Iterated conjugation by a fixed cycle: the functional graph of $p \mapsto p\,s\,p^{-1}$ on n-cycles

Frédéric Lefebvre-Naré*

October 2026 (second version)

Abstract

Fix an n-cycle s and, starting from any n-cycle p, repeatedly replace it by its conjugate $D(p) = p\,s\,p^{-1}$. Equivalently, D reads the one-line word of images $(p(0), \dots, p(n-1))$ back as a cycle — a conjugation cousin of the classical fundamental transform. Iterating D organises the $(n-1)!$ n-cycles into a functional graph, and this paper draws a first map of it.

Two principles organise the picture. In the coordinate $y = ps^{-1}$, D becomes the commutator map $y \mapsto [y, s]$; the system is therefore functorial in the pair (S_n, s): subgroups containing s carry subsystems, and homomorphisms carry factor systems. And the conjugation σ by s is a $\mathbb{Z}/n$ symmetry of the whole graph; it forces congruences on the sizes of the basins, constrains which periods and tail lengths can occur (sharply, with explicit exceptions at small n), and yields a closed count of the cycles it fixes.

Functoriality gives two structure theorems: for a prime $p \mid n$, a recursive projection maps the $\sigma^{n/p}$-symmetric cycles onto the system at n/p; for coprime n_1, n_2, the product cycles form a union of basins isomorphic to the product of the systems at n_1 and n_2. The unique fixed point s has exactly $\varphi(n)$ preimages, and its in-tree is shallow unless $8 \mid n$ or $p^2 \mid n$ for an odd prime (the Hull–Dobell threshold). A companion paper [3] identifies this tree, for $n = p^e$, with the n-cycles of a Sylow p-subgroup of S_n (for general n, with a product over the prime powers dividing n), so that its depth is governed by the nilpotency class p^{e-1} of that group: it equals p^{e-1} for odd p and $2^{e-1} - 1$ for $p = 2$. The periodic points correspond to the smallest Engel sink of s in S_n: Baer's theorem explains why there are several basins as soon as $n \geq 4$, and a recent theorem of Khukhro and Shumyatsky shows that the number of periodic points tends to infinity. The sequence of basin counts $1, 2, 2, 6, 7, 18, 17, 29, 56, 157$ ($n \leq 12$) appears to be new, and D deviates sharply from a uniformly random mapping, the sign of the deviation tracking the arithmetic of n.

2020 MSC: 05A05, 20B30, 20F45, 37P99. *Keywords:* n-cycles, conjugation, functional graph, basins of attraction, commutator map, cyclic group action, cyclic sieving, Euler totient, Hull–Dobell, Engel sinks.

* *Provenance and status.* The results below were obtained by artificial-intelligence models (Anthropic's Claude) in interactive dialogue with the author, and the proof elements were subsequently reviewed by OpenAI models (mostly GPT-5.5); every numerical claim was verified by exact finite computation. The in-tree of s (§5) is described completely in a self-contained companion paper [3]. This second version reorganises the paper around the commutator form of D (§2), adds the functoriality principle, the coprime factorisation and the link with Engel sinks, obtained in a later session with Claude, and updates the account of the in-tree of s to the second version of the companion. This remains a provisional report: an end-to-end verification of the whole, and human peer review, are still to be done, and it should be examined critically before being relied upon.

1 Introduction

Let S_n be the symmetric group on $\mathbb{Z}/n = \{0, 1, \ldots, n-1\}$, with arithmetic modulo n throughout. Let $C(n) \subset S_n$ be the set of n-cycles, so $|C(n)| = (n-1)!$. Fix once and for all an n-cycle s; the standard choice is $s_0 = (0\,1\,\cdots\,n-1)$, that is $s_0(i) = i+1 \bmod n$.

An n-cycle p can be presented in two ways: by its cycle notation, e.g. $(0\,2\,4\,3\,1)$, or by its one-line word of images $(p(0), p(1), \ldots, p(n-1))$, here $(2, 0, 4, 1, 3)$. The construction studied here turns the second presentation into the first: it sends $p = (0\,2\,4\,3\,1)$ to $D(p) = (2\,0\,4\,1\,3)$.

Definition 1.1. The *derivation* is the map $D : C(n) \to C(n)$ that sends p to the n-cycle written in cycle notation as $\big(p(0)\ p(1)\ \cdots\ p(n-1)\big)$; equivalently, $D(p)$ is the n-cycle sending $p(i)$ to $p(i+1)$ for every i (indices modulo n).

Lemma 1.2. *With $s = s_0$, we have $D(p) = p\,s\,p^{-1}$ for all $p \in C(n)$.*

Proof. By Definition 1.1, $D(p)\big(p(i)\big) = p(i+1) = p\big(s(i)\big)$ for all i, i.e. $D(p) \circ p = p \circ s$, so $D(p) = p\,s\,p^{-1}$. □

Since conjugation preserves cycle type, $p\,s\,p^{-1}$ is again an n-cycle, so D maps $C(n)$ into itself. As $C(n)$ is finite, every forward orbit $(D^k(p))_{k\geq 0}$ is eventually periodic: there exist minimal $j < k$ with $D^k(p) = D^j(p)$.

Definition 1.3. The *functional graph* of D has vertex set $C(n)$ and a directed edge $p \to D(p)$ for each p. Each weakly connected component contains exactly one directed cycle—a *periodic orbit* of D—to which in-trees are attached. We call these components the *basins*, and write $P(n)$ for the resulting partition of $C(n)$.

There is a classical bijection $C(n) \cong S_{n-1}$. Writing the cycle of p as $\big(0\ p(0)\ p^2(0)\ \cdots\ p^{n-1}(0)\big)$ and deleting the initial 0 leaves the sequence $\big(p(0), p^2(0), \ldots, p^{n-1}(0)\big)$, a one-line permutation of $\{1, \ldots, n-1\}$; this is a bijection $C(n) \to S_{n-1}$, a variant of the fundamental transformation [13, 20]. Under it $C(n)$ is identified with the vertex set of the permutohedron Π_{n-1}, which we use for the figures.

Remark 1.4. The passage "read the word of images as a cycle" is the punning idea behind the Foata fundamental transformation [13], but D is not that bijection. (That transformation writes each cycle of a permutation starting with its largest element, orders the cycles by increasing largest element, and erases the parentheses to read the result as a one-line word, turning the number of cycles into the number of left-to-right maxima.) The fundamental transformation is a bijection of S_n, neither conjugation-equivariant nor a homomorphism; iterating it partitions S_n into the pure cycles ("Foata circuits") studied by Mason and Borghesan [18], who note that it has no fixed point for $n > 1$, so every such cycle has length at least two. Our D differs in two structural respects. It is conjugation by a fixed cycle, hence far from injective (Proposition 2.3), so its functional graph carries genuine in-trees and basins rather than pure cycles; and it is an endofunction of $C(n)$ with the *unique* fixed point s (Proposition 2.2), whereas the fundamental transformation has none. The two maps share only the underlying cycle/word pun. A different non-injective family, the *sorting operators*—West's stack-sorting map and its relatives [21, 10]—likewise carries in-trees, but drains every permutation to the single fixed point id in at most $n-1$ iterations; D instead splits $C(n)$ into several basins with a nontrivial spectrum of periodic orbits.

Figure 1 shows the smallest interesting case, $n = 4$.

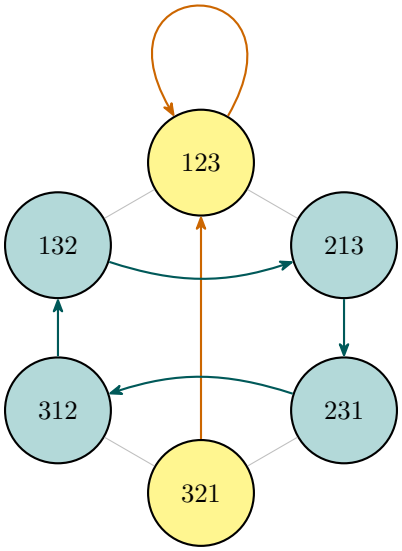


Figure 1: The permutohedron Π_3 (hexagon), $n = 4$. Vertices are the six 4-cycles in $C(4)$, labelled by their S_3 words in the coordinate of §1 (e.g. $s = 123$ is the 4-cycle $(0\,1\,2\,3)$ and 213 is $(0\,2\,1\,3)$); arrows are D. The fixed point $s = 123$ (loop) and its single predecessor 321 form the gold basin of size 2; the other four vertices form a single 4-cycle (teal), of size 4.

Figure 2 shows the next two cases, $n = 5$ and $n = 6$, on Π_4 and Π_5.

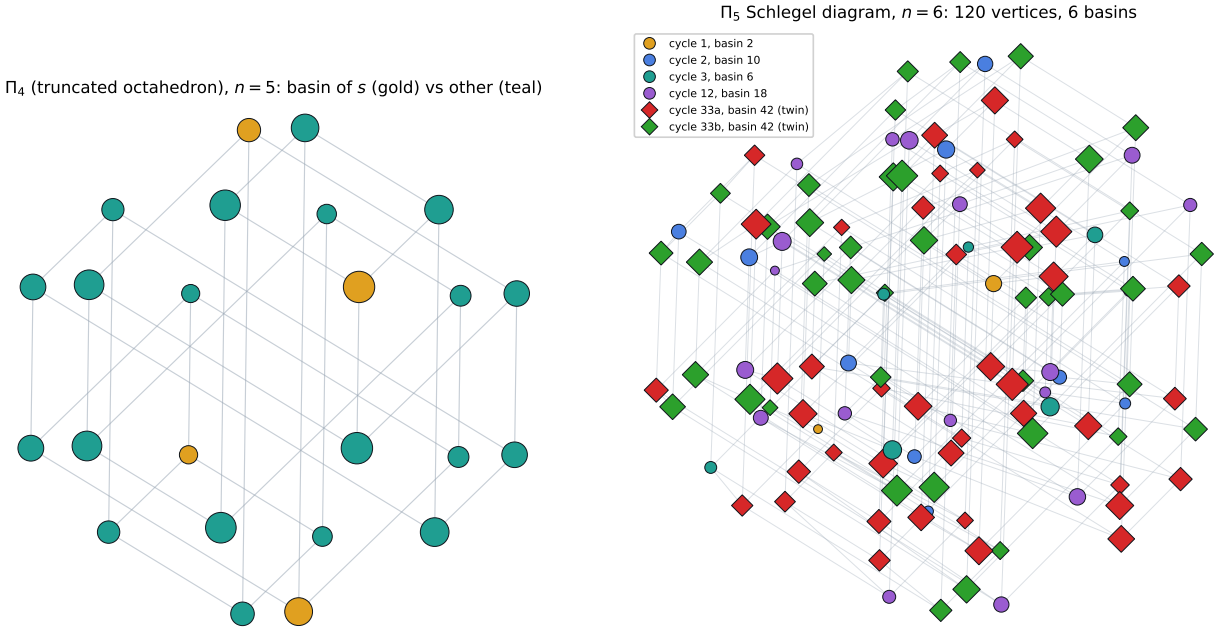


Figure 2: Left: the permutohedron Π_4 (truncated octahedron), $n = 5$, coloured by basin (gold: the basin of s, size 4; teal: the other basin, size 20). Right: a Schlegel diagram of the 4-dimensional permutohedron Π_5, $n = 6$, with 120 vertices coloured by the six basins; the two basins of size 42 (the red and green diamonds) are exchanged by the symmetry σ (Section 3).

