

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

Frédéric Lefebvre-Naré*

October 2026

Abstract

Fix the n -cycle $s: x \mapsto x + 1$ on $\mathbb{Z}/n$ and iterate the map $D(q) = q s q^{-1}$ on the set of n -cycles. Its only fixed point is s , and the n -cycles that eventually reach s form a rooted tree. We show that the height of this tree is p^{e-1} when $n = p^e$ with p an odd prime, $2^{e-1} - 1$ when $n = 2^e$, and, for general n , the largest of these numbers over the prime powers exactly dividing n .

The proof rests on two observations. First, in terms of the *defect* $y = q s^{-1}$ the map D is just $y \mapsto [y, s]$: the distance from q to s is the number of commutators with s needed to kill y . Second, when $n = p^e$ the cycles that reach s are exactly the n -cycles of a Sylow p -subgroup of the symmetric group — the group of maps that change each base- p digit by an amount depending only on the lower digits — and this group is nilpotent of class p^{e-1} (Kaloujnine). So the depth is the nilpotency class, except at $p = 2$, where being a full cycle forces the defect into the derived subgroup and costs exactly one step. The Chinese Remainder Theorem reduces general n to prime powers.

2020 MSC: 05A05, 20B30, 20D15, 37P99. *Keywords:* n -cycles, conjugation, functional graph, in-tree depth, Sylow subgroups of symmetric groups, lower central series, Engel condition.

1 Introduction

Let $C(n)$ be the set of n -cycles in the symmetric group $\text{Sym}(\mathbb{Z}/n)$, where $\mathbb{Z}/n = \{0, 1, \dots, n-1\}$, and let $s = s_n$ be the cycle $x \mapsto x + 1$. Permutations are composed from right to left. The *derivation* is the map

$$D = D_n: C(n) \rightarrow C(n), \quad D(q) = q s q^{-1}.$$

Since $D(q)$ sends $q(i)$ to $q(i+1)$, it is the n -cycle $(q(0) q(1) \cdots q(n-1))$: iterating D means reading the one-line notation of a cycle as a cycle notation, again and again. The cycle s is the

**Provenance and status.* The theorem and both of its proofs were obtained by artificial-intelligence models (Anthropic’s Claude) in dialogue with the author. The first proof [11] was reviewed module by module by OpenAI models. The proof given here is new and much shorter: it replaces the carry-cocycle analysis of [11] (transport of functionals, “obstruction law”, “master identity”) by Kaloujnine’s description of the Sylow subgroups of symmetric groups and its lower central filtration. Every statement below has also been checked by exact computation (Appendix A). The argument has not yet been refereed by a human mathematician and should be read critically. This note accompanies the survey [10].

only fixed point ($qsq^{-1} = q$ forces $q = s$). Some cycles fall into other periodic orbits; those that reach s form the *in-tree* of s ,

$$\text{basin}_n = \{q \in C(n) : D^t(q) = s \text{ for some } t \geq 0\}, \quad \text{dist}(q) = \min\{t : D^t(q) = s\},$$

and we study its height $\text{depth}(n) = \max_{q \in \text{basin}_n} \text{dist}(q)$.

Example 1.1 ($n = 8$). The 8-cycle $q = (0 \ 5 \ 6 \ 7 \ 4 \ 1 \ 2 \ 3)$, whose one-line notation is $[5, 2, 3, 0, 1, 6, 7, 4]$, gives the chain

$$q \xrightarrow{D} (x \mapsto 5x + 1) \xrightarrow{D} (x \mapsto x + 5) \xrightarrow{D} s.$$

It passes through an affine cycle and a rotation before reaching s ; we shall see that no 8-cycle needs more than three steps.

Theorem 1.2 (Main theorem). *For a prime p and $e \geq 1$,*

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

and for $n = \prod_p p^{e_p}$, $\text{depth}(n) = \max_p \text{depth}(p^{e_p})$. In particular $\text{depth}(n) \geq 2$ if and only if $8 \mid n$ or $p^2 \mid n$ for some odd prime p .

The threshold “ $8 \mid n$ or $p^2 \mid n$ ” is the Hull–Dobell condition [5, 8] for the existence of a full-period affine map $x \mapsto ax + b$ on $\mathbb{Z}/n$ with $a \neq 1$. This is no accident: the points at distance ≤ 2 from s are exactly the affine n -cycles (Example 2.2).

