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

Frédéric Lefebvre-Naré*

July 9, 2026

Abstract

Fix an n-cycle s in the symmetric group S_n and consider $D(p) = p\,s\,p^{-1}$, the conjugate of s by p, acting on the set $C(n)$ of all n-cycles. Equivalently $D(p)$ is the n-cycle sending $p(i)$ to $p(i+1)$, so iterating D repeatedly reads the one-line word of images as a cycle—the conjugation variant of the fundamental transform. We study its functional graph: the periodic orbits and the partition $P(n)$ of $C(n)$ into basins. The system is independent of s up to relabelling; s is the unique fixed point; conjugation by s generates a $\mathbb{Z}/n$-action σ commuting with D; and $\deg^-(s) = \varphi(n)$. The basin of s has size $\varphi(n)$ unless $8 \mid n$ or $p^2 \mid n$ for an odd prime p, the Hull–Dobell threshold. In that regime the in-tree of s deepens, and a companion paper [2] shows its depth is exactly p^{e-1} (p odd), resp. $2^{e-1}-1$ ($p = 2$), for $n = p^e$, and $\max_p \operatorname{depth}(p^{e_p})$ in general. The symmetry forces congruences on basin sizes ($|B| \equiv |B \cap F_p| \pmod p$ for σ-invariant B, with $|F_p| = (p-1)(n/p-1)!\,p^{\,n/p-1}$ and Wilson's theorem as the prime case), and constrains periods and tails: every non-fixed period shares a prime factor with n whenever the setwise σ-stabiliser acts non-trivially on the orbit, and $p \mid P \Leftrightarrow p \mid T$ off a symmetric locus. Both constraints are *sharp*—we exhibit periods coprime to n at $n = 11$ and period/tail mismatches at $n = 12, 14$, the latter explained by a recursive projection $F_p \to C(n/p)$ realising the symmetric reservoir as a smaller copy of the system. The in-trees attach to each periodic cycle as a necklace carrying the σ-rotation; the fixed-point counts $\#\mathrm{Fix}(\sigma^k) = \varphi(m)(g-1)!\,m^{g-1}$ ($g = \gcd(k, n)$, $m = n/g$) yield a cyclic sieving polynomial refining `A002619`. The basin counts $1, 2, 2, 6, 7, 18, 17, 29, 56, 157$ ($n \le 12$) form a new sequence. We close by comparing D to a uniformly random mapping.

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

1 Introduction

Let S_n be the symmetric group on $\{1, \ldots, n\}$; we use the labels $\{0, \ldots, n-1\}$ with arithmetic modulo n when convenient. 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 $s_0 = (1\,2\,\cdots\,n)$, 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. $(1\,3\,5\,4\,2)$, or by its one-line word of images $(p(1), p(2), \ldots, p(n))$. The construction studied here turns the second presentation into the first.

---

* *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 depth result (§5) is proved in a self-contained companion paper [2]. 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.

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 $\big(p(1)\ p(2)\ \cdots\ p(n)\big)$; 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 $D(p) = p\,s\,p^{-1}$. $\square$

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 $\big(n\ p(n)\ p^2(n)\ \cdots\ p^{n-1}(n)\big)$ and deleting the initial n leaves the sequence $\big(p(n), p^2(n), \ldots, p^{n-1}(n)\big)$, 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 [6, 12]. 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 [6], but D is not that bijection. 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 [10], 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 3.2), 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 3.1), 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 [13, 3]—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, $n = 4$.