Plan. Section 2 rewrites D, in the coordinate $y = ps^{-1}$, as the commutator map $y \mapsto [y, s]$. The elementary structure follows at once—s is the unique fixed point, D is uniformly n-to-1 as a map $S_n \to C(n)$, and the system does not depend on the choice of s—and so does a functoriality principle: subgroups containing s are invariant, homomorphisms give factor systems, and the automorphisms of S_n commuting with D are the powers of the conjugation σ by s. Section 3 exploits this $\mathbb{Z}/n$-symmetry: a closed count of the cycles fixed by each σ^k (generalising Wilson's theorem), congruences on basin sizes, sharp constraints on periods and tails, and the attachment necklaces of the in-trees. Section 4 gives two structure theorems derived from functoriality: a recursive projection $F_p \to C(n/p)$ for a prime $p \mid n$, realising the system as a smaller copy of itself, and an exact copy of the systems at n_1 and n_2 inside the one at $n = n_1 n_2$ when $\gcd(n_1, n_2) = 1$. Section 5 describes the in-tree of s: its first two layers are the rotations and the affine cycles, so it is flat unless $8 \mid n$ or $p^2 \mid n$ (Hull–Dobell); a carry coordinate linearises it on a "root fibre" carrying the deepest chains; and the companion [3] identifies it with the n-cycles of a Sylow subgroup, of depth p^{e-1} (resp. $2^{e-1} - 1$). Section 6 turns to the periodic part: up to a bijection, the periodic points form the smallest Engel sink of s in S_n; we also compare D with a random mapping. Section 7 lists open problems.

2 The commutator form and functoriality

The definition $D(q) = q\, s\, q^{-1}$ hides a simpler description, which organises much of what follows. The formula makes sense on all of S_n, and we extend D to S_n accordingly (Proposition 2.4 describes the extended graph). For $q \in S_n$ put

$$\delta(q) = q\, s^{-1},$$

the *defect* of q; it is trivial exactly when $q = s$, and δ is a bijection of S_n. We use the commutator $[a, b] = aba^{-1}b^{-1}$ and the iterated commutators $[y, {}_0 s] = y$, $[y, {}_{t+1} s] = \big[[y, {}_t s], s\big]$.

Lemma 2.1 (Commutator form)**.** *For every $q \in S_n$, $\delta(D(q)) = [\delta(q), s]$. Thus δ conjugates D on S_n to the commutator map $y \mapsto [y, s]$; in particular $\delta(D^t(q)) = [\delta(q), {}_t s]$, and $D^t(q) = s$ iff $[\delta(q), {}_t s] = 1$.*

Proof. Write $q = ys$ with $y = \delta(q)$. Then $\delta(D(q)) = qsq^{-1}s^{-1} = ys \cdot s \cdot s^{-1}y^{-1} \cdot s^{-1} = ysy^{-1}s^{-1} = [y, s]$. □

In this coordinate the elementary structure of D is transparent, and we record it first. For q in the in-tree of s, $\mathrm{dist}(q)$ is the number of commutators with s needed to kill $\delta(q)$—its *Engel length* relative to s. On an abelian subgroup normalised by s, commutation with s is a difference operator $a \mapsto a - s \cdot a$; this is why D becomes linear on the root fibre (Lemma 5.3).

Fixed point, fibres, and the extension to S_n

Proposition 2.2. *s is the unique fixed point of D in S_n: $D(p) = p$ if and only if $p = s$.*

Proof. Left-multiplying $p\, s\, p^{-1} = p$ by p^{-1} gives $s\, p^{-1} = e$, so $p = s$; conversely $D(s) = s$. □

Proposition 2.3. *As a map $D : S_n \to S_n$, the image of D is exactly $C(n)$, and D is uniformly n-to-1 onto $C(n)$: each fibre $D^{-1}(q)$ is a coset of $\langle s \rangle$ of size n. Every permutation that is not an n-cycle has in-degree 0 and maps in one step into $C(n)$.*

Proof. In the commutator form this is the identity $[ys^j, s] = [y, s]$. Directly, $D(p) = D(p')$ iff $(p'^{-1}p)\, s\, (p'^{-1}p)^{-1} = s$ iff $p'^{-1}p \in C_{S_n}(s) = \langle s \rangle$; hence the fibres are the cosets $p\langle s \rangle$, of size n, and the image is the conjugacy class of s, namely $C(n)$. Any preimage r of q satisfies $r\, s\, r^{-1} = q$, so q has a preimage only if $q \in C(n)$; thus a non-n-cycle has in-degree 0. □

The informal description of non-n-cycles as leaves grafted onto the periodic structure is made precise—and quantitative—by the next result, which also records how basin cardinalities behave under the extension of the domain to all of S_n.

Proposition 2.4. *Extend D to S_n. Each $q \in C(n)$ has in-degree exactly n in S_n, carrying $n - \deg^-_{C(n)}(q)$ pendant leaves (non-n-cycles), where $\deg^-_{C(n)}(q)$ is its in-degree within $C(n)$. Consequently, for each basin $B \subseteq C(n)$ of the restricted system, the corresponding basin in S_n has size exactly $n|B|$: the partition $P(n)$ is preserved up to the global dilation factor n, and the total becomes $n\,(n-1)! = n!$.*

Proof. In-degree n is the fibre size of Proposition 2.3. In the restricted graph each vertex has out-degree 1 with image in B, so the number of edges internal to B equals $|B|$, i.e. $\sum_{q \in B} \deg^-_{C(n)}(q) = |B|$. Hence the leaves on B number $\sum_{q \in B} \big(n - \deg^-_{C(n)}(q)\big) = (n-1)|B|$, and the basin in S_n has size $|B| + (n-1)|B| = n|B|$. □

Remark 2.5. The leaves attach directly to whichever n-cycle is their image, at every depth of the tree (including onto periodic vertices); for instance s itself carries $n - \varphi(n)$ leaves. Tree heights increase by at most one.

Independence of the chosen cycle

Theorem 2.6. *Let s, s' be two n-cycles and write $s' = g\, s\, g^{-1}$ (possible as all n-cycles are conjugate). Conjugation by g, $\sigma_g : C(n) \to C(n)$, $\sigma_g(p) = g\, p\, g^{-1}$, is a bijection with*

$$\sigma_g \circ D_s = D_{s'} \circ \sigma_g, \qquad \sigma_g \circ \sigma_s \circ \sigma_g^{-1} = \sigma_{s'},$$

where $D_t(p) = p\, t\, p^{-1}$ (the second identity is just the homomorphism law $\sigma_g \sigma_s \sigma_g^{-1} = \sigma_{gsg^{-1}} = \sigma_{s'}$). Thus $(C(n), D_s, \sigma_s) \cong (C(n), D_{s'}, \sigma_{s'})$ as dynamical systems with symmetry; g is determined up to right multiplication by $\langle s \rangle$.

Proof. $D_{s'}(\sigma_g(p)) = (gpg^{-1})(gsg^{-1})(gp^{-1}g^{-1}) = g(psp^{-1})g^{-1} = \sigma_g(D_s(p))$, and $\sigma_g \sigma_s \sigma_g^{-1}(q) = g\, s\, (g^{-1}qg)\, s^{-1} g^{-1} = s' q s'^{-1} = \sigma_{s'}(q)$. The solutions of $s' = gsg^{-1}$ form the coset $g\, C_{S_n}(s) = g\langle s \rangle$. □

Corollary 2.7. *Every isomorphism invariant of the functional graph—the number of basins, the multiset of pairs (period, basin size), the entire partition $P(n)$, and the $\mathbb{Z}/n$-symmetry—depends only on n. The standard cycle s_0 is merely a convenient coordinate; no n-cycle is dynamically distinguished.*

We verified this numerically: for every 6-cycle s the basin signature equals that of Table 2, and the unique fixed point is always s itself. Henceforth we fix $s = s_0$.

Functoriality

Since D is built from the group law and the single element s, it is natural with respect to subgroups and homomorphisms.

Proposition 2.8 (Functoriality)**.** *Let $H \leq S_n$ be a subgroup containing s.*

(a) $D(H) \subseteq H$; hence $H \cap C(n)$ is forward D-invariant.

(b) If $\phi\colon H \to S_m$ is a homomorphism and $t = \phi(s)$, then $\phi(D_s(h)) = D_t(\phi(h))$ for all $h \in H$. When t is an m-cycle, ϕ is thus a semiconjugacy from (H, D_s) to $(S_m, D_t) \cong (S_m, D_{s_m})$ (Theorem 2.6).

(c) If H is nilpotent of class κ, then $D^{\kappa}(h) = s$ for every $h \in H$: the whole of H lies in the in-tree of s, at distance at most κ.

(d) For $n \geq 3$, $n \neq 6$, the automorphisms of S_n that commute with D are exactly the powers of $\sigma = \sigma_s$, the conjugation by s.

Proof. (a) $hsh^{-1} \in H$. (b) $\phi(hsh^{-1}) = \phi(h)\,t\,\phi(h)^{-1}$. (c) $\delta(h) = hs^{-1} \in H$, and $[\delta(h),{}_{\kappa}s]$ lies in the $(\kappa+1)$-st term of the lower central series of H, which is trivial; conclude by Lemma 2.1. (d) If α commutes with D, then $D(\alpha(s)) = \alpha(D(s)) = \alpha(s)$, so $\alpha(s) = s$ by Proposition 2.2; conversely $\alpha(s) = s$ gives $\alpha(qsq^{-1}) = \alpha(q)\,s\,\alpha(q)^{-1}$. For $n \neq 6$ every automorphism of S_n is inner, by an element of $C_{S_n}(s) = \langle s\rangle$ when it fixes s. □

Most structures studied below are instances of Proposition 2.8. The rotations form the abelian group $\langle s\rangle$ (class 1: one step to s). The affine maps $x \mapsto ax + b$ form the normaliser of $\langle s\rangle$, and D sends them into $\langle s\rangle$ (Lemma 5.2). The automorphism σ generates the symmetry group of Section 3. The reservoir F_p is $C(n) \cap C_{S_n}(s^{n/p})$, and the recursive projection of Section 4 is (b) applied to the quotient map $C_{S_n}(s^{n/p}) \cong \mathbb{Z}/p \wr S_{n/p} \to S_{n/p}$; the subgroup $S_{n_1} \times S_{n_2}$ attached to a coprime factorisation gives the product structure of the same section. For $n = p^e$, the n-cycles of the Sylow p-subgroup of *triangular* permutations, which is nilpotent of class p^{e-1}, form the in-tree of s (Theorem 5.6); (c) is the source of its depth bound.

3 The cyclic symmetry

The conjugation σ by s commutes with D (Proposition 2.8(d)). This single property constrains the global shape of the graph—the multiplicities and sizes of basins, the lengths of periods and tails, the way trees attach to periodic orbits—and this section collects its consequences.