How the proof goes. Everything starts from an identity valid for any permutation q :

$$D(q)s^{-1} = [qs^{-1}, s], \quad \text{where } [a, b] = aba^{-1}b^{-1}. \quad (1)$$

Thus, in the *defect* coordinate $y = qs^{-1}$ (which is trivial exactly when $q = s$), D is the map $y \mapsto [y, s]$, and $\text{dist}(q)$ is the number of commutators with s needed to reduce y to the identity. In a nilpotent group of class κ one has $[y, {}_\kappa s] = 1$ for all y and s , so the depth is at most κ as soon as the in-tree lives inside a nilpotent group of class κ containing s . For $n = p^k$ the relevant group is completely explicit. Write numbers in base p ; the map $x \mapsto x + 1$ changes each digit by a carry that depends only on the digits below it. Call a permutation *triangular* if it has this property: it changes each digit by an amount depending only on the lower digits. The triangular permutations form a Sylow p -subgroup P_k of $\text{Sym}(\mathbb{Z}/p^k)$ (Kaloujnine [6]). We show:

- (1) the in-tree of s is exactly the set of p^k -cycles in P_k (§3, §4);
- (2) P_k has a central filtration of length p^{k-1} , defined by the polynomial degree of its digit increments (§4); hence every cycle in the tree reaches s in at most p^{k-1} steps;
- (3) an element of P_k is a full cycle iff its image in the abelianisation $P_k/[P_k, P_k] \cong \mathbb{F}_p^k$ has no zero coordinate. For $p = 2$ this pins every cycle to the coset $s[P_k, P_k]$: its defect starts one step down the filtration, and the bound improves to $2^{k-1} - 1$ (§§3–5);
- (4) the bounds are attained by explicit cycles that differ from s only in the top digit; there, commutation with s is the difference operator $a \mapsto a(r) - a(r - 1)$, whose nilpotency is plain to see (§5).

Section 6 reduces general n to prime powers by the Chinese Remainder Theorem, and §7 discusses the threshold, the relation with the first version [11], and open questions.

Prerequisites. Only elementary group theory and the arithmetic of polynomial functions over $\mathbb{F}_p$ are used. Kaloujnine’s theorems are quoted for orientation but never used: the facts we need about P_k are proved in full.

2 Conjugation as commutation

This section is valid for every n . We extend D to all of $\text{Sym}(\mathbb{Z}/n)$ by the same formula $D(q) = qsq^{-1}$ (an n -cycle in any case). We use the commutator $[a, b] = aba^{-1}b^{-1}$ and the iterated commutators $[y, {}_0s] = y$, $[y, {}_{t+1}s] = [[y, {}_ts], s]$.

Lemma 2.1. *Let $q \in \text{Sym}(\mathbb{Z}/n)$ and put $\delta(q) = qs^{-1}$ (the defect of q).*

(a) $\delta(D(q)) = [\delta(q), s]$. Hence $\delta(D^t(q)) = [\delta(q), {}_ts]$ for all $t \geq 0$, and for $q \in \text{basin}_n$,

$$\text{dist}(q) = \min\{t \geq 0 : [\delta(q), {}_ts] = 1\}.$$

(b) For every $m \in \mathbb{Z}$, $D(q)^m = q s^m q^{-1}$. In particular q maps each orbit of s^m onto an orbit of $D(q)^m$.

Proof. (a) Write $q = ys$ with $y = \delta(q)$. Then $\delta(D(q)) = qsq^{-1}s^{-1} = ys \cdot s \cdot s^{-1}y^{-1} \cdot s^{-1} = ysy^{-1}s^{-1} = [y, s]$. Iterate; and $D^t(q) = s$ iff $\delta(D^t(q)) = 1$. (b) $(qsq^{-1})^m = qs^mq^{-1}$, and conjugation by q carries the orbits of s^m to those of qs^mq^{-1} . $\square$

So, in the coordinate $y = \delta(q)$, the derivation is “commutation with s ”. In the language of group theory, $\text{dist}(q)$ is the *Engel length* of $\delta(q)$ relative to s .

Example 2.2 (the first two layers). Let $q \in C(n)$ and $y = \delta(q)$. Then $D(q) = s$ iff $[y, s] = 1$ iff y commutes with s iff $y \in \langle s \rangle$ (the centraliser of an n -cycle is the cyclic group it generates) iff q is a rotation $x \mapsto x + a$; such a rotation is an n -cycle iff $\gcd(a, n) = 1$. Next, $D^2(q) = s$ iff $[y, s] \in \langle s \rangle$ iff $ysy^{-1} \in \langle s \rangle$ iff y normalises $\langle s \rangle$ iff y , equivalently $q = ys$, is affine $x \mapsto ax + b$ with $a \in (\mathbb{Z}/n)^\times$ (if $ysy^{-1} = s^a$, then $y(x + 1) = y(x) + a$, so $y(x) = ax + y(0)$). Thus the vertices at distance exactly 2 are the affine n -cycles with $a \neq 1$, and $\text{depth}(n) \geq 2$ iff such cycles exist — which is the Hull–Dobell condition recalled in §7.