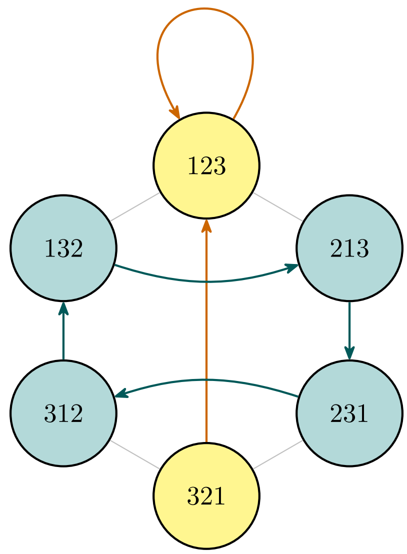

Figure 1: The permutohedron Π_3 (hexagon), $n = 4$. Vertices are the six 4-cycles in $C(4)$, labelled by their S_3 words in the coordinate of §1; arrows are D. The fixed point $s = 123$ (loop) and its single predecessor 321 form the gold basin of size 2; the other four vertices form a single 4-cycle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

Summary. Section 2 shows the system depends only on n, and Section 3 records the elementary structure (s the unique fixed point, D uniformly n-to-1 as $S_n \to C(n)$). Section 4 introduces the commuting $\mathbb{Z}/n$-symmetry σ, computes $\deg^-(s) = \varphi(n)$, and identifies the size of the basin of s with the Hull–Dobell full-period criterion for affine maps—the paper's main bridge to a classical theory. Section 5 develops the consequences: σ-congruences on basin sizes (with Wilson's theorem as the prime case), sharp constraints on periods and tails, a recursive projection $F_p \to C(n/p)$ realising the system as a smaller copy of itself, the attachment necklace of the in-trees, and—in the Hull–Dobell regime—the depth of the in-tree of s, which a carry coordinate linearises on a "root fibre" realising the deepest chains; the exact depth p^{e-1} (resp. $2^{e-1} - 1$) is proved in the companion [2]. Section 6 situates D against a random mapping; Section 7 gives the σ-fixed-point counts (generalising Wilson), which realise a cyclic sieving only tautologically, so the content is the count itself. Section 8 lists open problems.

2 Independence of the chosen cycle

Theorem 2.1. *Let s, s' be two n-cycles and write $s' = g\,s\,g^{-1}$ (possible as all n-cycles are conjugate). The relabelling $\Phi_g : C(n) \to C(n)$, $\Phi_g(p) = g\,p\,g^{-1}$, is a bijection with*

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

where $D_t(p) = p\,t\,p^{-1}$ and $\sigma_t(p) = t\,p\,t^{-1}$. 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. $D_{s'}(\Phi_g(p)) = (gpg^{-1})(gsg^{-1})(gp^{-1}g^{-1}) = g(psp^{-1})g^{-1} = \Phi_g(D_s(p))$, and $\Phi_g\sigma_s\Phi_g^{-1}(q) = g\,s\,(g^{-1}qg)\,s^{-1}g^{-1} = s'qs'^{-1} = \sigma_{s'}(q)$. The solutions of $s' = gsg^{-1}$ form the coset $g\,C_{S_n}(s) = g\langle s \rangle$. $\square$

Corollary 2.2. *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 1, and the unique fixed point is always s itself. Henceforth we fix $s = s_0$.

3 Elementary structure

Proposition 3.1. *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 3.2. *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. $D(p) = D(p')$ 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 3.3. *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 3.2. 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 3.4. 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.

4 The cyclic symmetry

Theorem 4.1. *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 4.2. *$\langle\sigma\rangle$ 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 4.1 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. □

