# The in-tree of an $n$-cycle under cyclic conjugation: depth $p^{e-1}$ for odd $p$, and $2^{e-1}-1$ for $p=2$

Frédéric Lefebvre-Naré*

July 24, 2026

**Abstract**

Fix the standard $n$-cycle $s=(1\,2\,\cdots\,n)$, and repeatedly replace an $n$-cycle $q$ by its conjugate $D(q)=q\,s\,q^{-1}$. The cycle $s$ is the unique fixed point of $D$; the $n$-cycles that eventually reach it under iteration form a tree feeding into $s$, and we determine the depth of that tree — the number of steps the slowest of these cycles needs.

The depth depends only on the factorization of $n$. It equals 1 unless $8 \mid n$ or $p^2 \mid n$ for an odd prime $p$ (the Hull–Dobell threshold); for $n=p^e$ it is $p^{e-1}$ for odd $p$ and $2^{e-1}-1$ for $p=2$, and for general $n$ it is the largest of these over the prime-power factors.

The proof turns conjugation, near $s$, into base-$p$ arithmetic. In a "carry" coordinate an $n$-cycle becomes a base permutation together with a vector of *carries* in $\mathbb{Z}/p$, and $D$ acts on the carries by an explicit affine map — the carrying of ordinary base-$p$ addition. The heart is the prime-power case $n=p^e$, where three things then happen: the cycles feeding $s$ are exactly the $n$-cycles in a classical group (the permutations preserving a binomial flag, whose Sylow $p$-subgroup is Kaloujnine's iterated wreath product); their deepest chains lie in a "root fibre" on which $D$ is a linear cellular automaton; and the depth is the nilpotency length of the shift difference $I-S$ — exactly it for odd $p$, one less for $p=2$. That single missing carry, which odd primes absorb and $p=2$ cannot, is the whole source of the two-branch answer. The Chinese Remainder Theorem reduces general $n$ to prime powers.

*2020 MSC:* 05A05, 20B30, 37P99, 11A07. *Keywords:* $n$-cycles, conjugation, functional graph, in-tree depth, carry propagation, binomial flag, Hull–Dobell, $p$-Sylow subgroup.

## 1 Introduction

Let $\mathrm{Sym}(\mathbb{Z}/n)$ be the symmetric group on $\mathbb{Z}/n=\{0,1,\dots,n-1\}$, $C(n)\subseteq\mathrm{Sym}(\mathbb{Z}/n)$ the set of $n$-cycles, and $s=s_n$ the standard cycle $x\mapsto x+1$. The *derivation* is

$$D=D_n\colon C(n)\to C(n),\qquad D(q)=q\,s\,q^{-1},$$

the conjugate of $s$ by $q$ (equivalently, the $n$-cycle sending $q(i)$ to $q(i{+}1)$). Since conjugation preserves cycle type, $D$ maps $C(n)$ into itself; its unique fixed point is $s$ (from $qsq^{-1}=q$ one gets $sq^{-1}=e$). Not every $n$-cycle reaches $s$: some fall into other periodic orbits. Those that *do* reach it form the *in-tree* of $s$ — the set $\mathrm{basin}_n$ of $n$-cycles $q$ with $D^t(q)=s$ for some $t\geq 0$ (a tree, since each vertex

*Provenance and status.* The proof below was obtained by artificial-intelligence models (Anthropic's Claude) in interactive dialogue with the author, and reviewed module by module by OpenAI models (mostly GPT-5.5); every intermediate claim was verified by exact finite computation over $\mathbb{F}_p$ (Appendix A). An end-to-end verification of the assembled whole, and human peer review, remain to be done; the argument should be examined critically before being relied upon. This companion accompanies [10].

has one outgoing edge and no cycle other than the loop at $s$), with $\mathrm{dist}(q) = \min\{t : D^t(q) = s\}$. This note computes the depth of that tree, $\mathrm{depth}(n) = \max_{q \in \mathrm{basin}_n} \mathrm{dist}(q)$.

**Theorem 1.1** (Main theorem)**.** *For a prime $p$ and $e \geq 1$,*

$$\mathrm{depth}(p^e) = \begin{cases} p^{\,e-1}, & p \text{ odd}, \\ 2^{\,e-1} - 1, & p = 2, \end{cases}$$

*and for general $n = \prod_p p^{e_p}$, $\mathrm{depth}(n) = \max_p \mathrm{depth}(p^{e_p})$. In particular $\mathrm{depth}(n) = 1$ unless $8 \mid n$ or $p^2 \mid n$ for some odd prime $p$.*

The threshold "$8 \mid n$ or $p^2 \mid n$ (odd $p$)" is exactly the Hull–Dobell criterion [1] for the existence of a full-period non-translation affine map $x \mapsto ax+b$ on $\mathbb{Z}/n$ — the criterion underlying full-period linear congruential generators [2] and single-cycle $T$-functions [3]. This is no coincidence: the affine $n$-cycles occupy the top two layers of the in-tree, and $D$ collapses the multiplier $a$ to 1 in one step, so the tree is deep precisely when non-translation affine cycles exist. The exact depth, and its two-branch form, come from the finer arithmetic of carries in base $p$.

**The idea, in words.** Conjugation by $s$ is intricate on all of $C(n)$, but near the fixed point it becomes transparent. Fix $n = p^e$ (the Chinese Remainder Theorem, §6, then assembles general $n$). The cycles that can reach $s$ all commute with $g = s^{\,p^{e-1}}$; such a cycle splits into a coarse "base" permutation on $p^{e-1}$ blocks and a vector of *carries* in $\mathbb{Z}/p$ recording how it shifts within the blocks, and $D$ transforms the carries by an explicit affine map — the very carrying of base-$p$ addition (§2). This one change of coordinates has three consequences, one per section, which together compute the depth:

$$\text{conjugation on } C(p^e)\ (\S2) \longrightarrow \text{basin} = \text{a classical group}\ (\S3) \longrightarrow \text{depth} = \text{nilpotency height}\ (\S4) \longrightarrow \text{a carry cascade}\ (\S5).$$

*More precisely:*

(a) the in-tree of $s$ at level $p^k$ consists of exactly the $n$-cycles in the group of *triangular* permutations for the binomial flag $\varphi_j = \binom{\cdot}{j}$ — an iterated affine (wreath) tower whose $p$-part is the $p$-Sylow subgroup of $S_{p^k}$ (§3);

(b) on the "root fibre" the carry map is the shift difference $I - S$, nilpotent of index $d = p^{e-1}$; a cycle's distance to $s$ splits as its base-distance plus the nilpotency height of the carry it enters with (§4), reducing the depth to one linear-algebra statement, (L2);

(c) (L2) holds because a chain of functionals transported along the tree first fails to close up only at step $d - 2$ (the *obstruction law*, §5), with a single "deviation" at odd primes that an identity about rotation carries exactly compensates — and this lone carry is what makes the answer $p^{e-1}$ for odd $p$ but one less for $p = 2$.

**Reading guide and status.** The paper is self-contained. Sections 2 (foundations) and 3 (the flag tower) are elementary; §4 is the reduction, §5 its arithmetic core, §6 the multiplicative step. Every proposition has been verified by exact computation over $\mathbb{F}_p$ on small prime powers; these certificates are collected in Appendix A and are reproducible, but form no part of the proof. As stated in the title footnote, the argument is machine-generated and has not been refereed; the reader should treat it critically.

## 2 Carry coordinates, the cocycle, and the finite calculus

*Goal of this section.* We install the one change of coordinates that drives everything: near the fixed point a cycle splits into a coarse *base* permutation and a vector of *carries* in $\mathbb{Z}/p$, and $D$ acts on the pair by an explicit affine *cocycle* (Lemma 2.3) — the carrying of base-$p$ addition. We also record the finite difference calculus attached to the binomial flag, used from §3 on. A running example ($n = 8$) is threaded through §§2–4.

Throughout, $p$ is a fixed prime. We use two consecutive levels of a $p$-power tower: a level $m = p^k$ and its *base* $c = p^{k-1}$ ($k \geq 1$). Each $x \in \mathbb{Z}/m$ decomposes as $x = \mu(x) + c\,\ell(x)$ with $\mu(x) = x \bmod c \in \{0, \dots, c-1\}$ and $\ell(x) = \lfloor x/c \rfloor \in \{0, \dots, p-1\}$.

### 2.1 Carry coordinates

Let $g = s_m^c$ (the map $x \mapsto x+c$ on $\mathbb{Z}/m$), of order $p$; its orbits are the *fibres* $\{r, r+c, \dots, r+(p-1)c\}$, $r \in \mathbb{Z}/c$. Its centraliser in $\mathrm{Sym}(\mathbb{Z}/m)$ is the wreath product $\mathbb{Z}/p \wr S_c$: an element commuting with $g$ permutes the fibres and translates inside each.