Theorem 3.1. *Let $n \geq 3$ and $\sigma(p) = s\,p\,s^{-1}$. Then $\sigma \circ D = D \circ \sigma$, and $\langle\sigma\rangle \cong \mathbb{Z}/n$ acts on $C(n)$ by automorphisms of the functional graph. (At $n = 2$, $C(n) = \{s\}$ is a single point and σ is trivial, s being central in S_2.)*

Proof. $D(\sigma p) = (sps^{-1})\,s\,(sp^{-1}s^{-1}) = s(psp^{-1})s^{-1} = \sigma(Dp)$. For $n \geq 3$, $\sigma^k = \mathrm{id}$ iff $s^k \in Z(S_n) = \{e\}$ iff $n \mid k$, so σ has order n. □

Corollary 3.2. *$\langle\sigma\rangle$ permutes the basins; basins in one σ-orbit are isomorphic (equal period, equal size), and σ-orbit sizes divide n (orbit–stabiliser, the stabiliser of p being $\langle s\rangle \cap \langle p\rangle$). The fixed points of σ are exactly the $\varphi(n)$ generators $\{s^a : \gcd(a, n) = 1\}$ of $\langle s\rangle$, and $\deg^-_{C(n)}(s) = \varphi(n)$.*

Proof. The first claims follow from Theorem 3.1 and orbit–stabiliser. $\sigma(p) = p$ iff $s \in \langle p\rangle$; since $|\langle s\rangle| = |\langle p\rangle| = n$, this forces $\langle p\rangle = \langle s\rangle$, i.e. p is a generator. Finally $D^{-1}(s) \cap C(n) = \langle s\rangle \cap C(n)$ has $\varphi(n)$ elements. □

Figure 3 shows this action at $n = 6$: σ turns each periodic orbit rigidly about s and permutes the basins.

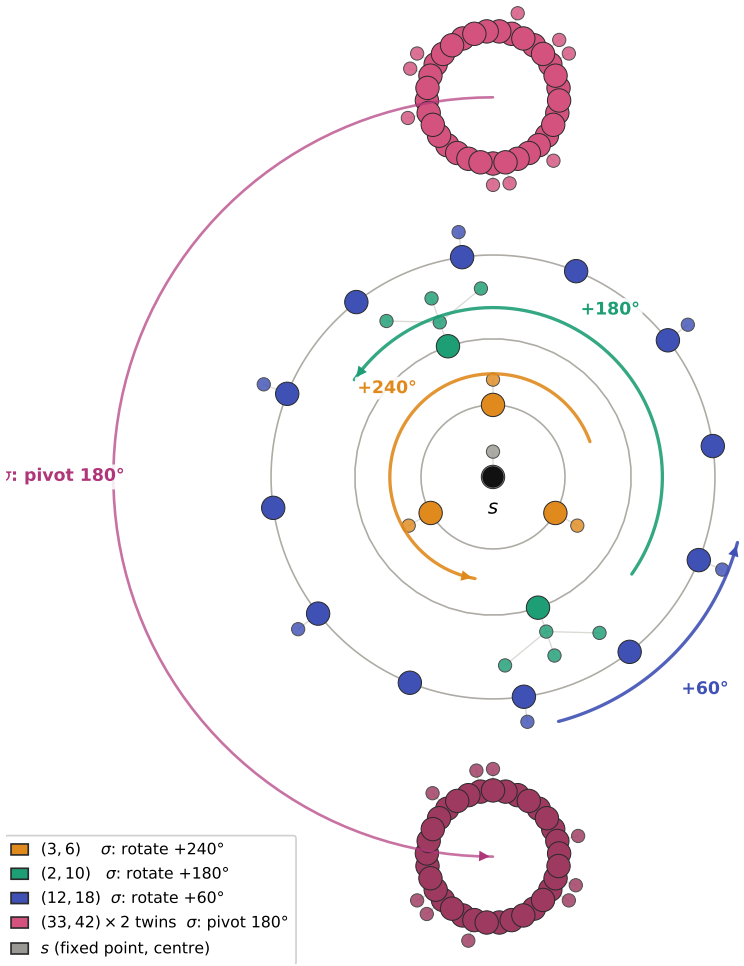


Figure 3: The basin system at $n = 6$ drawn as a polar diagram centred on s, chosen so that σ acts by rotation (Theorem 3.1, Corollary 3.2). The fixed point s sits at the centre; each σ-invariant basin is a concentric ring of its periodic n-cycles (joined by D, drawn counter-clockwise), with the attached in-trees as light pendants. One step of σ rotates each ring rigidly about s by its own amount, marked by an arc arrow: $+60°$ on $(12, 18)$, $+180°$ on $(2, 10)$, $+240°$ on $(3, 6)$. These angles are $2\pi r/P$ where $\sigma|_O = (D|_O)^r$; whenever $P \mid n$ one has $r \equiv -1$, i.e. σ acts as D^{-1}—one step backwards, hence $2\pi(P - 1)/P$. The two isomorphic basins $(33, 42)$ form a σ-orbit of size two: placed antipodally, they are exchanged by a $180°$ pivot. Colour encodes the isomorphism class $(P, |B|)$. What the picture fixes is the rotational action of σ (each ring, and the cluster, turning rigidly about s); the radii, the ordering of the basins and the starting phases are drawing conventions. Produced by `code/viz_polarN.py`.

Fixed points of the powers of σ

The cycles fixed by σ^k have a closed count, which generalises Wilson's theorem (Corollary 3.7).

Proposition 3.3 (Fixed-point counts)**.** *For $0 \le k < n$, with $c = \gcd(k,n)$ and $m = n/c$,*

$$\#\mathrm{Fix}(\sigma^k) \;=\; \#\{q \in C(n) :\; s^k \in \langle q\rangle\} \;=\; \varphi(m)\,(c-1)!\,m^{\,c-1}.$$

In particular $\#\mathrm{Fix}(\sigma^k)$ depends only on $\gcd(k,n)$.

Proof. $\sigma^k(q) = q$ iff s^k commutes with q iff $s^k \in C_{S_n}(q) = \langle q\rangle$. Now $\langle s^k\rangle = \langle h\rangle$ with $h = s^c$, of order m, a product of c disjoint m-cycles. As $\langle q\rangle$ is cyclic of order n, its unique subgroup of order m is $\langle q^c\rangle$; thus $h \in \langle q\rangle$ iff $q^c = h^t$ for some t prime to m. The targets h^t share a cycle type, so the numbers $A_t = \#\{q \in C(n) : q^c = h^t\}$ are all equal to $A = A_1$, and $\#\mathrm{Fix}(\sigma^k) = \varphi(m)\,A$.

Any q with $q^c = h$ commutes with h, hence lies in $C_{S_n}(h) \cong \mathbb{Z}/m \wr S_c = (\mathbb{Z}/m)^c \rtimes S_c$. Identify each block (an m-cycle of h) with $\mathbb{Z}/m$ so that h acts by $+1$; an element $(\vec{a},\tau)$ sends residue i in block j to residue $i + a_j$ in block $\tau(j)$. If τ is a single c-cycle, then $(\vec{a},\tau)^c$ fixes every block and acts there by $+T$ with $T = \sum_j a_j$; so $(\vec{a},\tau)^c = h^T$, and $(\vec{a},\tau)$ is a single n-cycle iff $\gcd(T,m) = 1$. Since an n-cycle in $C_{S_n}(h)$ permutes the blocks transitively, $q^c = h$ holds iff τ is a c-cycle and $T \equiv 1 \pmod m$ (which also forces the single-cycle condition). There are $(c-1)!$ such τ and m^{c-1} vectors $\vec{a}$ with $\sum a_j \equiv 1$, so $A = (c-1)!\,m^{c-1}$. □

For a prime $p \mid n$, put $g = s^{n/p}$ (an element of order p, a product of n/p disjoint p-cycles) and call

$$F_p = \mathrm{Fix}(\sigma^{n/p}) = \{q \in C(n) :\; s^{n/p} \in \langle q\rangle\} = C(n) \cap C_{S_n}(g)$$

the *symmetric reservoir*.

Corollary 3.4. *For each prime $p \mid n$,*

$$|F_p| \;=\; (p-1)\left(\tfrac{n}{p}-1\right)!\,p^{\,n/p-1}.$$

Proof. Take $k = n/p$ in Proposition 3.3: $c = n/p$ and $m = p$. □

Table 1: The symmetric reservoir $|F_p| = (p-1)(n/p-1)!\,p^{n/p-1}$.

n	p	$\lvert F_p\rvert$
4	2	2
5	5	4
6	2, 3	8, 6
7	7	6
8	2	48
9	3	36

Remark 3.5. These counts realise a cyclic sieving phenomenon [19]: the orbit polynomial $X(t) = \sum_O [\,|O|\,]_{t^{\,n/|O|}}$ (sum over σ-orbits $O \subseteq C(n)$, $[d]_u = 1+u+\cdots+u^{d-1}$) lies in $\mathbb{Z}_{\ge 0}[t]$ with $\deg X < n$, $X(1) = (n-1)!$, and $X(\zeta^k) = \#\mathrm{Fix}(\sigma^k)$ for $\zeta = e^{2\pi i/n}$ and all k. But this is the *tautological* sieving carried by any $\mathbb{Z}/n$-set—non-negativity is automatic—so the content is the count of Proposition 3.3, not the phenomenon. The polynomial merely packages the σ-orbit-size data; its constant term $c_0 = \frac{1}{n}\sum_k \#\mathrm{Fix}(\sigma^k)$ is the number of σ-orbits, the sequence $2, 3, 8, 24, 108, 640, 4492, \cdots =$ `A002619` (circular permutations up to rotation [23]), which X refines by orbit size. The same count arises for Yordzhev's σ-equivalence classes—the "factor set" of S_n under the two-sided action $\alpha \mapsto s^k \alpha s^{-l}$ with k, l *independent* [22]; our σ-orbits are the coupled case $k = l$ (conjugation) restricted to n-cycles, equinumerous with it though a different relation. What would be substantive—an *intrinsic* statistic realising X, read from q rather than from its orbit—is open (Section 7).

Congruences on basin sizes

By Corollary 3.2, basins of a common isomorphism type that are not σ-fixed occur with multiplicity divisible by their σ-orbit size, a divisor of n greater than 1; for example the two basins of size 42 at $n = 6$ (Table 2) form a σ-orbit of size 2. The symmetry also constrains the basin sizes themselves.

Table 2: Basins of D on $C(n)$ for small n: the number of basins and the pairs (period, basin size). A superscript k denotes a multiplicity of k isomorphic basins of equal period and size; these form a single σ-orbit (Cor. 3.2) *except* for $(4, 16)^2$ at $n = 8$, where the two isomorphic basins are each individually σ-invariant (like the $n = 7$ pairs below), not σ-conjugate. No superscript is used for the repeated pairs at $n = 7$: $(7, 14)$ and $(14, 28)$ are isomorphic but *not* σ-conjugate—a σ-orbit of basins has size dividing n, and $2 \nmid 7$—so each is a separate σ-invariant basin. Shown through $n = 9$; for $n = 10, 11, 12$ the basin counts are $29, 56, 157$ (Section 7), and the full signatures through $n = 12$ are provided as ancillary data.

n	#basins	basins (period, size)
3	1	$(1, 2)$
4	2	$(1, 2)$, $(4, 4)$
5	2	$(1, 4)$, $(5, 20)$
6	6	$(1, 2)$, $(2, 10)$, $(3, 6)$, $(12, 18)$, $(33, 42)^2$
7	7	$(1, 6)$, $(7, 14)$, $(7, 14)$, $(14, 28)$, $(14, 28)$, $(35, 119)$, $(49, 511)$
8	18	$(1, 16)$, $(4, 4)^4$, $(4, 6)^4$, $(4, 10)^4$, $(4, 16)^2$, $(8, 216)$, $(8, 4568)$, $(16, 128)$
9	17	$(1, 36)$, $(3, 195)^3$, $(9, 36)$, $(9, 102)^3$, $(9, 378)$, $(9, 1332)$, $(9, 3384)$, $(9, 4422)^3$, $(18, 72)$, $(18, 12177)$, $(54, 8748)$

Theorem 3.6. *F_p is invariant under both σ and D. For every σ-invariant basin B,*

$$|B| \equiv |B \cap F_p| \pmod{p}.$$

A basin meets F_p only if its periodic orbit lies in F_p; hence a σ-invariant basin whose periodic orbit is not $\sigma^{n/p}$-symmetric has size divisible by p. For a basin that is not σ-invariant the congruence applies to its full σ-orbit, not to the basin alone.