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

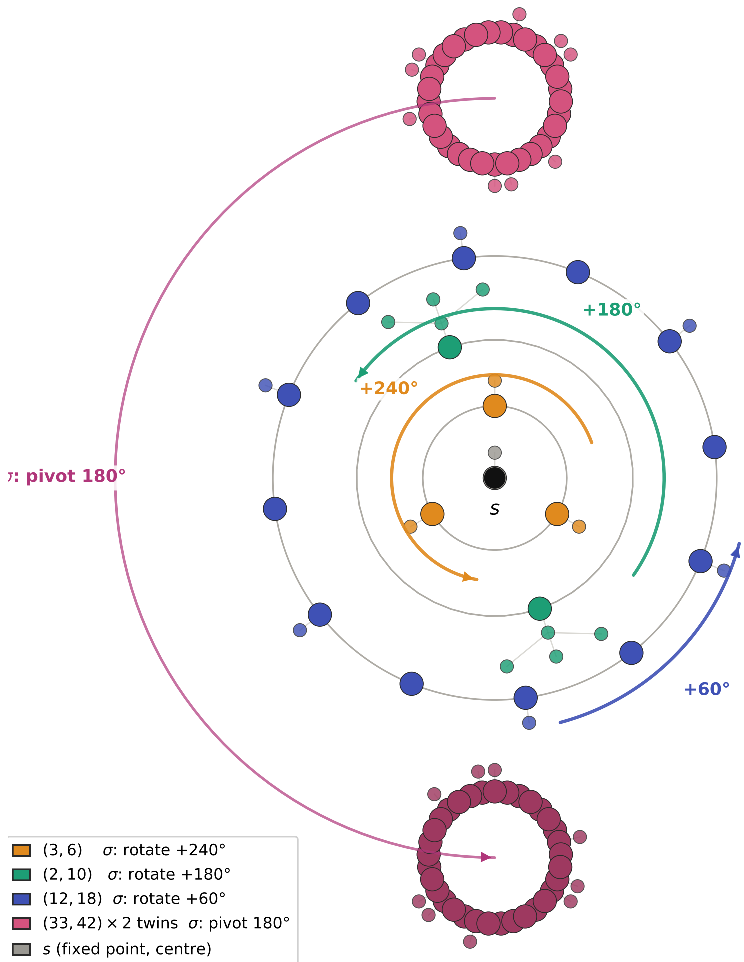

Figure 2: The basin system at $n = 6$ drawn as a polar diagram centred on s, chosen so that σ acts by rotation (Theorem 4.1, Corollary 4.2). The fixed point s sits at the centre; each σ-invariant basin is a concentric ring of its periodic n-cycles (joined by D, drawn counter-clockwise), with the attached 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`.

Proposition 4.3. $|\mathrm{basin}(s)| = \varphi(n)$ *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 [7], 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. $\square$

Proposition 4.3 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 4.4 (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 $\{a \equiv 1 \,(\mathrm{mod}\ 4)\} = \langle 5 \rangle$, 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 4.3; 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 $\equiv 1 \pmod 4$. $\square$

The same full-cycle criterion underlies full-period linear congruential generators [9] and single-cycle T-functions [8]. 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. The invariant $\deg^-_{C(n)}(s) = \varphi(n)$ holds for all n.

Figure 3 displays the basins on Π_4 and Π_5.

