Cycles and Exact Girths in Lazebnik–Ustimenko Graphs

Tyler B. Hughes [co-author]

Second draft · November 22, 2026

DRAFT WRITTEN BY AN AI AGENT, FOR THE AUTHORS TO CHECK. NOT FOR SUBMISSION AS IS. Every sentence below was drafted by an AI agent from audited research records. No human mathematician has checked it yet. Treat this text as a verified scaffold for the authors to review and rewrite in their own words before submission. Places marked [to check] need a primary source the authors must fetch and read themselves.

Abstract

A shortest cycle in a Lazebnik–Ustimenko graph $D(k, q)$ must have length at least g_k, where $g_k = k+5$ for odd k and $g_k = k+4$ for even k. We give a one-parameter family of simple 14-cycles at $k = 9, 10$ over every finite field of order at least 4 and every infinite field. Its admissible parameters can be counted exactly. The same walk fails to close in dimension 11, where its last coordinate is an explicit nonzero rational function. For larger k, a symmetry exchanging the two halves of a shortest walk reduces its closure conditions to one polynomial identity in a 2×2 matrix. The resulting witnesses and published lifting theorems give equality with g_k for every $q \geq 4$ in 24 of the 26 dimensions from 2 through 27. Over $\mathbb{F}_3$ we determine the 19 previously unresolved entries through dimension 50. Two follow from explicit cycles and the general lower bound alone. The other 17 use five external exhaustive-search lower bounds. Lean 4 verifies the 14-cycle theorem, the known binary girth law for all dimensions, and 27 individual ternary girths through dimension 104.

2020 Mathematics Subject Classification: 05C38, 05C35, 05E16, 11T06, 68V20.
Keywords: Lazebnik–Ustimenko graphs, girth of algebraic bipartite graphs, extremal graphs without short cycles, continuant polynomials, cage problem, Lean 4 formal verification.

1 Introduction and main results

A walk in $D(k, q)$ can be described with one field element per step. Its vertices alternate between points and lines, each a k-tuple over $\mathbb{F}_q$. Once a vertex and the first coordinate of its neighbor have been chosen, the incidence equations determine the other $k-1$ coordinates in order. Thus $D(k, q)$ is q-regular on $2q^k$ vertices. The difficulty is to choose a short sequence of first coordinates that returns *every* coordinate to its starting value without retracing an edge.

Lazebnik and Ustimenko [7] developed the family from an earlier graph isomorphic to $D(9, q)$. Their lower bound is

$$\operatorname{girth} D(k, q) \;\geq\; g_k := \begin{cases} k+5, & k \text{ odd}, \\ k+4, & k \text{ even}. \end{cases} \tag{1}$$

Füredi, Lazebnik, Seress, Ustimenko and Woldar [5] conjectured equality for odd k and $q \geq 5$. Lazebnik, Sun and Wang [6] extended the question to even dimensions and $q = 4$. The later survey of Lazebnik and Wang [9] asks for equality for every $k \geq 2$ and $q \geq 4$ (Conjecture 46) and for the actual girth at $q = 3$ (Problem 47). The latter can exceed the lower bound.

A rational family. For $k = 9, 10$ the target length is 14. Pikuta's integer cycle gives the odd-dimensional result in characteristic $p > 3$ [11], and the dimension-pair equality of Xu, Cheng and Tang [17] gives its even partner. We construct a single walk over a rational function field. Its first ten coordinates close identically and the eleventh has a nonzero residue. Specialization gives a simple cycle over every field with at least four elements, including the outstanding cases in characteristics 2 and 3 (Theorem 1). Figure 2 follows those two characteristics one coordinate at a time.

Short cycles in higher dimension. A shortest possible walk in dimensions $4s + 1$ and $4s+2$ of length $4s+6$ has a strong constraint. Increments in the second half equal those in the first half multiplied alternately by λ and λ^{-1}. Knowing one half and this scalar determines the other half. The remaining equations say that a weighted sum of the diagonal entries of a polynomial matrix is constant (Theorem 2). We use this identity to exhibit witnesses valid over whole families of fields. Together with the 14-cycle, we obtain ten base dimensions $9, 10, 12, 13, 14, 20, 21, 22, 25, 26$ for every $q \geq 4$. Prior results and lifts bring the total to 24 of the 26 dimensions $2 \leq k \leq 27$. At $k = 17, 18$ only certain extensions of $\mathbb{F}_3$ remain, beginning with $\mathbb{F}_{2187}$ (Theorem 3).

Small fields. Over $\mathbb{F}_2$ a non-backtracking walk has only one continuation. Counting its steps in blocks of four gives a kernel proof of the known power-of-two girth law (Proposition 3.5). Over $\mathbb{F}_3$ there are two continuations. An explicit closed walk gives an upper bound, but some true girths exceed g_k and require stronger lower bounds. For example, $g_{39} = 44$ while girth $D(39, 3) = 48$. To prove that value we give a 48-step witness at $k = 39$, rule out shorter walks at $k = 36$ by exhaustive search, and use coordinate projection between these dimensions (Theorem 4). Figure 1 identifies the evidence behind each result.

A cycle over five elements. Take $c = 3$ in (7). In $\mathbb{F}_5$ this gives $(a, b, c, d) = (2, 3, 3, 4)$. The following ten lines apply the incidence equations in dimension 11. Array indices start at zero. Each pair (a, b) in `pairs` gives the product $p_a l_b$ on the right side of the next incidence equation. The final assertion checks both that the 14 bipartite vertices stay distinct after projection to dimension 9 and that the return has final coordinate 4 in dimension 11.

Start with a walk	What it yields	How it is proved
A 14-step word Match two searches in characteristics 2 and 3. Solve for one parameter.	Girth 14 at $k = 9, 10$ for every field $\lvert F\rvert \geq 4$.	Lean checks closure, simplicity and the matching integral-domain lower bound.
Two halves of a cycle Pair opposite turns of a shortest possible walk.	With earlier results, the lower bound is attained for all field sizes $q \geq 4$ in 24 of 26 dimensions, 2–27.	A continuant identity gives the paper proof. Further lifts use published theorems.
Ternary walks Fix the initial point. Search walks of increasing length for a collision.	The ternary girths are known throughout 2–50.	Lean proves 18 exact values in this range. For 17 new values, external searches supply the lower bounds.
Four binary steps Over the binary field, the next turn is forced.	Girth doubles at dimensions 5, 13, 29, ...	Lean proves the period of the affine four-step map.

Figure 1: How to read the proofs. The universal lower bound serves both the rational 14-cycle construction and the individual ternary certificates. The higher-dimensional families also use polynomial identities and lifting theorems. Five exhaustive searches supply the extra lower bounds needed at the ternary plateaus.

```
pairs = [(0,0),(0,1),(1,0),(2,0),(0,3),(0,4),(5,0),(6,0),(0,7),(0,8)]
v, seen = [0]*11, set()
for step, first in enumerate((0, 1, 2, 3, 3, 4, 2, 3, 3, 0, 0, 1, 1, 0)):
    seen.add((step % 2, tuple(v[:9])))
    w = [first]
    point, line = (v, w) if step % 2 == 0 else (w, v)
    for i, (a, b) in enumerate(pairs, 1):
        w.append((point[a] * line[b] - v[i]) % 5)
    v = w
assert len(seen) == 14 and v == [0]*10 + [4]
```

2 Definitions, notation, and setup

Throughout this paper, R denotes a nontrivial commutative ring with 1 (most often an integral domain or a finite field $\mathbb{F}_q$ of prime-power order $q = p^m$). To eliminate any ambiguity between the three coordinate conventions used across the literature [1, 7, 8, 9], we state each model explicitly using 1-based mathematical indices $i \in \{1, \ldots, k\}$ alongside the 0-based indices $j = i - 1 \in \mathrm{Fin}\, k$ used in our Lean 4 formalization `lean/LazebnikUstimenko/Defs.lean`.

Definition 2.1 (Coordinate models of $D(k, R)$ and $A(n, R)$)**.** Let $k \geq 2$. Each graph below is bipartite with vertex set $P_k(R) \sqcup L_k(R)$ (in Lean 4, `abbrev Vertex (k : Nat) (R : Type*) := (Fin k → R) ⊕ (Fin k → R)`, with `Sum.inl p` for a point $(p) = (p_1, \ldots, p_k) \in R^k$ and `Sum.inr l` for a line $[l] = [l_1, \ldots, l_k] \in R^k$):

(i) *Simplified survey model* $D(k,R)$ ([9], Eq. (22) and Proposition 38; Lean 4 `DGraph k R` via `PLAdj` and `rhsD`): (p) is adjacent to $[l]$ if and only if $p_i + l_i = f_i(p,l)$ for every $2 \le i \le k$, where

$$f_2 = p_1 l_1, \quad f_3 = p_1 l_2, \quad \text{and for } i \ge 4, \quad f_i = \begin{cases} p_{i-2} l_1, & i \equiv 0,1 \pmod 4, \\ p_1 l_{i-2}, & i \equiv 2,3 \pmod 4. \end{cases} \tag{2}$$

(In 0-based Lean 4 coordinates $j = i-1 \ge 1$: `p 0 * l 0` at $j=1$, `p 0 * l 1` at $j=2$, `p (j - 2) * l 0` when $(j+1) \bmod 4 \in \{0,1\}$, and `p 0 * l (j - 2)` when $(j+1) \bmod 4 \in \{2,3\}$.)

(ii) *Alternating-sign survey model* $D_{\mathrm{orig}}(k,R)$ ([9], Eqs. (18)–(21) written in additive form $p_i + l_i = \widetilde{f}_i(p,l)$; Lean 4 `DGraphOrig k R`): $\widetilde{f}_2 = p_1 l_1$, $\widetilde{f}_3 = p_1 l_2$, and for $i \ge 4$, $\widetilde{f}_i = -p_{i-2} l_1$ when $i \equiv 0,1 \pmod 4$ and $\widetilde{f}_i = p_1 l_{i-2}$ when $i \equiv 2,3 \pmod 4$.

(iii) *Original 1995 difference model* $D_{\mathrm{LU95}}(k,R)$ ([7, 8], Eq. (2.1)): (p) is adjacent to $[l]$ if and only if $l_i - p_i = f_i(p,l)$ for every $2 \le i \le k$, where $f_i(p,l)$ is the exact same bilinear monomial (2) ($l_2 - p_2 = p_1 l_1$, $l_3 - p_3 = p_1 l_2$, $l_i - p_i = p_{i-2} l_1$ for $i \equiv 0,1 \pmod 4$, and $l_i - p_i = p_1 l_{i-2}$ for $i \equiv 2,3 \pmod 4$).

(iv) *Ustimenko's alternating graph* $A(n,R)$ ($n \ge 2$; [9], Section 6.3; Lean 4 `PLAdjA`): on $R^n \sqcup R^n$, (u) is adjacent to $[v]$ if and only if $u_2 + v_2 = u_1 v_1$ and, for $3 \le i \le n$, $u_i + v_i = u_1 v_{i-1}$ when i is odd and $u_i + v_i = u_{i-1} v_1$ when i is even.

Because the right side of $p_i + l_i = f_i(p,l)$ uses only indices strictly smaller than i, every point $(p) \in R^k$ and prescribed line color $x = l_1 \in R$ uniquely determine a neighbor $\mathrm{stepLine}(p,x) = [l] \in L_k(R)$, and dually every $[l]$ and point color $x = p_1 \in R$ uniquely determine $\mathrm{stepPoint}(l,x) = (p) \in P_k(R)$. Thus $D(k,R)$ is q-regular whenever $|R| = q < \infty$, and truncating the last coordinate gives a graph homomorphism $\pi_k : D(k+1,R) \to D(k,R)$ that preserves first coordinates (and hence non-backtracking walks).

Lemma 2.2 (Explicit model isomorphisms)**.** *For every commutative ring R and every $k \ge 2$, define the involutive maps $\sigma, \nu, \tau : R^k \to R^k$ on 1-based coordinates $i \in \{1,\dots,k\}$ (0-based $j = i-1$) by*

$$\sigma(v)_i := (-1)^{\lfloor i/4 \rfloor} v_i, \qquad \nu(v)_i := \begin{cases} v_1, & i = 1, \\ -v_i, & i \ge 2, \end{cases} \qquad \tau := \sigma \circ \nu,$$

so in Lean 4 `signFactor R j` $= (-1)^{\lfloor (j+1)/4 \rfloor}$. Then:

(a) $(p) \mapsto (\sigma(p))$, $[l] \mapsto [\sigma(l)]$ is an involutive graph isomorphism $D(k,R) \xrightarrow{\sim} D_{\mathrm{orig}}(k,R)$ fixing p_1 and l_1 (Lean 4 definition `DGraph_iso_DGraphOrig`).

(b) $(p) \mapsto (\nu(p))$, $[l] \mapsto [l]$ is an involutive graph isomorphism $D_{\mathrm{LU95}}(k,R) \xrightarrow{\sim} D_{\mathrm{orig}}(k,R)$, and composing with (a) *yields the involutive isomorphism $(p) \mapsto (\tau(p))$, $[l] \mapsto [\sigma(l)]$ from $D_{\mathrm{LU95}}(k,R)$ onto $D(k,R)$ fixing p_1, l_1, and the zero edge $(0) \sim [0]$.*

Proof. For (a), set $s(i) := (-1)^{\lfloor i/4 \rfloor} \in \{\pm 1\}$. For $i \in \{1,2,3\}$ we have $s(i) = +1$, so $p_2 + l_2 = p_1 l_1$ and $p_3 + l_3 = p_1 l_2$ are unchanged. For $i \ge 4$, $\lfloor i/4 \rfloor = \lfloor (i-2)/4 \rfloor + 1$ when $i \equiv 0,1 \pmod 4$, and $\lfloor i/4 \rfloor = \lfloor (i-2)/4 \rfloor$ when $i \equiv 2,3 \pmod 4$; hence $s(i) = -s(i-2)$ for $i \equiv 0,1 \pmod 4$ and $s(i) = s(i-2)$ for $i \equiv 2,3 \pmod 4$. Since $s(1) = +1$, multiplying $p_i + l_i = f_i(p,l)$ by $s(i)$ gives $\sigma(p)_i + \sigma(l)_i = -s(i-2) p_{i-2} l_1 = -\sigma(p)_{i-2} \sigma(l)_1$ when $i \equiv 0,1$

(mod 4), and $\sigma(p)_i + \sigma(l)_i = \sigma(p)_1\sigma(l)_{i-2}$ when $i \equiv 2, 3 \pmod 4$, matching $\widetilde{f_i}(\sigma(p), \sigma(l))$ identically over R (`plAdj_iff_plAdjOrig_signFlip`). For (b), put $\tilde{p} := \nu(p)$, so $\tilde{p}_1 = p_1$ and $\tilde{p}_i = -p_i$ for $i \geq 2$. Then $\tilde{p}_i + l_i = l_i - p_i$; substituting $p_1 = \tilde{p}_1$ keeps $f_2(p, l) = \tilde{p}_1 l_1$, $f_3(p, l) = \tilde{p}_1 l_2$, and $f_i(p, l) = \tilde{p}_1 l_{i-2}$ ($i \geq 4$, $i \equiv 2, 3 \pmod 4$), whereas for $i \geq 4$ with $i \equiv 0, 1 \pmod 4$ we have $i-2 \geq 2$ and thus $f_i(p, l) = p_{i-2} l_1 = -\tilde{p}_{i-2} l_1 = \widetilde{f_i}(\tilde{p}, l)$. Composing with (a) gives $D_{\mathrm{LU95}}(k, R) \xrightarrow{\sim} D(k, R)$. □

Definition 2.3 (Simple cycles, exact girth, and non-backtracking walks)**.** Let $G = (V, E)$ be a simple graph (in Lean 4, `SimpleGraph V`):

(i) G has a simple cycle of length m (`HasCycleOfLen G m`) if $m \geq 3$ and there is an injective map $f : \operatorname{Fin} m \to V$ with $f(j)$ adjacent to $f((j+1) \bmod m)$ for all $j \in \operatorname{Fin} m$.

(ii) We write $\mathrm{GirthAtLeast}(G, g)$ if G has no simple cycle of length $< g$, $\mathrm{GirthAtMost}(G, g)$ if G has a simple cycle of length $m \leq g$, and $\mathrm{HasExactGirth}(G, g)$ (written $\operatorname{girth} G = g$) if both hold and G has a simple cycle of length g.

(iii) A closed non-backtracking walk of length $2r$ ($r \geq 2$) in a bipartite point-line graph (`ClosedNBWalk`) is a sequence $(p^{(0)}, l^{(0)}, \ldots, p^{(r-1)}, l^{(r-1)})$ with $l^{(t)}$ adjacent to $p^{(t)}$ and $p^{((t+1) \bmod r)}$, $p^{(t)} \neq p^{(t+1 \bmod r)}$, and $l^{(t)} \neq l^{(t+1 \bmod r)}$ for all t. Every simple $2r$-cycle projects to a closed non-backtracking $2r$-walk (`closed_nb_walk_projD_of_cycle`).