Proof. For $q \in F_p$, $\sigma^{n/p}(Dq) = D(\sigma^{n/p}q) = Dq$ by Theorem 3.1, so $Dq \in F_p$: thus F_p is forward D-invariant (and visibly σ-invariant). The group $\langle\sigma^{n/p}\rangle \cong \mathbb{Z}/p$ acts on the σ-invariant set B with orbits of size 1 or p, the size-1 orbits being $B \cap F_p$; counting gives the congruence. If $B \cap F_p \neq \varnothing$, the forward orbit of a point of $B \cap F_p$ stays in F_p and reaches the unique periodic orbit of B, which therefore lies in F_p. □

Corollary 3.7 (Prime case and Wilson)**.** *If $n = p$ is prime then F_p is the set of $p-1$ rotations, all lying in* basin(s) *(of size $p-1$); hence every σ-*invariant *basin other than* basin(s) *has size divisible by p. A non-invariant basin need not—at $n = 11$ the σ-orbit $(P, |B|) = (3, 56)$, repeated 11 times, has $56 \not\equiv 0 \pmod{11}$—but such an orbit consists of p isomorphic basins, so its union is divisible by p. Moreover Burnside's count for the $\mathbb{Z}/p$-action of $\sigma^{n/p}$ on $C(n)$ gives $(n-1)! \equiv |F_p| \pmod{p}$; for $n = p$ this is $(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$, Wilson's theorem.*

The values $|F_p|$ (Table 1) were confirmed by direct enumeration. For σ-invariant basins they pin the residue modulo $\mathrm{rad}(n)$ and confine the divisibility-breaking to those with symmetric periodic orbits; non-invariant basins are constrained only through their σ-orbit, and the precise distribution remains genuinely dynamical.

Periods

Proposition 3.8 (Periods for prime n)**.** *Let $n = p$ be prime. Among the periodic points of D, the only σ-fixed one is s; consequently the number of non-fixed periodic points is a multiple of p. If σ maps a non-fixed periodic orbit to itself, then p divides its length; hence every non-fixed period is a multiple of p, with one exception: a period* not *divisible by p is necessarily shared by a multiple of p orbits, none of them σ-stable.*

Proof. For $n = p$ the map σ has order p, and its fixed points are the $p-1$ rotations s^a (Corollary 3.2). Of these only s is periodic: $D(s^a) = s$ for every a, so s^a with $a \neq 1$ leaves its position under D and never returns. Thus the $\mathbb{Z}/p$-action of σ on the set U of periodic points has the single fixed point s; as p is prime all other σ-orbits in U have size p, so $|U| \equiv 1 \pmod p$ and $|U| - 1$ is a multiple of p.

Now let O be a non-fixed periodic orbit with $\sigma(O) = O$ and $|O| = \ell$. Then $\sigma|_O$ commutes with the ℓ-cycle $D|_O$, hence is a power of it (the centraliser of an ℓ-cycle is the cyclic group it generates). This power is non-trivial, for otherwise every point of O would be σ-fixed, forcing $O = \{s\}$; so it has order > 1 dividing p, i.e. order p, and $p \mid \ell$. Finally, σ permutes the periodic orbits of any fixed length ℓ in orbits of size 1 or p; a size-1 orbit is a σ-stable periodic orbit, for which the previous paragraph gives $p \mid \ell$. Hence if $p \nmid \ell$ then every orbit of length ℓ is σ-unstable, so these orbits fall into σ-orbits of size p, and their number is a multiple of p. □

For instance the non-fixed periods are $\{5\}$ at $n = 5$ and $\{7, 7, 14, 14, 35, 49\}$ at $n = 7$, all multiples of n, as no length is shared by a multiple of n orbits.

The argument of Proposition 3.8 extends to composite n and dispenses with the "shared length" caveat once it is run on the setwise stabiliser of a single orbit.

Proposition 3.9 (Periods meet n)**.** *Let O be a non-fixed periodic orbit of D on $C(n)$, of length ℓ, and let $\langle\sigma^t\rangle$ with $t \mid n$ be its setwise stabiliser in $\langle\sigma\rangle$ (so t is the size of the $\langle\sigma\rangle$-orbit of O among periodic orbits). If σ^t does not act as the identity on O, then $\gcd(\ell, n) > 1$; that is, ℓ shares a prime factor with n.*

Proof. By construction σ^t stabilises O setwise, and it commutes with D; hence $\sigma^t|_O$ lies in the centraliser of the ℓ-cycle $D|_O$ inside $\mathrm{Sym}(O)$, which is $\langle D|_O\rangle$. Thus $\sigma^t|_O$ is a power of an ℓ-cycle, and being non-trivial by hypothesis its order $e > 1$ divides ℓ. The same element has order dividing that of σ^t, namely $n/\gcd(t, n) = n/t$. Therefore $e \mid \gcd(\ell,\, n/t)$, whence $\gcd(\ell, n) \geq \gcd(\ell,\, n/t) \geq e > 1$. □

This contains Proposition 3.8: for prime n a σ-stable non-fixed orbit has $t = 1$, on which σ acts non-trivially (the only σ-fixed periodic point being s), giving $p \mid \ell$; an orbit lying in a σ-orbit of size p has instead $t = p$, where $\sigma^t = \sigma^p = \mathrm{id}$ acts trivially—the excluded "shared-length" case, on which the conclusion can fail (Remark 3.10). When the hypothesis holds, writing $\ell = d\,m$ with $d = \gcd(\ell, n) > 1$ a divisor of n exhibits every non-fixed period as a forced "seed" d times a free cofactor m carrying the irregular growth ($m = 11$ in $33 = 3 \cdot 11$ at $n = 6$, $m = 7$ in 49 at $n = 7$, $m = 6$ in 54 at $n = 9$). The lone hypothesis is that the setwise stabiliser act non-trivially on O; equivalently $s^t \notin \bigcap_{q \in O} \langle q\rangle$ for $O \neq \{s\}$. It holds for every non-fixed orbit at $n \leq 9$—the only orbit on which the setwise stabiliser acts trivially is then $\{s\}$ itself (already at $n = 10$ the five period-15 orbits form a σ-orbit on which σ^5 acts trivially)—but, like its hypothesis, the conclusion is *not* universal.

Remark 3.10 ($\gcd(\ell, n) > 1$ can fail)**.** At the prime $n = 11$ the derivation has non-fixed periodic orbits of lengths $\ell = 3, 9, 72$, each *coprime* to 11. (Verified on the full functional graph; the periods 3

and 9 were re-checked directly, $D^3 = \mathrm{id}$ and $D^9 = \mathrm{id}$ on the respective 11-cycles.) Each such length occurs with multiplicity 11: the eleven orbits form one $\langle\sigma\rangle$-orbit, so the setwise stabiliser of any one of them is trivial ($t = n = 11$, $\sigma^t = \mathrm{id}$) and acts trivially—exactly the excluded configuration, the "case B" anticipated for prime n in Proposition 3.8. Thus the unconditional reading "every non-fixed period shares a prime with n" is false; the hypothesis of Proposition 3.9 is essential. Composite $n = 10, 12$ exhibit no coprime period, so the phenomenon is not merely a matter of size.

Attachment necklaces

The same rotation governs how the in-trees attach to a periodic cycle.

Proposition 3.11 (Attachment necklace)**.** *Let B be a basin with periodic cycle O of length P and setwise stabiliser $\langle\sigma^t\rangle$ in $\langle\sigma\rangle$. Then $\sigma^t|_O = (D|_O)^r$ is a rotation of O by some step r, of order $P/\gcd(r, P)$ dividing n/t. As σ^t is an automorphism of the functional graph it preserves in-degree, so the sequence $\left(\deg^-_{C(n)}(q)\right)_{q\in O}$—equivalently the tree-attachment counts $\deg^-_{C(n)}(q) - 1$, the one remaining preimage being the cyclic predecessor—is a necklace invariant under that rotation: its period divides $\gcd(r, P)$. In particular, when r is coprime to P the in-degree is constant around O.*

Proof. σ^t stabilises O and commutes with D, so $\sigma^t|_O$ centralises the P-cycle $D|_O$, hence equals $(D|_O)^r$ for some r, of order $P/\gcd(r, P)$ dividing $\mathrm{ord}(\sigma^t) = n/t$. Being a graph automorphism, σ^t satisfies $\deg^-(\sigma^t q) = \deg^-(q)$, so the in-degree is constant on the rotation-by-r orbits of O, and its period divides $\gcd(r, P)$. □

For example at $n = 7$ the basin $(P, |B|) = (35, 119)$ has in-degree necklace of period 5 and $(49, 511)$ of period 7 (their cofactors $\ell/\gcd(\ell, n)$), whereas the period-7 and period-14 basins have constant in-degree 2; the bound was checked for all 52 basins at $n \le 9$ (8 are even more symmetric, with constant in-degree). The basin of s is the degenerate case $P = 1$, $\deg^-(s) = \varphi(n)$ (Corollary 3.2).

For a σ-invariant basin this pins the necklace period to the cofactor of the period, giving the cofactor a geometric meaning.

Observation 3.12 (The cofactor is the necklace period)**.** For every σ-invariant basin at $n \le 9$, $\sigma|_O$ is a rotation of order exactly $d = \gcd(P, n)$ (the seed); the cycle therefore splits into $m = P/d = \ell/\gcd(\ell, n)$ σ-orbits, of size d, on each of which the in-degree is constant. The attachment necklace thus has period dividing the cofactor m, with equality in the generic case; equivalently the in-degree ring carries d-fold rotational symmetry built from a motif of length m (so $P = d\,m$). The symmetry order is n exactly when $n \mid P$. Hence the otherwise unexplained cofactor of the period (Proposition 3.9) is realised as the number of σ-orbits of periodic points in the basin—the period of its attachment necklace. (For σ-twins, $t > 1$, the analogue uses σ^t: e.g. the two $(33, 42)$ basins at $n = 6$ show 3-fold symmetry on a motif of length 11, their wild cofactor.) See Figure 4.