3 Prime powers: the triangular group

Throughout §§3–5, p is a prime, $k \geq 1$, $n = p^k$, and $c = p^{k-1}$.

3.1 Digits and triangular maps

Each $x \in \mathbb{Z}/p^k$ has base- p digits $x = \sum_{i < k} x_i p^i$, $x_i \in \{0, \dots, p-1\}$, which we identify with elements of $\mathbb{F}_p$. We write $x_{<i} = (x_0, \dots, x_{i-1}) \in \mathbb{F}_p^i$; it encodes the residue $x \bmod p^i$.

Definition 3.1. A permutation g of $\mathbb{Z}/p^k$ is *triangular* if for each $i < k$ there is a function $g_i: \mathbb{F}_p^i \rightarrow \mathbb{F}_p$ such that

$$g(x)_i = x_i + g_i(x_{<i}) \quad \text{for all } x \in \mathbb{Z}/p^k \text{ and all } i < k$$

(addition in $\mathbb{F}_p$; g_0 is a constant). In words: g changes each digit by an amount that depends only on the digits below it. We call $(g_0, \dots, g_{k-1})$ the *increments* of g , and write P_k for the set of triangular permutations.

Any family of functions (g_i) defines a triangular permutation (it can be inverted digit by digit, from the bottom up), so $|P_k| = \prod_{i < k} p^{p^i} = p^{1+p+\dots+p^{k-1}}$. For $g, h \in P_k$,

$$(gh)(x)_i = h(x)_i + g_i(h(x)_{<i}) = x_i + h_i(x_{<i}) + g_i(h(x)_{<i}), \quad (2)$$

and $h(x)_{<i}$ depends only on $x_{<i}$; so P_k is closed under composition, and it is a group. Its order is the exact power of p dividing $(p^k)!$, so P_k is a Sylow p -subgroup of $\text{Sym}(\mathbb{Z}/p^k)$; this description, with (g_i) called the *tableau* of g , is due to Kaloujnine [6]. Equivalently, P_k is the k -fold iterated wreath product $\mathbb{Z}/p \wr \dots \wr \mathbb{Z}/p$; for $p = 2$ it is the group of invertible T -functions on k bits in the sense of Klimov–Shamir [7]. None of these identifications is needed below.

Example 3.2. (i) *The shift.* Adding 1 increases digit i by one exactly when all lower digits equal $p - 1$; so $s \in P_k$, with increments the *carries*

$$s_i = \epsilon_i, \quad \epsilon_i(u) = \begin{cases} 1 & \text{if } u = (p-1, \dots, p-1), \\ 0 & \text{otherwise} \end{cases} \quad (\epsilon_0 = 1).$$

For $n = 8$: $s = [1, x_0, x_0x_1]$ in increment notation.

- (ii) *The top layer.* For a function $a: \mathbb{Z}/c \rightarrow \mathbb{F}_p$ let $\tau_a(x) = x + a(x \bmod c)c$; it changes only the top digit, by a of the lower digits. These maps form an abelian subgroup $A_k = \{\tau_a\} \cong \mathbb{F}_p^c$, with $\tau_a\tau_b = \tau_{a+b}$.
- (iii) *A central element.* $z := \tau_1 = s^c$ is the map $x \mapsto x + c$. It is central in P_k : x and $x + c$ have the same lower digits, so $h(x + c) = h(x) + c$ for every $h \in P_k$.
- (iv) *Reduction.* Each $g \in P_k$ induces a triangular permutation $\bar{g}$ of $\mathbb{Z}/c$ (its action on $x \bmod c$, i.e. on the lower $k-1$ digits). The map $g \mapsto \bar{g}$ is a homomorphism $P_k \rightarrow P_{k-1}$ with kernel A_k , and $\bar{s} = s_c$. Conversely, each $h \in P_{k-1}$ acts on $\mathbb{Z}/p^k$ as $\tilde{h}$, changing the lower digits as h does and leaving the top digit alone; $h \mapsto \tilde{h}$ is a homomorphism, and every $g \in P_k$ factors uniquely as $g = \tau_a \tilde{g}$ with $\tau_a \in A_k$.