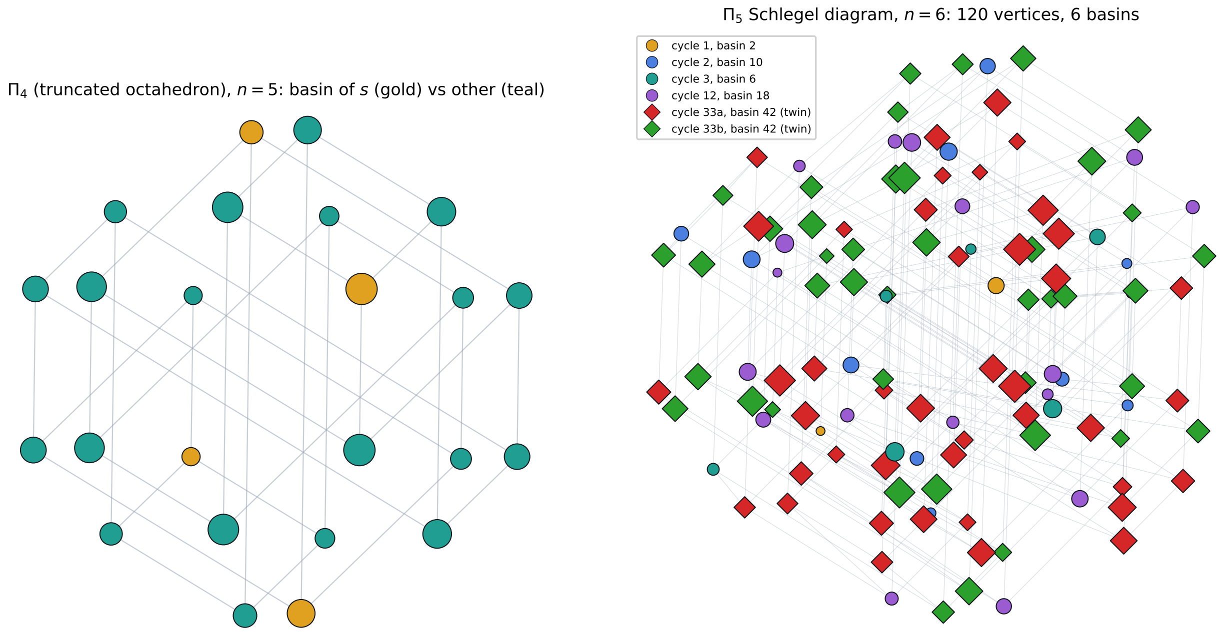

Figure 3: Left: the permutohedron Π_4 (truncated octahedron), $n = 5$, coloured by basin (gold: the basin of s, size 4; teal: the other basin, size 20). Right: a Schlegel diagram of the 4-dimensional permutohedron Π_5, $n = 6$, with 120 vertices coloured by the six basins; the two basins of size 42 (the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

5 Periods, tails, and the shape of basins

By Corollary 4.2, 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 1) form a σ-orbit of size 2. We now show σ also constrains the basin sizes themselves.

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

$$F_p = \mathrm{Fix}(\sigma^{n/p}) = \{q \in C(n) : \ s^{n/p} \in \langle q \rangle\}.$$

Theorem 5.1. *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 4.1, 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. $\square$

Theorem 5.2. *For each prime $p \mid n$,*

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

Proof. As $\langle q \rangle$ is cyclic of order n it has a unique subgroup of order p, namely $\langle q^{n/p} \rangle$; thus $g \in \langle q \rangle$ iff $q^{n/p} \in \{g, g^2, \ldots, g^{p-1}\}$, so $|F_p| = \sum_{m=1}^{p-1} \#\{q \in C(n) : q^{n/p} = g^m\}$. The targets g^m share a cycle type, so the summands are equal; write A for the common value, giving $|F_p| = (p-1)A$.

Put $d = n/p$. Any q with $q^d = g$ commutes with g, hence lies in $C_{S_n}(g) \cong \mathbb{Z}/p \wr S_d = (\mathbb{Z}/p)^d \rtimes S_d$. Identify each block (a p-cycle of g) with $\mathbb{Z}/p$ so that g 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 d-cycle then $(\vec{a}, \tau)^d$ fixes every block and acts there by $+T$ with $T = \sum_j a_j$; so $(\vec{a}, \tau)^d = g^T$, and $(\vec{a}, \tau)$ is a single n-cycle iff $T \not\equiv 0 \pmod p$. Hence $q^d = g$ iff τ is a d-cycle and $T \equiv 1 \pmod p$ (which also forces the single-cycle condition). There are $(d-1)!$ such τ and p^{d-1} vectors $\vec{a}$ with $\sum a_j \equiv 1$, so $A = (d-1)!\, p^{d-1}$. □

Corollary 5.3 (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 2) 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.

Proposition 5.4 (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 4.2). 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 5.4 extends to composite n and dispenses with the "shared length" caveat once it is run on the setwise stabiliser of a single orbit.

Proposition 5.5 (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 5.4: 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 5.6). 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 5.6 ($\gcd(\ell, n) > 1$ 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 5.4. Thus the unconditional reading "every non-fixed period shares a prime with n" is false; the hypothesis of Proposition 5.5 is essential. Composite $n = 10, 12$ exhibit no coprime period, so the phenomenon is not merely a matter of size.