**Proposition 2.1** (carry coordinates)**.** *Every $\theta \in \mathrm{Sym}(\mathbb{Z}/m)$ commuting with $g$ is uniquely*

$$\theta(r + jc) = \bar{\theta}(r) + \big((j + a_r) \bmod p\big)c, \qquad r \in \mathbb{Z}/c,\ j \in \{0, \dots, p-1\}, \tag{1}$$

*with* base $\bar{\theta} \in \mathrm{Sym}(\mathbb{Z}/c)$ *and* carry $a \in (\mathbb{Z}/p)^c$*; equivalently $\mu \circ \theta = \bar{\theta} \circ \mu$ and $\ell(\theta(x)) = \ell(x) + a_{\mu(x)}$* (mod $p$)*. The map $\theta \mapsto (\bar{\theta}, a)$ is a bijection onto* $\mathrm{Sym}(\mathbb{Z}/c) \times (\mathbb{Z}/p)^c$.

*Proof.* Commuting with $g$ means permuting the fibres (giving $\bar{\theta}$ via $\mu \circ \theta = \bar{\theta} \circ \mu$) and commuting with the $\mathbb{Z}/p$-translation inside them, i.e. acting on the $\ell$-coordinate by a shift $a_r$ depending only on the source fibre $r$. Conversely any $(\bar{\theta}, a)$ yields such a $\theta$, and the constructions are inverse. □

**Proposition 2.2** (cyclicity criterion)**.** *$\theta = (\bar{\theta}, a)$ is a single $m$-cycle iff $\bar{\theta} \in C(c)$ and $\sum_{r \in \mathbb{Z}/c} a_r \not\equiv 0$* (mod $p$)*.*

*Proof.* The projection $\mu$ semiconjugates $\theta$ to $\bar{\theta}$, so a single $m$-cycle projects to a single $c$-cycle. Assume $\bar{\theta} \in C(c)$. Then $\theta^c$ fixes each fibre and acts there by the translation by $T := \sum_r a_r$ (accumulating the fibre increments once around the base $c$-cycle; the sum runs over all of $\mathbb{Z}/c$, independent of the starting fibre), so $\theta^c = g^T$ on each fibre. Since $\bar{\theta}$ is a $c$-cycle, the $\theta$-orbit of any point projects onto all of $\mathbb{Z}/c$, hence meets every fibre; so $\theta$ is a single $m$-cycle iff $\theta^c$ is a single $p$-cycle on one fibre, i.e. iff $T \not\equiv 0$. □

We write $q = (\tau, a)$, $\tau \in C(c)$, $a = b(q) \in (\mathbb{Z}/p)^c$ for an $m$-cycle in these coordinates, and $F^{(k)} = \{q \in C(m) : q \text{ commutes with } g\}$ for the domain of (1) inside $C(m)$.

**Running example ($n = 8$).** Take $p = 2$, top level $m = 8$, base $c = 4$; the fibres of $g = s_8^4$ (the map $x \mapsto x + 4$) are $\{0,4\}, \{1,5\}, \{2,6\}, \{3,7\}$, indexed $r = 0, 1, 2, 3$. The 8-cycle $q = (5, 6, 3, 4, 1, 2, 7, 0)$ reads in these coordinates as base $\tau = s_4$ and carry $a = (1, 1, 0, 1)$; $\Sigma a = 1 \neq 0$ confirms it is a single cycle (Prop. 2.2). The fixed point is $s = (s_4, e_3) = (s_4, (0, 0, 0, 1))$. One step of the cocycle (2), with $(L_{s_4} a)_{r'} = a_{r'} - a_{r'-1}$ and $w_{s_4} = e_0$, sends the carry to $(1, 0, 1, 1)$: a single step of $D$ is a single step of base-2 carrying, the base $s_4$ left unchanged. We follow this $q$ to $s$ in §4.

## 2.2 The cocycle

Carries and functionals live in $(\mathbb{Z}/p)^c = \mathbb{F}_p^{\mathbb{Z}/c}$; $e_i$ denotes the $i$-th standard basis vector (indicator of $i \in \mathbb{Z}/c$), and all carry indices are read modulo $c$. Write $\Sigma a = \sum_r a_r$ and $\langle \chi,\, a\rangle = \sum_x \chi(x) a_x$.

**Lemma 2.3** (cocycle)**.** *For $q = (\tau, a) \in F^{(k)}$, $D_m(q) = (D_c\tau,\ L_\tau a + w_\tau)$ where*

$$(L_\tau a)_{r'} = a_{u+1} - a_u \quad (u = \tau^{-1}(r'),\ \textit{index } u+1 \bmod c), \qquad w_\tau = e_{\tau(c-1)}. \tag{2}$$

*Dually, for every $\varphi\colon \mathbb{Z}/c \to \mathbb{F}_p$, $\langle \varphi,\, L_\tau a + w_\tau\rangle = \langle \Delta(\varphi\circ\tau),\, a\rangle + \varphi(\tau(c-1))$, where $(\Delta\chi)(v) = \chi(v-1) - \chi(v)$. Consequently $\Sigma(L_\tau a + w_\tau) = 1$, $\operatorname{Im} L_\tau = \{\Sigma = 0\}$, and $\ker L_\tau = \mathbb{F}_p\mathbf{1}$.*

*Proof.* Use the defining identity $D_m(q)(q(x)) = q(x+1)$. Write $y = q(x)$: then $\mu(y) = \tau(\mu(x))$ and $\ell(y) = \ell(x) + a_{\mu(x)}$. On $\mathbb{Z}/m$, $\mu(x+1) = s_c(\mu(x))$, so $\mu(D_m(q)(y)) = \tau(s_c(\mu(x))) = D_c\tau(\mu(y))$: the base is $D_c\tau$. For the carry, $\ell(q(z)) = \ell(z) + a_{\mu(z)}$ and $\ell(x+1) = \ell(x) + [\mu(x) = c-1]$, so with $u = \mu(x)$, $r' = \mu(y) = \tau(u)$, $b(D_m q)_{r'} = \ell(D_m(q)(y)) - \ell(y) = a_{u+1} - a_u + [u = c-1]$, i.e. (2) with $w_\tau = e_{\tau(c-1)}$. For the dual form, put $\psi = \varphi\circ\tau$ and change the summation index from $r'$ to $u = \tau^{-1}(r')$: $\sum_{r'} \varphi(r')(a_{u+1} - a_u) = \sum_u \psi(u)(a_{u+1} - a_u)$; summing by parts (Abel) around $\mathbb{Z}/c$, with $v = u+1$ (all indices mod $c$), this is $\sum_v (\psi(v-1) - \psi(v)) a_v = \langle \Delta\psi,\, a\rangle$; and $\langle \varphi,\, w_\tau\rangle = \varphi(\tau(c-1))$. The consequences: $\Sigma(L_\tau a) = \langle \mathbf{1},\, L_\tau a\rangle = \langle \Delta(\mathbf{1}\circ\tau),\, a\rangle = 0$ (as $\Delta\mathbf{1} = 0$) and $\Sigma w_\tau = 1$; $L_\tau$ has corank 1 with kernel the constants (the only functions killed by $a \mapsto a_{u+1} - a_u$ around the $c$-cycle $\tau$). □

In the language of dynamics, this exhibits $D_m$ on $F^{(k)}$ as a *cocycle extension* (skew product) of the base map $D_c$ by the carry group $(\mathbb{Z}/p)^c$: the base coordinate evolves by $D_c$, and the carry by the affine cocycle $a \mapsto L_\tau a + w_\tau$ over it.

## 2.3 The binomial flag and the difference calculus

On $\mathbb{Z}/D$ ($D \geq 2$ a power of $p$) set $\varphi_j(x) = \binom{x}{j} \bmod p$ and $V_h = \operatorname{span}_{\mathbb{F}_p}(\varphi_0, \ldots, \varphi_{h-1})$; the *flag-degree* $\deg_V g$ of $g \neq 0$ is the largest $j$ with nonzero Newton coefficient, and its *head* is that coefficient.

**Lemma 2.4** (difference and primitive)**.** *On $\mathbb{Z}/D$:* (i) *for $1 \leq j < D$, $\Delta\varphi_j \equiv -\varphi_{j-1} \pmod{V_{j-1}}$, so $\Delta$ lowers flag-degree by exactly one and $V_h = \ker \Delta^h$; dually the primitive raises it by one.* (ii) *$\chi$ has a primitive $\Psi_\chi$ (with $\Delta\Psi_\chi = \chi$, $\Psi_\chi(0) = 0$, $\Psi_\chi(x) = -\sum_{u=1}^{x} \chi(u)$) iff $\Sigma\chi = 0$; for the truncated primitive of a general $\chi$, $\Delta\Psi_\chi = \chi - (\Sigma\chi)\, e_0$.* (iii) *$\mathbf{1} = \Delta(-\varphi_1)$.*

*Proof.* (i) Pascal gives $\varphi_j(v-1) - \varphi_j(v) = -\binom{v-1}{j-1}$ for $1 \leq v \leq D-1$, and again by Pascal $\binom{v-1}{j-1} = \binom{v}{j-1} - \binom{v-1}{j-2} \equiv \varphi_{j-1}(v) \pmod{V_{j-1}}$; the wrap at $v = 0$ adds a multiple of $\binom{D}{j} \equiv 0$ ($0 < j < D$, Kummer). (ii) $\Delta\Psi_\chi(v) = \chi(v)$ for $v \geq 1$, and at $v = 0$, $\Delta\Psi_\chi(0) = \Psi_\chi(D-1) = \chi(0) - \Sigma\chi$. (iii) $\Delta(-\varphi_1)(v) = -((v-1) - v) = 1$ for $v \geq 1$; at $v = 0$, $\varphi_1$ takes its representative values $\varphi_1(D-1) = D-1$ and $\varphi_1(0) = 0$ in $\{0, \ldots, D-1\}$, giving $-((D-1) - 0) = 1 - D$, which is $\equiv 1$ in $\mathbb{F}_p$ since $p \mid D$. (Throughout, integer binomial values are reduced mod $p$ only after these differences are formed.) □