For Theorems 2 and 3, we also recall the monomial model $\Lambda_{k,R}$ introduced by Cheng, Chen, and Tang [1] and used in [16, 17, 19]. Its left vertices $[l] = (l_0, l_1, \ldots, l_k) \in R^{k+1}$ satisfy $l_1 = l_2$, its right vertices $\langle r \rangle = (r_0, r_1, \ldots, r_k) \in R^{k+1}$ satisfy $r_1 = 0$, and $[l] \sim \langle r \rangle$ if and only if for every $2 \leq j \leq k$, $l_j + r_j = r_0 l_{j-2}$ when $j \equiv 2, 3 \pmod 4$ and $l_j + r_j = l_0 r_{j-2}$ when $j \equiv 0, 1 \pmod 4$; dropping the redundant coordinate $j = 1$ identifies $[l] \mapsto [l_0, l_2, \ldots, l_k] \in L_k(R)$ and $\langle r \rangle \mapsto (r_0, r_2, \ldots, r_k) \in P_k(R)$ directly with (2). Over a finite field, the graph is edge-transitive (Theorem 42 of [9]), so one may move any edge of a cycle to the zero edge. Over an integral domain we consider walks $[l^{(1)}] \sim \langle r^{(1)} \rangle \sim \cdots \sim [l^{(L+1)}] \sim \langle r^{(L+1)} \rangle$ rooted at the *zero edge* $[l^{(1)}] = [0] \sim \langle r^{(1)} \rangle = \langle 0 \rangle$ and closing at $[l^{(L+1)}] = [0]$, $\langle r^{(L+1)} \rangle = \langle 0 \rangle$. Following [1, 19], the *circuit type* of such a zero-edge walk ($l_0^{(1)} = l_0^{(L+1)} = r_0^{(1)} = r_0^{(L+1)} = 0$) is the tuple $\omega = (\omega_1, \ldots, \omega_{2L}) \in (R \setminus \{0\})^{2L}$ of forward first-coordinate increments

$$\omega_{2t-1} := l_0^{(t+1)} - l_0^{(t)}, \qquad \omega_{2t} := r_0^{(t+1)} - r_0^{(t)} \qquad (1 \leq t \leq L), \tag{3}$$

which are nonzero by non-backtracking and satisfy $\sum_{t=1}^{L} \omega_{2t-1} = \sum_{t=1}^{L} \omega_{2t} = 0$. Over an integral domain R, closing all higher coordinates of $\Lambda_{k,R}$ at the zero edge reduces to polynomial equations in $\omega_1, \ldots, \omega_{2L}$ expressed via the *Euler continuant polynomials* ρ_r [1, 19]: for any $m \geq 0$ and variables $z_1, \ldots, z_m$, put $\rho_0(z_1, \ldots, z_m) := \prod_{i=1}^{m} z_i$ (empty product 1 at $m = 0$), $\rho_r(z_1, \ldots, z_m) := 0$ for $2r > m$, and for $1 \leq r \leq \lfloor m/2 \rfloor$,

$$\rho_r(z_1, \ldots, z_m) := \sum_{1 \leq j_1 < j_2 < \cdots < j_r \leq m-1,\ j_{u+1} - j_u \geq 2} \ \prod_{i \notin \{j_1, j_1+1, \ldots, j_r, j_r+1\}} z_i, \tag{4}$$

the sum of products of the $m - 2r$ unmatched variables remaining after deleting r disjoint adjacent pairs (z_j, z_{j+1}). These polynomials satisfy the linear recursion $\rho_r(z_1, \ldots, z_m) = z_m \rho_r(z_1, \ldots, z_{m-1}) + \rho_{r-1}(z_1, \ldots, z_{m-2})$ and assemble directly into 2×2 transfer matrices over $R[T]$:

Lemma 2.4 (2×2 continuant matrix identity)**.** *For any commutative ring R and tuple $g = (g_1, \dots, g_n) \in R^n$ ($n \geq 2$), define*

$$\mathcal{M}(g;T) := \prod_{j=1}^{n} \begin{pmatrix} g_j & T \\ 1 & 0 \end{pmatrix} \in R[T]^{2\times 2}. \tag{5}$$

Then the entries of $\mathcal{M}(g;T)$ are the generating polynomials of ρ_r:

$$\mathcal{M}(g;T) = \begin{pmatrix} \displaystyle\sum_{r\geq 0} \rho_r(g_1,\dots,g_n)\,T^r & \displaystyle T\sum_{r\geq 0} \rho_r(g_1,\dots,g_{n-1})\,T^r \\ \displaystyle\sum_{r\geq 0} \rho_r(g_2,\dots,g_n)\,T^r & \displaystyle T\sum_{r\geq 0} \rho_r(g_2,\dots,g_{n-1})\,T^r \end{pmatrix}. \tag{6}$$

In particular, for every $r \geq 1$ and $A, B \in R$, the coefficient of T^r in $A\,\mathcal{M}_{1,1}(g;T) + B\,\mathcal{M}_{2,2}(g;T)$ equals $A\,\rho_r(g_1,\dots,g_n) + B\,\rho_{r-1}(g_2,\dots,g_{n-1})$, while the constant term T^0 equals $A\,\rho_0(g_1,\dots,g_n) = A\prod_{j=1}^{n} g_j$.

Proof. We prove (6) by induction on $n \geq 2$. For $n = 2$,

$$\begin{pmatrix} g_1 & T \\ 1 & 0 \end{pmatrix}\begin{pmatrix} g_2 & T \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} g_1g_2 + T & g_1T \\ g_2 & T \end{pmatrix},$$

matching (6) since $\rho_0(g_1, g_2) = g_1g_2$, $\rho_1(g_1, g_2) = 1$, and $\rho_0(\varnothing) = 1$. Multiplying on the right by $\left(\begin{smallmatrix} g_{n+1} & T \\ 1 & 0 \end{smallmatrix}\right)$ sends column 1 to $g_{n+1}\,\mathrm{col}_1(\mathcal{M}(g_1,\dots,g_n)) + \mathrm{col}_2(\mathcal{M}(g_1,\dots,g_n))$ and column 2 to $T\,\mathrm{col}_1(\mathcal{M}(g_1,\dots,g_n))$, which reproduces the deletion recursion $\rho_r(z_1,\dots,z_{m+1}) = z_{m+1}\rho_r(z_1,\dots,z_m) + \rho_{r-1}(z_1,\dots,z_{m-1})$ on both rows. □

3 Proof of the main results

The first result provides the lower bound used throughout and a family that attains it.

Theorem 1 (Universal lower bound and exact girth at $k = 9, 10$)**.**

(a) (Integral-domain lower bound and model equivalence; pure-kernel Lean 4). For every commutative integral domain R and every integer $k \geq 2$, the simplified graph $D(k, R)$ and the original alternating-sign graph $D_{\mathrm{orig}}(k, R)$ are explicitly isomorphic, and neither contains a simple cycle of length strictly less than g_k.

(b) (Exact girth 14 at $k = 9, 10$ across all characteristics; pure-kernel Lean 4). Let F be any field and let $c \in F$ satisfy $c \neq 0$, $c \neq 1$, $c + 1 \neq 0$, and $c^2 + 2c - 1 \neq 0$. Put

$$a = \frac{1-c}{1+c}, \qquad b = \frac{c-1}{c^2+2c-1}, \qquad d = \frac{2c}{c^2+2c-1}. \tag{7}$$

Then the alternating point-line sequence of 14 first coordinates

$$(0),\ [0],\ (1),\ [a],\ (b),\ [c],\ (d),\ [a],\ (b),\ [c],\ (0),\ [0],\ (1),\ [1] \tag{8}$$

lifts from the origin $(0,\dots,0)$ to a simple 14-cycle in $D(10, F)$ whose projection to $D(9, F)$ is also a simple 14-cycle. Every finite field with $|F| = q \geq 4$ (including $q = 2^m \geq 4$ and $q = 3^m \geq 9$) and every infinite field admits such an admissible parameter c (proved in Lean 4; the exact census in Section 3.2 gives at least two), whence

$$\mathrm{girth}\, D(9,F) = \mathrm{girth}\, D(10,F) = 14, \qquad \mathrm{girth}\, D_{\mathrm{orig}}(9,F) = \mathrm{girth}\, D_{\mathrm{orig}}(10,F) = 14.$$

This construction is doubly sharp in Lean 4: in $D(11, F)$ the 14-step lift ends at 11-th coordinate $c(c-1)/(c^2+2c-1) \neq 0$, in both sign conventions. Over $\mathbb{F}_3$ no admissible c exists while $\operatorname{girth} D(k, \mathbb{F}_3) \leq 18$ *for $9 \leq k \leq 14$ (outside Lean 4, Table 4 of [9] and BFS in* `recompute.py` *give* $\operatorname{girth} D(9, \mathbb{F}_3) = \operatorname{girth} D(10, \mathbb{F}_3) = 18$*).*

(c) (Cascade consequences; parameterized Lean 4 bridges). Combining part (b) *with Theorem 2 of [17] and Theorem 55 of [9] yields* $\operatorname{girth} D(k, q) = g_k$ *for all prime powers $q \geq 4$ at $k \in \{23, 24, 51\}$, for all $q = 2^m \geq 4$ along the dyadic ray $k \in \{7 \cdot 2^t - 5,\ 7 \cdot 2^t - 4\}$ ($t \geq 1$), and for all $q = p^m \geq 4$ along $k \in \{14p^s - 5,\ 14p^s - 4\}$ ($s \geq 0$), resolving the blank Table 9–12 cells $(52, 16)$, $(52, 32)$, $(37, 27)$, $(38, 27)$, $(79, 27)$, and $(80, 27)$ of [9].*

3.1 The universal lower bound over an integral domain

Classical proofs of $\operatorname{girth} D(k, q) \geq g_k$ either invoke Lie-algebra root automata [7] or divide by 2 when constructing point-transitive automorphisms [15]. Following our Lean 4 module `LowerBound.lean`, we give a division-free proof valid over *every* commutative integral domain R, in three steps: (1) a meet-in-the-middle leading-coordinate invariant in Ustimenko's graph $A(n, R)$ for walks rooted at (0), (2) an odd-coordinate projection $D(2m+1, R) \to A(m+2, R)$, and (3) explicit division-free triangular automorphisms acting transitively on $P_k(R)$.

Lemma 3.1 (Leading-coordinate invariant in $A(n, R)$)**.** *Let R be an integral domain and let $2 \leq r \leq n$. Let $w(0), w(1), \ldots, w(r)$ be any non-backtracking walk of r edges in $A(n, R)$ starting at the zero point $w(0) = (0, \ldots, 0) \in P_n(R)$ (1-based coordinates $1, \ldots, n$). Then for every step t with $2 \leq t \leq r$:*

(i) $w(t)_{t-1} \neq 0$*;*

(ii) $w(t)_t = w(t)_{t-1}\, w(t-1)_1$*;*

(iii) $w(t)_i = 0$ *for all $t+1 \leq i \leq n$.*

Consequently, no closed non-backtracking walk in $A(n, R)$ passing through $w(0) = 0$ can have length $2r \leq 2n$.

Proof. We give the argument of `walkA_invariant` and `no_closed_nb_walk_zero_A` in `LowerBound.lean`, with $i = j + 1$ for the corresponding Lean index j. At $t = 1$, $w(0) = 0$ implies $w(1)_i = 0$ for all $i \geq 2$ regardless of whether $w(1)_1$ is zero or nonzero. At $t = 2$, non-backtracking gives $w(2)_1 \neq w(0)_1 = 0$, Definition 2.1(iv) at $i = 2$ gives $w(2)_2 = w(2)_1 w(1)_1$. If $n \geq 3$ then $w(2)_3 = w(2)_1 w(1)_2 - w(1)_3 = 0$. For $i \geq 4$, both preceding entries $w(1)_{i-1}$ and $w(2)_{i-1}$ vanish by induction, giving $w(2)_i = 0$. Assuming (i)–(iii) hold at $t \geq 2$, consider step $t \to t+1$ ($t+1 \leq r \leq n$):

- At index $i = t$: Definition 2.1(iv) pairs coordinate $t-1$ of $w(t)$ with coordinate 1 of $w(t+1)$, giving $w(t)_t + w(t+1)_t = w(t)_{t-1}\, w(t+1)_1$. Subtracting hypothesis (ii) yields
$$w(t+1)_t = w(t)_{t-1} \big(w(t+1)_1 - w(t-1)_1\big) \neq 0,$$
since $w(t)_{t-1} \neq 0$, $w(t+1)_1 \neq w(t-1)_1$ by non-backtracking, and R is an integral domain.
- At index $i = t+1$: $w(t)_{t+1} = 0$ by (iii), and the parity of $t+1$ pairs coordinate t of $w(t+1)$ with coordinate 1 of $w(t)$, giving $w(t+1)_{t+1} = w(t+1)_t\, w(t)_1$.
- For $i \geq t+2$: $w(t)_i = 0$, and strong induction on i gives $w(t+1)_i = 0$.

Now suppose $w(0), w(1), \ldots, w(2r) = w(0)$ is a closed non-backtracking $2r$-walk in $A(n, R)$ with $w(0) = 0$ and $2 \le r \le n$. Applying (i) and (ii) at step $t = r$ both to the forward walk $w_f(t) = w(t)$ and to the reversed walk $w_b(t) = w(2r - t)$ gives

$$w(r)_{r-1}\, w(r-1)_1 = w(r)_r = w(r)_{r-1}\, w(r+1)_1.$$

Cancelling $w(r)_{r-1} \neq 0$ in the integral domain R forces $w(r-1)_1 = w(r+1)_1$, contradicting non-backtracking at $w(r)$.

Next, for odd dimension $D(2m+1, R)$ ($m \ge 1$), define the odd-coordinate projection $\psi : R^{2m+1} \to R^{m+2}$ (`idxDtoA` in `LowerBound.lean`) on 1-based coordinates by

$$\psi(z) := (z_1,\, z_2,\, z_3,\, z_5,\, z_7,\, \ldots,\, z_{2m+1}). \tag{9}$$

Comparing (2) at $i = 2, 3$ and odd $i = 2j + 1 \ge 5$ with Definition 2.1(iv) shows that ψ is a first-coordinate-preserving graph homomorphism $D(2m+1, R) \to A(m+2, R)$, ruling out closed non-backtracking walks through (0) of length $\le 2(m+2) = (2m+1)+3$, so every cycle through (0) in $D(2m+1, R)$ has even length $\ge (2m+1)+5 = g_{2m+1}$. For even $k = 2m \ge 4$, projecting $D(2m, R) \to D(2m-1, R)$ gives length $\ge (2m-1)+5 = 2m+4 = g_{2m}$, while in $D(2, R)$ any 4-cycle $(p) \sim [l] \sim (p') \sim [l']$ satisfies $(p_1 - p_1')(l_1 - l_1') = 0$, impossible in an integral domain R. Finally, point transitivity of $\mathrm{Aut}(D(k, R))$ over any commutative ring R follows by composing three explicit division-free triangular polynomial automorphisms (`t0P`/`t0L`, `t2P`/`t2L`, and `tjP`/`tjL` in `LowerBound.lean`) that clear coordinates 1, 3, and $i \neq 1, 3$ successively. This proves Theorem 1(a). □

3.2 Where the rational cycle closes

Let F be a field and let $c \in F$ satisfy the four admissibility conditions $c \neq 0$, $c \neq 1$, $c+1 \neq 0$, and $\Delta(c) := c^2 + 2c - 1 \neq 0$, with $a, b, d \in F$ defined by (7). Starting at $v_0 = (0, \ldots, 0) \in P_{10}(F)$ and stepping along the 14 first coordinates $w = (0, 0, 1, a, b, c, d, a, b, c, 0, 0, 1, 1)$ via $v_{2t+1} = \mathrm{stepLine}(v_{2t}, w_{2t+1})$ and $v_{2t+2} = \mathrm{stepPoint}(v_{2t+1}, w_{2t+2})$, direct polynomial evaluation in $F(c)$ (kernel-verified coordinate-by-coordinate in `Cycle14.lean` via `w14_0`–`w14_13`, with $q_1 := c + 1$ and $q_2 := \Delta(c)$) gives the explicit 14-vertex trajectory in $D(10, F)$:

- $v_0 = (0)^{10}$, $\quad v_1 = [0]^{10}$, $\quad v_2 = (1, 0^9)$, $\quad v_3 = [a, a, a, 0^7]$,
- $v_4 = \big(b,\ c(c-1)/q_2,\ c(c-1)/q_2,\ -c(c-1)^2/(q_1q_2),\ -c(c-1)^2/(q_1q_2),\ 0^5\big)$,
- $v_5 = \big[c,\ 0,\ -c(c-1)/q_2,\ c(c-1)/q_1,\ c(c-1)/q_1,\ c(c-1)^2/(q_1q_2),\ c(c-1)^2/(q_1q_2),\ 0^3\big]$,
- v_6, v_7, v_8 with tenth-coordinate entries $v_{7,10} = -2c^2(c-1)/(q_1q_2)$ and $v_{8,10} = c(c-1)/q_2$,
- and contracting through $v_9 = [c, -1, -1, c-1, c, -1, 0, c, 0, 0]$, $v_{10} = (0, 1, 1, 1, 0, 1, 0^4)$, $v_{11} = [0, -1, -1, -1, 0, -1, 0^4]$, $v_{12} = (1, 1, 0, 1, 0^6)$, and $v_{13} = [1, 0^9]$ back to $v_{14} = (0)^{10}$.

