. $\square$

Proof of Corollary 70. For $p \geq 10^4$ by hand: $\nu \in (p/34 - 1, p/34 + 1]$ and $k = 2\nu \in (p/17 - 2, p/17 + 2]$, so $M_B < 17(p - 1)/(p - 34) < 18$ and $M_A < 34(p - 3)/(p - 34) + 4 < 38.2$. Hence $1 - (k + M_A)/p \geq 16/17 - 40/p \geq 0.937$ and $(p - 3 - 2b)/(2p) \geq 33/68 - 3/(2p) \geq 0.485$, whose squares sum to more than 1.11; $1 - (2k + M_A)/p \geq 15/17 - 42/p \geq 0.878$ and $\eta \geq 33/68 - 35/(2p) \geq 0.483$, whose squares sum to more than 1.004; and $(1 - M_B/p)^2 \geq (1 - 17/p)^2$. The side conditions are immediate. For the 715 primes $3677 < p < 10^4$ the formula of Theorem 69 was evaluated in exact rational arithmetic, with the two coverings checked as set identities in $\mathbb{F}_p$ (c.a.). Lemma 2 gives quasi-uniformity. $\square$

A.6. Small Bases.

Proof of Proposition 75. All entries of $\vec{\mathcal{H}}$ lie in $\mathbb{F}_q(x)(\vartheta) = \bigoplus_{b < s'} \mathbb{F}_q(x)\vartheta^b$. Write each as $F = \sum_{b < s'} P_b \vartheta^b / E$ with one common denominator $E \in \mathbb{F}_q[x]$ and unique polynomial numerators P_b . Since $E(x)^q = E(x^q)$, inserting the Mahler equation and expanding by the binomial theorem gives

$$\mathcal{C}_r F = \sum_{a < s'} \frac{\vartheta^a}{E} \mathcal{C}_r \left(\sum_{b \geq a} \binom{b}{a} A^a B^{b-a} E^{q-1} P_b \right),$$

of the same form with the same E . As $\deg \mathcal{C}_r P \leq \deg P/q$, numerators of degree at most d stay of degree at most d once $d \geq ((s' - 1) \max(\deg A, \deg B) + (q - 1) \deg E)/(q - 1)$. The vectors of such numerators form a finite set stable under all $\mathcal{C}_r$, and $[x^0]F$ is linear in them. Finally $[x^l]\mathcal{H}_i = D_i(l)$, $[x^l]x\mathcal{H}_i = D_i(l - 1)$, and (6) applies; the words with a nonzero digit are the expansions of the integers $l \geq 1$. $\square$

Proof of Lemma 77. Put $\hat{G} = G/(1 + x)$. In characteristic two $(1 + x)^2 = 1 + x^2$, and for $n \geq 1$ the coefficients of x^n in the entries $\frac{1}{1+x^2}$, $\frac{x}{1+x}$, $\frac{1+u}{1+x}$ and $\frac{u}{x(1+x^2)}$ of $\hat{G}$ are, modulo 2, $[n \text{ even}]$, 1, $\lfloor \log_2 n \rfloor$, and 1 or $\lfloor \log_2(n + 1) \rfloor$ according as $n + 1$ is odd or even. By Proposition 22, $(D_i(l))_{i < j}$ involves $\hat{G}_n$ only for $l \leq n \leq l + j - 1$, and the last entry reads $\lfloor \log_2(n + 1) \rfloor$, so it depends only on the *pattern* of l : its parity and the bits $\lfloor \log_2 n \rfloor \bmod 2$ for $l \leq n \leq l + j$. Every $l \geq 64$ has a smaller l' with the same pattern. Let $2^k \leq l < 2^{k+1}$, so $2^{k-2} \geq j + 4$. If $l + j < 2^{k+1}$, the range $[l, l + j]$ lies in one octave and the bit is $k \bmod 2$ on it; the octave $[2^{k-2}, 2^{k-1})$ contains ranges of both parities with the same constant bit. Otherwise the range contains exactly one power of two, 2^{k+1} , and $l' = l - 3 \cdot 2^{k-1}$ has the parity of l , its range lies in $[2^{k-2}, 2^k)$ and contains 2^{k-1} at the same relative position, with the bit $k - 2 \equiv k$ before it and $k - 1 \equiv k + 1$ after it. The count 35 is a computation over $l \leq 63$. $\square$

APPENDIX B. BASE SEVEN IN DIMENSION THREE

At $p = 7$ in dimension three the residue sequences give nothing ($7 < 2^3$). The block-periodic residue sequence of Theorem 42(b) certifies $1 - 2/7$, but only at the levels $m \in 9\mathbb{N}$. This appendix gives a bound at every full level of a different kind, in which the admissible own response depends on the current cross responses of its column. It is the only history-aware bound of the paper.

TABLE 14. The table $w(\xi_1, \xi_2)$ over $\mathbb{F}_7$ of Theorem 95: row ξ_1 , column ξ_2 , entries in $\{0, \dots, 6\}$.

$\xi_1 \backslash \xi_2$	0	1	2	3	4	5	6
0	0	2	2	6	3	0	0
1	5	4	6	6	5	3	0
2	0	4	0	1	1	3	2
3	0	0	4	1	6	5	0
4	2	2	4	3	1	5	2
5	2	0	6	6	1	0	5
6	4	2	6	4	3	3	5

Let $s = 3$ and fix any frame of three distinct places in $\mathbb{F}_p$, a scale θ and constants λ_c . Indices of coordinates are taken modulo 3. For a column c' and a carry length $l \geq 1$, column c' of $D(l)$ is the triple

$$\mathbf{t}_{c'}(l) = (O_{c'}^{(l)}; \xi_1, \xi_2), \quad \xi_1 = X_{c'+1 \leftarrow c'}^{(l)}, \quad \xi_2 = X_{c'+2 \leftarrow c'}^{(l)}.$$

By Proposition 62(c) and Proposition 63, the cross partial sums $X_{c \leftarrow c'}^{(l)}$ contain the cross coefficients up to x^{l-1} and so depend only on $\psi_{c',0}, \dots, \psi_{c',l-1}$, while $O_{c'}^{(l)}$ is a function of $\psi_{c',0}, \dots, \psi_{c',l-1}$ minus $\theta^l \psi_{c',l}$. So the free digit $\psi_{c',l}$ can give the own response at length l any prescribed value, after the crosses at length l are known.

Definition 94 (Graph rule). Let $w : \mathbb{F}_p^2 \rightarrow \mathbb{F}_p$. The *graph rule* of w chooses, for every column c' and depth $l \geq 1$, the unique $\psi_{c',l}$ with

$$O_{c'}^{(l)} = w(X_{c'+1 \leftarrow c'}^{(l)}, X_{c'+2 \leftarrow c'}^{(l)}).$$

The *bound* of w is

$$\text{LB}(w)^2 := \min_e \min_{(\xi^{(c')})} \sum_c f_1(e_c, \sigma_c)^2, \quad \sigma_c = \sum_{c' \in \text{supp } e} e_{c'} \mathbf{t}(\xi^{(c')})[c],$$

over the steps $e \in \{-1, 0, 1\}^3 \setminus \{0\}$ up to sign and over one $\xi^{(c')} \in \mathbb{F}_p^2$ for each moving coordinate c' , where $\mathbf{t}(\xi^{(c')})$ is the column with own entry $w(\xi^{(c')})$ in row c' and the entries of $\xi^{(c')}$ in rows $c' + 1, c' + 2$.

By Proposition 63 every choice of the digits is realised, so the graph rule defines a self-similar scramble and, by Lemma 1, a digital $(0, 3)$ -sequence. Every column of every $D(l)$ lies on the graph $\{(w(\xi); \xi) : \xi \in \mathbb{F}_p^2\}$, whatever the frame. Unlike the window bound of Proposition 64, $\text{LB}(w)$ is not a minimum over each row separately: one choice of $\xi^{(c')}$ per moving column feeds all three rows.

Theorem 95 (Base seven). *Let $p = 7$ and let w be the table of Table 14. For every frame of three distinct places in $\mathbb{F}_7$, every scale and all constants λ_c , the graph rule of w gives a quasi-uniform digital $(0, 3)$ -sequence over $\mathbb{F}_7$ with*

$$\text{sep}(P_{3K}) \geq \frac{1}{7} \quad \text{for every } K \geq 1.$$

The proof is computer-assisted.

Proof. Lemma 23 with $j = 1$ ($7^K \geq 4$) gives $\text{sep}(P_{3K}) \geq \min(1, \text{LB}_K^{\text{act}})$. In a step e with carry lengths $l_{c'}$ the change of row c is $\sum_{c'} e_{c'} D(l_{c'})[c][c']$, and column c' of $D(l_{c'})$ is $\mathbf{t}(\xi^{(c')})$ for $\xi^{(c')} = (X_{c'+1 \leftarrow c'}^{(l_{c'})}, X_{c'+2 \leftarrow c'}^{(l_{c'})})$. So every term of LB_K^{act} is a term of $\text{LB}(w)$, and $\text{LB}_K^{\text{act}} \geq \text{LB}(w)$. It remains to show $\text{LB}(w) \geq \frac{1}{7}$. By Remark 24 every value of f_1 is a multiple of $\frac{1}{p}$, with

$f_1(\pm 1, \sigma) = 0$ only for $\sigma = \pm 1$ and $f_1(0, \sigma) = 0$ only for $\sigma \in \{-1, 0, 1\}$. Hence $\text{LB}(\mathbf{w}) \geq \frac{1}{p}$ unless some combination makes every term vanish, and this is a finite statement: up to sign and to the rotation of the coordinates, which maps the graph rule to itself, the steps form five classes, and each step has at most 7^6 combinations ($\xi^{(c')}$). An exhaustive enumeration finds no vanishing combination, so $\text{LB}(\mathbf{w}) = \frac{1}{7}$ (it is attained, for instance, by an axis step with $\xi = (0, 1)$). Quasi-uniformity follows from Lemma 2. $\square$

The table was found by a SAT solver. The bound does not use the frame, because it covers every pair of cross values, whether it occurs or not; for the same reason it is pessimistic. Two programs confirm $\text{LB}(\mathbf{w}) = \frac{1}{7}$ (Table 15), and a third confirms that for the archived instance (the cube roots of unity as places, $\theta = 1$) the bound from the actual responses is $\frac{1}{7}$ for $4 \leq K \leq 140$. On the Faure frame, for one choice of θ and constants, the exact separations at the first two levels are $\text{sep}(P_3) = 0.46$ and $\text{sep}(P_6) = 0.33$.