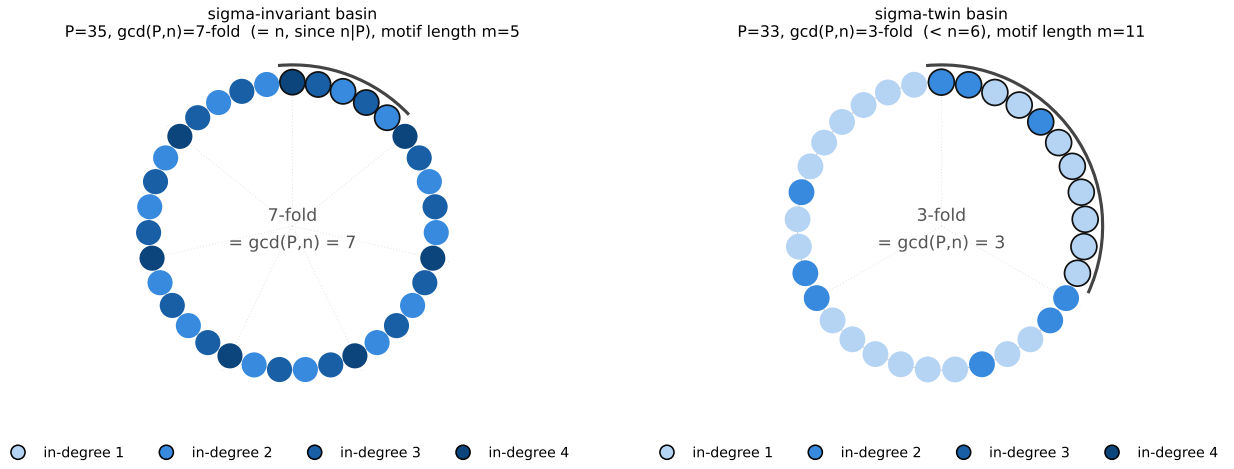


Figure 4: Attachment necklaces (Observation 3.12). Each dot is a periodic n-cycle on a basin's attractor, placed in D-order around the ring and coloured by in-degree (the number of attaching trees is $\deg^-_{C(n)} - 1$); one motif is outlined and the repeats are separated by spokes. Left: the σ-invariant basin $(P, |B|) = (35, 119)$ at $n = 7$; $\sigma|_O$ has order $\gcd(35, 7) = 7$, so the ring has 7-fold symmetry ($= n$ here, since $7 \mid 35$) built from a motif of length $m = 5$. Right: a σ-twin $(33, 42)$ at $n = 6$, with $\gcd(33, 6) = 3$-fold symmetry ($< n$) on a motif of length 11—its wild cofactor.

Tails

We turn to the off-orbit population of a basin. Write $P = |O|$ for the period of a basin B with attractor O, and $T = |B| - P$ for its *tail* (the non-periodic vertices). The σ-congruences of Theorem 3.6 constrain P and T *jointly*.

Proposition 3.13 (Tail mirrors period)**.** *Let B be a $\sigma^{n/p}$-invariant basin with attractor O, period P and tail T, for a prime $p \mid n$. If $O \not\subseteq F_p$, then $p \mid P$ and $p \mid T$.*

Proof. As a graph automorphism σ preserves the set of periodic vertices and its complement; since $\sigma^{n/p}(B) = B$ it follows that O and the tail $B \setminus O$ are each $\sigma^{n/p}$-invariant. The group $\langle \sigma^{n/p} \rangle \cong \mathbb{Z}/p$ acts on each with orbits of size 1 or p, the singletons being the points fixed by $\sigma^{n/p}$, i.e. the intersection with F_p; counting modulo p gives

$$P \equiv |O \cap F_p|, \qquad T \equiv |(B \setminus O) \cap F_p| \pmod{p}.$$

By Theorem 3.6 a basin meets F_p only if its attractor lies in F_p; as $O \not\subseteq F_p$ we get $B \cap F_p = \varnothing$, so both right-hand sides vanish and $p \mid P$, $p \mid T$. □

The hypothesis $O \not\subseteq F_p$ is exactly $\sigma^{n/p}|_O \neq \mathrm{id}$, and by itself forces $p \mid P$ (a non-trivial power of the P-cycle $D|_O$ has order p); the content of the proposition is that it forces $p \mid T$ as well, so that period and tail of such a basin carry the *same* prime divisors of n. Across $n \leq 9$ this covers all but two kinds of basin: those with a $\sigma^{n/p}$-symmetric attractor ($O \subseteq F_p$), which are precisely the basins on which the divisibility of Theorem 3.6 fails, and the rare σ-twin not individually $\sigma^{n/p}$-invariant (the two basins $(33, 42)$ at $n = 6$, swapped by σ^3). On both kinds the law $p \mid P \Leftrightarrow p \mid T$ happens to hold for $n \leq 9$, but—in contrast to the proposition—it is *not* a theorem: it fails from $n = 12$ on (Remark 4.4). The hypothesis $O \not\subseteq F_p$ is therefore essential; the projection of F_p onto a smaller copy of the same system (Section 4) both reaches those larger n cheaply and explains the failure.

4 Subsystems and factor maps

By Proposition 2.8, a subgroup $H \ni s$ of S_n carries a subsystem, and a homomorphism defined on H carries a factor system. Two choices of H give structure theorems. For a prime $p \mid n$, $H = C_{S_n}(s^{n/p})$ is a wreath product whose quotient map projects the reservoir F_p onto the system at level n/p; for a coprime factorisation $n = n_1 n_2$, $H = S_{n_1} \times S_{n_2}$ carries an exact copy of the product of the systems at n_1 and n_2.

A recursive projection of the symmetric reservoir

Fix a prime $p \mid n$, put $d = n/p$ and $g = s^{n/p}$. As in Proposition 3.3, g is a product of d disjoint p-cycles—its orbits are the residue classes $B_r = \{r, r+d, \dots, r+(p-1)d\}$, $0 \le r < d$—and $C_{S_n}(g) \cong \mathbb{Z}/p \wr S_d$. Every $q \in F_p$ commutes with g and so permutes the blocks; let $\pi(q) \in S_d$ be the induced block permutation, $\pi(q)(r) = q(r) \bmod d$.

Proposition 4.1 (Recursive projection)**.** *The map $\pi\colon F_p \to S_d$ takes values in $C(d)$, is onto, and has every fibre of size $(p-1)p^{d-1}$. Moreover $\pi(s) = s_d$ (the standard d-cycle), and*

$$\pi \circ D = D_d \circ \pi, \qquad \pi \circ \sigma = \sigma_d \circ \pi,$$

where D_d, σ_d are the derivation and the cyclic symmetry on $C(d)$. Thus π is a semiconjugacy *(a factor map of dynamical systems), mapping the functional graph of D on F_p onto that of D_d on $C(d)$, equivariantly for $\langle\sigma\rangle \twoheadrightarrow \langle\sigma_d\rangle$ (with $\sigma^d \mapsto \mathrm{id}$).*

Proof. Since $g \in \langle q\rangle$, q commutes with g and hence permutes its orbits; from $q(r+jd) = q(g^j r) = g^j q(r) = q(r) + jd$ the value $q(r) \bmod d$ is independent of the representative, so $\pi(q)$ is the genuine block permutation and π is the restriction of the quotient homomorphism $C_{S_n}(g) = \mathbb{Z}/p \wr S_d \twoheadrightarrow S_d$. Writing $q = (\vec{a}, \tau)$ with $\tau = \pi(q)$, the computation in the proof of Proposition 3.3 shows q is a single n-cycle iff τ is a d-cycle and $\sum_j a_j \not\equiv 0 \pmod p$, which is also the condition $g \in \langle q\rangle$; hence $\pi(F_p) \subseteq C(d)$, and over each d-cycle the fibre $\{\vec{a} : \sum a_j \not\equiv 0\}$ has $p^d - p^{d-1} = (p-1)p^{d-1}$ elements, so π is onto and uniformly $(p-1)p^{d-1}$-to-one. (This recovers $|F_p| = (d-1)!\,(p-1)p^{d-1}$, Corollary 3.4.) Being a homomorphism restricted to elements of $C_{S_n}(g)$, π satisfies $\pi(s) = s_d$ (as s sends $r \mapsto r+1$ on blocks), $\pi(Dq) = \pi(q)\pi(s)\pi(q)^{-1} = D_d(\pi q)$ and likewise $\pi(\sigma q) = \sigma_d(\pi q)$. □

In the terms of Section 2, $F_p = C(n) \cap C_{S_n}(g)$ and π is Proposition 2.8(b) for the quotient map $C_{S_n}(g) \to S_d$.

Corollary 4.2 (Symmetric attractors are lifts)**.** *If a periodic orbit O of D has $O \subseteq F_p$, then $\bar{O} = \pi(O)$ is a periodic orbit of D_d, and $|O| = k\,|\bar{O}|$ where k is the number of points of O in a single π-fibre; $D^{|\bar{O}|}$ cycles those k points. In particular every $\sigma^{n/p}$-symmetric period at level n is an integer multiple of a period at level n/p.*

Proof. π is D-equivariant, so $\bar{O} = \pi(O)$ is D_d-invariant; as $\pi|_O$ semiconjugates the $|O|$-cycle $D|_O$ onto the cyclic action $D_d|_{\bar{O}}$, the image is a single D_d-orbit, $|\bar{O}|$ divides $|O|$, and the fibres of $\pi|_O$ all have size $k = |O|/|\bar{O}|$, permuted in one k-cycle by $D^{|\bar{O}|}$. □

Conversely the projection reaches *every* lower orbit.

Corollary 4.3 (Surjectivity on periodic orbits)**.** *π is surjective on periodic orbits: each periodic orbit $\bar{O}$ of D_d on $C(d)$ is $\pi(O)$ for some periodic orbit O of D lying in F_p.*

Proof. Pick $\bar{q} \in \bar{O}$; by Proposition 4.1, $\bar{q} = \pi(q)$ for some $q \in F_p$. The forward orbit $(D^k q)_{k\geq 0}$ stays in F_p, which is forward D-invariant (Theorem 3.6), and is eventually periodic, reaching a periodic orbit $O \subseteq F_p$. By equivariance $\pi(D^k q) = D_d^k(\bar{q})$ runs through all of $\bar{O}$; hence $\pi(O)$, a single D_d-orbit meeting $\bar{O}$, equals $\bar{O}$. □

The number of periodic orbits of D in F_p above a given $\bar{O}$ is, however, not constant—it is already 1 or 2 at $n = 8$—so Corollary 4.3 does not by itself count the basins of $C(n)$.

For instance the symmetric attractor $(P, |B|) = (4, 16)$ at $n = 8$, $p = 2$ lifts the period-4 attractor of D_4 on $C(4)$ with $k = 1$; the basins $(3, 6)$ at $n = 6$, $p = 2$ and $(2, 10)$ at $n = 6$, $p = 3$ lift the *fixed point* s_d of D_d with $k = 3$ and $k = 2$. Because $|F_p| = (d-1)!\,(p-1)p^{d-1}$ is far smaller than $(n-1)!$, the projection lets one enumerate every symmetric attractor—and its lift—well past the range of a full graph; this is how the next remark was found.