**Lemma 2.5** (Lucas, Vandermonde, Faulhaber)**.** (i) (Lucas) $\varphi_j(x) \equiv \prod_i \binom{x_i}{j_i} \pmod p$ *for base-$p$ digits. Hence on $\mathbb{Z}/m$ with base $c$, for $j' < c$ and $0 \leq t < p$,*

$$\varphi_{j'+tc}(x) = \varphi_{j'}(\mu(x)) \binom{\ell(x)}{t}, \qquad \varphi_{j'}(x) = \varphi_{j'}(\mu(x)), \quad \varphi_c = \ell, \quad \binom{m}{j} \equiv 0\ (0 < j < m).$$

(ii) (Vandermonde mod $p$) $\binom{a+b}{t} \equiv \sum_{i=0}^{t} \binom{a}{i}\binom{b}{t-i}$ *for $0 \leq t < p$.* (iii) (Faulhaber) *for $0 \leq t \leq p-2$, $S_t(\ell) = \sum_{\ell' < \ell} \ell'^{\,t}$ is a polynomial of degree $t+1$ and leading coefficient $\frac{1}{t+1} \neq 0$ in $\mathbb{F}_p$.*

*Proof.* (i) Lucas, with the digits of $j' + tc$ being those of $j'$ (positions $0..k-2$) and $t$ (position $k-1$); specialise. (ii) Ordinary Vandermonde is a polynomial identity in $a, b$, valid mod $p$ for $t < p$. (iii) $S_t = \frac{1}{t+1}(B_{t+1}(\ell) - B_{t+1}(0))$ (Bernoulli), degree $t+1$, leading coefficient $\frac{1}{t+1}$, a unit for $t+1 \le p-1 < p$. □

## 3 The tower and the binomial-flag characterisation of the basin

*Goal of this section.* We pin down exactly which cycles reach $s$. The answer is clean and classical: they are precisely the $n$-cycles preserving the binomial flag (Theorem 3.4), equivalently the $n$-cycles of an iterated affine tower (Theorem 3.3) whose $p$-part is the Sylow $p$-subgroup of $S_{p^k}$. This is the structural backbone; the depth computation of §§4–5 takes place inside it.

We now describe $\mathrm{basin}_{p^k}$ (the basin of $s_{p^k}$) exactly. Recall $F^{(k)}$ from §2, $\pi\colon F^{(k)} \to C(c)$ the base map $\pi(q) = \bar{q}$ (which by Lemma 2.3 satisfies $\pi \circ D_m = D_c \circ \pi$), and $\varphi_j, V_h$ the flag on $\mathbb{Z}/p^k$. Call $\tau \in \mathrm{Sym}(\mathbb{Z}/p^k)$ *triangular* if its pullback $g \mapsto g \circ \tau$ preserves the flag, i.e. $\varphi_j \circ \tau \in V_{j+1}$ for all $j$.

**Lemma 3.1** (the basin commutes with $g$)**.** *For $n = p^e$, $\mathrm{basin}_{p^e} \subseteq F^{(e)}$: every $q$ in the basin of $s$ commutes with $g = s^d$, $d = p^{e-1}$.*

*Proof.* $F^{(e)} = \{q \in C(p^e) : q$ normalises and centralises $\langle g\rangle\}$; here, since $q$ is a $p^e$-cycle, $q$ commutes with $g$ iff $g \in \langle q\rangle$. We show $F^{(e)}$ is closed under $D$-preimages; as $s \in F^{(e)}$ and the basin is generated by backward steps from $s$, this gives the claim. Suppose $D(q) \in F^{(e)}$, i.e. $g \in \langle D(q)\rangle = q\langle s\rangle q^{-1}$; then $q^{-1}gq \in \langle s\rangle$, an element of order $p$, so $q^{-1}gq \in \langle g\rangle$ (the unique order-$p$ subgroup of the cyclic $\langle s\rangle$). Thus $q$ normalises $\langle g\rangle \cong \mathbb{Z}/p$, acting by some automorphism; the resulting map $\langle q\rangle \to \mathrm{Aut}(\mathbb{Z}/p)$ has image of order dividing $\gcd(p^e, p-1) = 1$, so $q$ centralises $g$, i.e. $q \in F^{(e)}$. □

**Lemma 3.2** (flag preliminaries)**.** *On $\mathbb{Z}/p^k$ with $c = p^{k-1}$: $V_c = \{$functions of $\mu(x)\}$ (dimension $c$, triangular basis $(\varphi_{j'})_{j'<c}$), $\varphi_c = \ell$, and $V_{c+1} = V_c \oplus \mathbb{F}_p\ell$.*

*Proof.* Lemma 2.5(i): the $\varphi_{j'}$ $(j' < c)$ depend only on $\mu$ and (Pascal-unitriangular) span all $c$ functions of $\mu$; $\varphi_c = \ell$; and $V_{c+1} = V_c + \mathbb{F}_p\varphi_c$. □

**Theorem 3.3** (tower)**.** *For $k \ge 2$, $\mathrm{basin}_{p^k} = \{(\bar{\tau}, b) : \bar{\tau} \in \mathrm{basin}_{p^{k-1}},\ \Sigma b \not\equiv 0\}$, and $\mathrm{basin}_p = \{$rotations $s^a : \gcd(a,p) = 1\}$. Hence $|\mathrm{basin}_{p^k}| = (p-1)\,p^{c-1}|\mathrm{basin}_{p^{k-1}}| = (p-1)^k\,p^{(p^k-1)/(p-1)-k}$.*

*Proof.* $\mathrm{basin}_p$: the immediate (indeed only) predecessors of the fixed point $s$ at prime level are the $p-1$ rotations $s^a$ $(a \neq 0)$, since $D(s^a) = s$ and any $q$ with $D(q) = s$ has $qsq^{-1} = s$, i.e. $q \in \langle s\rangle$.

$(\subseteq)$ Let $q \in \mathrm{basin}_{p^k}$. By Lemma 3.1, $q \in F^{(k)}$, so (1) applies and $\Sigma b(q) \not\equiv 0$ (Proposition 2.2); and $\pi(q) \in \mathrm{basin}_{p^{k-1}}$ since $\pi$ semiconjugates $D_m$ to $D_c$ (Lemma 2.3).

$(\supseteq)$ Let $q = (\bar{\tau}, b)$ with $\bar{\tau} \in \mathrm{basin}_{p^{k-1}}$ and $\Sigma b \not\equiv 0$; then $q \in C(p^k)$. Let $m' = \mathrm{dist}(\bar{\tau})$. By equivariance $\pi(D_m^{m'}q) = D_c^{m'}\bar{\tau} = s_c$, so $D_m^{m'}q$ lies in the root fibre $R = \pi^{-1}(s_c)$; and on $R$, $D$ is a nilpotent-affine map reaching $s$ in finitely many further steps (Lemma 4.1 below, with $\le c$ steps). Hence $q \in \mathrm{basin}_{p^k}$.

Cardinal: over each $\bar{\tau}$ the admissible carries number $p^c - p^{c-1} = (p-1)p^{c-1}$; unroll from $|\mathrm{basin}_p| = p-1$ using $\sum_{i=1}^{k} p^{i-1} = (p^k-1)/(p-1)$. □

**Theorem 3.4** (flag characterisation)**.** *For every $k \ge 1$, $\mathrm{basin}_{p^k} = \{\tau \in C(p^k) : \tau$ triangular$\}$. Moreover the pullback by $\tau \in \mathrm{basin}_{p^k}$ is unipotent on the flag: it fixes each quotient $V_{h+1}/V_h \cong \mathbb{F}_p$ up to a nonzero scalar.*

*Proof.* Induction on $k$. $k = 1$**:** on $\mathbb{Z}/p$, $V_h = \{\text{polynomials of degree} < h\}$, so triangular $\Leftrightarrow$ $\varphi_1 \circ \tau = \tau$ affine; an affine $p$-cycle has $a = 1$ (no fixed point), a rotation; and $\text{basin}_p = \{\text{rotations}\}$ (Theorem 3.3).

($\subseteq$) **(montée).** Let $\tau \in \text{basin}_{p^k}$; by Theorem 3.3, $\tau = (\bar\tau, b)$ with $\bar\tau \in \text{basin}_{p^{k-1}}$ triangular (induction). Fix $j = j' + tc$, $j' < c$, $t < p$. By Lemma 2.5(i), $\varphi_j = (\varphi_{j'} \circ \mu) \cdot \binom{\cdot}{t} \circ \ell$; using $\mu \circ \tau = \bar\tau \circ \mu$ and $\ell \circ \tau = \ell + b \circ \mu$, and Vandermonde (Lemma 2.5(ii)),

$$\varphi_j \circ \tau = \sum_{i=0}^{t} \left[(\varphi_{j'} \circ \bar\tau) \cdot \tbinom{b}{t-i}\right](\mu) \cdot \tbinom{\ell}{i}.$$

A summand $g(\mu)\binom{\ell}{i}$ ($g$ on $\mathbb{Z}/c$) has flag-degree $\deg_V g + ic$ (expand $g$ and use Lemma 2.5(i)). For $i < t$: $\le (c-1) + (t-1)c = tc - 1 < j + 1$, whatever $\bar\tau$. For $i = t$: $\binom{b}{0} = 1$ and $\deg_V(\varphi_{j'} \circ \bar\tau) \le j'$ (induction), so $\le j' + tc = j$. Hence $\varphi_j \circ \tau \in V_{j+1}$.