A table over $\mathbb{F}_{13}$ (not archived) certifies $\frac{1}{13}$ in the same way; for $p \geq 11$ the staggered residue sequences (Corollary 29) give at least as much. More generally one may replace the graph by any set of admissible triples per column that is closed under the depth step. At $p = 5$ a SAT solver reported that no bound of either kind has $\text{LB} > 0$, for any frame; no checkable proof was produced, so this is evidence about this class of bounds only (Remark 85).

APPENDIX C. COMPUTER-ASSISTED PARTS, DATA, VALIDATION AND LEAN

Every computer-assisted result consists of a written reduction, a theorem proved in the text, and an explicit finite predicate checked over a finite set. Table 15 lists these items, followed by the exact computations quoted as parameters or as results of exhaustive searches in a stated scope. The data (check vectors, designs, window systems, tables, certificates) are archived, each item with a verifier that reads only the data files, never the search programs. Searches (over check vectors, for window systems, SAT solvers) only produced the data (Section 2.5).

C.1. Verification. Every finite check used in a proof was carried out by at least two programs (Table 15), the second written from the statements of the paper only. Remark 105 and the brackets of Appendix C.4 for Theorems 80, 82 rest on one program each, the thresholds quoted after Theorem 68 on one program and the Lean kernel.

Residue and block-periodic sequences. The values $\lambda_{\text{jit}}(\Lambda_v)^2$ of Table 7 were computed by the search, by an independent enumeration in the audit, and by a short program that enumerates, for a claimed value L , the box $|b_c| \leq 1 + \lfloor \sqrt{L} \rfloor$ (which contains every lattice vector with $\|(|b| - \mathbf{1})_+\|_2^2 \leq L$); it also checks the Korobov column and the check vectors of Table 13. The entry $s = 4$, $p = 1009$ was also confirmed by a brute force over the box $|b_c| \leq 6$. For Theorem 42(c) the two programs evaluate the one-digit relaxation from its definition (from the two possible differences of positions, resp. by the minimum over all positions R) on one data file of U_4^* , U_5^* (for $s = 4$ the matrices printed after Theorem 42), and the second rejects a design whose largest diagonal entry is changed by one. For Theorem 42(d) two independent programs computed the hypothesis of Lemma 43 and $\text{LB}(F)$; the files of $U_4^*, \dots, U_7^*$ agree with an independent implementation of the definition in [18], which reproduces a_s^* and the largest entries listed there, and their reachability was checked by exact interpolation over $\mathbb{Q}$ (only the primes 2, 3, 5 occur in denominators and leading coefficients). The values β_q of Proposition 83 were computed by two audits with their own field arithmetic; for $s \leq 3$ also as maxima over every power-basis encoding and every weight (with the search program), and by a third program. The generator matrices of Table 13 were rebuilt entry by entry from Definition 33, and $\mathcal{J}$ was recomputed by an independent pipeline.

TABLE 15. The computer-assisted items: the finite check, its scope, and the independent verification. Below the middle rule: exact computations that are quoted but are not part of a proof of a theorem, proposition or corollary.

result	finite check	scope	verified by
Tab. 7 (Thm. 36, Cor. 37)	exact $\lambda_{\text{jit}}(\Lambda_v)^2$ by enumeration of Λ_v in a box; for entries marked E, all check vectors $(x, -1)$	the 18 rows, the Korobov column	three programs; a brute force at $s = 4$, $p = 1009$
Thm. 42(c) below its proof range	exact $\text{LB}(F)$ of U_4^* , U_5^* (Lem. 23, $j = 1$)	every prime $7 \leq p \leq 109$ ($s = 4$), $19 \leq p \leq 109$ ($s = 5$)	two programs; a third at 24 of them; Lean kernel
Thm. 42(d)	hypothesis of Lem. 43; exact $\text{LB}(F)$ below its range	$s = 4, \dots, 7$; primes as in the proof	two programs; Lean kernel in part (App. C.3)
Prop. 83	exact $\beta_q(k)$; for $s \leq 3$ for every f , k	the 26 rows of Tab. 11	two or three programs; Lean kernel
Thm. 95	no vanishing combination in $\text{LB}(\mathbf{w})$	5 classes of steps, $\leq 7^6$ combinations each	three programs (App. B); Lean kernel
Thm. 104	$\mathcal{P}(p_0)$, $p_0 = 19\,673\,600$	one exact evaluation	second evaluation of $\mathcal{P}$; Lean kernel
Rem. 105	hypotheses of Prop. 64 and Lem. 99, crosses in $\mathbb{F}_p$	1 035 877 primes in $[3 \cdot 10^6, 1.97 \cdot 10^7]$	checker with its own exact window bound
thresholds after Thm. 68, $s = 4, 5$ (not part of its proof)	$\mathcal{P}(p_0)$	one exact evaluation each	spot check above p_0 ; Lean kernel
Cor. 70	conditions of Thm. 69, coverings as set identities	715 primes, $3677 < p < 10^4$	second program; Lean kernel
Thms. 76, 80, 81, 82, Rem. 78	response sets (Prop. 75) and the minimum of Lem. 23	Tab. 10	second program; Lean kernel
Tab. 13, certified bounds	generator matrices rebuilt from Def. 33, exact $\lambda_{\text{jit}}(\Lambda_v)^2$	$p = 13, 17, 23, 31$	three programs
Tab. 4	orders ν , k and the levels L , m	$s = 2, \dots, 7$	second program
Cor. 7, explicit pairs	the two points of each pair are closer than the bound	244 cases of bases and carrying coordinate	exact distances of the pairs
Rem. 61 (exhaustive in its scope)	branch and bound over the check-vector sequences of the best class	$s = 2$; $p = 11, 13, 17$; $K_{\max} = 10, 8, 11$	independent reproduction
example after Cor. 58	dimension of a space of relations	$s = 4$, $J = 3$; $p = 11$, $K = 4, \dots, 11$; $p = 13, 17$, $K = 4$	two methods (and the audit)
Lem. 96 brackets	explicit close pairs of points	$K = 18$ ($\mathbb{F}_4$), $K = 75, 64$	second program for Thm. 81 only
optimality remark after Thm. 42(d)	no $\delta \in [0, A]^s$ with a smaller A in Lem. 43	$s = 4, 5, 6$	two programs
Sec. 10.4, Fig. 15	exact toroidal $\delta(\hat{P}_m)$ of the Hammersley lifts	$s = 2$: $p = 5, \dots, 19$, $m \leq 10$ ($p = 5$); $s = 3$: $p = 5, \dots, 13$, $m \leq 8$	$O(N^2)$ check for small N ; audit program with its own matrices

Window systems. The verifiers were in addition run by an adversarial audit with its own implementation. The common verifier checks for a record: admissibility of the λ_c and the places modulo p ; the crosses $\kappa_{c \leftarrow c'}$, recomputed by Proposition 62(c) in two normalisations, against the stored ones; integrality of the crosses of a rational system; condition (i) of Proposition 64; condition (ii) for every column, exactly (an exact scan for at most two restricted crosses, enumeration of $\mathbb{F}_p^j$ when $p^{j-1} \leq 2 \cdot 10^6$) or by Lemma 98 in the stored order of the rows; and $\text{LB}(W)$ from its

definition. All five archived window systems pass (the four ordered systems of Section 10 and the staggered system of Figure 18). Each of the 30 copies with one stored cross changed by one is rejected; of the 22 copies with an own window shortened by one at one end, 18 are rejected and 4 (two windows, both ends) are valid with the same bound: those windows were longer than needed. The exact separations quoted for figures and tables come from exact minimum-distance programs on the generated points.

C.2. Archive. The archive (directory `archive` of the repository named on the title page, release v1.0.0, archived at Zenodo) has one directory per item: `verify` (the verifier of the window systems, corruption test); `residue_tables` (Table 7, with the three enumeration programs); `block_lb` (the designs of Theorem 42(c),(d), the evaluations of $LB(F)$, the check of Lemma 43, the check of the files of U_s^* and the optimality search after Theorem 42(d), with the programs); `primepower` (Table 11 and the zeros of β_q after it, with the programs); `p7_graph_certificate` (Theorem 95); `bs_ruleB_s3` (Theorem 104, Remark 105); `bs_s45_thresholds` (Theorem 68); `selection_rule` (Remark 106, the window system of Figure 18); `practice` (the residue sequences of Table 13 by places, scale and check vector, with generator matrices and the computation of $\mathcal{J}$; the ordered window systems of Section 10; a point generator); `b2_dropin` (Theorem 76 as a table of 32-bit direction numbers, with a reference implementation in C and a check of its points); `failure` (Table 4, the explicit pairs of Section 3); `exact_relations` (Remark 61, the example after Corollary 58); `hammersley` (Section 10.4: the exact separations of the lifts and the check of the pairs of Proposition 88, with the programs); `common` (a shared C++ header). Each directory has a README with the statement it supports and the command that re-runs its check; every check runs in less than a minute on one core. Requirements: Python 3, C++17 and C compilers, SymPy (exact rational evaluations; one program in `block_lb`), NumPy (two programs in `practice`, one in `hammersley`). The record format of the window systems is described in `verify/README`. The automata of Section 9 and the range of Corollary 70 are part of the Lean development. The points shown in the figures are exact points of the constructions, computed from their generator matrices, except in the panels marked as schematic; the scripts that generate every figure, with their data, are in the directory `paper/scripts` of the same repository.