Remark 4.4 (The residual law of Proposition 3.13 is false)**.** For a $\sigma^{n/p}$-symmetric attractor ($O \subseteq F_p$) the conclusion $p \mid P \Leftrightarrow p \mid T$ can fail. At $n = 14$, $p = 2$ the basin $(P, |B|) = (35, 119)$, tail $T = 84$, has $2 \mid T$ but $2 \nmid P$; at $n = 12$, $p = 3$ the basin $(2, 20)$, tail $T = 18$, has $3 \mid T$ but $3 \nmid P$. Both basins are $\sigma^{n/p}$-invariant (their attractors are pointwise $\sigma^{n/p}$-fixed), and both sizes were confirmed by a backward breadth-first search in the full $C(n)$. Corollary 4.2 explains them: the $n = 14$ basin is the $k = 1$ lift of the basin $(35, 119)$ of $C(7)$, whose tail $84 = 2^2 \cdot 3 \cdot 7$ already carries the new prime $p = 2$ while its period $35 = 5 \cdot 7$ does not, and the lift copies both verbatim. Thus a symmetric attractor inherits the period and tail of a smaller-n basin, on which the freshly introduced prime $p \mid n$ need not divide the period even when it divides the tail. The matching divisibility of Proposition 3.13 is special to the non-symmetric locus $O \not\subseteq F_p$.

The companion projection $\mathrm{Fix}(\sigma^t) \to C(t)$ recasts the residual hypothesis of Proposition 3.9 the same way; whether it too admits symmetric counterexamples, and a closed recursion for the periods in n, we leave open.

Coprime factors

Let $n = n_1 n_2$ with $\gcd(n_1, n_2) = 1$. The isomorphism $\mathbb{Z}/n \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2$ carries s to $s_{n_1} \times s_{n_2}$; we identify the two and call a permutation a *product* $q_1 \times q_2$ if it acts coordinatewise. The *rows* are the sets $\{x_1\} \times \mathbb{Z}/n_2$, the *columns* the sets $\mathbb{Z}/n_1 \times \{x_2\}$. A product $q_1 \times q_2$ is an n-cycle iff each q_i is an n_i-cycle (its orbits have length lcm of the lengths of the coordinate orbits), and $D(q_1 \times q_2) = D(q_1) \times D(q_2)$, as products compose coordinatewise.

Lemma 4.5 (Backward closure)**.** *If $q \in S_n$ and $D(q)$ is a product, then q is a product.*

Proof. Write $D(q) = t_1 \times t_2$, with $t_i \in C(n_i)$. Since n_1 is invertible modulo n_2, the orbits of $s^{n_1} = \mathrm{id} \times s_{n_2}^{n_1}$ are the rows, and so are those of $D(q)^{n_1} = \mathrm{id} \times t_2^{n_1}$. As $D(q)^{n_1} = q\, s^{n_1} q^{-1}$, q maps rows onto rows; symmetrically, columns onto columns. Hence the first coordinate of $q(x)$ depends only on x_1 and the second only on x_2. □

Theorem 4.6 (Coprime factorisation)**.** *Let $\Pi \subseteq C(n)$ be the set of product n-cycles. Then Π is a union of basins of D, and $q_1 \times q_2 \mapsto (q_1, q_2)$ is an isomorphism from (Π, D) onto $\big(C(n_1) \times C(n_2),\, D_{n_1} \times D_{n_2}\big)$. Consequently, if B_1, B_2 are basins of D_{n_1}, D_{n_2} with periods P_1, P_2, then $B_1 \times B_2$ is the union of $\gcd(P_1, P_2)$ basins of D, each of period $\mathrm{lcm}(P_1, P_2)$, of total size $|B_1|\,|B_2|$; the distance of $q_1 \times q_2$ to its periodic orbit is the larger of the distances of q_1 and q_2. In particular*

$$\#\{\textit{basins at } n\} \;\geq \sum_{B_1, B_2} \gcd(P_1, P_2), \qquad \#\{\textit{periodic points at } n\} \;\geq\; \#\{\textit{at } n_1\} \cdot \#\{\textit{at } n_2\},$$

and the in-tree of s is the product of the in-trees of s_{n_1} and s_{n_2}.

Proof. Π is forward invariant, and backward closed in $C(n)$ by Lemma 4.5; a set of vertices of a functional graph with both properties is a union of components. The isomorphism is the identity $D(q_1 \times q_2) = D(q_1) \times D(q_2)$. In the product system the periodic points of $B_1 \times B_2$ form $O_1 \times O_2$, on which $D_{n_1} \times D_{n_2}$ is the product of a P_1-cycle and a P_2-cycle, i.e. $\gcd(P_1, P_2)$ cycles of length $\operatorname{lcm}(P_1, P_2)$; every vertex of $B_1 \times B_2$ reaches $O_1 \times O_2$, at the time when both coordinates have reached their periodic orbits. □

For instance the product basins are $(1, 2)$ at $n = 6$ (the basin of s), $(1, 4)$ and $(5, 20)$ at $n = 10$, and $(1, 4)$ and $(4, 8)$ at $n = 12$ (Table 2 and the ancillary signatures): two of 29, resp. 157, basins—the product locus is small, but it is an exact copy of the lower levels. It also transports arithmetic phenomena upwards: the period-3 and period-9 basins at $n = 11$ (Remark 3.10) reappear at $n = 22$, with periods still coprime to n. The coprime factorisation complements the recursive projection above, attached to a prime p dividing n: there π is a factor map defined on a reservoir, here the product locus is a union of whole basins.

5 The in-tree of s

The depth of the in-tree of s—the most D-steps any n-cycle needs to reach s—is the analogue, for D, of the stack-sorting *sorting time* (the least t with $s^t = \mathrm{id}$, at most $n - 1$ for West's map [21]); here it is governed by the arithmetic of n rather than by pattern avoidance. We describe the first two layers, then the deepest chains, and finally state the complete description proved in the companion paper [3].

The first two layers

Each generator satisfies $D(s^a) = s^a s s^{-a} = s$, so the $\varphi(n)$ rotations are the immediate predecessors of s (Corollary 3.2). Whether the basin of s consists of exactly these, or is strictly larger, is a number-theoretic threshold.

Proposition 5.1. *$|\mathrm{basin}(s)| = \varphi(n)$ if and only if no affine map $x \mapsto ax + b$ on $\mathbb{Z}/n$ with $a \not\equiv 1$ is a single n-cycle. By the Hull–Dobell theorem [14], such a full-cycle affine non-translation exists if and only if $8 \mid n$ or $p^2 \mid n$ for some odd prime p. In that case the rotations acquire n-cycle preimages and the basin is strictly larger.*

Proof. The D-preimages of a rotation s^a inside $C(n)$ are the n-cycles among the conjugators of s to s^a, which are precisely the affine maps $x \mapsto ax + b$. For $a = 1$ these are translations, full cycles iff $\gcd(b, n) = 1$—the rotations themselves. For $a \not\equiv 1$, Hull–Dobell states that $x \mapsto ax + b$ is a full n-cycle iff $\gcd(b, n) = 1$, $a \equiv 1 \pmod p$ for every prime $p \mid n$, and $a \equiv 1 \pmod 4$ when $4 \mid n$. A unit $a \not\equiv 1$ meeting these conditions exists iff $p^2 \mid n$ for an odd prime, or $8 \mid n$. Absent such a the rotations $s^a \neq s$ are sources, each mapping in one step to the fixed point s (which therefore has in-degree $\varphi(n)$ and is itself no source), and the basin is just the $\varphi(n)$ rotations; otherwise the in-tree deepens. □

Proposition 5.1 counts the preimages of a rotation; the forward map on affine cycles is equally explicit and pins down where they sit in the tree.

Lemma 5.2 (Affine maps and the multiplier)**.** *If $p\colon x \mapsto ax+b$ is an affine map on $\mathbb{Z}/n$ that is a single n-cycle, then*

$$D(p) = s^a.$$

Thus D collapses the multiplier to 1: an affine n-cycle reaches s in at most two steps, $p \to s^a \to s$, so the affine n-cycles occupy only the top two layers of the in-tree of s. By Hull–Dobell the admissible multipliers are the units $a \equiv 1 \pmod q$ for every prime $q \mid n$ (and $a \equiv 1 \pmod 4$ when $4 \mid n$). For $n = p^e$ with p odd they form the p-Sylow subgroup of $(\mathbb{Z}/n)^\times$, cyclic of order p^{e-1}. For $n = 2^e$ ($e \geq 2$) they form $\{a \equiv 1 \pmod 4\} = \langle 5\rangle$, cyclic of order 2^{e-2}; for $e \geq 3$ this is a proper index-2 subgroup of the non-cyclic 2-group $(\mathbb{Z}/2^e)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{e-2}$, not its 2-Sylow (which is the whole unit group, of order 2^{e-1}).

Proof. From $p^{-1}(x) = a^{-1}(x-b)$ we get $D(p)(x) = p\,s\,p^{-1}(x) = a\big(a^{-1}(x-b)+1\big)+b = x+a$, that is $D(p) = s^a$. Applying this to the rotation s^a (the affine map with multiplier 1) gives $D(s^a) = s$. The admissibility condition on a is exactly the Hull–Dobell criterion of Proposition 5.1; for an odd prime power it cuts out the p-Sylow of the unit group, while for $n = 2^e$ it cuts out the cyclic index-2 subgroup $\langle 5\rangle$ of units $\equiv 1 \pmod 4$. □

The same full-cycle criterion underlies full-period linear congruential generators [17] and single-cycle T-functions [15]. Numerically, $|\mathrm{basin}(s)| = \varphi(n)$ for $n \leq 7$ and $n = 10, \ldots, 15$, whereas $|\mathrm{basin}(s)| = 16, 36, 2048, 36, 32, 10000, 472392$ for $n = 8, 9, 16, 18, 24, 25, 27$—exactly the n divisible by 8 or by an odd square; all these values are given by the closed formula of Theorem 5.6. The invariant $\deg^-_{C(n)}(s) = \varphi(n)$ holds for all n.

The root fibre

Fix a prime $p \mid n$, put $d = n/p$, and consider the fibre $R = \pi^{-1}(s_d) \subseteq F_p$ of the projection of Proposition 4.1 over the root s_d: it consists of the n-cycles q with $q(x) \equiv x+1 \pmod d$. Writing $q(x) = x + 1 + d\,a_{x \bmod d}$ defines a *carry coordinate* $a = a(q) \in (\mathbb{Z}/p)^d$, with $a(s) = 0$.

Lemma 5.3. *R is forward D-invariant, and in the carry coordinate D acts* linearly*:*

$$a(Dq) = (I - S)\,a(q), \qquad (Sa)_r = a_{r-1 \bmod d}.$$

Moreover q is a single n-cycle iff $\sum_r a_r \not\equiv -1 \pmod p$.

Proof. For $b \in (\mathbb{Z}/p)^d$ let $\tau_b(x) = x + d\,b_{x \bmod d}$. These maps form the abelian kernel $A \cong (\mathbb{Z}/p)^d$ of the quotient map $C_{S_n}(s^d) \to S_d$, and $q = s\,\tau_{a(q)}$ for $q \in R$. Since $(x-1) + d\,b_{(x-1) \bmod d} + 1 = x + d\,(Sb)_{x \bmod d}$, we have $s\tau_b s^{-1} = \tau_{Sb}$, hence $[\tau_b, s] = \tau_b\,\tau_{-Sb} = \tau_{(I-S)b}$: on the abelian layer A, commutation with s is the difference operator $I - S$. Now $\delta(q) = s\tau_a s^{-1} = \tau_{Sa}$, so Lemma 2.1 gives $\delta(Dq) = \tau_{(I-S)Sa} = s\,\tau_{(I-S)a}\,s^{-1} = \delta\big(s\,\tau_{(I-S)a}\big)$, i.e. $Dq = s\,\tau_{(I-S)a}$: thus $D(R) \subseteq R$ and $a(Dq) = (I-S)a(q)$. For the cycle criterion, iterating from 0 gives $q^d(0) = d\,(1 + \sum a)$, so q^d permutes the block $\{0, d, \ldots, (p-1)d\}$ as the translation $m \mapsto m + 1 + \sum a$ of $\mathbb{Z}/p$; this is a single p-cycle—equivalently q is a single n-cycle—iff $1 + \sum a \not\equiv 0$. □

Proposition 5.4. *For $n = p^e$ in the Hull–Dobell regime the in-tree of s has depth at least*

$$p^{\,e-1}\ (p \text{ odd}), \qquad 2^{\,e-1} - 1\ (p = 2),$$

and this number is exactly the depth of the in-tree restricted to R.