($\supseteq$) **(descente).** Let $\tau \in C(p^k)$ be triangular. It preserves $V_c = \{\text{functions of } \mu\}$ (Lemma 3.2), so $\mu \circ \tau$ depends only on $\mu$: there is $\bar\tau \in \text{Sym}(\mathbb{Z}/c)$ with $\mu \circ \tau = \bar\tau \circ \mu$, a bijection (it permutes the fibres), transitive (quotient of $\langle\tau\rangle$) hence a $c$-cycle, and triangular at level $c$ (restrict the pullback to $V_c$); by induction $\bar\tau \in \text{basin}_{p^{k-1}}$. Next $\varphi_c = \ell$ and $\varphi_c \circ \tau \in V_{c+1} = V_c \oplus \mathbb{F}_p\ell$ give $\ell \circ \tau = A \circ \mu + \lambda\,\ell$ with $A\colon \mathbb{Z}/c \to \mathbb{F}_p$ and a *scalar* $\lambda$. Then $\ell(\tau(x+c)) = A(\mu(x)) + \lambda(\ell(x) + 1) = \ell(\tau(x)) + \lambda$ while $\mu(\tau(x+c)) = \mu(\tau(x))$, i.e. $\tau(x+c) = \tau(x) + \lambda c$, so $\tau g = g^\lambda \tau$ with $g = (x \mapsto x + c)$ of order $p$. If $\lambda = 0$, $\tau$ is not injective; so $\lambda \in \mathbb{F}_p^\times$ and $\tau$ normalises $\langle g\rangle$, acting by $\lambda \in \text{Aut}(\mathbb{Z}/p)$; the map $\langle\tau\rangle \to \mathbb{F}_p^\times$ has image of order dividing $\gcd(p^k, p-1) = 1$, so $\lambda = 1$. Then $\tau \in F^{(k)}$ with carry $b(\tau) = A$, and $\Sigma A \not\equiv 0$ (cyclicity); with $\bar\tau \in \text{basin}_{p^{k-1}}$, Theorem 3.3 gives $\tau \in \text{basin}_{p^k}$.

*Unipotence.* The pullback by a triangular $\tau$ is a flag-preserving linear automorphism, upper triangular in a flag-adapted basis; its diagonal entries $\lambda_h$ are units (invertibility). Its inverse (pullback by $\tau^{-1}$) is again flag-preserving, so $\tau^{-1}$ is triangular — the triangular *permutations* form a group. □

**Corollary 3.5** (triangular group; carry inversion)**.** *The triangular permutations of $\mathbb{Z}/p^k$ form a group $T_k$, the iterated affine tower ($\tau \mapsto \bar\tau$ with $\bar\tau \in T_{k-1}$, $\ell \circ \tau = A \circ \mu + \lambda\ell$, $A$ free, $\lambda \in \mathbb{F}_p^\times$), with $|T_k| = (p-1)^k p^{(p^k-1)/(p-1)}$ whose $p$-part is $|\text{Syl}_p(S_{p^k})|$ ($T_k$ is the iterated wreath product of Kaloujnine [4]); exactly a fraction $1/p^k$ of them are $p^k$-cycles, whence $|\text{basin}_{p^k}| = |T_k|/p^k$ (Theorem 3.3). Moreover, for $\tau \in \text{basin}_{p^k}$, $\ell \circ \tau^{-1} = \ell + \beta_\tau \circ \mu$ with $\beta_\tau = -\,b(\tau) \circ \bar\tau^{-1}$ and $\mu \circ \tau^{-1} = \bar\tau^{-1} \circ \mu$.*

*Proof.* The tower description is the descente of Theorem 3.4 without cyclicity; the count is immediate, and comparison with $|\text{basin}_{p^k}|$ (Theorem 3.3) gives the ratio $p^{-k}$. Inversion: from $\ell(\tau(x)) = \ell(x) + b(\tau)_{\mu(x)}$ set $y = \tau(x)$ to get $\ell(\tau^{-1}y) = \ell(y) - b(\tau)_{\bar\tau^{-1}(\mu(y))}$; and $\mu \circ \tau^{-1} = \bar\tau^{-1} \circ \mu$. □

**Running example ($n = 8$), the basin.** At $p^k = 8$ the tower gives $|T_3| = 2^7 = 128 = |\text{Syl}_2(S_8)|$, of which the fraction $1/8$ are 8-cycles, so $|\text{basin}_8| = 16$. Our $q = (s_4, (1,1,0,1))$ is one of them: it preserves the binomial flag on $\mathbb{Z}/8$, its base $s_4$ lies in $\text{basin}_4$, and $\Sigma a \neq 0$ (Theorem 3.3).

## 4 The root fibre, and the reduction to a linear-algebra statement

*Goal of this section.* Inside the basin, the deepest chains live over the base fixed point $s_d$, on the *root fibre*, where $D$ is a single linear map — the shift difference $I - S$, nilpotent of index $d$. A cycle's distance to $s$ then splits as its base-distance plus a nilpotency height ((3)), which reduces the whole depth question to one linear-algebra statement, (L2), provable from a single arithmetic input MI (deferred to §5).

From here we fix the level $n = p^e$ ($e \geq 2$), base $d = p^{e-1}$, sub-base $c = p^{e-2}$; carries live in $(\mathbb{Z}/p)^d$, functionals on $\mathbb{Z}/d$. For $\tau \in \mathrm{basin}_d$, $m = \mathrm{dist}(\tau)$ and the base path is $\tau = \tau_0 \to \cdots \to \tau_m = s_d$. The *root fibre* is $R = \pi^{-1}(s_d)$. For $q = (\tau, a)$ the forward carries are $a_0 = a$, $a_{i+1} = L_{\tau_i} a_i + w_{\tau_i}$; the affine composite over the $m$ steps is $\Phi_\tau(a) = M_\tau a + v_\tau$, $M_\tau = L_{\tau_{m-1}} \cdots L_{\tau_0}$, and

$$\mathrm{Sol}(\tau) = \{a : \ \Phi_\tau(a) = e_{d-1}\} = \{a : \ D_n^m(\tau, a) = s\}.$$

Write $S$ for the shift $(Sa)_r = a_{r-1}$ and $N = I - S$, and $\rho = d$ ($p$ odd), $d - 1$ ($p = 2$).

**Lemma 4.1** (root fibre is linear; lower bound)**.** *On $R$ the cocycle is the affine map $a \mapsto Na + e_0$ with unique fixed point $e_{d-1}$; in the recentred coordinate $\hat{a} = a - e_{d-1}$ it is the linear map $\hat{a} \mapsto N\hat{a}$, nilpotent of index $d$ (a single Jordan block), with $\mathrm{Im}\, N^h = \{v : \langle \varphi_j, v \rangle = 0, \ j < h\}$ and a vector of $\mathrm{Im}\, N^h$ of $N$-height $\leq d - h$. Consequently, for $q$ with base $\tau$ at distance $m$,*

$$\mathrm{dist}(q) = m + \mathrm{height}\big(\Phi_\tau(a) - e_{d-1}\big). \tag{3}$$

*The whole fibre $R$ is a single in-tree of $\mathbf{0}$ of height $d$, and $\mathrm{depth}(p^e) \geq \rho$: $R$ contains an* admissible *carry of height exactly $\rho$.*

*Proof.* For $\tau = s_d$: $(L_{s_d} a)_{r'} = a_{r'} - a_{r'-1} = (Na)_{r'}$ and $w_{s_d} = e_{s_d(d-1)} = e_0$ (Lemma 2.3). The fixed point solves $Na + e_0 = a$, i.e. $Sa = e_0$, $a = e_{d-1}$; and $N(a - e_{d-1}) = Na - (e_{d-1} - e_0) = (Na + e_0) - e_{d-1}$, so $\hat{a} \mapsto N\hat{a}$. Over $\mathbb{F}_p$, $S^d = I$ and $X^d - 1 = (X-1)^d$ ($d$ a $p$-power), so $N$ is nilpotent of index $d$, one Jordan block; and since $\Delta$ lowers flag-degree by exactly one with $V_h = \ker \Delta^h$ (Lemma 2.4), the same holds for $N$ (they share the flag), giving $\mathrm{Im}\, N^h = \{v : \langle \varphi_j, v \rangle = 0, \ j < h\}$ (dimension $d - h$) and the height bound; (3) follows since $D^m(q) \in R$ has recentred carry acted on by $N$.