C.3. Lean. The written proofs are the primary evidence; the formalization is an additional, independent check, not a replacement. The library `GeoSeq` (Lean 4 with Mathlib), which extends the Lean development of [18], contains formal statements and proofs of most results of this paper. Every formalized statement is restated in a separate statement file and compared with its proof by the Comparator tool, which re-checks the proofs with two independent kernels (the Lean kernel and NanoDa) and admits only the three standard axioms (propositional extensionality, quotient soundness, choice). No proof uses `sorry` or `native_decide`; finite computations are evaluated by the Lean kernel.

Formalized results of this version. Section 3: every definition, lemma, theorem and corollary, and Remarks 9 and 15; the results on carry pairs also over every finite field, for every digit code with a carry pair, e.g. every natural identification (`carryPair_nat`, `nonqu.code`). Lemma 21 ((b) over every field), Lemma 91 over every commutative ring (`reschange`), Lemma 2 and Remark 3. Section 5: every definition, lemma, theorem, corollary and example (Theorem 32 for Definition 31). Section 6: Theorem 42(i)–(iii) for every reachable design, with the design multipliers over every field (`designNum_exists`, `designNum_order`); cases (a), (b); (c) for every $s \geq 3$ at $p \geq 5a_s^* + 4$ (`blkS_block`), and for $s = 4, 5$ with the computer-assisted ranges and the equality of $LB(F)$ (`blk4_LB_eq`, `blk5_LB_eq`); (d) for $s = 4, 5, 6$ at every prime $p \geq 11, 23, 125$ (`blk4d_block`, ..., `blk6d_block`), with Lemma 43 (`sc_LB`); Theorem 45, Proposition 46, Corollary 47. Section 7: every definition, lemma, theorem, proposition and corollary (with the upper densities).

Section 8 and Appendix D: every lemma, proposition, theorem and corollary (Section 8.5 is new). Lemma 86. Section 10.4: Propositions 87 and 88 with the constant γ (`liftslab_i`, `liftslab_ii`, `liftcarry_sharp`, `liftcarry_closed0`, `liftcarry_closedMu`, `lift_not_wellsep`; the display of Proposition 88 as a sum over the coordinates), (i) and (ii) of Proposition 87 over every finite field and digit code, Proposition 88 for every digital shift. Proposition 83 for every finite field and digit code (`primepower_of_check`), with all rows of Table 11 evaluated on explicit models $\mathbb{F}_p[x]/(f)$ (increments checked per model). Theorem 84 (`coverage_pp_of_parts`, `coverage_pp_new`), except $p = 11, 13, 17$ in (d) and case (e). Kept from the previous version, with statements that agree up to wording: Lemmas 1 and 23, Remark 24, Proposition 22, Example 18; Theorems 76, 80, 81, 82 and 95 and Remark 78 with their automata (for the instances used), Lemma 77, Corollary 79, and Propositions 92 and 93.

Where the formal statements differ in form. The theorems of Sections 7 and 8.5 are proved in residue form and transferred to Definition 20 by bridge theorems (e.g. `selfsim_joint_ii`); Propositions 54(i) and 55 are derived from Theorem 51, for every scramble of a frame. In Theorem 42(c),(d) the computer-assisted parts are checkers (one-digit relaxation, hypothesis of Lemma 43) proved sound once and evaluated by the kernel; the upper bounds behind the equalities hold for every prime (`axis_term`). Case (c) for general s uses the formal U_s^* of the nets library, defined by choice: a_s^* is not evaluated, and the equality of $\text{LB}(F)$ is proved under the hypothesis $\alpha_0 = a_s^*$ (`blkS_LB_eq_of`), checked in the paper for $s \leq 10$; the column of ones is proved for every s (`ustar_col0`). For $s = 4, 5, 6$ the literal matrices of the nets' computation are used, with reachability proved directly. The square-lattice clause of Corollary 47 is formalized as an inclusion, Theorem 84 as an assembly.

Not formalized. Theorem 42(d) for $s = 7$, for $s = 6$ below $p = 125$, for $s = 4, 5$ below $p = 11, 23$; a_s^* for $s \geq 6$; the optimality remark after Theorem 42(d); Remark 15(a),(b) for prime powers; Tables 7, 4, 13, and the optimality over f, k in Table 11; Remark 105, Lemmas 90 and 96, the binary-sequence clauses of Theorems 81 and 82, Remark 16; in Section 10.4 the list of covered sequences after Proposition 88 (of which the residue and staggered residue sequences with the places 0, 1 are formalized), in-slab bounds for the lifts of the sequences over $\mathbb{F}_4$, and the computed comparison; the other remarks and the figures.

Configurations. The new results are compared in 59 Comparator configurations with 730 theorems: 32 with 311 theorems from the first stages, 27 with 419 added for this version (`comparatorGeoSeqV10_1*`, `V10_2`, `V10_3`, `V10_3x`, `V10_4*`, `V10_5`, the last with the 51 theorems of Section 10.4). All of them, and the Palomar entry below, were accepted by both kernels. Results kept from the previous version are compared in its configurations. All configurations, of both versions and of the Palomar entry, were re-run once in sequence on the final state of the library and accepted by both kernels; the configuration of Section 10.4 was added afterwards, without changing any earlier Lean module.

Palomar entry. A self-contained entry in the format of the Palomar collection (one file of 195 lines importing only Mathlib) states the two headline results with their own definitions, checked against those of the library by bridge theorems: Corollary 7, and Theorem 36 with Corollaries 37 and 38 for the Korobov check vector and Faure places $((0, s)$ -sequence for every prime $p > 2^s$, separation bound at every prefix P_{sK-1} , bounded mesh ratio).

C.4. The Small-Base Bounds: Explicit Close Pairs. The certified bounds of Theorems 80, 81 and 82 are far below the exact separations of Table 10, but this is not a weakness of the bound (for Theorem 81 by two programs, for the others by one). A carry of length l exists only from level $K = l$ on, and the binding steps involve long carries, which the computable prefixes do not contain. The next lemma turns a binding configuration into a pair of points.

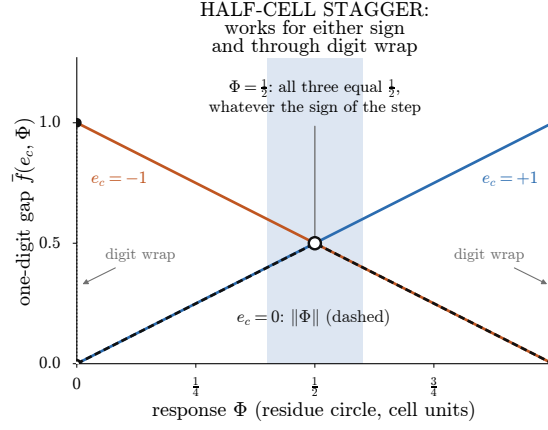


FIGURE 16. The half-cell stagger: the one-digit gap $\bar{f}(e, \Phi)$ of Lemma 66 for $e = +1, -1, 0$. $\Phi = \frac{1}{2}$ is the only response where all three agree, whatever the sign of the step; a window $\frac{1}{2} \pm 0.1$ is shaded (schematic).

Lemma 96 (Explicit close pairs). *Let the offset map be the same at every level, and fix j , a step e , carry lengths and carry digits of the moving coordinates, with the changes σ_c of Lemma 23. At a level K at least the largest carry length, the cells with this carry pattern are given by prescribing some of their finest digits. If the affine map from the remaining cell digits to the geometric digits $(R_c)_c \in \mathbb{F}_q^{sj}$ is onto, then $\text{sep}(P_{sK}) \leq (\sum_c (f_j(e_c, \sigma_c) + 2q^{-j})^2)^{1/2}$.*

Proof. Choose R_c^* attaining the minimum in $f_j(e_c, \sigma_c)$ and, by surjectivity, a cell n with the carry pattern and $R(n) = R^*$. The neighbour $n + e$ has the geometric digits $R_c^* \oplus \sigma_c$, so by (3) the two points differ in coordinate c by at most $f_j(e_c, \sigma_c) + 2q^{-j}$ cell units. $\square$

For Theorem 81 the binding configuration (carry lengths 9 and 16) is realisable at $K = 18$, where the map has full rank, and gives two points of P_{54} at distance 0.112940 cell units. So $0.112930 \leq \inf_K \text{sep}(P_{3K}) \leq 0.112940$ (computer-assisted), to 0.01%. Likewise $\text{sep}(P_{225}) \leq 0.05616$ for Theorem 80 and $\text{sep}(P_{256}) \leq 0.03176$ for Theorem 82. Larger constants in these frames need other multipliers, not better bounds.

As binary sequences, the prefixes of 2^M points of Theorem 81 have base-2 quality parameter $t \leq 3$ for $M \leq 18$, $t = 0$ at every $M = 6K$; those of Theorem 82 have $t \leq 4$ for $M \leq 20$ (computations); the three- and four-dimensional Sobol' sequences have $t = 1$ and 3.

Remark 97 (Why these bases). Heuristically: in a Kummer frame $[x^n] \tau^{-b} = \prod_i \binom{b}{n_i}$ over the base- q digits n_i of n . For $q = 3$ only $b \leq 1$ occurs, and for $q = 4$, $(1+x)^2 = 1+x^2$ keeps all coefficients in $\{0,1\}$, so the automata stay small; over $\mathbb{F}_5$ the coefficients 2, 3 appear, and the symmetric scrambles we screened had over 300 response columns per coordinate at $j = 3$, without positive bound.