3.2 Laps and the cycle criterion

For $g \in P_k$ and $i < k$ put

$$\Sigma_i(g) = \sum_{u \in \mathbb{F}_p^i} g_i(u) \in \mathbb{F}_p,$$

the total increment of digit i during one full lap of the lower digits.

Lemma 3.3. (a) *Each $\Sigma_i: P_k \rightarrow \mathbb{F}_p$ is a group homomorphism, and $\Sigma_i(s) = 1$ for all i .*
(b) *$g \in P_k$ is a p^k -cycle iff $\Sigma_i(g) \neq 0$ for every $i < k$.*

Proof. (a) By (2), $(gh)_i = h_i + g_i \circ \bar{h}^{(i)}$, where $\bar{h}^{(i)}$ is the bijection of $\mathbb{F}_p^i$ induced by h ; summing over $\mathbb{F}_p^i$ gives $\Sigma_i(gh) = \Sigma_i(h) + \Sigma_i(g)$. And ϵ_i is the indicator of a single point.

(b) Induction on k . For $k = 1$, $g(x) = x + g_0$ is a p -cycle iff $g_0 \neq 0$. Let $k \geq 2$. If g is a p^k -cycle, then $\bar{g}$ is transitive on $\mathbb{Z}/c$, i.e. a c -cycle. Conversely, let $\bar{g}$ be a c -cycle. Then g^c fixes every lower part $x \bmod c$, and during these c steps the lower part runs once through all of $\mathbb{Z}/c$, so the top digit has been increased by $\Sigma_{k-1}(g)$: thus $g^c = z^{\Sigma_{k-1}(g)}$. The g -orbit of x therefore has c elements if $\Sigma_{k-1}(g) = 0$ and $cp = p^k$ elements otherwise. So g is a p^k -cycle iff $\bar{g}$ is a c -cycle and $\Sigma_{k-1}(g) \neq 0$; conclude by induction, since $\Sigma_i(\bar{g}) = \Sigma_i(g)$ for $i < k-1$. $\square$

3.3 The in-tree lies in the triangular group

Proposition 3.4. $\text{basin}_{p^k} \subseteq P_k$.

Proof. We argue by induction on k , the case $k = 0$ being empty ($\mathbb{Z}/1$ has a single point). Fix $k \geq 1$, assume the statement for p^{k-1} , and argue by induction on $\text{dist}(q)$. If $\text{dist}(q) = 0$ then $q = s \in P_k$. Otherwise $t := D(q)$ is in the basin and closer to s , so $t \in P_k$, and so are all $D^j(q)$, $j \geq 1$.

Step 1: q commutes with $z = s^c$. Since z is central in P_k , it commutes with the n -cycle t , hence lies in $\langle t \rangle$. A cyclic group of order p^k has a unique subgroup of order p , here $\langle t^c \rangle$; so $\langle z \rangle = \langle t^c \rangle$. By Lemma 2.1(b), $t^c = qzq^{-1}$. Hence $qzq^{-1} = z^\lambda$ for some $\lambda \in \{1, \dots, p-1\}$, and inductively $q^j z q^{-j} = z^{\lambda^j}$. Taking $j = p^k$ (the order of the cycle q) gives $\lambda^{p^k} \equiv 1$, while $\lambda^{p^k} \equiv \lambda \pmod{p}$ by Fermat. So $\lambda = 1$.

Step 2: reduction. As $q(x+c) = q(x) + c$, the residue $q(x) \bmod c$ depends only on $x \bmod c$: q induces a permutation $\bar{q}$ of $\mathbb{Z}/c$, a c -cycle since q is transitive. Reduction modulo c is a homomorphism on the group of permutations commuting with z , which contains q , s and all $D^j(q)$; it sends s to s_c . Therefore $D_c^j(\bar{q}) = \overline{D^j(q)}$ for all j , and $D_c^{\text{dist}(q)}(\bar{q}) = s_c$: $\bar{q} \in \text{basin}_c$, so $\bar{q} \in P_{k-1}$ by the induction hypothesis on k . Finally, writing $x = \bar{x} + x_{k-1}c$ with $0 \leq \bar{x} < c$, we get $q(x) = q(\bar{x}) + x_{k-1}c$, so the top digit of $q(x)$ is $x_{k-1} + q(\bar{x})_{k-1}$, an increment depending only on the lower digits. Thus $q \in P_k$. $\square$

Remark 3.5. The hypothesis that q is an n -cycle is used in Step 1 and cannot be dropped: for p odd, the involution $q(x) = -x$ satisfies $D(q) = s^{-1} \in P_k$, but $q \notin P_k$.