The map $\hat{a} \mapsto N\hat{a}$ is the additive cellular automaton of rule $1 - x$ on the cyclic lattice $\mathbb{Z}/d$ ("rule 60" at $p = 2$); as $d = p^{e-1}$ is a $p$-power and the rule shares the single factor $x - 1$ with $x^d - 1 = (x-1)^d$, this is the purely nilpotent case of Martin–Odlyzko–Wolfram [6] (their Theorem 4.3, with $D_p(d) = d$ and multiplicity $X = 1$, gives in-tree height $\lceil D_p(d)/X \rceil = d$): all of $R$ is one in-tree of $\mathbf{0}$ of height $d$. It remains to locate the deepest *admissible* carry (those $a = \hat{a} + e_{d-1}$ with $\Sigma a \neq 0$). For $p$ odd a height-$d$ vector can be taken admissible, so depth $\geq d = \rho$; for $p = 2$ the admissibility constraint excludes the top height $d$ but a height-$(d-1)$ carry is admissible (e.g. $\hat{a} = (1, 1, 0, \ldots, 0)$), so depth $\geq d - 1 = \rho$. □

**Running example ($n = 8$), the deepest chain.** Here $d = 4$, $c = 2$, $\rho = d - 1 = 3$. Our $q = (s_4, (1, 1, 0, 1))$ has base $s_4$, so it lies in the root fibre $R = \pi^{-1}(s_4)$; recentred, $\hat{a} = a - e_3 = (1, 1, 0, 0)$, with $N\hat{a} = (1, 0, 1, 0)$, $N^2\hat{a} = (1, 1, 1, 1)$, $N^3\hat{a} = 0$: $N$-height 3. By (3) (base-distance $m = 0$) $\mathrm{dist}(q) = 3$, realised by the carry chain

$$(1,1,0,1) \xrightarrow{D} (1,0,1,1) \xrightarrow{D} (1,1,1,0) \xrightarrow{D} (0,0,0,1) = e_3, \qquad \text{i.e. } q \to Dq \to D^2 q \to s.$$

The top height $d = 4$ is unreachable by an admissible carry (a height-4 vector has $\Sigma\hat{a} = 1$, forcing $\Sigma a = \Sigma\hat{a} + 1 = 0$), so 3 is the deepest admissible height, and $q$ realises $\mathrm{depth}(8) = 3 = 2^{\,e-1} - 1$.

**Remark 4.2.** The height-$d$ nilpotency above is the additive-cellular-automaton result of [6]; our contribution at this level is only the admissibility refinement (the "$-1$" at $p = 2$, forced by single-cycleness), and, upstream, the reduction of the permutation dynamics $D(q) = q\, s\, q^{-1}$ to this automaton on $R$.

### 4.1 The adjoint, the rank, and rigidity

**Lemma 4.3** (adjoint). *$L_\tau^*\varphi = \Delta(\varphi \circ \tau)$; and for $\tau \in \mathrm{basin}_d$, $\deg_V L_\tau^*\varphi \le \deg_V \varphi - 1$.*

*Proof.* The dual cocycle (Lemma 2.3) minus the constant $\langle \varphi, w_\tau\rangle = \varphi(\tau(d-1))$ gives $\langle \varphi, L_\tau a\rangle = \langle \Delta(\varphi\circ\tau), a\rangle$. For $\tau \in \mathrm{basin}_d$, (F) (Theorem 3.4) gives $\deg_V(\varphi\circ\tau) \le \deg_V\varphi$, and $\Delta$ lowers flag-degree by one (Lemma 2.4). □

**Proposition 4.4** (rank, image, rigidity). *$\operatorname{rank} M_\tau = d-m$, $\operatorname{Im} M_\tau = \operatorname{Im} N^m$, $\operatorname{Im} M_\tau^* = V_{d-m}$. As $m \le \mathrm{depth}(d) < d$, we have $\mathbf{1} = \varphi_0 \in V_{d-m} = (\ker M_\tau)^\perp$, so $\Sigma|_{\ker M_\tau} = 0$: $\Sigma$ is **constant** on $\mathrm{Sol}(\tau)$ whenever nonempty (*rigidity*).*

*Proof.* $M_\tau^* = L_{\tau_0}^* \cdots L_{\tau_{m-1}}^*$ composes $m$ maps each lowering flag-degree by $\ge 1$ (Lemma 4.3), so $\deg_V M_\tau^*\varphi_j \le j-m$; thus $M_\tau^*\varphi_j = 0$ for $j < m$ and $\langle \varphi_j, M_\tau a\rangle = 0$ for all $a$, i.e. $\operatorname{Im} M_\tau \subseteq \operatorname{Im} N^m$ (dimension $d-m$). Each $L_{\tau_i}$ has corank 1 (Lemma 2.3), so $\operatorname{rank} M_\tau \ge d-m$; equality follows, and $\operatorname{Im} M_\tau = \operatorname{Im} N^m$. Dually $\operatorname{Im} M_\tau^*$ has dimension $d-m$ and lies in $V_{d-m}$ by the degree bound, so equals it. Finally $\varphi_0 \in V_{d-m} = (\ker M_\tau)^\perp$ (as $m < d$), so $\Sigma$ kills $\ker M_\tau$ and is constant on the coset $\mathrm{Sol}(\tau)$. □

### 4.2 Transport and the closed form

**Lemma 4.5** (transport). *Set $\chi_0 = \tau_0^{-1}$ and, when $\chi_i$ is zero-mean, $\chi_{i+1} = \Psi_{\chi_i} \circ \tau_{i+1}^{-1}$. Then $\langle \chi_i, a_{i+1}\rangle = \langle \chi_{i+1}, a_{i+2}\rangle - \Psi_{\chi_i}(d-1)$.*

*Proof.* Apply the dual cocycle at step $i+1$ with $\varphi = \Psi_{\chi_i}\circ\tau_{i+1}^{-1}$ (so $\varphi\circ\tau_{i+1} = \Psi_{\chi_i}$, $\Delta(\varphi\circ\tau_{i+1}) = \chi_i$): $\langle \varphi, a_{i+2}\rangle = \langle \chi_i, a_{i+1}\rangle + \Psi_{\chi_i}(d-1)$. □

**Proposition 4.6** (closed form). *If $\chi_0, \dots, \chi_{m-2}$ are all zero-mean, the constant value of $\Sigma$ on $\mathrm{Sol}(\tau)$ (Proposition 4.4) is*

$$V(\tau) = -\chi_{m-1}(d-1) + \sum_{i=0}^{m-2} \Psi_{\chi_i}(d-1) - 1. \tag{4}$$

*Proof.* Iterate Lemma 4.5 from $\Sigma a = -\langle \chi_0, a_1\rangle - 1$ (Lemma 2.4(iii) and the dual cocycle with $\varphi = -\varphi_1 \circ \tau_0^{-1}$); for $a \in \mathrm{Sol}(\tau)$, $a_m = e_{d-1}$, so $\langle \chi_{m-1}, a_m\rangle = \chi_{m-1}(d-1)$. □

### 4.3 Geometrisation, and the reduction theorem

**Definition 4.7.** (L2) holds at $\tau$ if $\langle \varphi_j, \Phi_\tau(a) - e_{d-1}\rangle = 0$ for all admissible $a$ and all $j < m$; and, for $p = 2$, the same holds at $j = m$ for those admissible $a$ with $\Sigma a = 1$.

**Proposition 4.8** (geometrisation). *(L2) at $\tau \Leftrightarrow \mathrm{Sol}(\tau) \neq \varnothing$ (and, for $p = 2$, with a representative of sum 1).*

*Proof.* The linear part $a \mapsto \langle \varphi_j, M_\tau a\rangle$ vanishes for $j < m$ since $\varphi_j \perp \operatorname{Im} M_\tau = \operatorname{Im} N^m$ (Proposition 4.4). So (L2) ($j < m$) is the constant condition $\langle \varphi_j, v_\tau - e_{d-1}\rangle = 0$, i.e. $e_{d-1} - v_\tau \in \operatorname{Im} N^m = \operatorname{Im} M_\tau$, i.e. $M_\tau a = e_{d-1} - v_\tau$ solvable, i.e. $\mathrm{Sol}(\tau) \neq \varnothing$. For $p = 2$ the level $j = m$ says the (constant, by rigidity) value of $\Sigma$ on $\mathrm{Sol}(\tau)$ is 1. □

**Theorem 4.9** (reduction). *If (L2) holds at every $\tau \in \mathrm{basin}_d$, then $\mathrm{depth}(p^e) = \rho$.*

*Proof.* For $q = (\tau, a)$ with base distance $m$: by (L2), $\langle \varphi_j, \Phi_\tau(a) - e_{d-1}\rangle = 0$ for $j < m$ (and $j = m$ if $p = 2$, as $\Sigma a = 1$), so $\Phi_\tau(a) - e_{d-1} \in \operatorname{Im} N^m$ (resp. $\operatorname{Im} N^{m+1}$), of height $\le d-m$ (resp. $\le d-1-m$) (Lemma 4.1). By (3), $\mathrm{dist}(q) \le d = \rho$ ($p$ odd), resp. $\le d-1 = \rho$ ($p = 2$). With the lower bound (Lemma 4.1), equality. □

### 4.4 From the master identity to (L2)

**Corollary 4.10** (non-leaf carries sum to 1)**.** *If $\tau = D_d(\sigma)$ for some $\sigma \in \mathrm{basin}_d$, then $\Sigma b(\tau) = 1$.*

*Proof.* $b(\tau) = L_\sigma b(\sigma) + w_\sigma$ is a cocycle image (Lemma 2.3). □

Call MI the statement: *for every $\tau \in \mathrm{basin}_d$ the transport chain is non-obstructed and $V(\tau) = \Sigma b(\tau)$* (established in §5).