APPENDIX D. WINDOW SYSTEMS

This appendix contains the details of the staggered windows of Section 8 at a finite prime: the coverings by a hierarchy of step sizes (Appendix D.1); the staggered windows at a finite prime, which prove Theorem 68 (Appendix D.2); their data and thresholds (Appendix D.3); and

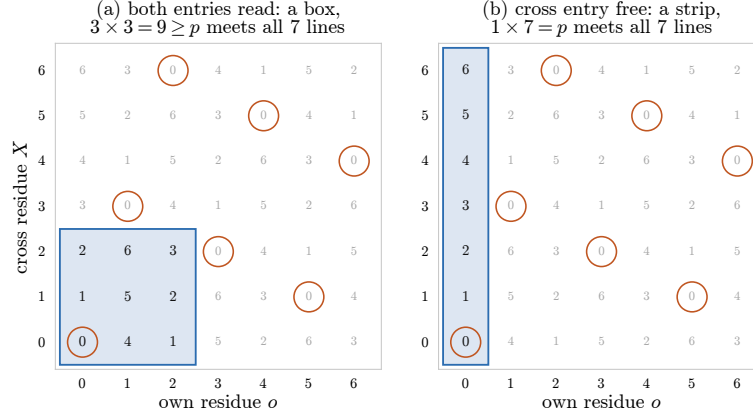


FIGURE 17. The volume bound (Lemma 65) for $s = 2$, $p = 7$, $\alpha = (1, 3)$. The free digit of column c' moves its responses along a line $\beta + \mathbb{F}_p \alpha_{c'}$, so the column window must meet every line; each pair (own, cross) is labelled by its line. (a) A 3×3 box meets all 7 lines. (b) A strip with one own value and the full cross axis also meets all 7 lines; an entry that the bound never reads costs nothing. Both coverings are checked exhaustively.

a deterministic selection rule for the free digits (Appendix D.4). Throughout, $p \geq 5$ is prime and all window systems are instances of Proposition 64.

D.1. Coverings by a Hierarchy of Step Sizes. For product windows the covering condition (ii) of Proposition 64 is a statement about translates. In column j the point $\beta + t\alpha_j$ has own entry $o = \beta_j + t$ and cross entries $\sigma_c + o\kappa_{c \leftarrow j}$ with $\sigma_c = \beta_c - \beta_j\kappa_{c \leftarrow j}$, and σ runs over $\mathbb{F}_p^{s-1}$ as β varies. So column j satisfies (ii) if and only if for every σ some $o \in W_o^{(j)}$ puts every $\sigma_c + o\kappa_{c \leftarrow j}$ into its window $W_{c \leftarrow j}$; by Lemma 65 the column window has at least p^{s-1} elements (Figure 17).

The covering is certified by a mixed-radix hierarchy. Let the own value o run through consecutive integers. If the largest step $\kappa_{c \leftarrow j}$ is at most the width of the window of its row, the translates of that window go once round the circle in a few steps; that row is the *fast row*, like the last digit of an odometer. If the next step is much smaller, its row stays inside its window while the fast row goes once round, and successive rounds move it across the circle; it is a *slow row*. An *arc* is a set of at most p consecutive residues in $\mathbb{Z}/p$.

Lemma 98 (Mixed-radix covering). *Let $k \geq 1$, let $\mathbf{m} \in \mathbb{Z}^k$ with $\nu_t := |m_t| \geq 1$, and let $I_1, \dots, I_k$ be arcs. Suppose*

$$\nu_1 \leq |I_1|, \quad N_1 := 1 + \left\lceil \frac{p - |I_1|}{\nu_1} \right\rceil, \quad N_{t-1}\nu_t \leq |I_t|, \quad N_t := N_{t-1} - 1 + \left\lceil \frac{p}{\nu_t} \right\rceil \quad (2 \leq t \leq k).$$

Then for every $\sigma \in (\mathbb{Z}/p)^k$, every set of N_k consecutive integers contains an o with $\sigma + o\mathbf{m} \in I_1 \times \dots \times I_k$.

Proof. By induction on t : every N_t consecutive integers contain an o with $\sigma_r + om_r \in I_r$ for all $r \leq t$. *Fast row.* For N_1 consecutive o , the residues σ_1 with some $\sigma_1 + om_1 \in I_1$ form the union of the translates $I_1 - om_1$; consecutive translates are shifted by $\nu_1 \leq |I_1|$, so the union is an arc of $\min(p, |I_1| + (N_1 - 1)\nu_1) = p$ residues. *Slow rows.* We may assume $m_t = \nu_t > 0$. Write $I_t = \{L, \dots, L + |I_t| - 1\} \bmod p$, fix an integer representative $\hat{\sigma}$ of σ_t , and put $o(n) = \lceil (L + np - \hat{\sigma})/\nu_t \rceil$ for $n \in \mathbb{Z}$. For the N_{t-1} integers $o(n), \dots, o(n) + N_{t-1} - 1$ we have

$\hat{o} + o\nu_t \in [L + np, L + np + |I_t| - 1]$, so $\sigma_t + o\nu_t \in I_t$. The $o(n)$ increase, are unbounded in both directions and satisfy $o(n+1) - o(n) \leq \lceil p/\nu_t \rceil$; so a run of N_t consecutive integers contains a whole run $o(n), \dots, o(n) + N_{t-1} - 1$, which by induction contains an o that is good for every $r < t$, and it is good for t as well. $\square$

D.2. Staggered Windows at a Finite Prime. This subsection proves Theorem 68: the bound for staggered windows at a finite prime (Lemma 99), the realization of the depth-zero crosses with the half from a power of two (Lemmas 100 and 101), the staggered rule (Definition 102) and its thresholds (Proposition 103, Theorem 104). Throughout, p is an odd prime and $C = \{c \neq c_\star\}$.

At a finite prime the windows of Section 8.2 become integer intervals. We use three half-widths in row $\leftarrow$ column order: $B_{C\leftarrow C}$ (into a coordinate of C from another one), $B_{\star\leftarrow C}$ (the half-cell offsets) and $B_{C\leftarrow \star}$ (into C from $c_\star$). For integers $A \geq 0$, $M_i \geq 1$ ($i \in C$) and $M_\star \geq 1$, with $M := \max_i M_i$, the *staggered windows at p* are: in column $i \in C$, own $[-(A + M_i - 1), -A]$, $W_{\star\leftarrow i} = \frac{1}{2} + [-B_{\star\leftarrow C}, B_{\star\leftarrow C}]$, $W_{j\leftarrow i} = [-B_{C\leftarrow C}, B_{C\leftarrow C}]$ for $j \in C \setminus \{i\}$; in column $c_\star$, own $[-(M_\star - 1), 0]$ and $W_{j\leftarrow \star} = [-B_{C\leftarrow \star}, B_{C\leftarrow \star}]$ for $j \in C$.

Lemma 99 (Bound for staggered windows). *Let $s \geq 2$ and suppose*

$$(D) A \geq (s-2)B_{C\leftarrow C} + B_{C\leftarrow \star}, \quad (N) A + M + (s-2)B_{C\leftarrow C} + B_{C\leftarrow \star} \leq p, \quad 2B_{\star\leftarrow C} + 2M_\star \leq p-3.$$

Then $\text{LB}(W) \geq \text{LB}_W$, where $\text{LB}_W^2 = \min(T_\star, T_{C_\star}, T_2)$ with

$$T_\star = \left(1 - \frac{M_\star}{p}\right)^2, \quad T_{C_\star} = \left(1 - \frac{A + M + B_{C\leftarrow \star}}{p}\right)^2 + \left(\frac{p-1-2B_{\star\leftarrow C}-2M_\star}{2p}\right)^2, \\ T_2 = 2\left(1 - \frac{A + M + (s-2)B_{C\leftarrow C} + B_{C\leftarrow \star}}{p}\right)^2 \quad (\text{omitted for } s=2).$$

In particular, with $x := 1 - ((s-2)B_{C\leftarrow C} + 2B_{C\leftarrow \star})/p$, $y := \frac{1}{2} - B_{\star\leftarrow C}/p$ and $A = (s-2)B_{C\leftarrow C} + B_{C\leftarrow \star}$: if $x \geq M/p$, $p(x^2 + y^2 - 1) \geq 2xM + 2y(M_\star + \frac{1}{2})$ and $1 - (2A + M)/p \geq 1/\sqrt{2}$, then $\text{LB}_W = 1 - M_\star/p$.