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

Proposition 5.7 (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 $n \leq 9$ (8 are even more symmetric, with constant in-degree). The basin of s is the degenerate case $P = 1$, $\deg^-(s) = \varphi(n)$ (Corollary 4.2).

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

Observation 5.8 (The cofactor is the necklace period)**.** For every σ-invariant basin at $n \leq 9$, $\sigma|_O$ 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 5.5) 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.

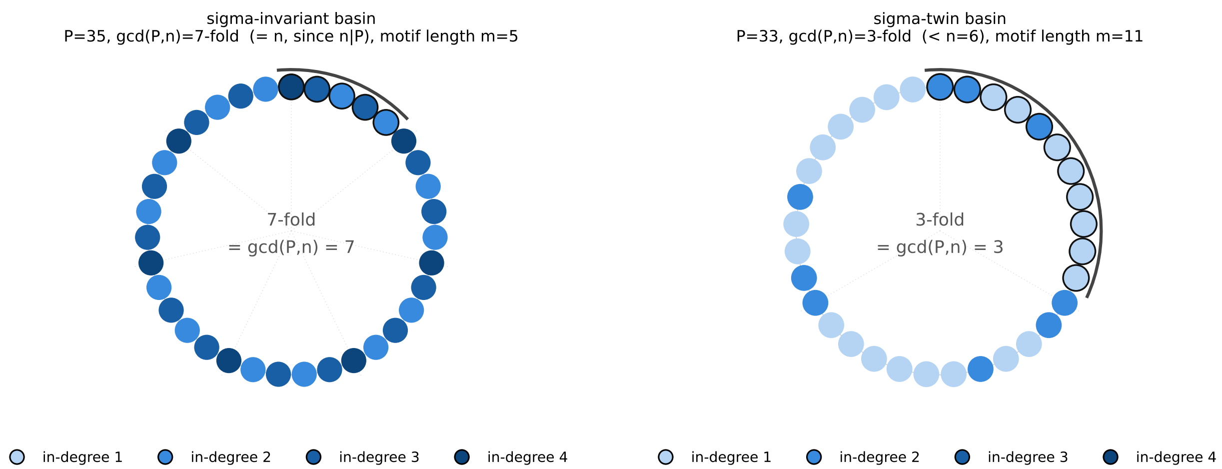

Figure 4: Attachment necklaces (Observation 5.8). Each dot is a periodic n-cycle on a basin's attractor, placed in D-order around the ring and coloured by in-degree (the number of attaching trees is $\deg^-_{C(n)} - 1$); one motif is outlined and the repeats are separated by spokes. Left: the σ-invariant 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.

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 5.1 constrain P and T *jointly*.

Proposition 5.9 (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 5.1 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 $p \mid P$, $p \mid T$. $\square$

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 $n \le 9$ 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 5.1 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 $n \le 9$, but—in contrast to the proposition—it is *not* a theorem: it fails from $n = 12$ on (Remark 5.13 below). The hypothesis $O \nsubseteq F_p$ is therefore essential, and a projection of F_p onto a smaller copy of the same system, which we now make precise, both reaches those larger n cheaply and explains the failure.

A recursive projection of the symmetric reservoir

Fix a prime $p \mid n$, put $d = n/p$ and $g = s^{n/p}$. As in Theorem 5.2, 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 5.10 (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 maps 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 Theorem 5.2 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 $|F_p| = (d-1)!\,(p-1)p^{d-1}$.) 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 $\pi(\sigma q) = \sigma_d(\pi q)$. ☐

Corollary 5.11 (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 5.12 (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 5.10, $\bar{q} = \pi(q)$ for some $q \in F_p$. The forward orbit $(D^k q)_{k \ge 0}$ stays in F_p, which is forward D-invariant (Theorem 5.1), 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 5.12 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 5.13 (The residual law of Proposition 5.9 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 5.11 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 5.9 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 5.5 the same way; whether it too admits symmetric counterexamples, and a closed recursion for the periods in n, we leave open.