**Theorem 4.11** (tree lemma)**.** MI *implies* $\mathrm{Sol}(\tau) \neq \varnothing$ *for all* $\tau \in \mathrm{basin}_d$*; hence* (L2) *everywhere and* $\mathrm{depth}(p^e) = \rho$.

*Proof.* Induction on $m = \mathrm{dist}(\tau)$, with invariant $\mathrm{Sol}(\tau) \neq \varnothing$ and $\Sigma \equiv \Sigma b(\tau)$ on $\mathrm{Sol}(\tau)$ (recall $\Sigma b(\tau) \neq 0$, cyclicity). Base $m = 0$: $\mathrm{Sol}(s_d) = \{e_{d-1}\}$, $\Sigma e_{d-1} = 1 = \Sigma b(s_d)$. Let $m \geq 1$, $\tau_1 = D_d\tau$; put $P = \{a : L_\tau a + w_\tau \in \mathrm{Sol}(\tau_1)\}$.

(a) $P \neq \varnothing$*:* the affine step is onto $\{\Sigma = 1\}$ (Lemma 2.3), and $\mathrm{Sol}(\tau_1) \subseteq \{\Sigma = 1\}$ since $\tau_1$ is non-leaf, so $\Sigma b(\tau_1) = 1$ (Corollary 4.10) and (induction) $\Sigma \equiv 1$ on $\mathrm{Sol}(\tau_1)$.

(b) $\Sigma \equiv \Sigma b(\tau)$ *on* $P$*:* for $a \in P$, $a_m = e_{d-1}$, so Proposition 4.6 (chain non-obstructed by MI) gives $\Sigma a = V(\tau) = \Sigma b(\tau)$ (by MI).

(c) *Admissibility:* $\Sigma b(\tau) \neq 0$, so every $a \in P$ has $\Sigma a \neq 0$, hence $(\tau, a) \in C(n)$ and $a \in \mathrm{Sol}(\tau)$. Thus $\mathrm{Sol}(\tau) = P \neq \varnothing$.

Then (L2) everywhere (Proposition 4.8; for $p = 2$, $\Sigma b(\tau) \neq 0$ in $\mathbb{F}_2$ is $\Sigma \equiv 1$), and Theorem 4.9 concludes. □

By Theorem 4.11 it remains to prove MI: the transport chain is non-obstructed on $\mathrm{basin}_d$, and $V(\tau) = \Sigma b(\tau)$. This is the content of §5.

## 5 The obstruction law and the compensation

*Goal of this section.* This proves MI, the one arithmetic fact left open in §4. Transporting a chain of functionals along the base path, it first fails to close up at step exactly $d - 2$ (the *obstruction law*), and the resulting invariant $V(\tau)$ equals $\Sigma b(\tau)$ (the *master identity*). This is where the odd-$p$ vs $p = 2$ dichotomy is finally pinned to a single carry.

The transport chain $\chi_0 = \tau_0^{-1}$, $\chi_{i+1} = \Psi_{\chi_i} \circ \tau_{i+1}^{-1}$ is defined as long as the $\chi_i$ are zero-mean; call $\mathrm{Ob}(\tau) = \min\{i : \Sigma\chi_i \neq 0\}$ (extending the base path stationarily at $s_d$), and $\mathrm{Ob}(d) = \min_\tau \mathrm{Ob}(\tau)$.

### 5.1 The graded module

Decompose each $\chi\colon \mathbb{Z}/d \to \mathbb{F}_p$ as $\chi(x) = \sum_{j=0}^{p-1} f_j(\mu(x))\,\ell(x)^j$ with $f_j\colon \mathbb{Z}/c \to \mathbb{F}_p$ (Vandermonde on the $p$ values of $\ell$); write $\deg_\ell \chi = \max\{j : f_j \neq 0\}$ and $A_j = \sum_r f_j(r)$.

**Lemma 5.1** (graded calculus)**.** (i) $\Sigma_{\mathbb{Z}/d\chi} = -A_{p-1}$ *(the mean sees only the top $\ell$-degree).* (ii) *If $\deg_\ell \chi = j \leq p - 2$ with top component $f_j$, the primitive $\Psi_\chi$ has $\ell^{j+1}$-component $\kappa_j A_j \mathbf{1}$ with $\kappa_j = -\frac{1}{j+1} \neq 0$; and, when $A_j = 0$ (equivalently $\deg_V f_j \leq c - 2$, since $A_j =$ head of $f_j$ times $[\deg_V f_j = c - 1]$ by Lucas), the $\ell^j$-component is the truncated $r$-primitive of $f_j$, of flag-degree $\deg_V f_j + 1 \leq c - 1$ with head equal to that of $f_j$, plus strictly lower flag-degree.* (iii) *Composition by $\tau^{-1}$ ($\tau \in \mathrm{basin}_d$) maps $\ell$-degree $j$ to $\leq j$ (strictly lower only for the below-top parts), acting on the top component by the flag-preserving pullback $f_j \mapsto f_j \circ \bar{\tau}^{-1}$ (head times a nonzero scalar, Theorem 3.4).*

*Proof.* (i) $\Sigma\chi = \sum_j A_j \sum_\ell \ell^j$; $\sum_{\ell=0}^{p-1} \ell^j \equiv 0$ for $0 \le j \le p-2$ and $\equiv -1$ for $j = p-1$. (ii) Split $\Psi_\chi(r + c\ell) = -\sum_{\ell'<\ell}(\sum_{r'} \sum_t f_t(r')\ell'^t) - \sum_{r'\le r} \sum_t f_t(r')\ell^t$; the first sum is $-\sum_t A_t S_t(\ell)$ (Faulhaber), top part $t = j$ contributing $\ell^{j+1}$-coefficient $-\frac{1}{j+1}A_j$; when $A_j = 0$ the $\ell^j$-part is the $r$-primitive of $f_j$ (head climbs one flag-degree, Lemma 2.4), the remaining Faulhaber terms being constants in $r$ at lower $\ell$-degree. (iii) $\ell \circ \tau^{-1} = \ell + \beta_\tau \circ \mu$ (Corollary 3.5) gives $\ell^j \circ \tau^{-1} = \sum_{i\le j} \binom{j}{i} (\beta_\tau \circ \mu)^{j-i} \ell^i$, of $\ell$-degree $\le j$ with top coefficient 1; and $f_j(\mu) \circ \tau^{-1} = (f_j \circ \bar\tau^{-1})(\mu)$. □

## 5.2 The obstruction law

**Theorem 5.2** (obstruction law)**.** *For every prime power $d = p^k$ and every $\tau \in \mathrm{basin}_d$, $\mathrm{Ob}(\tau) = d-2$; in particular the chain is non-obstructed for all steps $< d-2$, hence (as $\mathrm{dist}(\tau) \le \mathrm{depth}(d) < d-1$) for all steps up to $\mathrm{dist}(\tau) - 2$.*

*Proof.* Induction on $k$. $k = 1$ **($d = p$, $c = 1$):** $\chi_0 = s_p^{-B}$ is an affine (degree-1) function of $\ell = x$; each primitive raises the polynomial degree by one (Lemma 5.1(ii), $c = 1$) and composition by a rotation preserves degrees, so $\deg_\ell \chi_i = i + 1$; by (i) the chain is zero-mean until the top degree reaches $p - 1$, first obstructed at $i = p - 2 = d - 2$.

**Heredity ($d = pc$):** we track the graded decomposition. *No upward pollution:* by Lemma 5.1(ii,iii), composition never raises $\ell$-degree and the primitive raises the top $\ell^t$ to $\ell^{t+1}$ only when $A_t \ne 0$; a component of degree $t < j$ thus reaches at most $t+1 \le j < j+1$, so only the current top degree $j$, and only when $A_j \ne 0$, seeds $j+1$. *Stage 0:* while $f_1 = \cdots = f_{p-1} = 0$, $f_0$ is the sub-level chain (pullback), whose mean $A_0 = \Sigma_c f_0$ first becomes nonzero at $i = \mathrm{Ob}(c) = c-2$ (induction); this seeds degree 1, first present at step $t_1 = c - 1$. *Stage $j$ ($1 \le j \le p-1$):* once seeded (top component $f_j$ with head $\varphi_0$), while $A_j = 0$ the head climbs the $\mathbb{Z}/c$ flag by one per step (Lemma 5.1(ii,iii)), staying nonzero; by Lucas $\sum_r \varphi_h = [\,h = c-1\,]$, so $A_j$ vanishes until the head reaches $\varphi_{c-1}$, at $s = c - 1$ steps, i.e. step $t_j + c - 1$, where it seeds $j+1$ (if $j \le p-2$, $\kappa_j \ne 0$): $t_{j+1} = t_j + c$. Count: $t_1 = c - 1$, $t_{j+1} = t_j + c$, so the mean $-A_{p-1}$ (i) first becomes nonzero at $t_{p-1} + (c-1) = (c-1) + (p-2)c + (c-1) = pc - 2 = d - 2$. □

In particular MI's non-obstruction clause holds: for $\tau \in \mathrm{basin}_d$, $\mathrm{dist}(\tau) - 2 < \mathrm{depth}(d) \le d-2 = \mathrm{Ob}(d)$, so $\chi_0, \ldots, \chi_{\mathrm{dist}(\tau)-2}$ are zero-mean and $V(\tau)$ is defined (Proposition 4.6).