After 14 steps from $(0)^{11}$ in $D(11, F(c))$, coordinates 1 through 10 of v_{14} vanish identically over $\mathbb{Z}[c, (1+c)^{-1}, \Delta(c)^{-1}]$, while coordinate 11 equals the nonzero rational residue

$$v_{14,11} = \frac{c(c-1)}{c^2 + 2c - 1} \neq 0, \tag{10}$$

proving both closure in $D(10, F)$ (and in $D(9, F)$ by projection π_9) and sharpness at $k = 11$ (`walk14_D11_fails_closure`). Figure 2 displays the full trajectories from v_0 to v_{14} in the 11 coordinates in $\mathbb{F}_4$ and $\mathbb{F}_9$. The first nonzero entry in coordinate 10 occurs at v_7 over $\mathbb{F}_9$

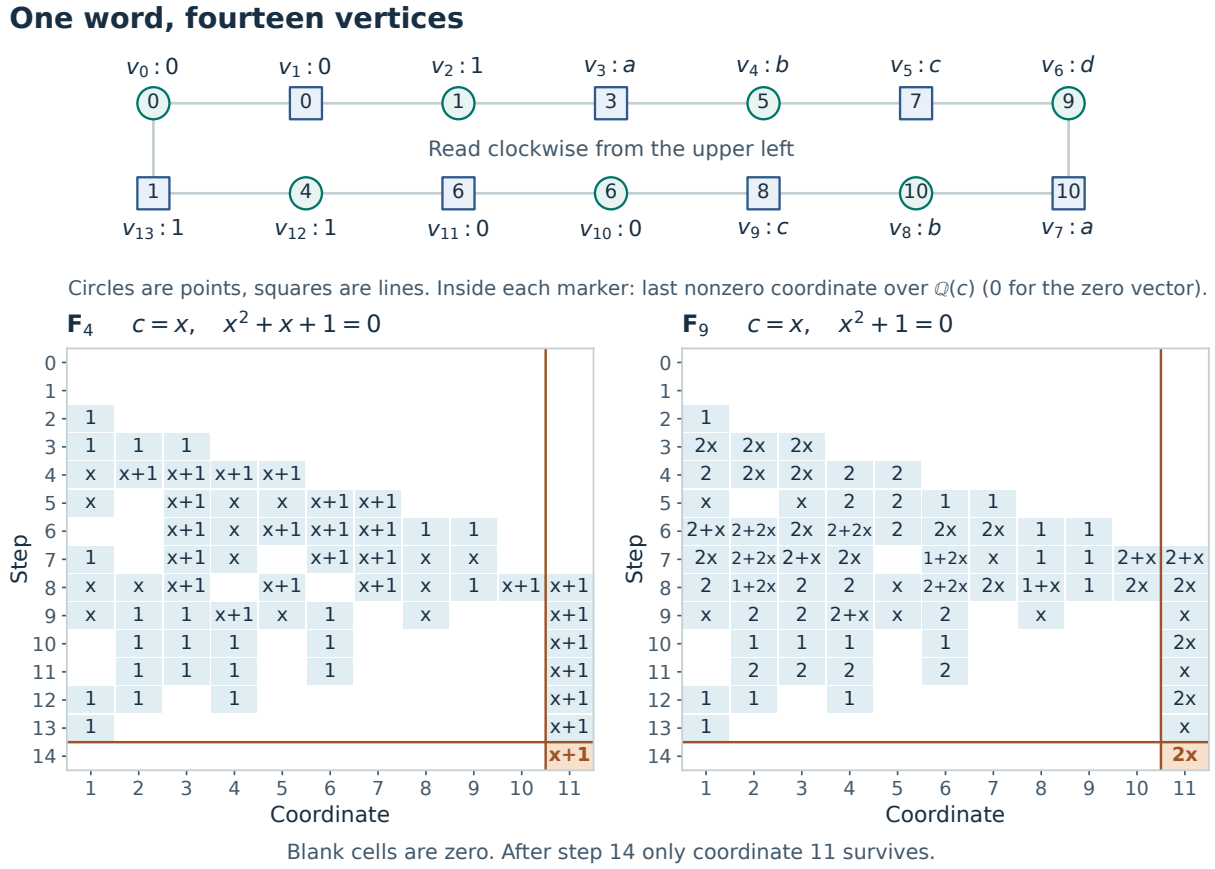

Figure 2: Anatomy of the universal 14-cycle `walk14`(c) across characteristics: (a) bipartite point-line ring with the last nonzero coordinate in $D(10, \mathbb{Q}(c))$ at each step. Panels (b) and (c) show complete 15-state, 11-coordinate trajectories at $c = x$ in $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$ and $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1)$, closing at $v_{14,1\ldots10} = 0$ while leaving nonzero $k = 11$ residues $x + 1$ and $2x$ in column 11.

and at v_8 over $\mathbb{F}_4$, since the coefficient at v_7 contains a factor 2. At v_{14} only coordinate 11 remains.

To verify simplicity (all 14 vertices distinct in $D(9, F)$, and hence also in $D(10, F)$): first, non-backtracking requires the 7 cyclic point-coordinate differences $w_{2t} - w_{2t+2}$ and 7 cyclic line-coordinate differences $w_{2t-1} - w_{2t+1}$ to be nonzero. Up to sign, these 14 differences are

$$1, \quad a, \quad c - a, \quad c, \quad 1, \quad b, \quad b - 1, \quad d - b,$$

and over $\mathbb{Z}[c, (1 + c)^{-1}, \Delta(c)^{-1}]$ every one of them factors into units times powers of c, $c - 1$, $c + 1$, and $\Delta(c)$:

$$a = \frac{1 - c}{1 + c}, \qquad c - a = \frac{\Delta(c)}{1 + c}, \qquad b = \frac{c - 1}{\Delta(c)},$$
$$b - 1 = \frac{-c(c + 1)}{\Delta(c)}, \qquad d - b = \frac{c + 1}{\Delta(c)}.$$

Hence admissibility of c makes the 14-walk closed and non-backtracking in $D(10, F)$ (`walk14_closedNBWalk_D10`, which with `D9_girthAtLeast_14`, `D10_girthAtLeast_14`,

and `hasExactGirth_of_closed_nb_walk_of_girthAtLeast` already yields exact girth 14 in Lean 4). We can also see directly on coordinates $1, \dots, 9$ that all 14 vertices are pairwise distinct: among the 7 points $v_0, v_2, v_4, v_6, v_8, v_{10}, v_{12}$, their first coordinates are $(0, 1, b, d, b, 0, 1)$. Since $0, 1, b$ are pairwise distinct ($b \notin \{0, 1\}$), $d - 1 = (1 - c^2)/\Delta(c) \neq 0$, $d - b = (c + 1)/\Delta(c) \neq 0$, and $d = 2c/\Delta(c)$ vanishes only in $\operatorname{char} F = 2$, the only point pairs sharing a first coordinate are:

- (v_0, v_{10}) (plus v_6 when $\operatorname{char} F = 2$): $v_{0,2} = 0$, $v_{10,2} = 1$, and in $\operatorname{char} F = 2$ we have $\Delta(c) = (c + 1)^2$, so $v_{6,2} = 0$ and $v_{6,6} = c(c - 1)/\Delta(c) = c/(c + 1) \notin \{0, 1\}$, separating v_6 from both v_0 ($v_{0,6} = 0$) and v_{10} ($v_{10,6} = 1$);
- (v_2, v_{12}): $v_{2,2} = 0 \neq 1 = v_{12,2}$;
- (v_4, v_8): $v_{4,9} = 0 \neq c^2(c - 1)/\Delta(c) = v_{8,9}$.

Similarly, the 7 lines $v_1, v_3, v_5, v_7, v_9, v_{11}, v_{13}$ have first coordinates $[0, a, c, a, c, 0, 1]$ (with $a \notin \{0, c\}$, $c \notin \{0, 1\}$, and in $\operatorname{char} F = 2$, $a = 1$ is separated from $v_{13} = [1, 0^8]$ by $v_{3,2} = 1 \neq 0$ and $v_{7,4} = c \neq 0$), and the three pairs (v_1, v_{11}), (v_3, v_7), (v_5, v_9) are separated by coordinates 2, 4 ($v_{3,4} = 0 \neq -c = v_{7,4}$), and 8 ($v_{5,8} = 0 \neq c = v_{9,8}$), respectively. Thus all 14 vertices are pairwise distinct in $D(9, F)$ and $D(10, F)$.

The same calculation counts the members of the family. Write $N(q)$ for the number of admissible parameters in $\mathbb{F}_q$. Completing the square gives

$$N(q) = \begin{cases} q - 2, & q \text{ even}, \\ q - 5, & q \text{ odd and 2 is a square in } \mathbb{F}_q, \\ q - 3, & q \text{ odd and 2 is a nonsquare in } \mathbb{F}_q. \end{cases}$$

Indeed the excluded elements are $0, 1, -1$ and the roots of $(c + 1)^2 = 2$. In characteristic two this set is $\{0, 1\}$. In odd characteristic the three displayed elements are distinct and none solves the quadratic, which has either two roots or none. In particular $N(2) = N(3) = 0$ and $N(q) \geq 2$ for $q \geq 4$ (at $q = 5$ the two parameters are $2, 3$). An infinite field loses at most five elements. The first coordinate of v_5 is c, so distinct parameters give distinct rooted, labelled walks. Counting cycles up to automorphisms or changes of starting vertex would require further identifications. The count and parameter injectivity are proved in `Char2AndStructure.lean`.

Combining $\operatorname{girth} D(k, F) \leq 14$ with Theorem 1(a) and Lemma 2.2 proves Theorem 1(b). Part (c) follows immediately by substituting $\operatorname{girth} D(10, q) = 14$ into Theorem 2 parts (2)–(4) of [17] (giving $2 \cdot 10 + 4 = 24$, 23, and $4 \cdot 10 + 11 = 51$ for all $q \geq 4$, plus the characteristic-2 doubling induction $g_{k_{t+1}} = 2g_{k_t} = 14 \cdot 2^t$) and into Theorem 55 of [9] ($g \mapsto p^s g = 14p^s$ in characteristic p), as verified by `cascade_*` in `CascadeAndDk3.lean`.

3.3 Recovering a circuit from half its increments

Theorem 2 (Twisted half-turn law, continuant criterion, and characteristic-2 families)**.**

(a) (Exact characterization on $\Lambda_{4s+1,R}$ and $\Lambda_{4s+2,R}$). Let R be an integral domain with fraction field K, let $s \geq 1$, and put $n = 2s + 3$. A tuple $\omega = (\omega_1, \dots, \omega_{2n}) \in (R \setminus \{0\})^{2n}$ is the circuit type of a backtrackless closed walk of length $2n = 4s + 6$ rooted at the zero edge $[0] \sim \langle 0 \rangle$ in $\Lambda_{4s+1,R}$—equivalently, in $\Lambda_{4s+2,R}$—if and only if there exists $\lambda \in K^\times$

such that, writing $g = (\omega_1, \dots, \omega_n)$,

$$\omega_{j+n} = \lambda^{(-1)^{j-1}}\,\omega_j \qquad (1 \le j \le n), \tag{11}$$

$$\rho_r(g_1, \dots, g_n) + \lambda^{-1}\rho_{r-1}(g_2, \dots, g_{n-1}) = 0 \qquad (1 \le r \le s+1), \tag{12}$$

where $\rho_0(z_1, \dots, z_m) := \prod_{i=1}^{m} z_i$. *(When* $R = \mathbb{F}_q$ *with* $q \ge 4$, $\lambda = \omega_{1+n}/\omega_1 \in \mathbb{F}_q^{\times}$, *and by edge-transitivity every girth-*$(4s+6)$ *cycle of* $D(4s+1, q)$ *and* $D(4s+2, q)$ *is equivalent to one of this form.) Equivalently, in terms of the* 2×2 *continuant product* $\mathcal{M}(g; T) = \prod_{j=1}^{n} \left(\begin{smallmatrix} g_j & T \\ 1 & 0 \end{smallmatrix}\right) \in R[T]^{2\times 2}$, *condition* (12) *with* $\lambda = A/B$ *(*$A, B \in R \setminus \{0\}$*) holds if and only if*

$$A\,\mathcal{M}_{1,1}(g; T) + B\,\mathcal{M}_{2,2}(g; T) = A\prod_{j=1}^{n} g_j \quad \text{in } R[T]. \tag{13}$$

Moreover, the rescaling map $\tilde{g}_{2i-1} = Ag_{2i-1}$, $\tilde{g}_{2i} = Bg_{2i}$ *produces a strictly periodic circuit* $(\tilde{g}, \tilde{g})$ *in* $\Lambda_{4s+2,R}$ *with twist* $\tilde{\lambda} = 1$. *When* $\lambda \in R^{\times}$, *the choice* $A = \lambda$, $B = 1$ *realizes the rescaling by multiplying the first coordinates of lines by* λ *while fixing the first coordinates of points. (At* $s = 0$, $k = 2$, $n = 3$, *the same criterion holds with the single equation* $\rho_1(g_1, g_2, g_3) + \lambda^{-1}\rho_0(g_2) = g_1 + g_3 + \lambda^{-1}g_2 = 0$.*)*

(b) (Doubly-infinite characteristic-2 families). Over the polynomial ring $\mathbb{F}_2[c]$, *for every pair of integers* $a, b \ge 1$ *with* $a + b \ge 3$, *the half-type tuples*

$$g^{(a,b)}(c) := \big(c,\ \underbrace{1, \dots, 1}_{2^a-1},\ \underbrace{c+1, \dots, c+1}_{2^b-1}\big) \qquad (n = 2^a + 2^b - 1), \tag{14}$$

$$g^{(a,b)}_{\mathrm{iter}}(c) := \big(\underbrace{1, \dots, 1, c, \dots, 1, \dots, 1, c}_{2^b - 1 \text{ blocks of } (1^{2^a-1},\, c)},\ c+1\big) \qquad (n = (2^b - 1)2^a + 1) \tag{15}$$

satisfy (13) *identically at* $A = B = 1$. *Evaluating at any* $c \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ *(*$m \ge 2$*) proves Conjecture 46 of [9] for every* $q = 2^m \ge 4$ *at all dimensions* $k \in \{2(2^a + 2^b) - 7,\ 2(2^a + 2^b) - 6\}$ *and* $k \in \{2^{a+b+1} - 2^{a+1} - 3,\ 2^{a+b+1} - 2^{a+1} - 2\}$, *together with all dyadic cascades* $k \in \{2^t n - 5,\ 2^t n - 4\}$ *(*$t \ge 1$, $n \in \{2^a + 2^b - 1,\ 2^{a+b} - 2^a + 1\}$*) via Corollary 1 of [17]. (At the boundary* $(a, b) = (1, 1)$, $n = 3$ *closes in even dimension* $k = 2$, *giving* $\operatorname{girth} D(2, 2^m) = 6$ *and dyadic cascades for* $t \ge 2$, *whereas the odd value* $2n - 5 = 1$ *lies outside the domain* $k \ge 2$ *of* $D(k, q)$, *where* $D(1, q) \cong K_{q,q}$ *has girth* $4 \ne 6$.*)*

Verification scope: Proved algebraically in Section 3.3 and verified in zero-float exact arithmetic by `recompute.py` *(outside* `lean/LazebnikUstimenko`*).*

Let R be an integral domain with fraction field K, let $s \ge 1$, and put $n = 2s + 3$, so a candidate girth walk in $\Lambda_{4s+1,R}$ or $\Lambda_{4s+2,R}$ has length $2n = 4s + 6$. We use the endpoint polynomials of Zhang et al. [19], Section 2, Lemmas 1, 3, 4, 5 and 7 and Theorem 1(3), with their parameter equal to $s+1$. Although the published theorem is stated for finite fields, the rooted closure calculation is valid over R. Indeed, stepping the incidence equations from the zero edge gives coordinates that are integer polynomials in the increments. The endpoint identities in Lemma 5 follow by those recurrences. Identity (19) of that paper, which removes the redundant last-coordinate equation in dimension $4s + 2$, is a polynomial identity with leading coefficient $\Delta_0 = 1$. Thus the same vanishing tests apply over R in both dimensions.

In finite fields, Theorem 1 of [17] also proves this equivalence for the *same circuit type*. We record the identities used below.