Proof. By Remark 24, $f_1(1, -a) = 1 - (a+1)/p$ for $0 \leq a < p$, $f_1(1, \sigma) = (\sigma-1)/p$ for $\sigma \in [1, p-1]$, $f_1(-1, \sigma) = f_1(1, -\sigma)$, and $f_1(0, \sigma) = \max(0, |\sigma| - 1)/p$. Fix a step e , $E = \text{supp } e$, $k = |E \cap C|$. A moving coordinate $i \in C$ receives its own response and one cross from each other moving column, so by (D) and (N) $e_i \sigma_i \in [-(A+M-1) - (s-2)B_{C\leftarrow C} - B_{C\leftarrow \star}, 0] \subseteq [-(p-1), 0]$, and $f_1(e_i, \sigma_i) \geq 1 - (A+M + (s-2)B_{C\leftarrow C} + B_{C\leftarrow \star})/p$; if besides i only $c_\star$ moves, this improves to $1 - (A+M + B_{C\leftarrow \star})/p$, and if i moves alone to $1 - (A+M)/p$. If $k \geq 2$, two such coordinates give T_2 . If $E = \{c_\star\}$, $f_1(1, O_\star) \geq 1 - M_\star/p$, which is $T_\star$. If $E = \{i\}$, the staggered coordinate does not move and receives $\frac{1}{2} + \xi$ with $|\xi| \leq B_{\star\leftarrow C}$, of centred absolute value at least $(p-1)/2 - B_{\star\leftarrow C}$; the term is at least $(1 - (A+M)/p)^2 + ((p-3-2B_{\star\leftarrow C})/(2p))^2 \geq T_{C_\star}$. If $E = \{i, c_\star\}$, then $e_\star \sigma_\star = \pm(\frac{1}{2} + \xi) + O_\star$ is an integer in $[(p-1)/2 - B_{\star\leftarrow C} - M_\star + 1, (p+1)/2 + B_{\star\leftarrow C}] \subseteq [1, p-1]$ by (N), so $f_1 \geq (p-1-2B_{\star\leftarrow C}-2M_\star)/(2p)$, and with coordinate i this is $T_{C_\star}$. For the last statement, $1 - (A+M + B_{C\leftarrow \star})/p = x - M/p$ and the second base of $T_{C_\star}$ is at least $y - (M_\star + \frac{1}{2})/p$; since $(x - \eta_1)^2 + (y - \eta_2)^2 \geq x^2 + y^2 - 2x\eta_1 - 2y\eta_2$, the hypothesis gives $T_{C_\star} \geq 1$, and $T_2 \geq 1$ directly. $\square$

The lemma is Theorem 67 at finite p : with half-widths about εp and $A = (s-1)B$ its bases tend to $1 - \varepsilon$, $\frac{1}{2} - \varepsilon$ and $1 - 2(s-1)\varepsilon$, and $x^2 + y^2 > 1$ holds for $\varepsilon < \varepsilon_s$. Under the last statement the only loss of order $1/p$ is the own window of $c_\star$.

Realising the windows. The fixed depth-zero crosses must lie in the windows (condition (i) of Proposition 64): the half-cell offsets $-\kappa_{\star\leftarrow i}$ near $\frac{1}{2}$ and all others within $O(p)$ of 0; and every column must cover (condition (ii)). A cross $\kappa \equiv x/2$ with a small odd integer x is close to $p/2$, and its multiples alternate between the two half-circles, so no mixed-radix hierarchy sees it as

a small step. Its double is the small odd number x , and doubling the column costs a factor 2 in the own window and nothing else.

Lemma 100 (Doubling). *Let $\xi \in \mathbb{F}_p^k$, let $\mathbf{m} \in \mathbb{Z}^k$ represent 2ξ , and suppose that $\mathbf{m}$ satisfies the hypotheses of Lemma 98 for arcs $I_1, \dots, I_k$, with number N_k . If W_o contains $2N_k - 1$ consecutive integers, then for every $\sigma \in \mathbb{F}_p^k$ some $o \in W_o$ has $\sigma + o\xi \in I_1 \times \dots \times I_k$.*

Proof. W_o contains $o_0, o_0 + 2, \dots, o_0 + 2(N_k - 1)$, and $\sigma + (o_0 + 2o')\xi = (\sigma + o_0\xi) + o'\mathbf{m}$ for $o' = 0, \dots, N_k - 1$; Lemma 98 applies to $\sigma + o_0\xi$. $\square$

By the computation at the start of Appendix D.1, this is condition (ii) for a column with steps $\xi = (\kappa_{c \leftarrow c'})_{c \neq c'}$; we call such a column a *doubled column*. The half itself comes from the 2-adic valuation of the scale. By Proposition 62(c), with the constant terms $g_c = g_c(0)$ of the multipliers,

$$\kappa_{c \leftarrow c'} = \frac{\theta g_c}{g_{c'} \Delta_{cc'}}, \quad \Delta_{cc'} := w'(a_{c'}) (a_{c'} - a_c).$$

Staggered data $\mathcal{D}$ consist of distinct rational places $a_0, \dots, a_{s-1}$, a staggered coordinate $c_\star$, an order $j_1, \dots, j_{s-1}$ of C , and positive rationals $Q_1, \dots, Q_{s-1}$ with odd numerators and odd denominators. Let $\delta \geq 0$ be the least integer with $1 + 2\delta \geq v_2(\Delta_{j_t \star} \Delta_{\star j_t})$ and $\delta + v_2(\Delta_{\star j_r}) - v_2(\Delta_{\star j_t}) - v_2(\Delta_{j_t j_r}) \geq 0$ for all $t \neq r$, where v_2 is the 2-adic valuation, and let L be the least odd positive integer such that every L/Q_r and every $L n_{cc'}^\circ$, $c \neq c_\star$, is an integer, where $n_{cc'}^\circ$ is the value of the rational $n_{cc'}$ below at $L = 1$ (it exists by the choice of δ).

Lemma 101 (The half from a power of two). *For staggered data put $g_{c_\star} = 1$, $g_{j_r} = 2^{1+\delta} Q_r / \Delta_{\star j_r}$ and $\theta = 2^\delta L T$ with an odd integer T . Then $\kappa_{c \leftarrow c'} = T n_{cc'}$ with*

$$n_{j_t \leftarrow \star} = \frac{2^{1+2\delta} L Q_t}{\Delta_{j_t \star} \Delta_{\star j_t}} \in \mathbb{Z}, \quad n_{j_t \leftarrow j_r} = 2^\delta L \frac{Q_t}{Q_r} \cdot \frac{\Delta_{\star j_r}}{\Delta_{\star j_t} \Delta_{j_t j_r}} \in \mathbb{Z}, \quad n_{\star \leftarrow j_r} = \frac{L}{2 Q_r} \in \frac{1}{2} + \mathbb{Z}.$$

For every prime p that divides none of the numerators and denominators of the $a_c - a_{c'}$, the Q_r , L , T and 2, the same identities hold in $\mathbb{F}_p$; there every $\kappa_{c \leftarrow c'}$ with $c \neq c_\star$ is the integer $T n_{cc'}$, and each half-cell offset is $\kappa_{\star \leftarrow j_r} \equiv \frac{1}{2} + (TL/Q_r - 1)/2$, half a cell plus an integer.

Proof. Substitute g and θ . In the row of $c_\star$ the frame factor cancels,

$$\frac{\theta}{g_{j_r} \Delta_{\star j_r}} = \frac{2^\delta L T}{2^{1+\delta} Q_r} = \frac{TL}{2 Q_r},$$

and L/Q_r is an odd integer. The other two expressions are integers by the choice of L , which is possible because their 2-adic valuations are $1 + 2\delta - v_2(\Delta_{j_t \star} \Delta_{\star j_t}) \geq 0$ and $\delta + v_2(\Delta_{\star j_r}) - v_2(\Delta_{\star j_t}) - v_2(\Delta_{j_t j_r}) \geq 0$. Modulo p , a half-odd rational $x/2$ is $(x + p)/2 = \frac{1}{2} + (x - 1)/2$. $\square$

So the half needs no congruence condition on p and no root of unity, and all crosses are fixed rational multiples of one odd integer T .

Definition 102 (Staggered rule). Let $\mathcal{D}$ be staggered data, $\varepsilon_{C \leftarrow \star}, \varepsilon_{C \leftarrow C}, \varepsilon_{\star \leftarrow C}$ positive rationals (window fractions) and $u > 0$ rational. At a prime p as in Lemma 101 with $up \geq 1$: (S1) T is the largest odd integer $\leq \lfloor up \rfloor$; θ and the constants g_c are those of Lemma 101, so $\kappa_{c \leftarrow c'} = T n_{cc'}$; (S2) $B_\bullet = \lfloor \varepsilon_\bullet p \rfloor$ for the three half-widths, $A = (s - 2)B_{C \leftarrow C} + B_{C \leftarrow \star}$, and the windows of Lemma 99; (S3) $M_\star$ is the number N_{s-1} of Lemma 98 for column $c_\star$ (steps $|\kappa_{j \leftarrow \star}|$ in decreasing order, arcs $[-B_{C \leftarrow \star}, B_{C \leftarrow \star}]$), and $M_i = 2N^{(i)} - 1$, where $N^{(i)}$ is the number of Lemma 98 for the doubled column i (steps $|2\kappa_{c \leftarrow i}|$ in decreasing order, the half-cell offset contributing the odd integer $\lfloor TL/Q_r \rfloor$; arcs of the rows); (S4) any selection rule (Appendix D.4).

The rule is a fixed computation of $O(s^2)$ integer operations plus the selection of the free digits; it involves no search and no covering check. It satisfies the hypotheses of Proposition 64 and Lemmas 98, 100 and 99 for all large p as soon as its limit as $p \rightarrow \infty$ does. For a column, let $\bar{\nu}_1 \geq \dots \geq \bar{\nu}_{s-1} > 0$ be its steps divided by p in the limit, $\bar{\nu} = u|n_{c \leftarrow \star}|$ in column $c_\star$ and $\bar{\nu} = 2u|n_{c \leftarrow i}|$ in a doubled column $i \in C$, and let $\lambda_t = 2\varepsilon_\bullet$ be the window fraction of the corresponding row. The data satisfy the *limit hierarchy* if in every column

$$\bar{\nu}_1 < \lambda_1, \quad \bar{N}_{t-1} \bar{\nu}_t < \lambda_t \quad (2 \leq t \leq s-1), \quad \bar{N}_1 = 2 + \frac{1 - \lambda_1}{\bar{\nu}_1}, \quad \bar{N}_t = \bar{N}_{t-1} + \frac{1}{\bar{\nu}_t},$$

and the fixed depth-zero crosses lie strictly inside their windows: $u|n_{c \leftarrow c'}| < \varepsilon_\bullet$ for $c \neq c_\star$ and $2u|n_{\star \leftarrow i}| < 2\varepsilon_{\star \leftarrow C}$. These are the limits of the hypotheses of Lemma 98 and of condition (i).