## 5.3 $V(\tau) = \Sigma b(\tau)$

We compute $\Sigma b(\tau)$ by the level-$c$ transport applied to the carry sequence, and compare to $V(\tau)$.

**Theorem 5.3** (master identity)**.** *$V(\tau) = \Sigma b(\tau)$ for every $\tau \in \mathrm{basin}_d$.*

*Proof.* Let $\bar\chi_i$ be the sub-level chain on $\mathbb{Z}/c$ (from the projected base path $\bar\tau_i$), and $\beta^{(i)} = b(\tau_i)$ the carries of the base path, evolving by the level-$c$ cocycle $\beta^{(i+1)} = L_{\bar\tau_i}\beta^{(i)} + w_{\bar\tau_i}$ with $\beta^{(m)} = b(s_d) = e_{c-1}$. Set $G_i = \langle \bar\chi_i, \beta^{(i+1)} \rangle$; the level-$c$ analogue of $\Sigma a = -\langle \chi_0, a_1 \rangle - 1$ gives $\Sigma b(\tau) = -G_0 - 1$.

*Non-deviated case ($m < c$, or generally while the sub-level chain is zero-mean).* By Theorem 5.2 at level $c$, the sub-level chain is non-obstructed for $i \le m-2$ iff $m - 2 < \mathrm{Ob}(c) = c - 2$, i.e. $m < c$. Then each transport step is clean, $G_i = G_{i+1} - \bar\Psi_{\bar\chi_i}(c-1)$, and $\Sigma b(\tau) = -\bar\chi_{m-1}(c-1) + \sum_{i=0}^{m-2} \bar\Psi_{\bar\chi_i}(c-1) - 1 = \bar V$. Meanwhile the level-$d$ chain is the pullback $\chi_i = \bar\chi_i \circ \mu$ (the primitive of a zero-$c$-mean pullback is a pullback, Lemma 5.1(ii) with $A = 0$; composition preserves pullbacks, Corollary 3.5), so evaluating (4) with $\mu(d-1) = c - 1$ gives $V(\tau) = \bar V$. Hence $V(\tau) = \Sigma b(\tau)$.

*Deviated case ($m = c$).* Now $\mathrm{dist}(\tau) = m = \mathrm{depth}(d)$, and the sub-level chain is obstructed at exactly the last sollicited step $i = c - 2$ ($\mathrm{Ob}(c) = c - 2$), with $T := \Sigma_c \bar\chi_{c-2} \ne 0$. For $i \le c - 3$ the pullback persists; at $i = c - 2$, the primitive of the mean-$T$ pullback carries a *deviation*:

$\Psi_{\chi_{c-2}} = \bar{\Psi}_{\bar{\chi}_{c-2}} \circ \mu - T\ell$ (from $\Psi_{g\circ\mu}(r+c\ell) = \bar{\Psi}_g(r) - (\Sigma_c g)\ell$). Composing with $\tau_{c-1}^{-1}$ (Corollary 3.5), $\chi_{c-1} = \bar{\chi}_{c-1} \circ \mu - T\ell - T(\beta_{c-1} \circ \mu)$. In (4) (using $\ell(d-1) = p-1$) the two $\pm T(p-1)$ terms cancel, leaving

$$V(\tau) = \bar{V} + T\,\beta_{c-1}(c-1), \qquad \bar{V} := -\bar{\chi}_{c-1}(c-1) + \textstyle\sum_{i=0}^{c-2} \bar{\Psi}_{\bar{\chi}_i}(c-1) - 1. \tag{5}$$

On the $\Sigma b$ side, the level-$c$ telescope is clean for $i \le c-3$, and at $i = c-2$ the raw transfer with the mass jump $\Delta\bar{\Psi}_{\bar{\chi}_{c-2}} = \bar{\chi}_{c-2} - Te_0$ (Lemma 2.4(ii)) gives, with $\varphi = \bar{\Psi}_{\bar{\chi}_{c-2}} \circ \bar{\tau}_{c-1}^{-1}$,

$$G_{c-2} = \left[\bar{\chi}_{c-1}(c-1) - \bar{\Psi}_{\bar{\chi}_{c-2}}(c-1)\right] + T\,\beta_0^{(c-1)},$$

the extra $+T\beta_0^{(c-1)} = +T\,b(\tau_{c-1})_0$ being the mass-jump term evaluated against $\beta^{(c-1)}$. Telescoping the clean steps into $\Sigma b(\tau) = -G_0 - 1$,

$$\Sigma b(\tau) = \bar{V} - T\,b(\tau_{c-1})_0. \tag{6}$$

Comparing (5), (6), MI is equivalent to $\beta_{c-1}(c-1) = -b(\tau_{c-1})_0$. Now $\tau_{c-1}$ is a rotation $s_d^B$ (base-distance 1); its sub-base carry is $b(s_d^B)_r = \lfloor((r+B) \bmod d)/c\rfloor$, so $b_0 = B_1$ (writing $B = \bar{B} + B_1 c$, $1 \le \bar{B} < c$), while by $\ell \circ \tau^{-1} = \ell + \beta \circ \mu$ (Corollary 3.5) a direct evaluation gives $\beta_{c-1}(c-1) = -B_1 = -b_0$. Hence $V(\tau) = \Sigma b(\tau)$ in all cases. □

**Corollary 5.4** (prime-power depth)**.** $\mathrm{depth}(p^e) = \rho$: $p^{\,e-1}$ *for* $p$ *odd,* $2^{\,e-1} - 1$ *for* $p = 2$.

*Proof.* By Theorems 5.2 (non-obstruction) and 5.3, MI holds; Theorem 4.11 gives $\mathrm{depth}(p^e) = \rho$. (Base cases $e \le 2$, where $c = p^{e-2} \le 1$ is degenerate, are direct: $\mathrm{depth}(p) = 1$ for $p$ odd, $\mathrm{depth}(2) = 0$, $\mathrm{depth}(p^2) = p$ resp. $\mathrm{depth}(4) = 1$, from Theorem 3.3 and the root fibre.) □

## 6 General $n$ via the Chinese Remainder Theorem

*Goal of this section.* The prime-power computation is complete; we assemble general $n$. Everything factors along coprime factors — basin, distance, hence depth — so $\mathrm{depth}(n)$ is simply the largest prime-power depth.

Let $n = n_1 n_2$ with $\gcd(n_1, n_2) = 1$. The isomorphism $\mathbb{Z}/n \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2$ ($x \mapsto (x \bmod n_1, x \bmod n_2)$) carries $s_n$ to $(s_{n_1}, s_{n_2})$; we identify the two, write points $(x_1, x_2)$, and call a permutation a *product* $q_1 \times q_2$ if it acts coordinatewise.

**Lemma 6.1.** (i) $q_1 \times q_2 \in C(n)$ *iff* $q_i \in C(n_i)$; (ii) $D_n(q_1 \times q_2) = D_{n_1}(q_1) \times D_{n_2}(q_2)$; (iii) *if* $q \in C(n)$ *and* $D_n(q)$ *is a product, then* $q$ *is a product.*

*Proof.* (i) The orbit of $(x_1, x_2)$ has size $\mathrm{lcm}(\ell_1, \ell_2)$, $= n = \mathrm{lcm}(n_1, n_2)$ for all points iff each $q_i$ is a full cycle. (ii) $s_n = s_{n_1} \times s_{n_2}$ and products conjugate coordinatewise. (iii) Let $t = D_n(q) = t_1 \times t_2$ ($t_i \in C(n_i)$). Then $g := s_n^{n_1}$ advances only the second coordinate by $n_1$ (invertible mod $n_2$), so $\langle g\rangle$ has the rows $\{a\} \times \mathbb{Z}/n_2$ as orbits; and $t^{\,n_1} = q\,g\,q^{-1}$ (as $t = qsq^{-1}$) while $t^{\,n_1} = \mathrm{id} \times t_2^{n_1}$ (since $t_1$ has order $n_1$, and $t_2^{n_1}$ is a full $n_2$-cycle) also has the rows as orbits. Conjugation transports orbits, so $q(\text{rows}) = \text{rows}$: $q$ maps each row $R_a$ onto a single row, hence the first coordinate of $q(x)$ depends only on $x_1$. Symmetrically (with $s_n^{n_2}$ and the columns) the second depends only on $x_2$; so $q$ is a product. □

**Theorem 6.2** (multiplicativity)**.** *For coprime* $n_1, n_2$, $\mathrm{basin}_n = \{q_1 \times q_2 : q_i \in \mathrm{basin}_{n_i}\}$ *and* $\mathrm{dist}(q_1 \times q_2) = \max(\mathrm{dist} q_1, \mathrm{dist} q_2)$. *Hence* $|\mathrm{basin}_n| = |\mathrm{basin}_{n_1}||\mathrm{basin}_{n_2}|$ *and* $\mathrm{depth}(n) = \max(\mathrm{depth}\, n_1, \mathrm{depth}\, n_2)$.