4 Degree, and a central filtration of length p^{k-1}

4.1 Polynomial functions of the digits

Every function $f: \mathbb{Z}/p^k \rightarrow \mathbb{F}_p$ is a function of the digits $(x_0, \dots, x_{k-1}) \in \mathbb{F}_p^k$, and as such is given by a unique *reduced* polynomial $f = \sum_\alpha f_\alpha x^\alpha$, where $x^\alpha = \prod_i x_i^{\alpha_i}$ and $0 \leq \alpha_i \leq p-1$ (the p^k monomials span the p^k -dimensional space of functions, since every indicator function $\prod_i (1 - (x_i - u_i)^{p-1})$ is such a polynomial; so they form a basis). We weight digit i by p^i : the *weight* of x^α is $|\alpha| = \sum_i \alpha_i p^i$ — the integer whose base- p digits are the exponents — and the *degree* of $f \neq 0$ is

$$\deg f = \max\{|\alpha| : f_\alpha \neq 0\}, \quad \deg 0 = -\infty.$$

(D1) $\deg(f+g) \leq \max(\deg f, \deg g)$ and $\deg(fg) \leq \deg f + \deg g$. (A product of monomials adds exponents; reducing an exponent $\geq p$ by $x_i^p = x_i$ only lowers the weight.)

(D2) The digit function $x \mapsto x_i$ has degree p^i .

(D3) A function f of $x_{<i}$ alone has degree $\leq p^i - 1$, and $\deg f \leq p^i - 2$ iff $\sum_{u \in \mathbb{F}_p^i} f(u) = 0$.

Indeed the only monomial in $x_{<i}$ of weight $p^i - 1$ is $(x_0 \cdots x_{i-1})^{p-1}$, and $\sum_{u \in \mathbb{F}_p^i} u^\alpha = \prod_{j < i} \sum_{v \in \mathbb{F}_p} v^{\alpha_j}$ vanishes unless every $\alpha_j = p-1$ (as $\sum_{v \in \mathbb{F}_p} v^a = 0$ for $0 \leq a \leq p-2$ and $= -1$ for $a = p-1$); so $\sum_u f(u) = (-1)^i \times$ the coefficient of $(x_0 \cdots x_{i-1})^{p-1}$.

Remark 4.1 (binomial basis). By Lucas' theorem, $\binom{x}{j} \bmod p = \prod_i \binom{x_i}{j_i}$, a polynomial whose monomial of highest weight is $\prod_i x_i^{j_i}/j_i!$, of weight j . Hence $\deg f$ is also the largest j with a nonzero coefficient in the Newton expansion $f = \sum_j b_j \binom{x}{j}$, and the filtration by degree is the “binomial flag” of [11]. We do not need this.

4.2 The filtration

Definition 4.2. For $t \geq 1$ let $\Gamma_t = \{g \in P_k : \deg g_i \leq p^i - t \text{ for every } i < k\}$.

By (D3), $\Gamma_1 = P_k$; and $\Gamma_t = \{1\}$ for $t > c = p^{k-1}$, since then $p^i - t < 0$ for all $i < k$. The shift has increments of maximal degree $\deg \epsilon_i = p^i - 1$, so $s \in \Gamma_1 \setminus \Gamma_2$. On the top layer, $\tau_a \in \Gamma_t$ iff $\deg a \leq c - t$.

Lemma 4.3 (triangular maps lower the degree). *Let $g \in P_k$ and $t \geq 1$. Then $g \in \Gamma_t$ if and only if*

$$\deg(f \circ g - f) \leq \deg f - t \quad \text{for every } f: \mathbb{Z}/p^k \rightarrow \mathbb{F}_p.$$

Proof. ($\Leftarrow$) Take $f = x_i$: then $f \circ g - f = g_i$, and $\deg x_i = p^i$ by (D2).

($\Rightarrow$) By (D1) it suffices to treat a monomial $f = x^\alpha$. Then

$$f \circ g = \prod_i (x_i + g_i)^{\alpha_i} = \sum_{\beta \leq \alpha} \binom{\alpha}{\beta} \prod_i x_i^{\beta_i} g_i^{\alpha_i - \beta_i}, \quad \binom{\alpha}{\beta} = \prod_i \binom{\alpha_i}{\beta_i}.$$

The term $\beta = \alpha$ is f itself. By (D1), any other term has degree at most

$$\sum_i \left(\beta_i p^i + (\alpha_i - \beta_i)(p^i - t) \right) = |\alpha| - t \sum_i (\alpha_i - \beta_i) \leq |\alpha| - t. \quad \square$$

In words: for $t = 1$, triangular maps act *unipotently* on functions — composing with g changes f only by terms of lower degree — and the elements of Γ_t are those that lower it by at least t .