Proposition 103 (Threshold). *For the staggered rule with given data there are an explicit finite conjunction $\mathcal{P}(p)$ of inequalities between rational functions of a real variable p and an explicit function $M_\star^+(p)$ such that (a) and (b) hold; if moreover the data satisfy the limit hierarchy, $0 < \varepsilon_{\star \leftarrow C} < \frac{1}{2}$, and $x = 1 - (s-2)\varepsilon_{C \leftarrow C} - 2\varepsilon_{C \leftarrow \star}$ and $y = \frac{1}{2} - \varepsilon_{\star \leftarrow C}$ satisfy $x^2 + y^2 > 1$ and $1 - 2(s-2)\varepsilon_{C \leftarrow C} - 2\varepsilon_{C \leftarrow \star} > 1/\sqrt{2}$, then also (c) holds.*

- (a) *At every prime p as in Lemma 101 with $\mathcal{P}(p)$, the staggered rule satisfies (i) and (ii) of Proposition 64 and the hypotheses of Lemma 99 including its last statement, with $M_\star \leq M_\star^+(p)$.*
- (b) *$\mathcal{P}(p)$ implies $\mathcal{P}(p')$ for every $p' \geq p$, and $M_\star^+$ is non-increasing.*
- (c) *$\mathcal{P}(p)$ holds for all large p .*

Consequently, if $\mathcal{P}(p_0)$ holds, then for every prime $p \geq p_0$ as in Lemma 101 the staggered rule gives a digital $(0, s)$ -sequence over $\mathbb{F}_p$ with $\text{sep}(P_{sK}) \geq 1 - C''/p$ for every K , where $C'' := M_\star^+(p_0)$; under the hypotheses of (c) such a p_0 exists.

The list $\mathcal{P}$ and the proof are in Appendix D.3; any p_0 with $\mathcal{P}(p_0)$ is a valid threshold, certified by one exact rational evaluation.

Theorem 104 (The staggered rule in dimension three). *Let $s = 3$ and take the staggered data with the Faure places $(0, 1, 2)$, $c_\star = 0$, order $(1, 2)$ and $(Q_1, Q_2) = (7, 3)$; then $\delta = 2$, $L = 21$, $\theta = 84T$, $g = (1, -56, 6)$, and*

$$\kappa_{1 \leftarrow 0} = 2352T, \quad \kappa_{2 \leftarrow 0} = -126T, \quad \kappa_{0 \leftarrow 1} = \frac{3}{2}T, \quad \kappa_{0 \leftarrow 2} = \frac{7}{2}T, \quad \kappa_{1 \leftarrow 2} = -392T, \quad \kappa_{2 \leftarrow 1} = -9T.$$

With $u = 891/78\,400\,000$ and $(\varepsilon_{C \leftarrow \star}, \varepsilon_{C \leftarrow C}, \varepsilon_{\star \leftarrow C}) = (\frac{27}{1000}, \frac{1}{200}, \frac{1}{10})$, the staggered rule gives for every prime $p \geq 1.97 \cdot 10^7$ a quasi-uniform digital $(0, 3)$ -sequence over $\mathbb{F}_p$ with $\text{sep}(P_{3K}) \geq 1 - 742/p$ for every $K \geq 1$.

Proof. The six crosses are Lemma 101 (the excluded primes are 2, 3, 7). The condition $\mathcal{P}(p_0)$ holds at $p_0 = 19\,673\,600$, with $M_\star^+(p_0) = 742.355\dots$, by one exact rational evaluation (proof^{*}); as $M_\star$ is an integer, $M_\star \leq 742$. Lemma 2 gives quasi-uniformity. $\square$

The half-cell offsets are $\frac{3}{2}T$ and $\frac{7}{2}T$; in column $c_\star$ the fast row has the step $\kappa_{1 \leftarrow 0} \approx 0.027p$; the first-order deficit 742 is the size of the own window of $c_\star$.

Remark 105 (Below the threshold). The hypotheses of Proposition 64 and Lemma 99 for this rule are integer conditions at each prime. Checked at all $1\,035\,877$ primes in $[3 \cdot 10^6, 1.97 \cdot 10^7]$ by a program that computes the crosses in $\mathbb{F}_p$ from the constants g_c (not from Lemma 101), they hold with $(1 - \text{LB}_W)p \leq 779$ (c.a.). So the staggered rule gives $\text{sep}(P_{3K}) \geq 1 - 779/p$ for every prime $p \geq 3 \cdot 10^6$.

TABLE 16. The staggered data: Faure places $(0, 1, \dots, s-1)$, staggered coordinate $c_\star$, order of C , the rationals Q_r , the 2-adic data δ , L and the constants g_c of Lemma 101 (for $c = 0, \dots, s-1$), window fractions, u , the threshold p_0 (exact bisection endpoint, rounded up in the last digit shown) and the first-order deficit $C'' = M_\star^+(p_0)$ (rounded up).

	$s = 3$ (Thm. 104)	$s = 4$	$s = 5$
$c_\star$; order	0; (1, 2)	0; (1, 2, 3)	4; (0, 1, 2, 3)
Q_r	(7, 3)	153 ^r	99 ^r
δ ; L	2; 21	2; 3 581 577	5; 96 059 601
g_c	(1, -56, 6)	(1, 612, -46818, 1591812)	(-66, 34848, -7762392, 1024635744, 1)
$(\varepsilon_{C \leftarrow \star}, \varepsilon_{C \leftarrow C}, \varepsilon_{\star \leftarrow C})$	$(\frac{27}{1000}, \frac{1}{200}, \frac{1}{10})$	$\varepsilon = \frac{7}{250}$	$\varepsilon = \frac{23}{1000}$
u	891/78 400 000	259/(1.1730858534 · 10 ¹⁶)	851/(4.860548184640896 · 10 ²¹)
p_0	19 673 600	1.43146 · 10 ¹⁶	1.97832 · 10 ²¹
C''	742.356	32044.14	2.72224 · 10 ⁹

Proof of Theorem 68. Take any staggered coordinate, the natural order of C , uniform window fractions $\varepsilon < \varepsilon_s$, and $Q_r = R^r$ with an odd integer R . By Lemma 101, $n_{cc'} = 2^\delta L R^e f_{cc'}$, where $f_{cc'}$ does not depend on R and $e = t$ in row j_t of column $c_\star$, $e = t - r$ in row j_t of column j_r , and $e = -r$ for the half-cell offset of column j_r . The exponents in one column are distinct, so for R large consecutive steps of every column differ by a factor at least $1 + 1/\varepsilon$, and the largest step of every column $i \in C$ (exponent at most $s - 2$) is smaller than the largest step of column $c_\star$ (exponent $s - 1$). Choose u so that the latter is $(1 - \eta)\varepsilon$ with $0 < \eta < 1$. Then $\bar{\nu}_1 < \lambda_1 = 2\varepsilon$ in every column, the fixed depth-zero crosses are strictly inside their windows, and for $t \geq 2$

$$\bar{N}_{t-1}\bar{\nu}_t \leq 2\bar{\nu}_t + \sum_{r < t} \frac{\bar{\nu}_t}{\bar{\nu}_r} \leq 2\bar{\nu}_t + \sum_{j \geq 1} \left(1 + \frac{1}{\varepsilon}\right)^{-j} = 2\bar{\nu}_t + \varepsilon < 2\varepsilon = \lambda_t,$$

because $2\bar{\nu}_t \leq 4\varepsilon/(1 + 1/\varepsilon) < \varepsilon$ for $\varepsilon < \frac{1}{3}$. So the limit hierarchy holds. With uniform widths, $x = 1 - s\varepsilon$ and $y = \frac{1}{2} - \varepsilon$, and $x^2 + y^2 > 1$ follows from $\varepsilon < \varepsilon_s$ (proof of Theorem 67); as $y^2 < \frac{1}{4}$, this forces $(1 - s\varepsilon)^2 > \frac{3}{4}$, hence $1 - 2(s-1)\varepsilon > 1 - (2 - \sqrt{3}) > 1/\sqrt{2}$. Proposition 103 gives $p_0(s)$ and C_s'' ; the primes excluded in Lemma 101 are finitely many, and Lemma 2 gives quasi-uniformity. $\square$

For $s = 4$ (staggered coordinate 0, $R = 153$, $\varepsilon = 7/250$) Proposition 103 gives $p_0 = 1.44 \cdot 10^{16}$ and $C_4'' = 32\,044$, and for $s = 5$ (staggered coordinate 4, $R = 99$, $\varepsilon = 23/1000$) $p_0 = 1.98 \cdot 10^{21}$ and $C_5'' = 2.73 \cdot 10^9$ (exact rational evaluations, proof^{*}; Table 16). Coverings of lattice type instead of one shared hierarchy of step sizes are a possible route to lower thresholds (Section 11). Figure 18 shows the geometry of Section 8.2 in a staggered window system at a moderate prime, with coverings checked exactly instead of by the rule.

D.3. Staggered Data and Thresholds. *Staggered data.* Table 16 gives the three staggered rules of Theorems 104 and 68. In each, $\theta = 2^\delta L T$ and $\kappa_{c \leftarrow c'} = T n_{cc'}$ with the rationals $n_{cc'}$ of Lemma 101; for $s = 4, 5$ the window fractions are uniform, $\varepsilon_{C \leftarrow \star} = \varepsilon_{C \leftarrow C} = \varepsilon_{\star \leftarrow C} = \varepsilon$, with $u = \frac{999}{1000} \varepsilon / \max_t |n_{j_t \leftarrow \star}|$, which puts the step of the fast row of column $c_\star$ just inside its window.