(i) *Endpoint and split recurrences:* $\rho_r(u_1,u_2,\beta)=\rho_{r-1}(\beta)+u_1\rho_r(u_2,\beta)$ and $\rho_r(\alpha,u_1,u_2)=\rho_{r-1}(\alpha)+u_2\rho_r(\alpha,u_1)$, together with $\rho_r(\alpha,u_1,u_2,\beta)=\sum_j \rho_j(\alpha,u_1)\rho_{r-j}(u_2,\beta)+\sum_j \rho_j(\alpha)\rho_{r-1-j}(\beta)$. For $K_0<N_0\le M_0$,

$$\begin{aligned}\Omega_{M_0,N_0,K_0}(w_1,\dots,w_{M_0}) := &\sum_j \rho_j(w_1,\dots,w_{M_0})\,\rho_{K_0-j}(w_2,\dots,w_{N_0})\\ &-\sum_j \rho_j(w_2,\dots,w_{M_0})\,\rho_{K_0-j}(w_1,\dots,w_{N_0})=0.\end{aligned} \tag{16}$$

(ii) *Zero-edge closure in $\Lambda_{4s+1,R}$ and $\Lambda_{4s+2,R}$:* A tuple $\omega=(\omega_1,\dots,\omega_{4s+6})\in(R\setminus\{0\})^{4s+6}$ closes at $[0]\sim\langle 0\rangle$ in $\Lambda_{4s+2,R}$ (equivalently $\Lambda_{4s+1,R}$) if and only if

$$\begin{aligned}\rho_r(\omega_2,\dots,\omega_{4s+6})=\rho_r(\omega_1,\dots,\omega_{4s+5})=\rho_r(\omega_1,\dots,\omega_{4s+6})=0 \quad (s+2\le r\le 2s+2),\\ \rho_r(\omega_2,\dots,\omega_{4s+5})=0 \quad (s+1\le r\le 2s+1).\end{aligned} \tag{17}$$

(iii) *Step grids:* For $0\le\kappa\le T$ and $l\in\mathbb{Z}$, set $\Upsilon_{T,\kappa}:=\{(i,j):0\le i<\kappa,\ 0\le j-i\le T-\kappa\}\cup\{(i,j):\kappa\le i\le T,\ i\le j\le T\}$, $A(l):=\{(i+1,j+l):(i,j)\in A\}$, and let $\pi(A,l)$ be the set of pairs (i,j) for which $\{(i,j+1),(i,j+2)\}\subseteq A(l)$ or $\{(i-1,j),(i-2,j)\}\subseteq A(l)$. By Lemma 7 of [19], $\pi(\Upsilon_{T,\kappa},l)=\Upsilon_{T+1,\kappa+2}(l-1)$ for $0<\kappa<T$, and $\pi(\Upsilon_{T,0},l)=\Phi_{T+1}(l-1)$ where $\Phi_{T+1}:=\Upsilon_{T+1,0}\setminus\{(0,T),(0,T+1),(1,T),(1,T+1)\}$. Whenever $0\le\kappa<T$, the grid graph $G(\Upsilon_{T,\kappa})$ is connected via $(i,i)\sim(i,i+1)\sim(i+1,i+1)$.

Lemma 3.2 (Box-propagation equivalence for $\Lambda_{4s+2,R}$)**.** *Let R be an integral domain and $s\ge 1$. A tuple $\omega=(\omega_1,\dots,\omega_{4s+6})\in(R\setminus\{0\})^{4s+6}$ satisfies* (17) *if and only if*

$$\rho_1(\omega_m,\dots,\omega_{m+2s+3})=0 \quad (1\le m\le 2s+3), \qquad \rho_j(\omega_1,\dots,\omega_{2s+3+j})=0 \quad (2\le j\le 2s+2). \tag{18}$$

Proof. ($\Rightarrow$) Assume (17). At $r=2s+2$, (17) gives $\rho_{2s+2}(\omega_i,\dots,\omega_j)=0$ on $\{(1,4s+5),(1,4s+6),(2,4s+6)\}=\Upsilon_{1,0}(4s+5)$. By the endpoint recurrences (since every $\omega_m\neq 0$ in the integral domain R), vanishing of ρ_r on $\{(i,j-1),(i,j)\}$ forces $\rho_{r-1}(\omega_i,\dots,\omega_{j-2})=0$, and vanishing on $\{(i,j),(i+1,j)\}$ forces $\rho_{r-1}(\omega_{i+2},\dots,\omega_j)=0$; hence ρ_{r-1} vanishes on $\pi(\Upsilon_{t+1,0},4s+5-t)=\Phi_{t+2}(4s+4-t)$. For $0\le t\le s-1$, $r-1=2s+1-t\ge s+2$, so (17) supplies all four missing corners $\{(1,4s+5),(1,4s+6),(2,4s+5),(2,4s+6)\}$, giving $\rho_{2s+2-t}(\omega_i,\dots,\omega_j)=0$ on $\Upsilon_{t+1,0}(4s+5-t)$ for $0\le t\le s$. At $t=s$ ($r=s+2$), $\pi(\Upsilon_{s+1,0},3s+5)=\Phi_{s+2}(3s+4)$, and (17) supplies the single $r=s+1$ corner $(2,4s+5)=(1+1,(s+1)+(3s+4))$. Crucially, $\Phi_{s+2}\cup\{(1,s+1)\}=\Upsilon_{s+2,2}$ by checking $i=0$ ($0\le j\le s$), $i=1$ ($1\le j\le s+1$), and $2\le i\le s+2$ ($i\le j\le s+2$). Putting $T_u=s+2+u$ and $\kappa_u=2+2u$ ($0\le u<s$), we have $0<\kappa_u<T_u$, so Lemma 7 of [19] propagates $\rho_{s+1-u}=0$ on $\Upsilon_{s+2+u,2+2u}(3s+4-u)$ for all $0\le u\le s$. At $u=s$ ($r=1$), $\Upsilon_{2s+2,2s+2}(2s+4)=\{(m,m+2s+3):1\le m\le 2s+3\}$, while $(0,0)\in\Upsilon_{T,\kappa}$ evaluates to $\rho_j(\omega_1,\dots,\omega_{2s+3+j})=0$ ($2\le j\le 2s+2$).

($\Leftarrow$) Assume (18). For $u=s,s-1,\dots,1$, $\rho_{s+1-u}=0$ on $\Upsilon_{s+2+u,2+2u}(3s+4-u)=\pi(\Upsilon_{s+1+u,2u},3s+5-u)$; since $0\le 2u<s+1+u$, $G(\Upsilon_{s+1+u,2u})$ is connected and anchored at $(0,0)\mapsto(1,3s+5-u)$ where $\rho_{s+2-u}=0$ by (18), propagating $\rho_{s+2-u}=0$ across $\Upsilon_{s+1+u,2u}(3s+5-u)$ down to $u=0$ ($r=s+1$, which includes $(2,4s+5)$). Likewise, $\pi(\Upsilon_{s+1,0},3s+$

$5) = \Phi_{s+2}(3s+4) \subset \Upsilon_{s+2,2}(3s+4)$ and connected-grid induction on $G(\Upsilon_{t+1,0})$ anchored at $(1, 4s+5-t)$ from (18) establish $\rho_{2s+2-t} = 0$ on $\Upsilon_{t+1,0}(4s+5-t)$ for $t = s, \dots, 0$, recovering all remaining equations of (17). □

Proof of Theorem 2(a). By Lemma 3.2, closure at $[0] \sim \langle 0 \rangle$ is equivalent to (18).

($\Rightarrow$) Assume (18) with $n = 2s+3$. For each $1 \le m \le n-1$, expanding $\rho_1(\omega_m, \dots, \omega_{m+n})$ at its left end and $\rho_1(\omega_{m+1}, \dots, \omega_{m+n+1})$ at its right end gives

$$\omega_{m+n+1}\rho_1(\omega_m, \dots, \omega_{m+n}) - \omega_m\rho_1(\omega_{m+1}, \dots, \omega_{m+n+1}) = (\omega_{m+n}\omega_{m+n+1} - \omega_m\omega_{m+1}) \prod_{u=m+2}^{m+n-1} \omega_u. \tag{19}$$

By (18) and $\omega_u \neq 0$ in the integral domain R, we get $\omega_{m+n}\omega_{m+n+1} = \omega_m\omega_{m+1}$ for $1 \le m \le n-1$. Setting $\lambda := \omega_{1+n}/\omega_1 \in K^\times$ gives $\omega_{2+n}/\omega_2 = \lambda^{-1}$ and by induction $\omega_{j+n} = \lambda^{(-1)^{j-1}}\omega_j$ for all $1 \le j \le n$ because $n = 2s+3$ is *odd* (whereas for even half-length $2s+2$ in [19], $r = s+1$ forces antiperiodicity $\mu = -1$).

Write $\omega'_r := \omega_{n+r}$. Because $\lambda \cdot \lambda^{-1} = 1$, bidegree scaling gives $\rho_t(\omega'_1, \dots, \omega'_{2r}) = \rho_t(\omega_1, \dots, \omega_{2r})$, $\rho_t(\omega'_1, \dots, \omega'_{2r+1}) = \lambda\rho_t(\omega_1, \dots, \omega_{2r+1})$, $\rho_t(\omega'_2, \dots, \omega'_{2r+1}) = \rho_t(\omega_2, \dots, \omega_{2r+1})$, and $\rho_t(\omega'_2, \dots, \omega'_{2r+2}) = \lambda^{-1}\rho_t(\omega_2, \dots, \omega_{2r+2})$. We prove by induction on $1 \le m \le 2s+2$ that $\rho_m(g_1, \dots, g_n) = -\lambda^{-1}\rho_{m-1}(g_2, \dots, g_{n-1})$:

- At $m = 1$, $\rho_1(\omega_1, \dots, \omega_{n+1}) = \omega_1\big(\lambda\rho_1(g_1, \dots, g_n) + \rho_0(g_2, \dots, g_{n-1})\big) = 0$. At $m = 2$, substituting the $m = 1$ relation into $\rho_2(\omega_1, \dots, \omega_{n+2})$ gives $\omega_1\omega_2\big(\rho_2(g_1, \dots, g_n) + \lambda^{-1}\rho_1(g_2, \dots, g_{n-1})\big) = 0$.
- Assuming the claim for $1 \le j \le 2c$ ($1 \le c \le s$), put $g^\circ := (g_2, \dots, g_{n-1})$ and $g^\flat := (g_1, \dots, g_{n-1})$. Splitting $\rho_{2c+1}(\omega_1, \dots, \omega_{n+2c+1})$ and $\rho_{2c+2}(\omega_1, \dots, \omega_{n+2c+2})$ across $(\omega_1, \dots, \omega_{n-1} \mid \omega_n, \omega'_1 \mid \omega'_2, \dots)$ leaves

$$\rho_0(\omega_1, \dots, \omega_{2c+1})\big(\lambda\rho_{2c+1}(g) + \rho_{2c}(g^\circ)\big) + \Omega_{n-1,2c+1,2c}(g^\flat) = 0,$$
$$\rho_0(\omega_1, \dots, \omega_{2c+2})\big(\rho_{2c+2}(g) + \lambda^{-1}\rho_{2c+1}(g^\circ)\big) + \lambda^{-1}\Omega_{n-1,2c+2,2c+1}(g^\flat) = 0.$$

  Since $2c+1 < 2c+2 \le n-1$, both Ω-terms vanish by (16), completing the induction and giving (12) for $1 \le r \le s+1$ (while $r \ge s+2$ is $0 = 0$).

($\Leftarrow$) Conversely, if (11) and (12) hold, then $\rho_m(g_1, \dots, g_n) + \lambda^{-1}\rho_{m-1}(g_2, \dots, g_{n-1}) = 0$ holds for all $1 \le m \le 2s+2$, so the exact same $m = 1, 2$ and split identities yield $\rho_j(\omega_1, \dots, \omega_{n+j}) = 0$ for all $1 \le j \le 2s+2$. Because (11) implies $\omega_{m+n}\omega_{m+n+1} = \omega_m\omega_{m+1}$, (19) propagates $\rho_1(\omega_m, \dots, \omega_{m+n}) = 0$ from $m = 1$ to $1 \le m \le n$, establishing (18). Lemma 2.4 (with $\deg_T \mathcal{M}_{1,1}, \deg_T \mathcal{M}_{2,2} \le s+1$) gives (13), and bidegree scaling of odd entries by A and even entries by B clears $\lambda = A/B$ to twist 1. (At $s = 0$, $k = 2$, $n = 3$, closure in $\Lambda_{2,R}$ reads $\omega_1 + \omega_3 + \omega_5 = \omega_2 + \omega_4 + \omega_6 = 0$ and $\rho_1(\omega_2, \dots, \omega_5) = \rho_1(\omega_1, \dots, \omega_6) = 0$, which eliminate ω_5, ω_6 to $(\omega_1\omega_2 - \omega_4\omega_5) = 0$ and $\omega_4/\omega_1 = \lambda = \omega_2/\omega_5$ with $g_1 + g_3 + \lambda^{-1}g_2 = 0$.) □

Proof of Theorem 2(b). Work over $S = \mathbb{F}_2[c, T]$, where $-1 = +1$ and $\mathrm{tr}(I_2) = 0$. Set $U(x) := \left(\begin{smallmatrix} x & T \\ 1 & 0 \end{smallmatrix}\right)$ and $V(x) := \left(\begin{smallmatrix} 0 & T \\ 1 & x \end{smallmatrix}\right) = U(x) + xI_2$. For any $P \in S^{2\times 2}$ with $\tau_P = \mathrm{tr}(P)$ and $\delta_P = \det(P)$, Cayley–Hamilton gives $P^2 = \tau_P P + \delta_P I_2$; squaring repeatedly in characteristic 2 yields by induction on $r \ge 1$:

$$P^{2^r} = \tau_P^{2^r-1}P + \Big(\sum_{j=0}^{r-1} \tau_P^{2^r-2^{j+1}}\delta_P^{2^j}\Big)I_2. \tag{20}$$

Since $P\,(P+\tau_P I_2)=\delta_P I_2$ and $\delta_P = T$ (or T^{2^a}) is a nonzerodivisor in S dividing every term $\delta_P^{2^j}$ $(j\ge 0)$, cancelling P from (20) gives the exact polynomial identity

$$P^{2^r-1} = \tau_P^{2^r-1} I_2 + \Psi_r(\tau_P,\delta_P)\,(P+\tau_P I_2), \qquad \Psi_r(\tau,\delta) := \sum_{j=0}^{r-1} \tau^{2^r-2^{j+1}}\delta^{2^j-1} \in S. \tag{21}$$

At $A=B=1$ in characteristic 2, $A\mathcal{M}_{1,1}+B\mathcal{M}_{2,2} = \operatorname{tr}\mathcal{M}(g;T)$.

Family 1*:* $g^{(a,b)}(c) = (c,\, 1^{2^a-1},\, (c+1)^{2^b-1})$. Applying (21) to $P=U(1)$ $(\tau=1,\delta=T)$ and $P=U(c+1)$ $(\tau=c+1,\delta=T)$ gives

$$\mathcal{M}(g^{(a,b)};T) = U(c)\big(I_2+\Psi_a(1,T)V(1)\big)\big((c+1)^{2^b-1}I_2+\Psi_b(c+1,T)V(c+1)\big).$$

Direct multiplication in characteristic 2 shows that all three cross products have trace zero: $\operatorname{tr}(U(c)V(1)) = \operatorname{tr}\left(\begin{smallmatrix} T & (c+1)T \\ 0 & T\end{smallmatrix}\right) = 0$, $\operatorname{tr}(U(c)V(c+1)) = \operatorname{tr}\left(\begin{smallmatrix} T & T \\ 0 & T\end{smallmatrix}\right) = 0$, and $\operatorname{tr}(U(c)V(1)V(c+1)) = \operatorname{tr}\left(\begin{smallmatrix} (c+1)T & T^2+(c+1)^2T \\ T & (c+1)T\end{smallmatrix}\right) = 0$. Hence $\operatorname{tr}\mathcal{M}(g^{(a,b)};T) = c(c+1)^{2^b-1} = \prod_{j=1}^{n} g_j^{(a,b)}(c)$ holds identically in $\mathbb{F}_2[c,T]$.