Table 1: 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. 4.2) *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 8), 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	$(1, 36)$, $(3, 195)^3$, $(9, 36)$, $(9, 102)^3$, $(9, 378)$, $(9, 1332)$, $(9, 3384)$, $(9, 4422)^3$, $(18, 72)$, $(18, 12177)$, $(54, 8748)$

The in-tree of s: a linear coordinate on the root fibre

The depth of this in-tree—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 [13]); here it is governed by the arithmetic of n rather than by pattern avoidance.

Table 2: 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

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 5.10 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 5.14. *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. Put $\alpha(x) = a_{x \bmod d}$ and $u = q^{-1}(x)$. Then $D(q)(x) = q(u+1) = (u+1) + 1 + d\,\alpha(u+1)$, while $x = u + 1 + d\,\alpha(u)$, so $D(q)(x) = x + 1 + d\big(\alpha(u+1) - \alpha(u)\big)$; as $x \equiv u + 1 \pmod d$ the carry of Dq at x is $a_{x \bmod d} - a_{(x-1) \bmod d}$, i.e. $(I - S)a$. Since S preserves $\sum_r a_r$, the image has zero sum, so $D(R) \subseteq R$. For the cycle criterion, iterating from 0 gives $q^d(0) = d\,(1 + \sum a)$, so q^d permutes the block $\{0, d, \dots, (p-1)d\}$ 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 $1 + \sum a \not\equiv 0$. $\square$

Proposition 5.15. *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 5.14 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 $(I-S)^{d-1}a = \big(\sum_r a_r\big)v$ for a fixed nonzero v, so the height equals d iff $\sum a \neq 0$. By Lemma 5.14 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 $a = (1, 1, 0, \dots, 0)$). 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. $\square$

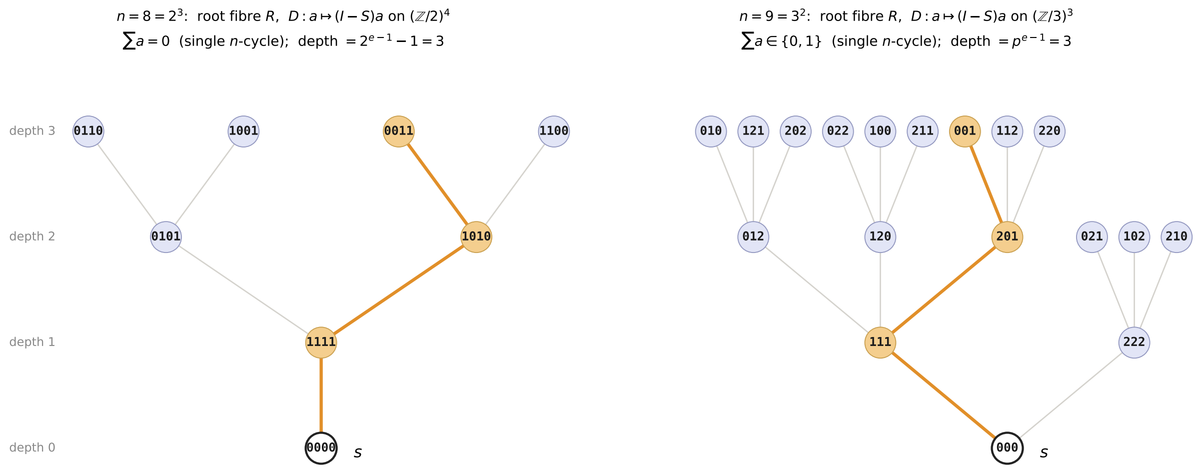

Figure 5: The root fibre $R \subseteq \mathrm{basin}(s)$ of the in-tree of s—the forward D-invariant part that carries its deepest chain to s—in the Hull–Dobell regime, $n = 8 = 2^3$ and $n = 9 = 3^2$, drawn in its carry coordinate (Lemma 5.14). Each vertex is its carry vector $a \in (\mathbb{Z}/p)^d$ ($d = p^{e-1}$, 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 5.15: $2^{e-1} - 1 = 3$ 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`.