The predicate $\mathcal{P}(p)$. Fix staggered data and a real $p > 0$. For a column, sort its steps by $|n|$ in decreasing order, $n_1, \dots, n_{s-1}$; let $k = 1$ for column $c_\star$ and $k = 2$ for a column $i \in C$ (Lemma 100; there the half-cell offset contributes $2|n_{\star \leftarrow i}| = L/Q_r$), and let $\lambda_t = 2\varepsilon_\bullet$ be the

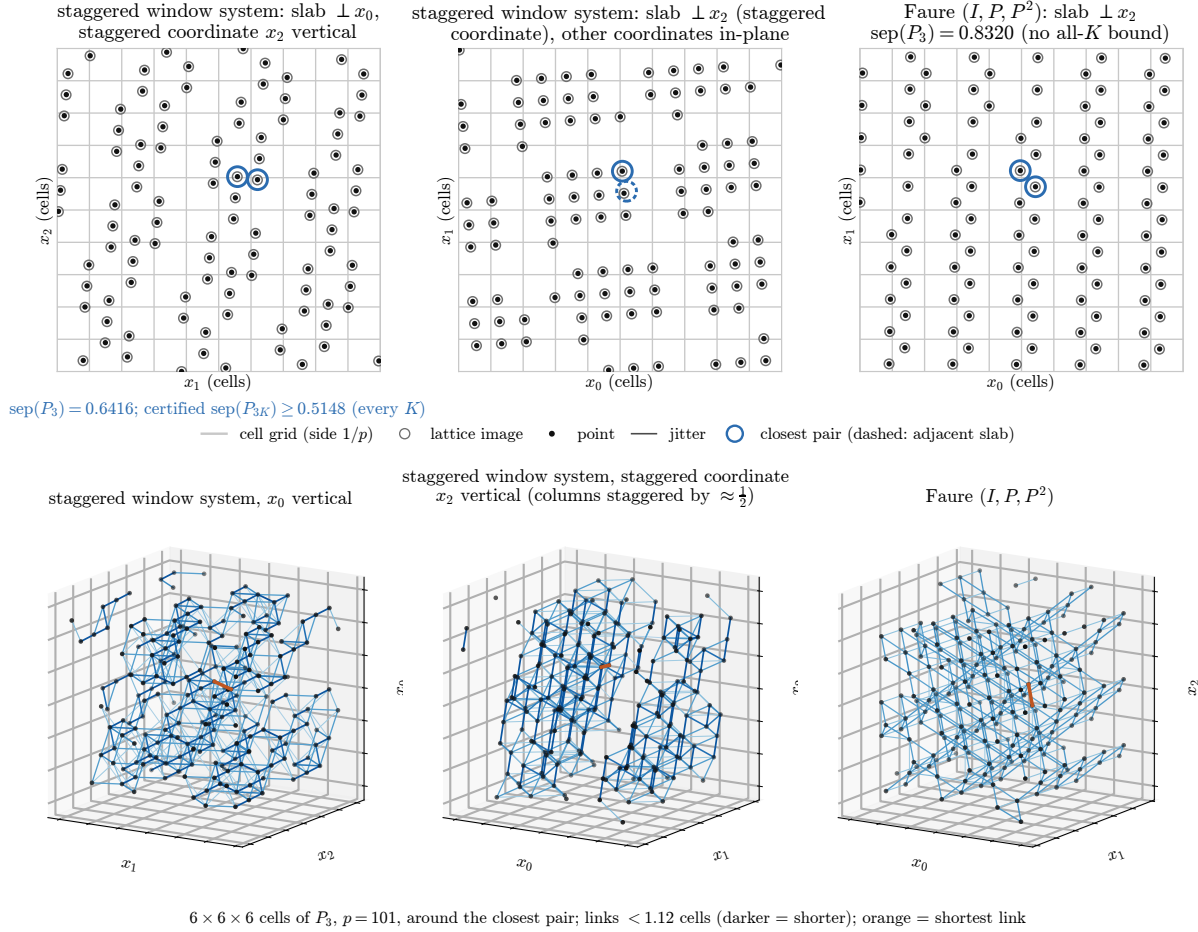


FIGURE 18. Staggered windows in dimension three: a staggered window system at $p = 101$ with exactly checked coverings (certified $\text{sep}(P_{3K}) \geq 0.5148$ for every K) and one admissible choice of the free digits. Top: slabs of P_3 one cell thick, 10×10 cells around the closest pair. Left, staggered coordinate vertical: the columns are staggered by about half a cell. Middle, orthogonal to the staggered coordinate: the coordinates of C are pushed together and wrap around along staircases. Right, Faure (I, P, P^2) . Exact $\text{sep}(P_3)$: 0.6416, and 0.8320 for Faure, which has no bound for all levels. Bottom: $6 \times 6 \times 6$ cells around the closest pair, links shorter than 1.12 cells (darker = shorter, orange = shortest), in the same three views.

window fraction of the row of step t . Put

$$\nu_t^- = k|n_t|(up - 2), \quad \nu_t^+ = k|n_t|up,$$

$$N_1^+ = 2 + \max\left(0, \frac{p - (p\lambda_1 - 1)}{\nu_1^-}\right), \quad N_t^+ = N_{t-1}^+ + \frac{p}{\nu_t^-},$$

let $M_\star^+$ be N_{s-1}^+ of column $c_\star$ and M^+ the maximum of $2N_{s-1}^+ - 1$ over the columns $i \in C$, and let x, y be as in Proposition 103. Then $\mathcal{P}(p)$ is the conjunction of (P1) $up > 2$; (P2) in every column, $\nu_1^+ \leq p\lambda_1 - 1$ and $N_{t-1}^+ \nu_t^+ \leq p\lambda_t - 1$ for $2 \leq t \leq s-1$; (P3) $|n_{c \leftarrow c'}| up \leq \varepsilon_\bullet p - 1$ for every cross with $c \neq c_\star$, where $\varepsilon_\bullet$ is the fraction of its window, and $|2n_{\star \leftarrow i}| up \leq 2(\varepsilon_{\star \leftarrow C} p - 1) - 1$ for

every half-cell offset; (P4) $x^2 + y^2 > 1$ and $p(x^2 + y^2 - 1) \geq 2xM^+ + 2y(M_\star^+ + \frac{1}{2})$; (P5) $z := 1 - 2(s-2)\varepsilon_{C \leftarrow C} - 2\varepsilon_{C \leftarrow \star} - M^+/p \geq 0$ and $2z^2 \geq 1$; (P6) $(2(s-2)\varepsilon_{C \leftarrow C} + 2\varepsilon_{C \leftarrow \star})p + M^+ + 2 \leq p - 1$, $2\varepsilon_{\star \leftarrow C}p + 2M_\star^+ + 2 < p - 1$ and $x > M^+/p$. At a prime p , $T \in (up - 2, up]$ and every arc of row t has at least $p\lambda_t - 1$ elements, so (P2) gives the hypotheses of Lemma 98 (with $N_t \leq N_t^+$), (P3) condition (i) of Proposition 64, and (P4)–(P6) the hypotheses of Lemma 99 including its last statement ((P5) is $z \geq 1/\sqrt{2}$; under (P6) the difference of the two sides of $p(x^2 + y^2 - 1) \geq 2xM + 2y(M_\star + \frac{1}{2})$ increases in x and y).

Proof of Proposition 103. $\mathcal{P}$ is obtained from the hypotheses by four substitutions: $T \in (up - 2, up]$, so every step lies in $[k|n|(up-2), k|n|up]$; every arc has at least $p\lambda_t - 1$ elements; $\lceil z \rceil \leq z + 1$ in the recursion of Lemma 98, which bounds the numbers N_t by the sums N_t^+ , and hence $M_\star$, M by $M_\star^+$, M^+ ; and Lemma 99 is replaced by its last statement. Since T is common to all entries, sorting the steps of a column by size is sorting by $|n|$, independently of p . (a) is the statement that each substituted inequality implies the original one; for the half-cell offsets, $2\kappa_{\star \leftarrow i} = TL/Q_r$ is an odd integer and $-\kappa_{\star \leftarrow i} \equiv \frac{1}{2} - (TL/Q_r + 1)/2$. (b) Each N_t^+ is a sum of terms that decrease in p for $up > 2$, and after division by p every inequality of $\mathcal{P}$ has the form “non-increasing $\leq$ non-decreasing”. (c) The hypotheses give $\varepsilon_{\star \leftarrow C} < \frac{1}{2}$ and $2(s-2)\varepsilon_{C \leftarrow C} + 2\varepsilon_{C \leftarrow \star} < 1$, so every window fraction is below $\frac{1}{2}$, $\lambda_1 < 1$ and the maximum in N_1^+ is its second term. As $p \rightarrow \infty$, $N_t^+ \rightarrow \bar{N}_t$ and $M^+/p \rightarrow 0$, so the strict inequalities of the limit hierarchy give $\mathcal{P}(p)$ for large p . The bound is Proposition 64 with Lemma 99: $\text{LB}(W) \geq 1 - M_\star/p \geq 1 - M_\star^+(p_0)/p$. $\square$

By Proposition 103(b), $\mathcal{P}$ is monotone, and a bisection in exact rational arithmetic gives a point p_0 where $\mathcal{P}(p_0)$ holds: 19 673 600, 14 314 526 192 182 751 and 1 978 313 734 082 584 379 393 for $s = 3, 4, 5$. Theorems 104 and 68 round these up to $1.97 \cdot 10^7$, $1.44 \cdot 10^{16}$ and $1.98 \cdot 10^{21}$; since the own size $M_\star$ is an integer at most $M_\star^+(p_0)$, the first-order deficits are at most 742, 32 044 and $2.73 \cdot 10^9$ (for $s = 4$, $\mathcal{P}$ fails at $1.43 \cdot 10^{16}$).