Family 2*:* For $g_{\mathrm{iter}}^{(a,b)}(c) = ((1^{2^a-1},c)^{2^b-1},\, c+1)$, set $P := U(1)^{2^a-1}U(c) = U(c) + \Psi_a(1,T)V(1)U(c)$. Since $V(1)U(c) = \left(\begin{smallmatrix} T & 0 \\ c+1 & T\end{smallmatrix}\right)$ has trace zero, $\tau_P = c$ and $\delta_P = T^{2^a}$. Applying (21) to P at exponent 2^b-1, multiplying on the right by $U(c+1)$, and noting that $\operatorname{tr}(V(c)U(c+1))=0$ and $\operatorname{tr}(V(1)U(c)U(c+1))=0$ in characteristic 2, we obtain

$$\operatorname{tr}\mathcal{M}(g_{\mathrm{iter}}^{(a,b)};T) = c^{2^b-1}(c+1) = \prod_{j=1}^{n} g_{\mathrm{iter},j}^{(a,b)}(c)$$

identically in $\mathbb{F}_2[c,T]$. For $a+b\ge 3$ ($n\ge 5$, so $2n-5\ge 5\ge 2$), evaluating either family at any $c\in\mathbb{F}_{2^m}\setminus\{0,1\}$ $(m\ge 2)$ produces a closed non-backtracking $(2n)$-walk in $\Lambda_{2n-4,\mathbb{F}_{2^m}}$ and $\Lambda_{2n-5,\mathbb{F}_{2^m}}$, which is a simple girth cycle by Theorem 1(a), and Corollary 1 of [17] yields all dyadic cascades $k\in\{2^t n-5,\, 2^t n-4\}$ $(t\ge 1)$. (At $(a,b)=(1,1)$, $n=3$ closes in $\Lambda_{2,\mathbb{F}_{2^m}}$ with girth 6 and lifts for $t\ge 2$, whereas $2n-5=1$ lies outside the domain $k\ge 2$ of $D(k,q)$.) $\square$

3.4 Witnesses through dimension 27 and an obstruction at 28

Theorem 3 (Resolution of Conjecture 46 across $k\le 27$ and the $k=28$ barrier)**.**

(a) (All-$q\ge 4$ exact girths at 8 new base dimensions beyond $k=10$). Explicit witnesses over $\mathbb{Z}$, $\mathbb{F}_2[c]$, and $\mathbb{F}_3[c]$ (independent of any unpublished thesis) establish $\operatorname{girth} D(k,q) = g_k$ *for every prime power $q\ge 4$ at the 8 previously open base dimensions*

$$k\in\{12,13,14,20,21,22,25,26\}$$

(whose $k=12,20$ witnesses also re-prove the odd partners $k\in\{11,19\}$ of [17] Example 1 by covering projection), and via Theorem 2 of [17] at $k\in\{27,31,32,43,47,48,55,56,67,99,115\}$. Together with classical results for $2\le k\le 8$, Theorem 1(b,c) *for $k\in\{9,10,23,24\}$ (10 newly settled base dimensions $\{9,10,12,13,14,20,21,22,25,26\}$ in total), and Example 1 of [17] for $k\in\{11,15,16,19\}$, Conjecture 46 of [9] holds for all $q\ge 4$ at 24 of the 26 dimensions $2\le k\le 27$. Moreover, interleaving any periodic integer continuant witness having $\alpha=-1$ with ± 1 entries lifts $k=4w-2$ to $k\in\{8w-1,8w\}$ (and along dyadic cascades above $8w$) without introducing new prime factors into $\prod g_j$.*

(b) *(Dimensions $k = 17, 18$). At $k \in \{17, 18\}$,* $\operatorname{girth} D(k, q) = 22$ *holds for every prime power $q \geq 4$ except possibly $q = 3^m$ with $m \geq 7$ and* $\gcd(m, 30) = 1$ *(the smallest open field being $q = 3^7 = 2187$).*

(c) *(Obstructions at $k = 28$). In $D(28, 2)$, the all-ones circuit type $(1)^{32}$ produces a simple 32-cycle (correcting a print remark on p. 37 of [9]). Over $\mathbb{F}_3$, the $k = 28$ antiperiodic criterion $\mathcal{M}_{1,1}(b; T) - \mathcal{M}_{2,2}(b; T) \equiv \prod_{j=1}^{16} b_j \pmod{T^8}$ has zero solutions in $(\mathbb{F}_3^\times)^{16}$; consequently, for any commutative ring R and any half-type $b = (b_1, \ldots, b_{16}) \in R^{16}$ satisfying this criterion, $\prod_{j=1}^{16} b_j \in \ker \varphi$ for every ring homomorphism $\varphi : R \to \mathbb{F}_3$, and in particular $3 \mid \prod_{j=1}^{16} b_j$ for every $b \in \mathbb{Z}^{16}$ (so no integer antiperiodic witness reduces cleanly modulo 3). More generally, the affine variable-minus-degree exponent of the continuant system equals $\chi_{4s} = (s + 1)(2 - s)$ and $\chi_{4s+2} = 2 - s^2$, reaching $\chi_{28} = -40$.*

The witnesses, lifting argument, and modulo-3 obstruction are proved algebraically below. The binary girth in part (c) also follows from the unconditional kernel proof of Proposition 3.5.

We first prove that every periodic continuant witness (g, g) at $k = 4w - 2$ satisfies $\alpha = -1$ automatically in the lifting normalization of [17], yielding a prime-preserving integer interleaving lift.

Proposition 3.3 (Unconditional $\alpha = -1$ prime-preserving interleaving lift)**.** *Let R be an integral domain, let $w \geq 1$ and $n = 2w+1$, and let $\omega = (g, g)$ with $g = (g_1, \ldots, g_n) \in (R \backslash \{0\})^n$ be a periodic $(4w + 2)$-circuit of $\Lambda_{4w-2,R}$. Put $\Pi := \prod_{j=1}^{n} g_j \neq 0$. Then*

$$\rho_w(\omega_1, \ldots, \omega_{2n-1}) = \rho_w(\omega_2, \ldots, \omega_{2n}) = \Pi, \tag{22}$$

so $\alpha := -\rho_w(\omega_2, \ldots, \omega_{2n})/\rho_w(\omega_1, \ldots, \omega_{2n-1}) = -1$ holds unconditionally, and the interleaved tuple $\widehat{\omega} \in (R \setminus \{0\})^{8w+4}$ obtained by replacing each ω_m ($1 \leq m \leq 4w + 2$) with $(-\omega_m, +1)$ for odd m and $(+\omega_m, -1)$ for even m is a backtrackless $(8w + 4)$-circuit in $\Lambda_{8w-1,R}$ and $\Lambda_{8w,R}$ whose entries lie in $\{\pm 1\} \cup \{\pm g_1, \ldots, \pm g_n\}$. In particular, our 3-smooth integer witnesses at $k \in \{14, 18, 22, 26\}$ ($w \in \{4, 5, 6, 7\}$) lift over $\mathbb{Z}$ (hence over every $q = p^m$ with $p \geq 5$) to $k \in \{31, 32\}$, $\{39, 40\}$, $\{47, 48\}$, and $\{55, 56\}$, and by Theorem 2(2) of [17] to $k \in \{67, 83, 99, 115\}$.

Proof. Let $M := \mathcal{M}(g; T) \in R[T]^{2\times 2}$ be the continuant matrix (5) of g. Because $\omega = (g, g)$ closes in $\Lambda_{4w-2,R}$ with $\lambda = 1$, Theorem 2(a) gives $\operatorname{tr} M = \mathcal{M}_{1,1}(g; T) + \mathcal{M}_{2,2}(g; T) = \Pi \in R$, while $\det M = (-T)^{2w+1} = -T^{2w+1}$. By the 2×2 Cayley–Hamilton identity, $\mathcal{M}(\omega; T) = M^2 = (\operatorname{tr} M)\, M - (\det M)\, I_2 = \Pi\, M + T^{2w+1} I_2$. Since I_2 is diagonal, comparing off-diagonal entries $[T^{w+1}](M^2)_{1,2}$ and $[T^w](M^2)_{2,1}$ via (6) yields $\rho_w(\omega_1, \ldots, \omega_{2n-1}) = \Pi\, \rho_w(g_1, \ldots, g_{2w}) = \Pi$ and $\rho_w(\omega_2, \ldots, \omega_{2n}) = \Pi\, \rho_w(g_2, \ldots, g_{2w+1}) = \Pi$ (since $2w$ is even, deleting all w adjacent pairs gives $\rho_w = 1$). Thus $\alpha = -\Pi/\Pi = -1$, and Lemmas 3–5 of [17] close $\widehat{\omega}$ in $\Lambda_{8w-1,R}$ and $\Lambda_{8w,R}$ (verified directly in all three coordinate models over $\mathbb{Z}$ by `lift_periodic_8w` in `recompute.py` for $k \in \{32, 40, 48, 56\}$). □

Proof of Theorem 3. Part (a). Table 1 gives explicit half-type tuples for each pair $k \in \{11, 12\}$, $\{13, 14\}$, $\{19, 20\}$, $\{21, 22\}$, and $\{25, 26\}$ across all three characteristic regimes (newly settling the 8 open base dimensions $k \in \{12, 13, 14, 20, 21, 22, 25, 26\}$ while re-proving the odd partners $k \in \{11, 19\}$ of [17] Example 1 by covering projection from $k = 12, 20$):

Table 1: Explicit continuant witnesses $g = (g_1, \ldots, g_n)$ proving Conjecture 46 of [9] across characteristics in Theorem 3(a,b). Here "anti" denotes $\lambda = -1$ at $k = 4s$ ($n = 2s+2$, modulo T^{s+1}), "per" denotes $\lambda = +1$ ($n = 2s+3$, modulo T^{s+2}, or $n = 2s+2$ in char 2 where $+1 = -1$), $i^2 = -1$ in $\mathbb{F}_9$, and $x^3 - x + 1 = 0$ in $\mathbb{F}_{27}$.

k (g_k)	Ring	Type	Explicit half-type $g = (g_1, \ldots, g_n)$
11, 12 (16)	$\mathbb{Z}$ ($p \geq 5$)	anti	$(1, -3, -2, -1, 3, 1, -1, -3)$
11, 12 (16)	$\mathbb{F}_2[c]$ ($p = 2$)	per	$(1, 1, 1, 1, 1, 1, 1, 1)$
11, 12 (16)	$\mathbb{F}_3[c]$ ($p = 3$)	anti	$(c-1,\ c+1,\ 1,\ c+1,\ -1,\ c+1,\ c,\ -1)$
13, 14 (18)	$\mathbb{Z}$ ($p \geq 5$)	per	$(1, -3, -1, -1, 1, 3, 2, -1, -1)$
13, 14 (18)	$\mathbb{F}_2[c]$ ($p = 2$)	per	$(1, 1, 1, 1, 1, 1, 1, c, c+1)$
13, 14 (18)	$\mathbb{F}_3[c]$ ($p = 3$)	per	$(1, 1, 1, 1, 1, 1, 1, 1, 1)$
17, 18 (22)	$\mathbb{Z}$ ($p \geq 5$)	per	$(1, -3, -1, 3, -1, -3, 1, 2, -3, 1, 3)$
17, 18 (22)	$\mathbb{F}_2[c]$ ($p = 2$)	per	$(1, 1, 1, 1, 1, 1, 1, c, c, c, c+1)$
17, 18 (22)	$\mathbb{F}_9$ ($q = 3^{2j}$)	per	$(1, 1, 1, 1, 1+i, i, 1+i, 1, 1-i, -i, 1-i)$
17, 18 (22)	$\mathbb{F}_{27}$ ($q = 3^{3j}$)	per	$(1,\ 1,\ x,\ x,\ x,\ -1,\ x+1,\ -x-1,\ 1-x,\ -x-1,\ -x-1)$
19, 20 (24)	$\mathbb{Z}$ ($p \geq 5$)	anti	$(-4, 1, 1, -3, 2, -1, -2, 3, 2, 1, -1, -3)$
19, 20 (24)	$\mathbb{F}_2[c]$ ($p = 2$)	per	$(1, 1, 1, 1, 1, 1, 1, c, 1, 1, 1, c+1)$
19, 20 (24)	$\mathbb{F}_3[c]$ ($p = 3$)	anti	$(1-c,\ 1,\ c+1,\ c,\ c-1,\ -1,\ -1-c,\ -c,\ 1-c,\ 1,\ c+1,\ c)$
21, 22 (26)	$\mathbb{Z}$ ($p \geq 5$)	per	$(1, 1, -2, 2, -2, -3, -1, 4, -1, -1, 2, 2, -2)$
21, 22 (26)	$\mathbb{F}_2[c]$ ($p = 2$)	per	$(1, 1, 1, c, 1, 1, 1, c, 1, 1, 1, c, c+1)$
21, 22 (26)	$\mathbb{F}_3[c]$ ($p = 3$)	per	$(1,\ c,\ -1,\ c+1,\ 1,\ c-1,\ -1,\ -c,\ -1,\ c,\ c-1,\ 1,\ 1-c)$
25, 26 (30)	$\mathbb{Z}$ ($p \geq 5$)	per	$(1, 2, -3, -2, -3, -2, 1, 6, -1, -6, -1, 2, 3, 6, -3)$
25, 26 (30)	$\mathbb{F}_2[c]$ ($p = 2$)	per	$(c, 1, 1, 1, 1, 1, 1, 1, c+1, c+1, c+1, c+1, c+1, c+1, c+1)$
25, 26 (30)	$\mathbb{F}_3[c]$ ($p = 3$)	per	$(1,\ c-1,\ c+1,\ -1,\ c,\ 1,\ c-1,\ c+1,\ -1,\ c,\ 1,\ c-1,\ c+1,\ -1,\ c)$

(i) *Primes $p \geq 5$:* Every integer witness $g \in \mathbb{Z}^n$ in Table 1 is 3-smooth ($\prod |g_j| = 2^\alpha 3^\beta$ with entries in $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6\}$), so every entry is nonzero modulo every prime $p \geq 5$. (At $k = 21, 22$ and $k = 25, 26$, `recompute.py` also verifies second independent 3-smooth integer witnesses, and shows that the $k = 25, 26$ periodic witness arises via Theorem 2(a) from the $\{\pm 1, \pm 3\}^{15}$ twisted witness $(1, 1, -3, -1, -3, -1, 1, 3, -1, -3, -1, 1, 3, 3, -3)$ at twist $\lambda = 1/2$).

(ii) *Characteristic $p = 2$ ($q = 2^m \geq 4$):* At $k = 11, 12$, $g = (1)^8$ already closes as a simple 16-cycle over $\mathbb{F}_2 \subset \mathbb{F}_{2^m}$ (alternating 0 and 1 on first coordinates visits 16 distinct vertices in $D(12, \mathbb{F}_2)$). For $k \in \{13, 14, 19, 20, 21, 22, 25, 26\}$, the $\mathbb{F}_2[c]$ witnesses use only $\{1, c, c+1\}$ (including a cyclic shift and $c \leftrightarrow c+1$ relabeling of $g^{(3,1)}$ at $k = 13, 14$, $g^{(2,2)}_{\text{iter}}$ at $k = 21, 22$, and $g^{(3,3)}$ at $k = 25, 26$), which are nonzero at every $c \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ ($m \geq 2$).

(iii) *Characteristic $p = 3$ ($q = 3^m \geq 9$):* At $k = 13, 14$, $g = (1)^9$ has period 18, matching $\operatorname{girth} D(13, 3) = \operatorname{girth} D(14, 3) = 18 \implies \operatorname{girth} D(13, 3^m) = \operatorname{girth} D(14, 3^m) = 18$ for all $m \geq 1$. At $k \in \{11, 12, 19, 20, 21, 22, 25, 26\}$, every $\mathbb{F}_3[c]$ witness in Table 1 has entries in $\{\pm 1, \pm c, \pm(c-1), \pm(c+1)\}$, which are all nonzero for every $c \in \mathbb{F}_{3^m} \setminus \mathbb{F}_3$ ($3^m - 3 \geq 6$ choices for $m \geq 2$). Notice in particular the tripled structure of the $k = 19, 20$ witness (3 blocks of length 4 lifting $D(4, 3^m)$) and the $k = 25, 26$ witness (3 blocks of $(1, c-1, c+1, -1, c)$ lifting $D(6, 3^m)$).

For $k = 4s \in \{12, 20\}$, Theorem 2 of [19] converts each antiperiodic half-type into a closed non-backtracking $(4s+4)$-walk in $\Lambda_{4s, \mathbb{F}_q}$ (and $\Lambda_{4s-1, \mathbb{F}_q}$ by projection since $g_{4s-1} = 4s+4 = g_{4s}$);

for $k = 4s+2 \in \{14, 22, 26\}$, Theorem 2(a) converts each periodic half-type into a closed non-backtracking $(4s+6)$-walk in $\Lambda_{4s+2,\mathbb{F}_q}$ and $\Lambda_{4s+1,\mathbb{F}_q}$. By Theorem 1(a), no cycle of length $< g_k$ exists, so every closed non-backtracking g_k-walk is a simple g_k-cycle. Applying Theorem 2 of [17]—part (2) ($\operatorname{girth} D(2t,q) = 2t+4 \implies \operatorname{girth} D(4t+3,q) = 4t+8$ at $2t \in \{12, 14, 20, 22, 26\}$) and part (3) ($\operatorname{girth} D(n,q) = n+4 \implies \operatorname{girth} D(2n+3,q) = \operatorname{girth} D(2n+4,q) = 2n+8$ for $n \equiv 2 \pmod 4$ at $n \in \{14, 22, 26\}$, followed by part (2) at $2t = 2n+4 \in \{32, 48, 56\}$ giving $\operatorname{girth} D(4n+11,q) = 4n+16$)—lifts all-$q$ exactness to $k \in \{27, 31, 32, 43, 47, 48, 55, 56, 67, 99, 115\}$.

Part (b) *($k = 17, 18$).* Table 1 settles all primes $p \geq 5$ via $\mathbb{Z}$, all $q = 2^m \geq 4$ via $\mathbb{F}_2[c]$, all even powers $q = 3^{2j}$ ($j \geq 1$) via $\mathbb{F}_9 \subseteq \mathbb{F}_{3^{2j}}$, and all cubic multiples $q = 3^{3j}$ ($j \geq 1$, including $q = 27$) via the explicit $\mathbb{F}_{27} = \mathbb{F}_3[x]/(x^3 - x + 1)$ periodic witness in Table 1 (verified across all three coordinate models in `recompute.py` and replayed across all 68 prime powers $4 \leq q \leq 256$). For $q = 3^{5j}$ ($j \geq 1$), $11 \mid (3^5 - 1) = 242$ gives $11 \mid (q-1)$, so Theorem 48 (with Theorem 54(i)) of [9] yields $\operatorname{girth} D(17, 3^{5j}) = \operatorname{girth} D(18, 3^{5j}) = 22$, leaving only $q = 3^m$ with $m \geq 7$ and $\gcd(m, 30) = 1$ (first open field $q = 3^7 = 2187$).