Proposition 4.4. (a) *Each Γ_t is a normal subgroup of P_k , and $[\Gamma_t, \Gamma_u] \subseteq \Gamma_{t+u}$. In particular $[\Gamma_t, P_k] \subseteq \Gamma_{t+1}$, so $P_k = \Gamma_1 \supseteq \Gamma_2 \supseteq \dots \supseteq \Gamma_{c+1} = \{1\}$ is a central series, and P_k is nilpotent of class at most p^{k-1} .*

(b) $\Gamma_2 = \{g \in P_k : \Sigma_i(g) = 0 \text{ for all } i < k\}$.

(c) $\Gamma_2 = [P_k, P_k]$; hence $(\Sigma_0, \dots, \Sigma_{k-1})$ identifies the abelianisation $P_k/[P_k, P_k]$ with $\mathbb{F}_p^k$.

Proof. (a) For $g \in P_k$ let g^* be the linear operator $f \mapsto f \circ g$ on functions; then $(gh)^* = h^*g^*$. Call a linear operator E of order $\geq t$ if $\deg Ef \leq \deg f - t$ for all f . Operators of order $\geq t$ form a vector space, and the composite of operators of orders $\geq t$ and $\geq u$ has order $\geq t + u$. Lemma 4.3 says: $g \in \Gamma_t$ iff $g^* - 1$ has order $\geq t$; in particular every g^* ($g \in P_k$) has order ≥ 0 . Let $g, g' \in \Gamma_t$ and $h \in \Gamma_u$, and put $G = g^* - 1$, $H = h^* - 1$. Then

$$(gg')^* - 1 = g'^*G + (g'^* - 1), \quad (g^{-1})^* - 1 = -(g^{-1})^*G$$

have order $\geq t$, so Γ_t is a subgroup; and since $[g, h]^* = (h^{-1})^*(g^{-1})^*h^*g^*$,

$$[g, h]^* - 1 = (h^{-1})^*(g^{-1})^*(h^*g^* - g^*h^*) = (h^{-1})^*(g^{-1})^*(HG - GH)$$

has order $\geq t + u$, i.e. $[g, h] \in \Gamma_{t+u}$. Normality follows from $hgh^{-1} = [h, g]g$ and $[\Gamma_1, \Gamma_t] \subseteq \Gamma_{t+1} \subseteq \Gamma_t$.

(b) is (D3) applied to each increment g_i .

(c) $[P_k, P_k] = [\Gamma_1, \Gamma_1] \subseteq \Gamma_2$ by (a). Conversely let $g \in \Gamma_2$, and induct on k (for $k = 1$, $\Gamma_2 = \{1\}$). Write $g = \tau_a h$ with $h = \bar{g}$ (Example 3.2(iv)). By (2) the top increment of g is $a \circ h$, so $\sum_r a(r) = \Sigma_{k-1}(g) = 0$, while $\Sigma_i(h) = \Sigma_i(g) = 0$ for $i < k - 1$. By induction $h \in [P_{k-1}, P_{k-1}]$,

so $\tilde{h} \in [P_k, P_k]$. And a has zero sum, so $a = b - Sb$ for some b , where $(Sb)(r) = b(r-1)$ (the map $b \mapsto b - Sb$ on $\mathbb{F}_p^c$ has kernel the constants, so its image is the hyperplane of zero-sum functions); then $\tau_a = [\tau_b, s]$ by Lemma 5.3(a) below. Hence $g \in [P_k, P_k]$. The last assertion follows from (b), since each Σ_i is onto. $\square$

Remark 4.5. Kaloujnine [6] proved that the Γ_t are exactly the terms $\gamma_t(P_k)$ of the lower central series (which coincides with the upper central series), so that the class of P_k is exactly p^{k-1} and $\Gamma_2 = [P_k, P_k]$; see [2] for a recent account. We only need the inclusions $\gamma_t(P_k) \subseteq \Gamma_t$ and the equality $\Gamma_2 = [P_k, P_k]$ proved above; sharpness will come from explicit examples.