Proof. By Lemma 5.3 the distance from $q \in R$ to s is the nilpotency height of $a(q)$ under $I - S$. As $d = p^{e-1}$ is a power of p, $X^d - 1 = (X-1)^d$ over $\mathbb{F}_p$, so $I - S$ is nilpotent of index exactly d; and $(I-S)^{d-1} = I + S + \cdots + S^{d-1}$ maps a to the constant vector $\left(\sum_r a_r\right)\mathbf{1}$, so the height equals d iff $\sum a \neq 0$. By Lemma 5.3 the admissible carries are those with $\sum a \not\equiv -1$. For p odd one may take $\sum a = 1$, giving height $d = p^{e-1}$; for $p = 2$ the criterion forces $\sum a = 0$, so the height is at most $d - 1 = 2^{e-1} - 1$, attained (e.g. at $a = (1, 1, 0, \ldots, 0)$). Since $R \subseteq \mathrm{basin}(s)$ (every carry is killed by a power of $I - S$), this bounds the depth of the full in-tree from below. □

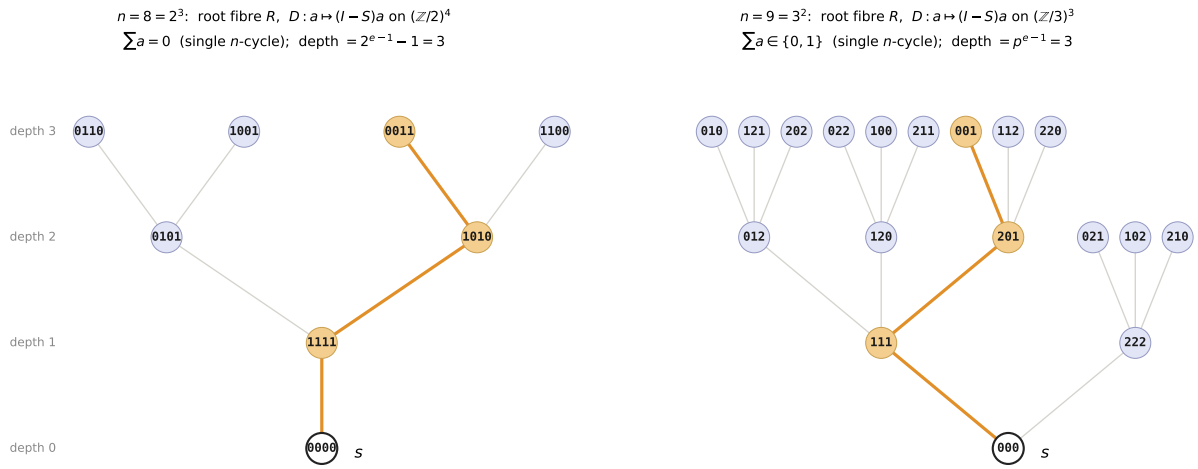


Figure 5: The root fibre $R \subseteq \mathrm{basin}(s)$ of the in-tree of s—the forward D-invariant part that carries its deepest chain to s—in the Hull–Dobell regime, $n = 8 = 2^3$ and $n = 9 = 3^2$, drawn in its carry coordinate (Lemma 5.3). Each vertex is its carry vector $a \in (\mathbb{Z}/p)^d$ ($d = p^{e-1}$, with $s = \mathbf{0}$ at the bottom); each edge is one step of D, which on R acts as the linear map $a \mapsto (I - S)a$ (carry minus its cyclic shift). The figure is therefore the nilpotency tower of $I - S$ over $\mathbb{F}_p$: the admissible carries are those with $\sum a \not\equiv -1$ (the single-n-cycle condition—$\sum a = 0$ for $p = 2$, $\sum a \in \{0, 1\}$ for $p = 3$), and the longest chain to $\mathbf{0}$ (highlighted) realises the depth of Proposition 5.4: $2^{e-1} - 1 = 3$ for $n = 8$ and $p^{e-1} = 3$ for $n = 9$. Both prime powers happen to give depth 3; the two branches of the formula separate only for larger e (depth 7 at $n = 16$, 9 at $n = 27$, whose basins—of 2048 and 472392 nodes—are too large to draw). Produced by `code/gen_fig_stree.py`.

The complete description

The basin cannot leave F_p:

Lemma 5.5. *For $n = p^e$ the entire basin of s lies in F_p.*

Proof. Write $g = s^{n/p}$, of order p. For an n-cycle q the centraliser is $\langle q \rangle$, so $q \in F_p$ iff $g \in \langle q \rangle$. Since $\langle D(q) \rangle = q\langle s \rangle q^{-1}$, we have $D(q) \in F_p$ iff $q^{-1}gq \in \langle s \rangle$; as $q^{-1}gq$ has order p and the cyclic group $\langle s \rangle$ has a unique subgroup of order p—namely $\langle g \rangle$—this says exactly that q normalises $\langle g \rangle$. But an n-cycle normalising $\langle g \rangle$ acts on $\langle g \rangle \cong \mathbb{Z}/p$ by an automorphism, and the resulting homomorphism $\langle q \rangle \to \mathrm{Aut}(\mathbb{Z}/p)$ has image of order dividing both $\mathrm{ord}(q) = p^e$ and $|\mathrm{Aut}(\mathbb{Z}/p)| = p - 1$; as $\gcd(p^e, p - 1) = 1$ the image is trivial, i.e. q centralises g and $q \in F_p$. Hence $D(q) \in F_p \Rightarrow q \in F_p$: F_p is closed under D-preimages, and since $s \in F_p$ the whole basin lies in F_p. □

Iterating Lemma 5.5 down the tower $p^e \to p^{e-1} \to \cdots \to p$ (through the projection π, which maps the in-tree of s into that of s_d) confines the in-tree to a single nilpotent group. Write the elements of $\mathbb{Z}/p^e$ in base p, and call a permutation *triangular* if it changes each digit by an amount that depends only on the lower digits; the map $x \mapsto x+1$ is triangular, the amounts being the carries. The triangular permutations form a Sylow p-subgroup P_e of S_{p^e}—Kaloujnine's iterated wreath product $\mathbb{Z}/p \wr \cdots \wr \mathbb{Z}/p$—which is nilpotent of class p^{e-1} [4].

Theorem 5.6 (The in-tree of s [3])**.** *Let P_e be the triangular group just described.*

(a) For $n = p^e$, $\operatorname{basin}(s) = C(n) \cap P_e$, of size $(p-1)^e\, p^{(p^e-1)/(p-1)-e}$; for $p = 2$ it is the coset $s\,[P_e, P_e]$ of the derived subgroup.

(b) $\operatorname{depth}(p^e) = p^{e-1}$ for p odd and $2^{e-1}-1$ for $p = 2$: the root-fibre bound of Proposition 5.4 is exact, and the deepest chains are the root-fibre ones.

(c) For $n = \prod_p p^{e_p}$, $\operatorname{basin}(s)$ is the product of the in-trees at the prime powers (Theorem 4.6), with dist *the maximum of the distances of the factors. Hence*

$$|\operatorname{basin}(s)| = \prod_p (p-1)^{e_p}\, p^{(p^{e_p}-1)/(p-1)-e_p}, \qquad \operatorname{depth}(n) = \max_p \operatorname{depth}(p^{e_p}).$$

Idea of the proof. By Lemma 2.1, $\operatorname{dist}(q)$ is the number of commutators with s needed to kill $\delta(q) = qs^{-1}$. The in-tree lies in P_e, as just explained, and conversely every element of P_e reaches s within p^{e-1} steps (Proposition 2.8(c)): this is the upper bound for odd p. An element of P_e is an n-cycle iff its image in the abelianisation $P_e/[P_e, P_e] \cong \mathbb{F}_p^e$ has no zero coordinate. For $p = 2$ this forces $q \equiv s$ modulo $[P_e, P_e]$, so $\delta(q)$ starts one step down the lower central series and one commutator is saved: $2^{e-1}-1$. The lower bounds are the root-fibre chains of Proposition 5.4, and general n follows from Theorem 4.6. The size formula reproduces the values $16, 36, 2048, 36, 32, 10000, 472392$ observed at $n = 8, 9, 16, 18, 24, 25, 27$, and gives $\varphi(n)$ outside the Hull–Dobell regime.

Remark 5.7 (The basin as single-cycle T-functions)**.** The affine n-cycles occupying the top two layers (Lemma 5.2) are exactly the full-period linear congruential generators of Hull–Dobell [14, 17]; and for $n = 2^e$ the entire basin coincides with the single-cycle *T-functions* of Klimov–Shamir [15] — the permutations of $\mathbb{Z}/2^e$ whose bit i depends only on bits $\le i$, i.e. the 2^e-cycles of the triangular group P_e, which form the single coset $s\,[P_e, P_e]$ (Theorem 5.6) — whose transitivity is the subject of Anashin's non-Archimedean ergodic theory [16]. The derivation thus unfolds inside the very arithmetic of full-period generators. Its depth, however, is *orthogonal* to cryptographic strength: single-cycleness saturates the standard measures uniformly across the basin. The cyclicity condition $\sum a \not\equiv 0$ is exactly "the carry has maximal algebraic degree", so every basin element attains the maximal degree; and the affine low-order bits force zero map-nonlinearity and worst-case differential uniformity throughout (verified exhaustively on $C(16)$ and by sampling on $C(32)$). No such metric varies with position in the tree; only the dichotomy $\operatorname{dist} \le 2 \Leftrightarrow$ affine is meaningful, so $\operatorname{dist} \ge 3$ certifies "genuinely non-affine (not a linear congruential generator in disguise)" and nothing finer. The very computability of dist in closed form (Theorem 5.6) — a virtue here — is, in any keyed conjugation-based setting, exactly what a length-based attack would descend.

6 The periodic part

Every basin contains exactly one periodic orbit, and the periodic points carry the global information about the graph—the number of basins and their periods. The commutator form identifies them with an object of group theory; we then compare their number with that of a random mapping.

Periodic points and Engel sinks

Following Khukhro and Shumyatsky [5, 6, 7], with the convention $[x, g] = x^{-1}g^{-1}xg$ standard in that literature, a subset $\mathcal{E} \subseteq G$ is a (left) *Engel sink* of $g \in G$ if for every $x \in G$ all sufficiently long commutators $[x, g, \ldots, g]$ lie in $\mathcal{E}$. In a finite group, g has a smallest Engel sink $\mathcal{E}(g)$: the set of periodic points of the map $x \mapsto [x, g]$. And $\mathcal{E}(g) = \{1\}$ means that g is a *left Engel element*.