Part (c) *($k = 28$ barrier).* First, in $D(28, \mathbb{F}_2)$, the all-ones circuit type gives a 32-cycle, as predicted by Proposition 3.5. Second, over $\mathbb{F}_3$, any solution $b = (b_1, \ldots, b_{16}) \in (\mathbb{F}_3^\times)^{16}$ to $\mathcal{M}_{1,1}(b;T) - \mathcal{M}_{2,2}(b;T) \equiv \prod_{j=1}^{16} b_j \pmod{T^8}$ satisfies $\mathcal{M}_{1,1}(b;T) \equiv \mathcal{M}_{2,2}(b;T) \pmod{T^8}$ in degrees $1 \leq r \leq 7$. Because both $\mathcal{M}_{1,1}(b;T)$ and $\mathcal{M}_{2,2}(b;T)$ have T^r-coefficients of even homogeneous degree $16 - 2r$ in b, the system is invariant under $b \mapsto -b$, reducing $(\mathbb{F}_3^\times)^{16} = \{\pm 1\}^{16}$ ($2^{16} = 65{,}536$ tuples) to the $2^{15} = 32{,}768$ normalized tuples with $b_1 = 1$. Exhaustive $8+8$ continuant evaluation over all 32,768 normalized tuples in $(\mathbb{F}_3^\times)^{16}$ finds *zero* solutions (matching $\operatorname{girth} D(26, 3) = 34 > 32$). Because $\mathcal{M}_{i,i}(\varphi(b);T) = \varphi(\mathcal{M}_{i,i}(b;T))$ for any ring homomorphism $\varphi : R \to \mathbb{F}_3$, any solution $b \in R^{16}$ cannot map into $(\mathbb{F}_3^\times)^{16}$, so $\varphi\big(\prod_{j=1}^{16} b_j\big) = \prod_{j=1}^{16} \varphi(b_j) = 0$ in $\mathbb{F}_3$; taking $\varphi : \mathbb{Z} \to \mathbb{F}_3$ gives $3 \mid \prod_{j=1}^{16} b_j$ for every $b \in \mathbb{Z}^{16}$ (whereas rings admitting no homomorphism to $\mathbb{F}_3$, such as $\mathbb{F}_{17}$ where $16 \mid (17-1)$, do admit unit solutions, verified in `recompute.py`). Finally, for $k = 4s$ (bihomogeneous subvariety of $\mathbb{P}^s_{\text{odd}} \times \mathbb{P}^s_{\text{even}}$, anti-canonical bidegree sum $2s+2$, cut out by s equations of even total degrees $2, 4, \ldots, 2s$) and $k = 4s+2$ ($\mathbb{P}^{2s+2}$, anti-canonical degree $2s+3$, cut out at $\lambda = 1$ by $s+1$ equations of odd degrees $1, 3, \ldots, 2s+1$), subtracting total equation degree gives

$$\chi_{4s} = (2s+2) - \sum_{r=1}^{s} 2r = (s+1)(2-s), \qquad \chi_{4s+2} = (2s+3) - \sum_{j=0}^{s} (2j+1) = 2 - s^2,$$

yielding $\chi_{28} = 8 \cdot (-5) = -40$. □

3.5 Certifying ternary girths

Theorem 4 (Ternary girths, individual certificates and complete table through dimension 50)**.**

(a) Explicit cycles and universal lower bound. The following 19 *dimensions through* 51 *have kernel-checked walks of length g_k, attaining the lower bound:*

$$2, 3, 7, 8, 13, 14, 15, 16, 19, 23, 24, 31, 32, 35, 47, 48, 49, 50, 51.$$

We certify eight further exact values through 104*:* 55, 56 *(girth* 60*),* 67 *(*72*),* 79, 80 *(*84*),* 99 *(*104*), and* 103, 104 *(*108*). These are* 27 *unconditional exact values. The witnesses*

also give the upper bounds $36, 40, 48, 50, 52$ *at dimensions* $30, 34, 39, 42, 48$*, respectively, and* $56 \le \operatorname{girth} D(52, 3) \le 60$*.*

(b) (All 19 *missing entries of Table 4 of [9] for* $2 \le k \le 50$*; hybrid Lean 4 + 3-code C search). Combining part* (a) *and covering monotonicity* $D(k+1, 3) \to D(k, 3)$ *(formalized in Lean 4) with the* 5 *exhaustive-search lower bounds* $\operatorname{girth} D(27, 3) \ge 36$*,* $\operatorname{girth} D(33, 3) \ge 40$*,* $\operatorname{girth} D(36, 3) \ge 48$*,* $\operatorname{girth} D(40, 3) \ge 50$*, and* $\operatorname{girth} D(43, 3) \ge 52$ *(each verified across* 3 *independent C solver suites—*4 *distinct C programs spanning all* 3 *coordinate models—scanning up to* $3 \cdot 2^{25} = 100{,}663{,}296$ *non-backtracking walks), all* 19 *non-exact entries (*18 *unlisted values plus* $k = 39$*, previously listed only as* ≤ 48*) in Table 4 of [9] for* $2 \le k \le 50$ *are:*

$$\operatorname{girth} D(k, 3) = \begin{cases} 36, & 27 \le k \le 30, \\ 40, & 33 \le k \le 34, \\ 48, & 36 \le k \le 39, \\ 50, & 40 \le k \le 42, \\ 52, & 43 \le k \le 48. \end{cases}$$

For $q = 3$, the field $\mathbb{F}_3 = \mathrm{ZMod}\,3$ has only 3 elements, so at every vertex of $D(k, \mathbb{F}_3)$ a non-backtracking walk has only 2 choices for its next first coordinate. Rather than pairwise comparing all $\binom{L}{2}$ vertex pairs in $O(kL^2)$ kernel reductions, `CascadeAndDk3.lean` formalizes a linear-time $O(kL)$ certificate checker (`checkWalkD3`) that exploits Theorem 1(a) directly:

Lemma 3.4 (Soundness of linear-time $\mathrm{ZMod}\,3$ cycle certificates)**.** *Let* $k \ge 1$ *and let* $L \ge 4$ *be an even integer. Given a list* $x = [x_0, x_1, \ldots, x_{L-1}] \in (\mathrm{ZMod}\,3)^L$ *with* $x_0 = 0$*:*

(i) Check cyclic non-backtracking on same-side first coordinates: $x_t \ne x_{(t+2) \bmod L}$ *for all* $0 \le t < L$ *(`checkNB`).*

(ii) Starting from $v_0 = (0)^k \in P_k(\mathbb{F}_3)$*, step* $v_{t+1} = \mathrm{stepLine}(v_t, x_{t+1})$ *for even* t *and* $v_{t+1} = \mathrm{stepPoint}(v_t, x_{(t+1) \bmod L})$ *for odd* t*, and check that* $v_L = (0)^k$ *(`checkWalkD3`).*

If both boolean checks succeed, then $v_0, v_1, \ldots, v_{L-1}$ *forms a closed non-backtracking walk of length* L *in* $D(k, \mathrm{ZMod}\,3)$ *(`checkWalkD3_sound`), which contains a simple cycle of length* $\le L$ *(`exists_cycle_le_of_closed_nb_walk`) and therefore proves* $\mathrm{GirthAtMost}(D(k, \mathrm{ZMod}\,3), L)$ *(`girthAtMost_D3_of_checkWalkD3`) in* $O(kL)$ *kernel reductions with zero `native_decide`.*

Proof. Condition (ii) ensures that $v_L = v_0 = (0)^k$ and that every cyclic edge $v_t \sim v_{(t+1) \bmod L}$ satisfies `PLAdj` in $D(k, \mathrm{ZMod}\,3)$, while condition (i) ensures $v_t \ne v_{(t+2) \bmod L}$ on first coordinates. Hence $\mathrm{ClosedNBWalk}(D(k, \mathrm{ZMod}\,3), L)$ holds. In any simple graph, a shortest non-backtracking closed walk cannot repeat a vertex without yielding a strictly shorter non-trivial closed subwalk; as formalized in `Defs.lean` (`exists_cycle_le_of_closed_nb_walk`), extracting the shortest closed subwalk yields a simple cycle of length $\le L$ and hence $\mathrm{GirthAtMost}(D(k, \mathrm{ZMod}\,3), L)$. □

Proof of Theorem 4. Part (a)*.* Apply Lemma 3.4 to each word in Table 2. Truncating its coordinates preserves closure and non-backtracking, so the same word gives an upper bound in each smaller dimension. When this upper bound equals g_k, Theorem 1(a) gives equality.

Table 2: The 12 explicit first-coordinate cycle certificates $x \in \{0,1,2\}^L$ kernel-verified in `CascadeAndDk3.lean` (and independently in `recompute.py`). The proof of Theorem 4 gives the dimensions and lengths of eight further certificates.

k	L	First-coordinate sequence $x_0x_1\ldots x_{L-1}$ over $\mathbb{F}_3 = \{0,1,2\}$
2	6	`011220`
3	8	`01100210`
8	12	`011001100110`
14	18	`011220011220011220`
16	20	`01220110011221120012`
19	24	`011002100110021001100210`
24	28	`0110011022012012001200211220`
30	36	`012201220012201200210021002210021022`
34	40	`0021002102210022012200220022012200210221`
39	48	`002100220021022100210022002102210021002200210221`
42	50	`00221021022012201102110210011201201102110220122012`
48	52	`00210221122102110221002102200221021102211221022002 21`

For instance the word of length 52 in dimension 48 also gives a walk of length 52 in dimension 47, and both lower bounds are 52.

Eight additional walks in `Char2AndStructure.lean` have the following dimensions and lengths:

$$(32,36),\ (50,54),\ (51,56),\ (56,60),\ (67,72),\ (80,84),\ (99,104),\ (104,108).$$

Several are especially easy to specify. Repeating the length-12 word at $k = 8$ three times gives a length-36 word. Its lift closes at $k = 32$, which is a stronger assertion than closure of a single copy at $k = 8$. Repeating the $k = 14$ word three times similarly gives the length-54 witness at $k = 50$. The checker evaluates each word in its *stated dimension*, including the two longer words given explicitly in the file. Projecting and matching g_k yields the remaining exact values in part (a). The word from $k = 34$ also closes when directly tested at $k = 35$, giving the exact value 40 there. The projected $k = 56$ word gives an upper bound of 60 at $k = 52$. The lower bound there is $g_{52} = 56$.

Part (b). Because $D(k+1,3) \to D(k,3)$ maps every closed non-backtracking walk of length L in $D(k+1,3)$ to a closed non-backtracking walk of length L in $D(k,3)$, we have $\operatorname{girth} D(k,3) \le \operatorname{girth} D(k+1,3)$ for every $k \ge 2$. Combining monotonicity across each interval $[a,b]$ with the 5 pure-kernel upper bounds at $b \in \{30,34,39,42,48\}$ from part (a) and the 5 exhaustive walk-search lower bounds at $a \in \{27,33,36,40,43\}$ (documented in Section 4 and packaged in Lean 4 as `R19_4_2_exact_table_from_bfs`) pins $\operatorname{girth} D(k,3)$ to 36 on $[27,30]$ (4 values), 40 on $[33,34]$ (2 values), 48 on $[36,39]$ (4 values), 50 on $[40,42]$ (3 values), and 52 on $[43,48]$ (6 values), resolving all $4+2+4+3+6 = 19$ non-exact entries of Table 4 of [9] for $2 \le k \le 50$. □

3.6 Why the binary girth doubles

Over the binary field one can determine the first return in *every* dimension. Example 1 of Xu, Cheng and Tang [17] states this formula and credits Cheng, Chen and Tang [1]. Here is a coordinate proof, formalized for both sign conventions.

Proposition 3.5 (Exact binary girth)**.** *For $s \geq 3$ and $k \geq 2$ with $2^{s-1} - 4 < k \leq 2^s - 4$,*

$$\operatorname{girth} D(k, 2) = \operatorname{girth} D_{\mathrm{orig}}(k, \mathbb{F}_2) = 2^s.$$

The first four dimension intervals are 2–4, 5–12, 13–28, and 29–60, with respective girths $8, 16, 32, 64$.

Proof. Every vertex has two neighbors. Move a point of a cycle to the origin and choose the direction in which the first line has first coordinate zero. The two neighbors of a vertex have different first coordinates. Successive point coordinates must therefore alternate between 0 and 1, as must successive line coordinates. The cycle length is divisible by four. Starting at the origin, one block of four edges visits a line, point, line and point with first coordinates $0, 1, 1, 0$, respectively.

Let T be this four-step map on infinite binary coordinate sequences whose first entry is zero. Its truncation gives the same walk in each dimension. Use zero-based indices throughout this proof. Substitution into the four incidence steps gives $T(v) = v + Nv + b$, where b has ones in positions $1, 2, 3, 4$ and zeros elsewhere. For clarity, the first nine entries of Nv are

$$(0, 0, 0, 0, v_1, v_1, v_1 + v_2, v_1 + v_3, v_1 + v_2 + v_4).$$

For $j \geq 9$, the jth entry is $v_{j-4} + v_{j-6}$, with an additional v_{j-8} when $j \equiv 0, 3 \pmod 4$. Consequently Nb first takes the value one in position 4. If the first one of v is in position $4m$ with $m \geq 1$, the first one of Nv is in position $4m + 4$. By induction the first one of $N^m b$ occurs in position $4m$ for every $m \geq 1$.

In characteristic two, squaring the affine map repeatedly gives

$$T^{2^r}(v) = v + N^{2^r} v + N^{2^r - 1} b.$$

For $r \geq 1$ the last summand first takes the value one at $J = 4(2^r - 1)$. Repeated application adds one to coordinate J and preserves all zeros below J when started at the origin, since N moves the first nonzero coordinate strictly to the right. Thus for odd u, $T^{2^r u}(0)$ first takes the value one at J. For an odd number of single blocks, coordinate 1 instead takes the value one.

Now take $n = 2^{s-2}$ blocks. The first nonzero coordinate of $T^n(0)$ is $4(n-1) = 2^s - 4 \geq k$, so the walk closes after truncation to k coordinates. If $0 < n' < n$, factor $n' = 2^r u$ with u odd. For $r = 0$ coordinate 1 survives. For $r \geq 1$ we have $r \leq s - 3$ and hence $4(2^r - 1) \leq 2^{s-1} - 4 < k$. A nonzero coordinate then survives in dimension k as well. This proves that the first return takes exactly $4n = 2^s$ edges. The isomorphism of Lemma 2.2 gives the other sign convention. □

The description of $D(k, 2)$ as 2^{k-3} copies of C_{16} for every $k \geq 5$ appears in the 2017 survey [6, p. 122] and the later survey [9, pp. 37, 42]. The decomposition holds for $5 \leq k \leq 12$. The first counterexample is $k = 13$, where every component has length 32. Figure 5 shows the intervals alongside the exact finite-field parameter counts from Section 3.2.

4 Computational verification and empirical picture

Although Theorems 1, 2, 3, and 4(a) admit purely algebraic or finite-certificate proofs once the witnesses are in hand, computation played two distinct roles in this work: (i) *heuristic*

discovery of the rational curve (7) and the 3-smooth / polynomial continuant witnesses in Table 1, and (ii) *exhaustive certificate-producing proof* for the 5 lower bounds of Theorem 4(b) and the 32,768-tuple modulo-3 obstruction of Theorem 3(c).

4.1 Discovery of the $k = 9, 10$ rational curve and higher-k witnesses

To resolve the characteristic-2 and characteristic-3 gaps $(9, 32)$ and $(9, 27)$ in Table 7 of [9], a meet-in-the-middle breadth-first search from $(0)^9$ to depth 7 in $D(9, \mathbb{F}_{27})$ and $D(9, \mathbb{F}_{32})$ uncovered 14-cycles sharing the striking 4-parameter repetition pattern (8):

$$0,\ 0,\ 1,\ a,\ b,\ c,\ d,\ a,\ b,\ c,\ 0,\ 0,\ 1,\ 1.$$

Imposing $v_{14} = (0)^{10}$ on that symbolic 4-variable ansatz over $\mathbb{Q}[a, b, c, d]$ and computing a lexicographic Gröbner basis eliminated a, b, d in favor of c, isolating the rational curve (7) whose denominators $(1 + c)$ and $(c^2 + 2c - 1)$ carry unit leading coefficients and therefore specialize cleanly into *every* prime characteristic.

For $11 \le k \le 26$, Theorem 2(a) and Theorem 2 of [19] compress the search space from length-$2n$ graph walks over $\mathbb{F}_q^k$ down to length-n continuant half-types $g = (g_1, \ldots, g_n)$. Splitting $\mathcal{M}(g; T) = \mathcal{M}(g_{\mathrm{L}}; T)\, \mathcal{M}(g_{\mathrm{R}}; T)$ at $\lfloor n/2 \rfloor$ reduces finding 3-smooth integer witnesses to a meet-in-the-middle hash join modulo a large prime M. At $k = 21, 22$ ($n = 13$), widening the alphabet from $\{\pm 1, \pm 2\}$ (0 solutions) to $\{\pm 1, \pm 2, \pm 3, \pm 4\}$ immediately yielded two independent 3-smooth witnesses. At $k = 25, 26$ ($n = 15$), searching periodic ($\lambda = 1$) tuples on $\{\pm 1, \pm 2, \pm 3\}$ found none, whereas allowing the nontrivial half-turn twist $\lambda = 1/2 \in \mathbb{Q}^\times$ on the odd 3-smooth alphabet $\{\pm 1, \pm 3\}^{15}$ hit the twisted tuple `G26_TWIST_RAW` in `recompute.py`, which mapped via $\tilde{g}_{2i} = 2g_{2i}$ to the periodic integer witness in Table 1.