4.3 Consequences for the derivation

Corollary 4.6. *Let $q \in P_k$ with $\delta(q) = qs^{-1} \in \Gamma_t$. Then $\delta(D^j(q)) \in \Gamma_{t+j}$ for every $j \geq 0$; in particular $D^{c+1-t}(q) = s$.*

Proof. By Lemma 2.1(a), $\delta(D^j(q)) = [\delta(q), {}_js]$, and each commutator with $s \in \Gamma_1$ moves one step down the filtration (Proposition 4.4(a)). Since $\Gamma_{c+1} = \{1\}$, $\delta(D^{c+1-t}(q)) = 1$. $\square$

Corollary 4.7 (the in-tree). $\text{basin}_{p^k} = C(p^k) \cap P_k = \{g \in P_k : \Sigma_i(g) \neq 0 \text{ for all } i < k\}$. Consequently

$$|\text{basin}_{p^k}| = (p-1)^k p^{(p^k-1)/(p-1)-k},$$

and for $p = 2$ the in-tree is a single coset of the derived subgroup: $\text{basin}_{2^k} = s[P_k, P_k]$.

Proof. “ $\subseteq$ ” is Proposition 3.4; “ $\supseteq$ ” is Corollary 4.6 with $t = 1$; the second description is Lemma 3.3(b). For the count, the increment g_i ranges over the $(p-1)p^{p^i-1}$ functions on $\mathbb{F}_p^i$ with nonzero sum. For $p = 2$, the conditions read $\Sigma_i(g) = 1 = \Sigma_i(s)$, i.e. $\Sigma_i(gs^{-1}) = 0$ for all i , i.e. $gs^{-1} \in \Gamma_2 = [P_k, P_k]$ by Lemma 3.3(a) and Proposition 4.4(b,c). $\square$

5 The depth at prime powers

Theorem 5.1. $\text{depth}(p^k) = p^{k-1}$ if p is odd, and $\text{depth}(2^k) = 2^{k-1} - 1$.

5.1 Upper bound

Let $q \in \text{basin}_{p^k}$. By Proposition 3.4, $q \in P_k$, so $\delta(q) \in \Gamma_1$ and $\text{dist}(q) \leq c$ by Corollary 4.6. If $p = 2$, then $q \in s[P_k, P_k] = s\Gamma_2$ by Corollary 4.7, i.e. $\delta(q) \in \Gamma_2$, and Corollary 4.6 gives $\text{dist}(q) \leq c - 1$.

Remark 5.2 (where the “ -1 ” comes from). By Proposition 4.4(c), $(\Sigma_0, \dots, \Sigma_{k-1})$ identifies the abelianisation $P_k/[P_k, P_k] = P_k/\Gamma_2$ with $\mathbb{F}_p^k$; the shift s maps to $(1, \dots, 1)$, and the cycles are the elements whose image has no zero coordinate. For odd p there are $(p-1)^k$ such vectors, and a cycle may differ from s already in the abelianisation (the deepest examples below map to $(1, \dots, 1, 2)$). For $p = 2$ the only such vector is $(1, \dots, 1)$: every cycle agrees with s modulo Γ_2 , so its defect starts one step down the central series and one commutator is saved.

5.2 The top layer: the derivation as a difference operator

For $a: \mathbb{Z}/c \rightarrow \mathbb{F}_p$ write $(Sa)(r) = a(r-1)$ (indices in $\mathbb{Z}/c$) and $N = 1 - S$, so that $(Na)(r) = a(r) - a(r-1)$ is a discrete derivative.

Lemma 5.3. (a) $[\tau_a, s] = \tau_{Na}$. Hence, if $\delta(q) = \tau_a$, then $\delta(D^t(q)) = \tau_{N^t a}$ for all t .

(b) $N^c = 0$ and $N^{c-1}a = (\sum_{r \in \mathbb{Z}/c} a(r)) \mathbf{1}$.

Proof. (a) $s\tau_a s^{-1}$ maps x to $(x-1) + a((x-1) \bmod c)c + 1 = x + (Sa)(x \bmod c)c$, so $s\tau_a s^{-1} = \tau_{Sa}$ and $[\tau_a, s] = \tau_a(s\tau_a s^{-1})^{-1} = \tau_{a-Sa}$. The second claim follows from Lemma 2.1(a). (b) Since c is a power of p , $(1-X)^c = 1 - X^c$ in $\mathbb{F}_p[X]$, hence $(1-X)^{c-1} = 1 + X + \dots + X^{c-1}$. As $S^c = 1$, this gives $N^c = 0$ and $N^{c-1} = 1 + S + \dots + S^{c-1}$, which sends a to the constant function $\sum_r a(r)$. $\square$

On the coset $A_k s$ — the cycles that agree with s except in the top digit, called the *root fibre* in [11] — the derivation is therefore the linear map N , an additive cellular automaton on the cyclic lattice $\mathbb{Z}/c$ (“rule 60” for $p = 2$; compare [9]).