D.4. The Selection Rule. For reproducibility we fix one deterministic choice of the free digits. For the staggered window system of Figure 18 it gives $\text{sep}(P_3) = 0.6425$; the figure shows another admissible choice.

Remark 106 (A greedy selection rule). In all our window systems the own windows are integer intervals $[\text{lo}_c, \text{hi}_c] \subseteq [-(p-1), 0]$. Rank an admissible own value o (its representative in the interval) by its distance $|2o - \text{lo}_c - \text{hi}_c|$ from the centre, ties to the larger o . At depth 1 the responses are $D(1)$, with the own values on the diagonal and $-\kappa_{c \leftarrow c'}$ off it, and the admissible depth-one own values of different columns are independent. The rule chooses, over all combinations of admissible depth-one own values, one that maximises LB_1^{act} , ties broken by the ranking, column by column; at every depth $l \geq 2$ it takes the best-ranked admissible own value of each column. It uses no look-ahead and no randomness, so a sequence is determined by its places, θ , the λ_c and the windows. By Proposition 64 it has the same bound $\min(1, \text{LB}(W))$ at every full level as any other rule, and in addition $\text{sep}(P_s) \geq \min(1, \text{LB}_1^{\text{act}})$ with the best possible depth-one choice. That it maximises $\text{sep}(P_s)$ or $\text{sep}(P_{sK})$ is not claimed; among the selection rules we compared on $\text{sep}(P_3)$, it was within 10^{-3} of the best in 32 of 35 cases and never below 0.966 of it, while rules that look at one column at a time lost up to 40% at some primes (a computation that is not part of the archive).

REFERENCES

1. Abdalla G. M. Ahmed and Peter Wonka, *Optimizing dyadic nets*, ACM Trans. Graph. **40** (2021), no. 4, 141:1–141:17.
2. I. A. Antonov and V. M. Saleev, *An economic method of computing LP_τ -sequences*, USSR Comput. Math. Math. Phys. **19** (1979), no. 1, 252–256.

3. Nicolas Bonneel, David Coeurjolly, and Victor Ostromoukhov, *Perfectly equidistributed quasi-Monte Carlo sequences from Artin–Schreier polynomials*, 2026, arXiv:2607.15141.
4. Paul Bratley and Bennett L. Fox, *Algorithm 659: Implementing Sobol’s quasirandom sequence generator*, ACM Trans. Math. Software **14** (1988), no. 1, 88–100.
5. Per Christensen, Andrew Kensler, and Charlie Kilpatrick, *Progressive multi-jittered sample sequences*, Comput. Graph. Forum **37** (2018), no. 4, 21–33, Proc. EGSR 2018.
6. Gilles Christol, *Ensembles presque périodiques k -reconnaissables*, Theoret. Comput. Sci. **9** (1979), no. 1, 141–145.
7. Gilles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France **108** (1980), 401–419.
8. John H. Conway and Neil J. A. Sloane, *Sphere packings, lattices and groups*, 3 ed., Springer, 1999.
9. Josef Dick, Takashi Goda, Gerhard Larcher, Friedrich Pillichshammer, and Kosuke Suzuki, *On the quasi-uniformity properties of quasi-Monte Carlo point sets and sequences, Part I: lattices and Kronecker sequences*, Math. Comp. (2026), Published online; arXiv:2502.06202 (theorem numbers cited from arXiv v2).
10. Josef Dick, Takashi Goda, and Kosuke Suzuki, *On the quasi-uniformity properties of quasi-Monte Carlo point sets and sequences, Part II: digital nets and sequences*, Math. Comp. (2026), Published online; arXiv:2501.18226 (theorem numbers cited from arXiv v2).
11. Josef Dick and Friedrich Pillichshammer, *Digital nets and sequences: Discrepancy theory and quasi-Monte Carlo integration*, Cambridge Univ. Press, 2010.
12. Henri Faure, *Discrepance de suites associées à un système de numération (en dimension s)*, Acta Arith. **41** (1982), 337–351.
13. Henri Faure and Shu Tezuka, *Another random scrambling of digital (t, s) -sequences*, Monte Carlo and Quasi-Monte Carlo Methods 2000 (Kai-Tai Fang, Harald Niederreiter, and Fred J. Hickernell, eds.), Springer, Berlin, 2002, pp. 242–256.
14. Takashi Goda, *The Sobol’ sequence is not quasi-uniform in dimension 2*, Proc. Amer. Math. Soc. **152** (2024), no. 8, 3209–3213, arXiv:2311.05830.
15. ———, *Algebraic constructions of point sequences with quasi-uniform two-dimensional projections*, 2026, arXiv:2608.12690.
16. Takashi Goda, Roswitha Hofer, and Kosuke Suzuki, *Disproving the quasi-uniformity of the Halton sequences and of some Halton-type sequences*, J. Complexity **95** (2026), 102047, arXiv:2511.21153 (theorem numbers cited from arXiv v2).
17. Takashi Goda and Hengjun Xu, *Quasi-uniform designs from random candidates: optimal candidate complexity and farthest-point sampling*, 2026, arXiv:2609.05986.
18. Leonhard Gruenschloss, *Low-discrepancy quasi-uniform digital nets in every dimension*, Hexagon preprint hexagon:2610.00217v1, 2026, Version 1, 2026-10-13; manuscript, Lean formalization and blueprint deposited at Zenodo, doi:10.5281/zenodo.23327748; Lean entry in the Palomar registry, PALOMAR-2026-10-13-000011.
19. Leonhard Grünschoß, Johannes Hanika, Ronnie Schwede, and Alexander Keller, *(t, m, s) -nets and maximized minimum distance*, Monte Carlo and Quasi-Monte Carlo Methods 2006 (Alexander Keller, Stefan Heinrich, and Harald Niederreiter, eds.), Springer, 2008, pp. 397–412.
20. Leonhard Grünschoß and Alexander Keller, *(t, m, s) -nets and maximized minimum distance, Part II*, Monte Carlo and Quasi-Monte Carlo Methods 2008 (Pierre L’Ecuyer and Art B. Owen, eds.), Springer, 2009, pp. 395–409.
21. Andrew Helmer, Per Christensen, and Andrew Kensler, *Stochastic generation of (t, s) sample sequences*, Eurographics Symposium on Rendering – DL-only Track (Adrien Bousseau and Morgan McGuire, eds.), The Eurographics Association, 2021, pp. 21–33.
22. Roswitha Hofer, *A construction of low-discrepancy sequences involving finite-row digital (t, s) -sequences*, Monatsh. Math. **171** (2013), no. 1, 77–89.
23. ———, *Halton-type sequences in rational bases in the ring of rational integers and in the ring of polynomials over a finite field*, Math. Comput. Simulation **143** (2018), 78–88.
24. Roswitha Hofer and Kosuke 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, arXiv:1807.04383.
25. Stephen Joe and Frances Y. Kuo, *Constructing Sobol sequences with better two-dimensional projections*, SIAM J. Sci. Comput. **30** (2008), no. 5, 2635–2654.
26. N. M. Korobov, *The approximate computation of multiple integrals*, Dokl. Akad. Nauk SSSR **124** (1959), 1207–1210.
27. Gerhard Larcher and Friedrich Pillichshammer, *Walsh series analysis of the L_2 -discrepancy of symmetrized point sets*, Monatsh. Math. **132** (2001), no. 1, 1–18.

28. Jiří Matoušek, *On the L_2 -discrepancy for anchored boxes*, J. Complexity **14** (1998), 527–556.
29. David J. S. Mayor and Harald Niederreiter, *A new construction of (t, s) -sequences and some improved bounds on their quality parameter*, Acta Arith. **128** (2007), no. 2, 177–191.
30. Harald Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. **104** (1987), 273–337.
31. ———, *Random number generation and quasi-Monte Carlo methods*, CBMS-NSF Regional Conf. Ser. in Appl. Math., vol. 63, SIAM, Philadelphia, 1992.
32. Harald Niederreiter and Ferruh Özbudak, *Low-discrepancy sequences using duality and global function fields*, Acta Arith. **130** (2007), no. 1, 79–97.
33. Art B. Owen, *Randomly permuted (t, m, s) -nets and (t, s) -sequences*, Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing (Harald Niederreiter and Peter Jau-Shyong Shiue, eds.), Lecture Notes in Statist., vol. 106, Springer, 1995, pp. 299–317.
34. Luc Pronzato and Anatoly Zhigljavsky, *Quasi-uniform designs with optimal and near-optimal uniformity constant*, J. Approx. Theory **294** (2023), 105931, arXiv:2112.10401.
35. Naoki Sakai and Takashi Goda, *Space-filling lattice designs for computer experiments*, 2026, arXiv:2602.15390.
36. Ian H. Sloan and Stephen Joe, *Lattice methods for multiple integration*, Oxford Univ. Press, 1994.
37. I. M. Sobol’ and B. V. Shukhman, *Quasi-random points keep their distance*, Math. Comput. Simulation **75** (2007), no. 3–4, 80–86.
38. Ilya 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.
39. Kosuke Suzuki, *Separation properties of scrambled digital nets and related random point sets*, 2026, arXiv:2607.29063.
40. ———, *Exact ℓ^∞ -separation radius of the Sobol’ sequence in dimension 2*, J. Approx. Theory **321–322** (2027), 106356, arXiv:2508.14803 (titled “... of Sobol’ sequences in dimension 2” there).
41. Shu Tezuka, *Polynomial arithmetic analogue of Halton sequences*, ACM Trans. Model. Comput. Simul. **3** (1993), 99–107.
42. ———, *Uniform random numbers: Theory and practice*, Kluwer, 1995.