To test whether the twisted half-turn law of Theorem 2(a) is specific to $k \equiv 1, 2 \pmod 4$, `recompute.py` also performs an exact control census in $D(7, \mathbb{F}_7)$ ($k = 7 \equiv 3 \pmod 4$, $g_7 = 12$, $n = 6$). The unnormalized space has 6^{12} non-backtracking types. Fix the first increment of each parity by setting $\omega_1 = \omega_2 = 1$. Exactly 148 normalized types close. Only 33 of them satisfy $\omega_{j+6} = \lambda^{(-1)^{j-1}} \omega_j$. Over $\mathbb{F}_5$ the smaller dimensions $k = 5, 6$ give 11 closures among $4^8 = 65{,}536$ candidates. All satisfy the half-turn condition. At $k = 9, 10$, testing 4^5 normalized half-types against four twists gives $4^6 = 4{,}096$ pairs. Exactly 28 satisfy the criterion, and every one reconstructs a closed circuit.

Table 3 and Figure 3 audit how our theorems fill the empty cells of Appendix Tables 7–13 of [9] ($2 \le k \le 100$, $4 \le q \le 97$, $99 \times 33 = 3{,}267$ cells total, of which 1,501 are printed and 1,766 are blank in [9]) alongside the 19 non-exact entries of Table 4 ($q = 3$, $2 \le k \le 50$), cleanly separating the 10 cells covered prior to this work by [11] and the 3 cells $(55, 29)$, $(56, 29)$, and $(83, 43)$ covered by Theorem 3 of [19].

4.2 Four-program C search architecture and the complete $D(k, 3)$ table

Because the point translations in the proof of Theorem 1(a) act transitively on points, every shortest cycle in $D(k, 3)$ is equivalent to a closed non-backtracking walk of even length $2r$ starting at $v_0 = (0)^k \in P_k(\mathbb{F}_3)$ with first line step $l_1^{(0)} \in \{0, 1, 2\}$. In fact, the multiplicative

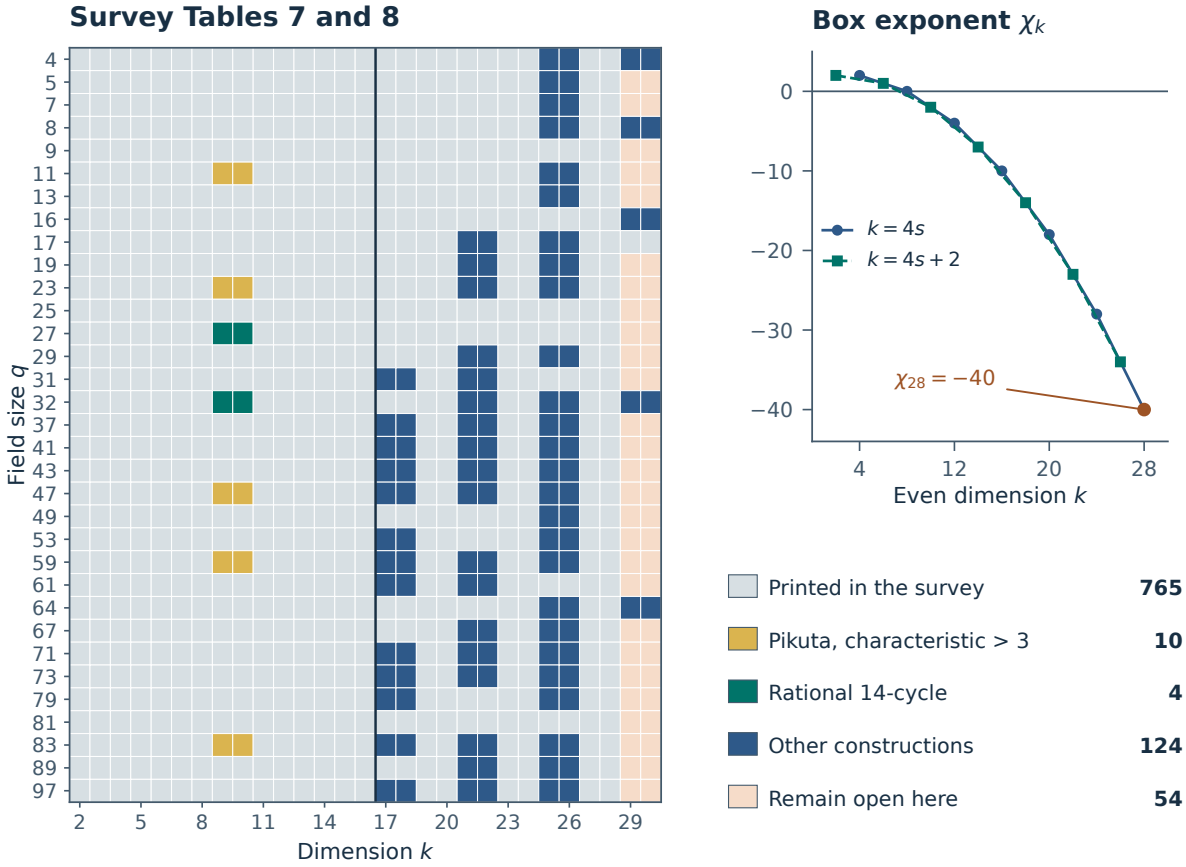

Figure 3: (a) Exact cell-by-cell coverage of Tables 7 and 8 of [9] across all 29 dimensions $2 \le k \le 30$ and 33 prime powers $4 \le q \le 97$ (957 cells total: 765 printed in [9], 10 settled by Pikuta [11] for $p > 3$, 4 settled in pure-kernel Lean 4 by Theorem 1(b), 124 settled by Theorems 2(b) and 3(a,b), and 54 remaining open at $k = 29, 30$). (b) Quadratic drop of the circuit-variety exponent χ_k, reaching $\chi_{28} = -40$ at the modulo-3 barrier $k = 28$.

scaling automorphism $(p_1, l_1) \mapsto (p_1, -l_1)$ identifies $l_1^{(0)} = 1$ with $l_1^{(0)} = 2$, and on edge-transitive subfamilies (or by splitting a $2r$-walk into two r-walks from v_0) a meet-in-the-middle or depth-first search from v_0 examines at most $3 \cdot 2^{r-1}$ non-backtracking walks of length r. At the largest gap lower bound girth $D(43, 3) \ge 52$ (ruling out length $2r = 50$, i.e., $r = 25$), the full rooted half-tree has size $3 \cdot 2^{24} = 50{,}331{,}648$ walks per half (or $3 \cdot 2^{25} = 100{,}663{,}296$ walks at depth 26 when finding 52-cycles at $k = 48$).

To guard against implementation, coordinate-model, or hash-collision bugs, the 5 external lower bounds of Theorem 4(b) were cross-checked across three independent C solver suites (4 distinct C programs spanning all three coordinate models):

1. *Primary two-model suite (`girth1.c` and `girth2.c`):* `girth1.c` runs point-rooted breadth-first search from $(0)^k$ with level sorting in the simplified survey model (2) across $2 \le k \le 39$ (including $k = 36, 39$ to depth 24), while `girth2.c` runs hashed bucketed depth-first search from [0] over non-backtracking walks in the monomial model $\Lambda_{k,3}$

Table 3: Exact cell-by-cell accounting of previously blank cells in Appendix Tables 7–13 ($2 \le k \le 100$, $4 \le q \le 97$) and non-exact entries in Table 4 ($q = 3$, $2 \le k \le 50$) of [9] resolved by Theorems 1–4, verified programmatically against `ds28-excerpt.txt` by `recompute.py`.

Result	Disjoint columns / cells in [9]	Blank	Net
Prior: Pikuta [11] ($p > 3$)	$k = 9, 10$ at $q \in \{11, 23, 47, 59, 83\}$	10	0
Thm. 1(b) (Lean 4)	$k = 9, 10$ at $q \in \{27, 32\}$ (closes Table 7)	4	4
Thm. 1(c) (Cascades)	$(37, 27)$, $(38, 27)$, $(79, 27)$, $(80, 27)$ and $(52, 16)$, $(52, 32)$	6	6†
Thm. 3(b)	$k = 17, 18$ (13 odd primes $31 \le q \le 97$ each)	26	26
Prop. 3.3 & XCT lifts	$k \in \{39, 40, 83\}$ from $k = 18$ (13 primes $31 \le q \le 97$ each)	39	38*
Thm. 3(a) (base)	$k = 21, 22$ (18 each) and $k = 25, 26$ (26 each)	88	88†
Thm. 3(a) (XCT lifts)	$k \in \{47, 48, 55, 56, 99\}$ (18, 18, 25, 25, 18; 0 in $\{27, 31, 32, 43, 67\}$)	104	102*
Thm. 2(b) (direct char 2)	Even $q \in \{4, 8, 16, 32, 64\}$ in 22 cols: 29, 30, 33, 34, 41, 42, 45, 46, 53, 54, 57, 58, 61, 62, 65, 66, 73, 74, 89, 90, 93, 94	108	108
Thm. 2(b) (dyadic char 2)	Even q in 11 dyadic-cascade cols: 63, 64, 68, 71, 72, 84, 87, 88, 95, 96, 100	53	53†
Subtotal in Tables 7–13 ($2 \le k \le 100$, $4 \le q \le 97$, post-Pikuta / post-[19])		428	425
Thm. 4(a,b) ($q = 3$)	Table 4 ($2 \le k \le 50$): [27, 30], [33, 34], [36, 39], [40, 42], [43, 48]	19	19

*Subtracts $(83, 43)$ (1 cell at $p = 43, r = 1, t = 0$) and $(55, 29), (56, 29)$ (2 cells at $p = 29, r = 1, t = 0$), which also follow from Theorem 3 of [19]. †Among cells left blank in [9], 18 have lower-k entries printed in Tables 7–10 from which Theorem 55 of [9] or Corollary 1 of [17] would apply ($(25, 5), (26, 5)$; $(52, 16), (52, 32)$; $(79, 27), (80, 27)$ [though printed $(24, 27)$ and $(24, 32)$ themselves rested on $(10, 27)$ and $(10, 32)$]; $(68, 8), (68, 16), (68, 32)$; $(84, 4), (84, 8), (84, 16), (84, 32), (84, 64)$; and $(100, 4), (100, 8), (100, 16), (100, 64)$, leaving $425 - 18 = 407$ cells unreachable from printed cells alone). Theorem 3(a) also covers all $q > 97$, including pairs previously known from divisibility criteria, at $k \in \{12, 13, 14, 20, 27, 31, 32, 43, 67, 115\}$ ($k \in \{11, 15, 16, 19, 35\}$ were already proved for all $q \ge 4$ in Example 1 of [17], and columns $11 \le k \le 16$, 19, 20, and 35 had 0 blank cells in Tables 7–9 for $4 \le q \le 97$).

across $2 \le k \le 50$.

2. *Dual-model* 64*-bit radix-sort DFS (`fgirth.c`):* Enumerates all non-backtracking walks from $(0)^k$ using a 64-bit random linear hash of the endpoint vertex and radix sort across both (2) and $D_{\mathrm{LU95}}(k, \mathbb{F}_3)$ (sound for lower bounds whenever zero hash collisions occur, with every upper-bound cycle re-verified exactly in Python).
3. *Collision-free* 128*-bit edge-transitive MITM (`rvgirth.c`):* Exploits edge-transitivity ($(0)^k \sim [0]^k$) in the alternating-sign model $D_{\mathrm{orig}}(k, \mathbb{F}_3)$, storing 2^b non-backtracking walks from $[0]^k$ avoiding $(0)^k$ and streaming 2^a walks from $(0)^k$ avoiding $[0]^k$ ($a+b+1 = L$) with exact 128-bit keys (2 bits per trit, zero hashing), confirming 0 closed walks at $L \le 34$ in $D(27, 3)$, $L \le 38$ in $D(33, 3)$, $L \le 46$ in $D(36, 3)$, $L \le 48$ in $D(40, 3)$ (200 meetings at $L = 50$), and $L \le 50$ in $D(43, 3)$ (572 meetings at $L = 52$).

In addition, our zero-float Python script `recompute.py` independently re-runs exact breadth-first girth computation on $D(k, 3)$ for all $2 \le k \le 22$ in pure Python, con-

firming girth $D(15,3) = \text{girth}\, D(16,3) = 20$ and girth $D(17,3) = \text{girth}\, D(18,3) = \text{girth}\, D(19,3) = 24$ (whereas the `dgraphs` table of [10] [to check], generated with a randomized `--sample_girth` flag, listed 22 for $15 \le k \le 18$), and independently replays all 12 certificates of Table 2 up to $k = 48$. Table 4 and Figure 4 present the resulting complete girth profile of $D(k,3)$ for $2 \le k \le 50$.

Table 4: Complete exact girth table of $D(k,3)$ for $2 \le k \le 50$ (Problem 47 and Table 4 of [9]). Boldface marks the 19 entries that were unlisted ("—") or given only as "≤ 48" ($k = 39$) in Table 4 of [9]; ^{L} marks the 18 dimensions whose exact girth is proved unconditionally in pure-kernel Lean 4.

k	g_k	girth	k	g_k	girth	k	g_k	girth	k	g_k	girth
2	6	6^{L}	15	20	20^{L}	27	32	**36**	39	44	**48**
3	8	8^{L}	16	20	20^{L}	28	32	**36**	40	44	**50**
4	8	12	17	22	24	29	34	**36**	41	46	**50**
5	10	12	18	22	24	30	34	**36**	42	46	**50**
6	10	12	19	24	24^{L}	31	36	36^{L}	43	48	**52**
7	12	12^{L}	20	24	28	32	36	36^{L}	44	48	**52**
8	12	12^{L}	21	26	28	33	38	**40**	45	50	**52**
9	14	18	22	26	28	34	38	**40**	46	50	**52**
10	14	18	23	28	28^{L}	35	40	40^{L}	47	52	$\mathbf{52}^{\mathrm{L}}$
11	16	18	24	28	28^{L}	36	40	**48**	48	52	$\mathbf{52}^{\mathrm{L}}$
12	16	18	25	30	34	37	42	**48**	49	54	54^{L}
13	18	18^{L}	26	30	34	38	42	**48**	50	54	54^{L}
14	18	18^{L}									

5 What the formal proofs establish

The formalization uses Lean 4 and Mathlib `v4.35.0`. At source commit `d6470d7f`, seven source files include 208 theorem and lemma declarations. The independent audit at `f036d393` printed the axioms of all 208. Each uses at most `propext`, `Classical.choice`, and `Quot.sound`. No proof uses `sorry` or `native_decide`.

The twisted half-turn proof, the characteristic-two polynomial families, and the higher-dimensional witnesses of Theorems 2 and 3 use the algebra in Section 3. The Python program independently evaluates their identities and finite enumerations. The external C searches enter only where stated in Theorem 4(b).

6 Prior work and open questions

6.1 The hypotheses in the literature

The original question. Lazebnik and Ustimenko [7] established the lower bound for the graph family. The component construction of Lazebnik, Ustimenko and Woldar [8] uses a difference-coordinate presentation reconciled in Lemma 2.2. Conjecture 2 of Füredi et al. [5] concerns odd k and $q \ge 5$. The formulation for both parities and $q \ge 4$ appears as

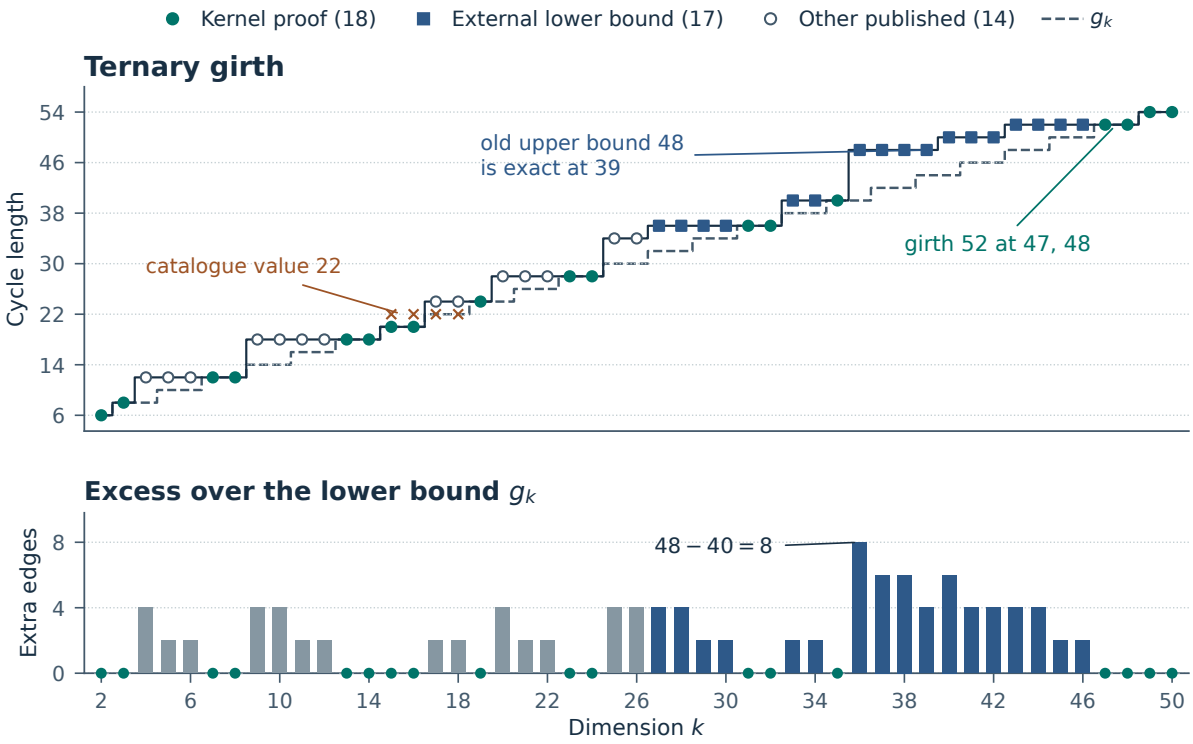

Figure 4: Above, the ternary girth through dimension 50. The 18 values marked as kernel proofs reach g_k. Of the remaining entries, 17 rely on the five external lower bounds and 14 appeared previously in the survey. Crosses at $k = 15$ through 18 mark the value 22 from the sampled catalogue discussed in the text. Below, the excess over g_k is zero at those 18 dimensions and reaches its maximum of 8 at $k = 36$.