Proposition 6.1 (Periodic points form an Engel sink)**.** *Let $f(x) = x^{-1}s^{-1}xs$ on S_n and $\Phi(q) = s\,q^{-1}$. Then $\Phi \circ D = \sigma \circ f \circ \Phi$. Consequently an n-cycle q is periodic for D iff $s\,q^{-1} \in \mathcal{E}(s)$, and the number of periodic points of D equals $|\mathcal{E}(s)|$.*

Proof. $\Phi(D(q)) = s\,qs^{-1}q^{-1}$, while $f(\Phi(q)) = (qs^{-1})s^{-1}(sq^{-1})s = qs^{-1}q^{-1}s$, whose conjugate by s is $sqs^{-1}q^{-1}$. Since σ is an automorphism fixing s, it commutes with f, and it has order n; so $(\sigma f)^{nm} = f^{nm}$, and a point is periodic for $\sigma \circ f$ iff it is periodic for f. As Φ is a bijection and D maps S_n into $C(n)$, the periodic points of D are the n-cycles q with $\Phi(q) \in \mathcal{E}(s)$. □

The dynamics differ only by the twist σ, which commutes with everything in sight: the periodic orbits of D are those of $\sigma \circ f$ on the sink. Two facts about Engel sinks now apply.

Corollary 6.2. *(a) D has a single basin iff $n \leq 3$.*
(b) The number of periodic points of D tends to infinity with n.

Proof. (a) A single basin means that every point reaches s, i.e. $\mathcal{E}(s) = \{1\}$: s is a left Engel element of S_n. By Baer's theorem [2] (see [9, 12.3.7]), the left Engel elements of a finite group form its Fitting subgroup. Now $F(S_3) = A_3 \ni s$, while $F(S_4)$ is the Klein four-group, which contains no 4-cycle, and $F(S_n) = 1$ for $n \geq 5$.

(b) Let $n \geq 5$, and let φ be the automorphism $x \mapsto s^{-1}xs$ of the simple group A_n (inner for n odd, outer for n even). With the convention $[x, \varphi] = x^{-1}x^{\varphi}$ of [7], $[x, \varphi] = f(x)$. Since f maps S_n into A_n, every periodic point of f lies in A_n, so $\mathcal{E}(s)$ is the smallest left Engel sink $\mathcal{L}(\varphi)$ of φ in A_n. As $\varphi \neq 1$ and A_n is simple, $[A_n, \varphi] = A_n$. By a theorem of Khukhro and Shumyatsky [7, Theorem 1.4], if φ is an automorphism of a finite group G with $G = [G, \varphi]$, then $|G|$ is bounded in terms of $|\mathcal{L}(\varphi)|$ (their proofs rely on the classification of finite simple groups). Hence $|\mathcal{E}(s)| \to \infty$. For this particular group an explicit, if weak, bound follows from one ingredient of their proof: by Guralnick and Tracey [8, Theorem 1.4], $A_n = \langle \mathcal{L}(\varphi) \rangle$; the centraliser $C_{A_n}(\varphi) = \langle s \rangle \cap A_n$, of order at least $n/2$, permutes $\mathcal{L}(\varphi)$ by conjugation, faithfully since the kernel centralises $\langle \mathcal{L}(\varphi) \rangle = A_n$, whose centre is trivial. Hence $|\mathcal{E}(s)|! \geq n/2$. □

Part (a) is of course visible in Table 2; the point is the mechanism. Periodic orbits other than $\{s\}$ exist because s lies outside the Fitting subgroup, i.e. because S_n is far from nilpotent. Inside a nilpotent subgroup containing s everything drains to s (Proposition 2.8(c)).

Comparison with a random mapping

To situate how structured D is, we compare it to a uniformly random endofunction on $N = (n-1)!$ nodes, whose expected number of components is $\sim \frac{1}{2}\ln N$ and of periodic points $\sim \sqrt{\pi N/2}$ [11, 12]. The deviation is large and its sign tracks the arithmetic of n (Table 3): arithmetically simple n have far more periodic points than random, while $8 \mid n$ or $p^2 \mid n$ give deep trees and far fewer (the Hull–Dobell regime of Proposition 5.1). This is a diagnostic, not a theorem. The column "#periodic" is also the size of the smallest Engel sink of s in S_n (Proposition 6.1).

Table 3: D against a uniformly random mapping on $N = (n-1)!$ nodes.

n	N	#basins	$\frac{1}{2}\ln N$	#periodic	$\sqrt{\pi N/2}$	% periodic
3	2	1	0.35	1	1.8	50.0
4	6	2	0.90	5	3.1	83.3
5	24	2	1.59	6	6.1	25.0
6	120	6	2.39	84	13.7	70.0
7	720	7	3.29	127	33.6	17.6
8	5040	18	4.26	89	89.0	1.8
9	40320	17	5.30	190	251.7	0.5
10	362880	29	6.40	1190	755.0	0.3
11	3628800	56	7.55	6898	2387.5	0.2
12	39916800	157	8.75	61212	7918.4	0.2

7 Open problems

Question 7.1. By Proposition 3.9 each non-fixed period ℓ carries a forced seed $d = \gcd(\ell, n) > 1$; the cofactor $m = \ell/d$ is the erratic part ($m = 11$ in $33 = 3 \cdot 11$ at $n = 6$, $m = 7$ in 49 at $n = 7$), realised geometrically as the attachment-necklace period (Observation 3.12), equivalently as the number of σ-orbits on the cycle. Is there a description of the multiset of cofactors across the basins of $C(n)$? The recursive projection (Corollary 4.3) organises these orbits—each is inherited along a lift—but its fibre is irregular (Section 4), and we have found no closed form.

Question 7.2. The numbers of basins $1, 2, 2, 6, 7, 18, 17, 29, 56, 157$ for $n = 3, \ldots, 12$ are absent from the OEIS [23] (unlike the orbit count c_0 = `A002619`), so the basin partition $P(n)$ is a genuinely new sequence. (Values for $n = 10, 11, 12$ were obtained by encoding each n-cycle as the Lehmer rank of its permutohedron word and computing the functional graph on integer arrays; the period multisets and the data of Remark 3.10 come from the same computation.) Is there a formula or generating function? Splitting the periodic orbits into those lying in some F_p (lifts, Corollary 4.3) and the rest reduces the count one level down, but the number of orbits above a given lower orbit is not constant—already 1 or 2 at $n = 8$—so no clean divisor recursion follows, and the sequence may be genuinely irregular. Theorem 4.6 gives a lower bound for coprime factorisations, $\sum_{B_1,B_2} \gcd(P_1, P_2)$.

Question 7.3. The number of periodic points, $1, 5, 6, 84, 127, 89, 190, 1190, 6898, 61212$ for $n = 3, \ldots, 12$, is the size of the smallest Engel sink of an n-cycle in S_n (Proposition 6.1). It tends to infinity with n (Corollary 6.2), but irregularly (it drops from 127 at $n = 7$ to 89 at $n = 8$), and far faster than the bound $|\mathcal{E}(s)|! \geq n/2$ given there. What is its growth? Can the sink, or its orbit structure under $\sigma \circ f$, be described group-theoretically—for instance through the nilpotent subgroups containing s, which meet it only in the identity (Proposition 2.8(c))?

Question 7.4. The cyclic sieving of Remark 3.5 holds for all n via σ-orbits, but only tautologically. Is there an *intrinsic* statistic $\mathrm{stat}\colon C(n) \to \mathbb{Z}/n$—defined from q directly, not from its σ-orbit, and ideally compatible with D—with $\sum_q t^{\mathrm{stat}(q)} = X(t)$? It must be σ-equivariant, $\mathrm{stat}(\sigma q) \equiv \mathrm{stat}(q) + n/|O_q| \pmod n$, which already rules out the standard permutation statistics.

Question 7.5. On which space do the $\mathbb{Z}/n$-symmetries become geometric? The permutohedron Π_{n-1} carries the vertices but not σ as an isometry; the cyclohedron of Bott–Taubes [1] carries the cyclic symmetry but its vertex set, of size $\binom{2d}{d}$, is not $C(n)$. Is there a polytope or cell complex carrying both?

Acknowledgements

The results were obtained by the AI model Claude Opus 4.8 (Anthropic) in dialogue with the author; the reorganisation around the commutator form, the functoriality principle, the coprime factorisation, the link with Engel sinks, and the revised account of the in-tree of s were added in a later session with Claude Opus 5.5 (Anthropic). The supporting computations are short and reproducible (the script `code/verify_derivation_v2.py` checks the statements new in this version). They remain to be studied and independently verified.

References

[1] R. Bott and C. Taubes, *On the self-linking of knots*, J. Math. Phys. **35** (1994), 5247–5287.

[2] R. Baer, *Engelsche Elemente Noetherscher Gruppen*, Math. Ann. **133** (1957), 256–270.

[3] F. Lefebvre-Naré, *The in-tree of an n-cycle under cyclic conjugation: depth p^{e-1} for odd p, and $2^{e-1}-1$ for $p=2$*, companion paper, second version (2026).

[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] E. I. Khukhro and P. Shumyatsky, *Almost Engel finite and profinite groups*, Internat. J. Algebra Comput. **26** (2016); arXiv:1512.06097.

[6] E. I. Khukhro and P. Shumyatsky, *Finite groups with Engel sinks of bounded rank*, Glasgow Math. J. **60** (2018), 695–701; arXiv:1707.04187.

[7] E. I. Khukhro and P. Shumyatsky, *On finite groups containing an element whose Engel sink is small*, arXiv:2605.08607v3 (2026).

[8] R. M. Guralnick and G. Tracey, *On the generalized Fitting height and insoluble length of finite groups*, Bull. London Math. Soc. **52** (2020), 924–931.

[9] D. J. S. Robinson, *A Course in the Theory of Groups*, 2nd ed., Graduate Texts in Math. **80**, Springer (1996).

[10] C. Defant, *Stack-sorting preimages of permutation classes*, Sém. Lothar. Combin. **82** (2020), Article B82b.

[11] P. Flajolet and A. M. Odlyzko, *Random mapping statistics*, in: Advances in Cryptology—EUROCRYPT '89, LNCS **434**, Springer (1990), 329–354.

[12] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge Univ. Press (2009).

[13] D. Foata and M.-P. Schützenberger, *Théorie géométrique des polynômes eulériens*, Lecture Notes in Math. **138**, Springer (1970).

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

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

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

[17] D. E. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 3rd ed., Addison-Wesley (1997).

[18] F. Mason and A. Borghesan, *Circuits of iterated Foata maps*, Working Paper 25/2014, Dept. of Management, Ca' Foscari University of Venice (2014); SSRN `id2534420`.

[19] V. Reiner, D. Stanton and D. White, *The cyclic sieving phenomenon*, J. Combin. Theory Ser. A **108** (2004), 17–50.

[20] R. P. Stanley, *Enumerative Combinatorics, Vol. 1*, 2nd ed., Cambridge Univ. Press (2012).

[21] J. West, *Permutations with forbidden subsequences and stack-sortable permutations*, Ph.D. thesis, Massachusetts Institute of Technology (1990).

[22] K. Yordzhev, *On the cardinality of a factor set in the symmetric group*, Asian-Eur. J. Math. **7** (2014), no. 2, 1450027.

[23] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, sequence `A002619`, https://oeis.org.