This root-fibre depth is in fact the *whole* depth. The basin cannot leave F_p:

Lemma 5.16. *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. □

Thus every $q \in \mathrm{basin}(s)$ has $\pi(q) \in \mathrm{basin}(s_d)$, and its distance to s splits as $m + h$ with m the distance of $\pi(q)$ in $C(d)$ and h the height inside R. The companion paper [2] proves that this bound is met with equality at every level, so that $\mathrm{depth}(p^e) = \rho$ exactly: *the deepest chains are the root-fibre ones of Proposition 5.15*, none through the rest of the basin being longer. The subtlety it must overcome is that *off* R the carry map is no longer linear but affine, $a(Dq) = L_{\pi(q)}\, a(q) + w_{\pi(q)}$ with L_τ a permuted copy of $I - S$, so the global depth is not that of a single nilpotent operator—the basin, of size $2^3 \cdot 3^{10}$ at $n = 27$, is not a $\mathbb{Z}/p$-linear in-tree.

6 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 $\sim \sqrt{\pi N/2}$ [4, 5]. 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 4.3). This is a diagnostic, not a theorem.

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 Cyclic sieving

The σ^k-fixed n-cycles have a closed count that generalises both Theorem 5.2 and Wilson's corollary.

Proposition 7.1 (Fixed-point counts)**.** *For $0 \le k < n$, with $g = \gcd(k, n)$ and $m = n/g$,*

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

Proof. $\langle s^k\rangle = \langle s^g\rangle$ is the order-m subgroup of $\langle s\rangle$; write $h = s^g$, a product of g disjoint m-cycles, with $C_{S_n}(h) = \mathbb{Z}/m \wr S_g$. As in Theorem 5.2, $q \in C(n)$ contains h in $\langle q\rangle$ iff $q \in C_{S_n}(h)$, its block permutation τ is a g-cycle, and $q^g = h^t$ with $\gcd(t, m) = 1$; there are $\varphi(m)$ admissible t, $(g-1)!$ such τ, and m^{g-1} block-vectors realising each, giving the product. The case $g = n/p$, $m = p$ recovers $|F_p|$ (Theorem 5.2); $\#\mathrm{Fix}(\sigma^k)$ depends only on $\gcd(k, n)$. $\square$

Remark 7.2. These counts realise a cyclic sieving phenomenon [11]: 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 7.1, 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 [15]), 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* [14]; 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 8).

8 Open problems

Question 8.1. By Proposition 5.5 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 5.8), 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 5.12) organises these orbits—each is inherited along a lift—but its fibre is irregular (Section 5), and we have found no closed form.

Question 8.2. The numbers of basins $1, 2, 2, 6, 7, 18, 17, 29, 56, 157$ for $n = 3, \ldots, 12$ are absent from the OEIS [15] (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 5.6 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 5.12) 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.

The depth (resolved). We conjectured in earlier versions that the root-fibre lower bound of Proposition 5.15 is the exact depth; this is now a theorem. The companion [2] proves $\mathrm{depth}(p^e) = p^{e-1}$ (p odd), resp. $2^{e-1} - 1$ ($p = 2$), so the deepest chains are the root-fibre ones, none through the rest of the basin being longer. (This is consistent with exhaustive backward search for all prime powers ≤ 27, for $n = 49$ depth 7, and for $n = 2^5$ depth 15.) The proof identifies the basin of s with the group of *flag-triangular* cycles and reduces the depth, via a transport cocycle, to an "obstruction law" proved by induction down the p-power tower; the essential difficulty is that off the root fibre the carry map is affine rather than linear, so the depth is not that of a single nilpotent operator.

Question 8.3. The cyclic sieving of Remark 7.2 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 8.4. 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 supporting computations are short and reproducible. 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] 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 (2026).

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

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

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

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

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

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

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

[10] 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`.

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

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

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

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

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