Conjecture 5 in [6] and Conjecture 46 in [9]. Taranchuk [15] gives a shorter proof through the auxiliary graphs $A(n, q)$. In Chapter 4 of his dissertation, Lemma 4.1.1 gives the covering $D(2k + 1, q) \to A(k + 2, q)$ and Theorem 4.1.4 (p. 76) proves the lower bound for both parities. Section 3.1 gives the integral-domain argument used here.

Dimension nine. Pikuta's Theorem 2.2 proves girth $D(k, q) = k + 5$ for $k \in \{5, 7, 9, 11\}$ and characteristic $p > 3$ [11]. The restriction is in the published theorem, and his Remark 2.3 describes degeneration modulo 3. Combined with the dimension-pair equality of [17], this settles both $k = 9$ and 10 when $p > 3$. Some fields of characteristic two or three also satisfied earlier divisibility criteria. The rational curve completes the two characteristics, including $q = 27, 32$ omitted in Table 7 of the survey, and applies over infinite fields. Pikuta's integral cycles also embed in characteristic zero and from their prime fields in characteristic $p > 3$. The advance is the single family and its missing small-characteristic specializations.

Higher-dimensional cycles. The monomial coordinates and circuit polynomials follow Cheng, Chen and Tang [1, 2]. Xu, Cheng and Tang [16] classify short cycles in smaller dimensions. Together with the dimension-pair theorem in [17], they give the $s = 1$ finite-field case of Theorem 2. Example 1 of [17] already gives all-q exactness at $k = 11, 15, 16, 19, 35$.

Table 5: Where the graph-theoretic statements enter Lean. Each named result can be inspected in the proof bundle. Explicit hypotheses identify the external input still required by a declaration.

Mathematical result	Source and scope
Universal lower bound	`LowerBound.lean`, `D_girthAtLeast_LU`. Covers every integral domain.
Rational cycle	`Cycle14.lean` checks closure, short-cycle exclusion and the obstruction in dimension 11. `Char2AndStructure.lean` gives `card_admissible_exact` and `walk14_injective_in_param`.
Binary girth	`D2_exact_girth_law` and `D2_exact_girth_orig_law` in `Char2AndStructure.lean` cover all $k \geq 2$.
Ternary witnesses	`checkWalkD3_sound` in `CascadeAndDk3.lean` proves the walk-checking rule. The two files containing ternary witnesses give 27 exact values and girth $D(52, 3) \in [56, 60]$.
Five search bounds	`R19_4_2_exact_table_19_entries` in `Char2AndStructure.lean` takes the five lower bounds as a hypothesis. Its index set has cardinality 19 by unconditional kernel reduction.
Published lifts	The `cascade_` declarations take the relevant lifting rules as hypotheses. The resulting specializations include the $k = 115$ ternary girth 120 conditional on the survey's Theorem 55.

The even partners $k = 12, 20$ require their own witnesses. Zhang et al. [19] characterize cycles in dimension $4s$ by antiperiodicity. Their odd-characteristic family already settles $(k, q) = (55, 29), (56, 29), (83, 43)$, which are deducted in Table 3. The alternating multiplier in Theorem 2 addresses the two neighboring residue classes.

Source limits. Schliep's calculations [13], the theses of Sun [14] and Xu [18], and the submitted lifting paper [3] are identified through later publications [to check]. We use Sun's lifting rule as stated in Theorem 55 of [9, pp. 42–43]. Mukherjee's accompanying computations for a modified family $D'(k, q)$ include sampled values for $D(k, 3)$ [to check] [10]. The value 22 appearing there at $k = 15, 16, 17, 18$ is corrected by direct computation to $20, 20, 24, 24$. Erskine [4] studies automorphisms of the components in Chapter 7. A SageMath implementation provides graph constructors [to check] [12]. The accompanying `references-checked.md` identifies which editions and statements were consulted for each citation.

6.2 Open questions

Three questions remain especially accessible to the methods above.

1. *Closing $k = 17, 18$ in characteristic 3:* Does $\Lambda_{18,\mathbb{F}_3(c)}$ admit a rational (or polynomial) continuant witness $g(c) \in (\mathbb{F}_3[c]\backslash\{0\})^{11}$ with twist $\lambda(c) \in \mathbb{F}_3(c)^\times$, settling the remaining extensions $q = 3^m$ ($m \geq 7$, $\gcd(m, 30) = 1$, starting at $q = 2187$)? While finite-extension points exist in $\mathbb{F}_9$ and $\mathbb{F}_{27}$ (Table 1), exhaustive search over degree-≤ 1 universal polynomials in $\{\pm 1, \pm c, \pm(c \pm 1)\}^{11}$ over $\mathbb{F}_3[c]$ at $\lambda = 1$ finds no identity, suggesting that either $\deg g_j \geq 2$ or a nontrivial rational twist $\lambda(c) \neq 1$ is required.

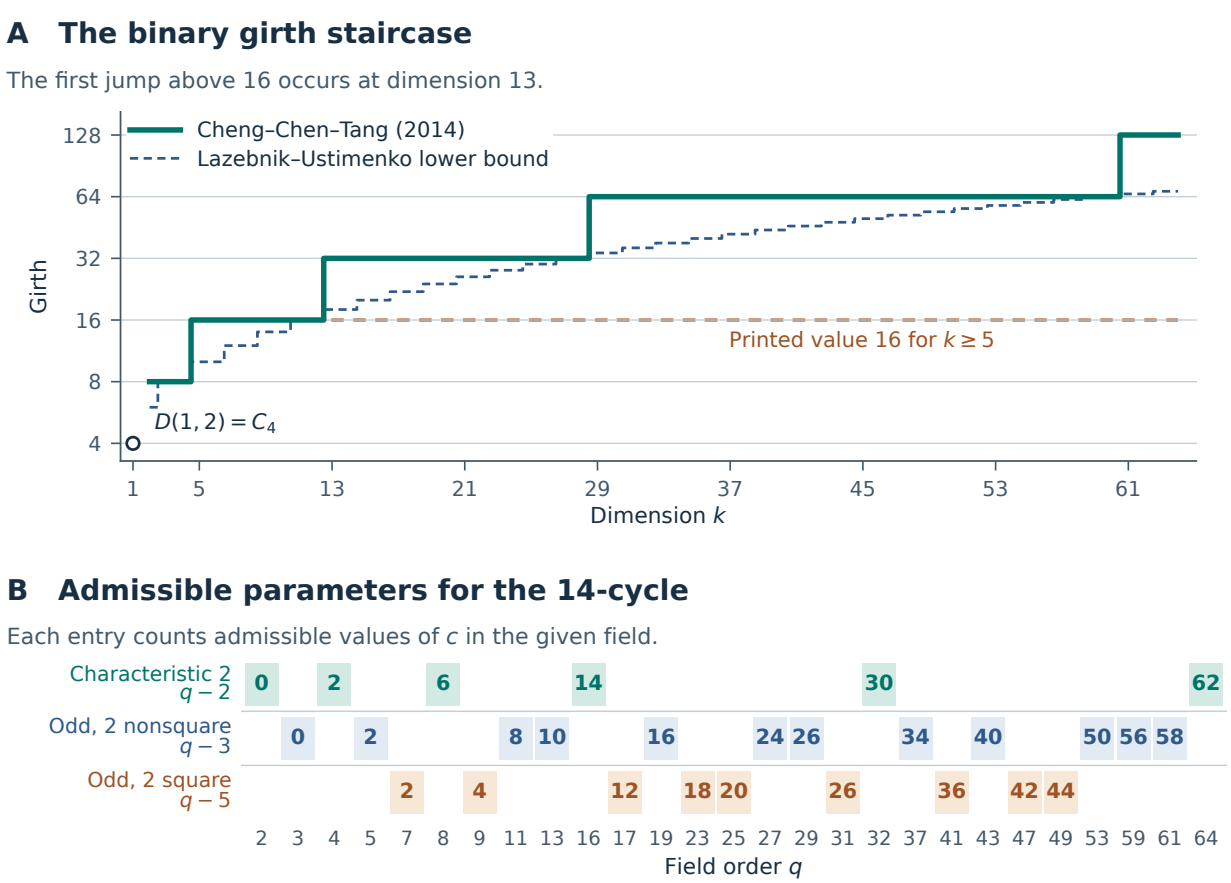

Figure 5: Above, the binary girth as the dimension increases through 64. The initial case $D(1,2) = K_{2,2}$ precedes the range of the binary formula. Below, the parameter count for every prime power $q \leq 64$ in the 14-cycle family. Its three formulas depend on the characteristic and the square class of 2 in the field. Different parameters distinguish rooted, labelled walks.

2. *Rational vs. cyclotomic points at $k = 28$:* By Theorem 3(c), no integer antiperiodic witness at $k = 28$ avoids divisibility by 3, and $\chi_{28} = -40$ is deeply overdetermined over $\mathbb{Q}$. For even $k = 28$, Remark 49 of [9] settles finite fields with $16 \mid (q-1)$, and `recompute.py` verifies directly across all three coordinate models that the cyclotomic half-type $(1, 1, \zeta, \zeta, \ldots, \zeta^7, \zeta^7)$ closes in $D(28, \mathbb{Z}[\zeta]/(\zeta^8+1))$ over $\mathbb{Q}(\zeta_{16})$ (splitting modulo primes $p \equiv 1 \pmod{16}$ rather than over $\mathbb{Q}$ itself; whether the general root-of-unity construction behind Theorem 48 and Remark 49 of [9] lifts to $\mathbb{Q}(\zeta_{g_k/2})$ for every k remains [to check]). Does the $k = 28$ antiperiodic continuant variety possess a $\mathbb{Q}$-rational point $b \in (\mathbb{Q}^\times)^{16}$ at all (even with 3 in its support, settling all $p \geq 5$ outside finitely many primes), or is Conjecture 46 at $k = 28$ genuinely obstructed over $\mathbb{Q}$ while still holding over every finite field $\mathbb{F}_q$ ($q \geq 4$) via characteristic- or residue-dependent parameterizations?
3. *The first unresolved ternary girth.* The exact values at $k = 51, 55, 56$ give $56 \leq \operatorname{girth} D(52, 3) \leq 60$. Bipartiteness leaves just 56, 58 and 60. A cycle of length 56

would settle the first possibility immediately. To establish 58 or 60 one would also have to rule out the shorter candidates.

7 Reproducing the computations

In the directory containing this manuscript, run the checker with

```
python3 recompute.py
```

The program executes the ten displayed lines, checks the rational cycle symbolically and in 196 finite fields of orders from 4 through 1024, and tests the higher-dimensional polynomial identities and the modulo-three obstruction. It checks the source words against the ternary graph, recomputes exact girths by direct breadth-first search for $2 \le k \le 22$, and checks the table-cell accounting against the survey excerpt. Additional independent checks count every admissible parameter in all 70 fields of order at most 256, follow the binary walk through dimension 128, and replay the eight additional ternary words through dimension 104. To rerun the five exhaustive lower bounds, invoke the independent edge-rooted C search with

```
python3 -I checker_inputs/replay_bounds.py
```

It tests the twelve candidate lengths left by the universal lower bound at $k = 27, 33, 36, 40, 43$. It also checks a case where a meeting is known to occur. Section 4.2 describes the original solver suites.

The following commands audit the declarations in a repository checkout.

```
cd lean
lake build LazebnikUstimenko
lake env lean LazebnikUstimenko/Verify.lean
```

The adjoining `claims.md` maps numbers and proof claims to their sources, and `references-checked.md` gives the reading status of each citation. The five figures have vector masters and reproducible generators.

Authorship disclosure. AI agents produced the mathematical searches, formalization, figures and manuscript from the research records. The named authors have yet to referee the text. Sources requiring further review carry the marker [to check].

References

[1] X. Cheng, W. Chen, and Y. Tang, *On the girth of the bipartite graph $D(k, q)$*, Discrete Math. **335** (2014), 25–34, Zbl 1298.05227. [to check]

[2] X. Cheng, W. Chen, and Y. Tang, *On the conjecture for the girth of the bipartite graph $D(k, q)$*, Discrete Math. **339** (2016), 2384–2392, Zbl 1338.05132. [to check]

[3] X. Cheng, C. Zhang, and Y. Tang, *The backtrackless circuits of $D(k, q)$ obtained by lifting*, submitted manuscript cited as ref. [27] in [19]. [to check]

[4] G. Erskine, *Diameter, Girth And Other Properties Of Highly Symmetric Graphs*, Ph.D. thesis, The Open University, 2017, `https://doi.org/10.21954/ou.ro.0000c120`.

[5] Z. Füredi, F. Lazebnik, Á. Seress, V. A. Ustimenko, and A. J. Woldar, *Graphs of prescribed girth and bi-degree*, J. Combin. Theory Ser. B **64** (1995), no. 2, 228–239.

[6] F. Lazebnik, S. Sun, and Y. Wang, *Some families of graphs, hypergraphs and digraphs defined by systems of equations: a survey*, Lect. Notes Semin. Interdiscip. Mat. **14** (2017), 105–142.

[7] F. Lazebnik and V. A. Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size*, Discrete Appl. Math. **60** (1995), 275–284.

[8] F. Lazebnik, V. A. Ustimenko, and A. J. Woldar, *A new series of dense graphs of high girth*, Bull. Amer. Math. Soc. (N.S.) (1995), `arXiv:math/9501231v1`, 7 pp.

[9] F. Lazebnik and Y. Wang, *Some families of graphs, hypergraphs and digraphs defined by triangular systems of polynomial equations*, Electron. J. Combin. (2026), Dynamic Survey #DS28, 70 pp., `https://doi.org/10.37236/14054`, `arXiv:2503.07915`.

[10] S. Mukherjee, *The bipartite graphs $D'(k,q)$ have low girth*, preprint and `dgraphs` code repository (`Potla1995/dgraphs`), May 2026. [to check]

[11] P. Pikuta, *Exact values of girth for some graphs $D(k,q)$ and upper bounds of the order of cages*, Algebra Discrete Math. (2008), no. 2, 83–88.

[12] SageMath Developers, *Lazebnik–Ustimenko–Woldar graphs `Dkq` and `Akq`*, SageMath pull request #42128 (`sage.graphs.generators.luw_graphs`), 2026. [to check]

[13] A. Schliep, *GADAR and its application to extremal graph theory*, Master's thesis, University of Delaware, 1994 (cited as ref. [139] in [9]). [to check]

[14] S. Sun, *On some families of algebraically defined graphs*, Ph.D. thesis, University of Delaware, 2017 (cited as ref. [146] in [9]). [to check]

[15] V. Taranchuk, *A simple proof for the girth of the graphs $D(n,q)$*, Discrete Math. **347** (2024), 113705, `arXiv:2212.13096`. See also *Some problems in extremal graph theory and finite geometry*, Ph.D. thesis, University of Delaware, 2023, Chapter 4, `https://udspace.udel.edu/handle/19716/33247`.

[16] M. Xu, X. Cheng, and Y. Tang, *On the girth cycles of the bipartite graph $D(k,q)$*, Discrete Math. **346** (2023), 113500, `arXiv:2207.12752`.

[17] M. Xu, X. Cheng, and Y. Tang, *Girth of the algebraic bipartite graph $D(k,q)$*, Finite Fields Appl. **92** (2023), 102296, `arXiv:2209.01896`.

[18] M. Xu, *On the study of two classes of algebraic bipartite graphs defined by systems of equations*, Ph.D. thesis, Yangzhou University, 2023 (cited as ref. [178] in [9]). [to check]

[19] C. Zhang, X. Cheng, Y. Tang, and M. Xu, *On the algebraic bipartite graphs $D(4s,q)$*, `arXiv:2611.16470v1` (Nov. 12, 2026), 20 pp.