*Proof.* ($\supseteq$) By Lemma 6.1(ii), $D_n^k(q_1 \times q_2) = D_{n_1}^k(q_1) \times D_{n_2}^k(q_2) = s_n$ iff $k \geq \mathrm{dist} q_1$ and $k \geq \mathrm{dist} q_2$. ($\subseteq$) For $q \in \mathrm{basin}_n$ with $D_n^t(q) = s_n$ (a product), backward induction with Lemma 6.1(iii) makes $q, \ldots, D_n^t(q)$ all products; $q = q_1 \times q_2$ with $q_i \in C(n_i)$, and projecting $D_n^t(q) = s_n$ gives $D_{n_i}^t(q_i) = s_{n_i}$, so $q_i \in \mathrm{basin}_{n_i}$. The consequences are immediate. □

*Proof of Theorem 1.1.* Corollary 5.4 gives $\mathrm{depth}(p^e)$; iterating Theorem 6.2 over the coprime prime-power factors of $n$ gives $\mathrm{depth}(n) = \max_p \mathrm{depth}(p^{e_p})$. The threshold statement is the observation that $\mathrm{depth}(p^e) \geq 2$ iff $8 \mid p^e$ (i.e. $p = 2$, $e \geq 3$) or $p^2 \mid p^e$ with $p$ odd (i.e. $p$ odd, $e \geq 2$). □

# 7 Discussion

**Interpreting the threshold.** $\mathrm{depth}(n) \geq 2$ iff $8 \mid n$ or $p^2 \mid n$ for an odd prime — verbatim the Hull–Dobell condition for a full-period non-translation affine map on $\mathbb{Z}/n$. The affine $n$-cycles $x \mapsto ax + b$ occupy the top two layers of the in-tree ($D$ sends such a map to $s^a$, then to $s$), and are full cycles exactly under Hull–Dobell; the tree is deep precisely when non-translation ones exist. This is *not* the squarefree threshold: at $n = 12$ (and $n = 4$) the level is non-squarefree yet the tree is shallow (depth $= 1$), because $4 \parallel n$ without $8 \mid n$.

**A single arithmetic thread.** Beneath the three structural steps lies one mechanism: near $s$, the dynamics of $D$ is the carrying of base-$p$ addition. From this vantage the classical ingredients the proof invokes — Hull–Dobell (full-period affine maps), Lucas and Kummer (digit carries), Faulhaber (power sums) — are facets of a single arithmetic rather than independent tools. In the same vein, the admissible carry maps are single-cycle $T$-functions in the sense of Klimov–Shamir [3], whose transitivity is the object of Anashin's non-Archimedean ergodic theory [5].

**Related work: carries elsewhere.** Carries have appeared in the combinatorics of the symmetric group in different guises: as a random Markov chain equivalent to riffle shuffling, with Eulerian eigenvalues and a Foulkes-character eigenbasis [7, 8], and as the 2-cocycle of the extension $\mathbb{Z}/b\mathbb{Z}$ measuring its non-splitting [9]. The carries here are of a different nature: a *deterministic* 1-cocycle of the conjugation dynamics over $\mathbb{F}_p$, and the invariant of interest is a tree depth rather than a mixing time or a cohomology class of an abelian extension.

**Open questions.** Two natural questions lie beyond the depth. *(i) The rest of the functional graph.* $D$ acts on all of $C(n)$, and the cycles that never reach $s$ fall into other components; their periodic orbits, and the number and sizes of the connected components of the graph of $D$, are not addressed here. *(ii) The shape of the in-tree.* We obtain $|\mathrm{basin}_{p^k}|$ in closed form (Theorem 3.3) but only the *height* of the tree; the distance profile — how many cycles sit at each distance from $s$ — remains open, as does whether it factors under the Chinese Remainder Theorem the way the height does (Theorem 6.2).

**Status and formalisation.** As stated in the title footnote, the argument was machine-generated and is not yet refereed. Reassuringly for a future check, all of §§2–6 is finite linear algebra over $\mathbb{F}_p$ together with elementary group theory — a natural candidate for a proof assistant. A Lean formalisation of the cocycle, the flag characterisation, and the obstruction law would settle the remaining status question definitively.

# A Computer verification

Every statement was checked by exact computation over $\mathbb{F}_p$ (Python), exhaustively at the levels indicated; these are falsification attempts and reproducibility aids, not part of the proof. Selected certificates:

- *Cocycle and carry coordinates* (Lemmas 2.3, Props. 2.1, 2.2): bijection, cyclicity, $w_\tau = e_{\tau(c-1)}$, dual form: 0 exceptions at $(p, c) = (2, 4), (3, 3), (2, 2)$.
- *Flag characterisation* (Theorem 3.4): $\mathrm{basin}_{p^k} = \{\text{triangular cycles}\}$ as sets at $p^k = 4, 8, 9$; inclusion on all 484,440 elements of the basins of $C(16), C(25), C(27)$; basin $\subseteq F^{(k)}$ and the descente identities ($\ell \circ \tau = A \circ \mu + \ell$, $\lambda = 1$, $A = b(\tau)$; $\ell \circ \tau^{-1} = \ell - b \circ \bar{\tau}^{-1}$): 0 exceptions at $p^k = 8, 9, 25, 27$.
- *Root fibre, rank, rigidity* (Lemmas 4.1, 4.3, Prop. 4.4): $D|_R = N$ recentred, $\mathrm{Im}\, N^h =$ moment kernel, $L_\tau^* = \Delta(\cdot \circ \tau)$, $\mathrm{rank}\, M_\tau = d - m$, $\Sigma|_{\ker M_\tau} = 0$: 0 exceptions at $n = 8, 16, 27$. Lower bound: root fibre reaches height $\rho$ at $n$ up to $2^5 = 32$.
- *Geometrisation* (Prop. 4.8) and *tree lemma* (Theorem 4.11): $\mathrm{Sol}(\tau) \neq \varnothing \Leftrightarrow$ moments vanish, and $\mathrm{Sol}(\tau) \neq \varnothing$ for all $\tau \in \mathrm{basin}_d$: 0 exceptions at $n = 8, 16, 27$; independent certificate $\mathrm{depth}(81) = 27$ on 3661 base points of $\mathrm{basin}_{27}$ (all distances), via the closed-form cocycle only.
- *Obstruction law* (Theorem 5.2): first obstruction at step $d - 2$, uniformly: $p = 2$: at $d = 4, 8, 16$; $p = 3$: $d = 9, 27$; $p = 5$: $d = 25, 125$; $p = 7$: $d = 49$; $p = 11$: $d = 121$ — all at the exact step, over all/thousands of base points.
- *Master identity* (Theorem 5.3): the graded rules, the mass jump, the carry telescope, and $V(\tau) = \Sigma b(\tau)$: 0 violations on all 18 deviated paths at $n = 27$ and on 400-path samples at $n = 81$ ($p = 3$) and $n = 125$ ($p = 5$).
- *Exhaustive depth*: $\mathrm{depth}(p^e) = \rho$ confirmed by full backward search for all prime powers $\leq 27$ and for $n = 49$ ($|\mathrm{basin}| = 4{,}235{,}364 = 36 \cdot 7^6$), and $\mathrm{depth}(2^5) = 15$ via the root fibre.
- *CRT* (Theorem 6.2): products, backward closure, dist $=$ max, multiplicativity: 0 exceptions at $n = 6, 12, 15$; and $|\mathrm{basin}_n|, \mathrm{depth}(n)$ against exhaustive values at $n = 18, 24, 36, 40, 45, 48, 50, 54, 72, 100$.

# References


[1] T. E. Hull and A. R. Dobell, *Random number generators*, SIAM Review **4** (1962), 230–254.

[2] D. E. Knuth, *The Art of Computer Programming, Vol. 2*, 3rd ed., Addison–Wesley (1997).

[3] A. Klimov and A. Shamir, *A new class of invertible mappings*, CHES 2002, LNCS **2523**, Springer (2003), 470–483.

[4] L. Kaloujnine, *La structure des p-groupes de Sylow des groupes symétriques finis*, Ann. Sci. École Norm. Sup. (3) **65** (1948), 239–276.

[5] V. Anashin and A. Khrennikov, *Applied Algebraic Dynamics*, de Gruyter Expositions in Mathematics **49**, Walter de Gruyter (2009).

[6] O. Martin, A. M. Odlyzko and S. Wolfram, *Algebraic properties of cellular automata*, Comm. Math. Phys. **93** (1984), 219–258.

[7] J. M. Holte, *Carries, combinatorics, and an amazing matrix*, Amer. Math. Monthly **104** (1997), no. 2, 138–149.

[8] P. Diaconis and J. Fulman, *Carries, shuffling, and an amazing matrix*, Amer. Math. Monthly **116** (2009), no. 9, 788–803.

[9] D. Isaksen, *A cohomological viewpoint on elementary school arithmetic*, Amer. Math. Monthly **109** (2002), 796–805.

[10] F. Lefebvre-Naré, *Iterated conjugation by a fixed cycle: the functional graph of $p \mapsto p\,s\,p^{-1}$ on $n$-cycles*, survey paper (2026).