5.3 Lower bound: the deepest cycles

Let $q = \tau_a s$, i.e. $q(x) = x + 1 + c a((x+1) \bmod c)$. Then $\delta(q) = \tau_a$, so by Lemma 5.3(a), $\text{dist}(q) = \min\{t : N^t a = 0\}$ whenever q is a cycle. By Lemma 3.3(a), $\Sigma_i(q) = \Sigma_i(\tau_a) + \Sigma_i(s)$, which is 1 for $i < k-1$ and $1 + \sum_r a(r)$ for $i = k-1$.

Write e_r for the indicator function of $r \in \mathbb{Z}/c$.

p odd. Take $a = e_0$:

$$q(x) = x + 1 + c \cdot [x \equiv -1 \pmod{c}].$$

Here $\Sigma_{k-1}(q) = 2 \neq 0$, so q is a cycle, and $N^{c-1}e_0 = \mathbf{1} \neq 0$ by Lemma 5.3(b): $\text{dist}(q) = c$.

$p = 2$, $k \geq 2$. Take $a = Ne_0 = e_0 - e_1 (= e_0 + e_1)$:

$$q(x) = x + 1 + c \cdot [x \equiv -1 \text{ or } x \equiv 0 \pmod{c}].$$

Now $\sum_r a(r) = 0$, so $\Sigma_{k-1}(q) = 1$ and q is a cycle; and $N^{c-2}a = N^{c-1}e_0 = \mathbf{1} \neq 0$ while $N^{c-1}a = 0$: $\text{dist}(q) = c-1$. (For $k = 1$, $C(2) = \{s\}$ and $\text{depth}(2) = 0 = c-1$.)

Incidentally, $[\tau_{e_0, c-1} s] = \tau_{\mathbf{1}} = z \neq 1$ for every p , so the class of P_k is exactly p^{k-1} , as Kaloujnine showed.

This proves Theorem 5.1. $\square$

Example 5.4 ($n = 8$ and $n = 9$). For $n = 8$ ($c = 4$) the deepest cycle above is the cycle q of Example 1.1. In increment notation $q = [1, x_0, (1+x_0)(1+x_1)]$, against $s = [1, x_0, x_0 x_1]$; its defect is τ_a with $a = 1 + x_1$, of degree $2 = c-2$, i.e. $\delta(q) \in \Gamma_2$ as it must be. The defects along the chain are $\tau_a, \tau_{Na}, \tau_{N^2 a}, 1$ with

$$a = (1, 1, 0, 0) \mapsto Na = (1, 0, 1, 0) \mapsto N^2 a = (1, 1, 1, 1) \mapsto 0$$

(values at $r = 0, 1, 2, 3$), of degrees $2, 1, 0, -\infty$; correspondingly $D(q) = \tau_{Na} s = (x \mapsto 5x + 1)$, $D^2(q) = z s = s^5$ and $D^3(q) = s$.

For $n = 9$ ($c = 3$), $q(x) = x + 1 + 3[x \equiv 2 \pmod{3}]$ is the 9-cycle $(0 \ 1 \ 2 \ 6 \ 7 \ 8 \ 3 \ 4 \ 5)$, and

$$q \xrightarrow{D} (x \mapsto 4x + 7) \xrightarrow{D} (x \mapsto x + 4) \xrightarrow{D} s.$$

n	2	4	8	16	3	9	27	5	25	7	49
$ \text{basin}_n $	1	2	16	2048	2	36	472392	4	10000	6	4235364
$\text{depth}(n)$	0	1	3	7	1	3	9	1	5	1	7

Table 1: Size and height of the in-tree of s for small prime powers (Corollary 4.7, Theorem 5.1), all confirmed by exhaustive search (Appendix A; $n = 49$ in [11]).

6 General n : the Chinese Remainder Theorem

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_n 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 $\mathbb{Z}/n_1 \times \{x_2\}$.

Lemma 6.1. (a) $q_1 \times q_2 \in C(n)$ iff $q_i \in C(n_i)$ for $i = 1, 2$.

(b) $D_n(q_1 \times q_2) = D_{n_1}(q_1) \times D_{n_2}(q_2)$.

(c) If $q \in \text{Sym}(\mathbb{Z}/n)$ and $D_n(q)$ is a product, then q is a product.

Proof. (a) The orbit of (x_1, x_2) has $\text{lcm}(\ell_1, \ell_2)$ elements, where ℓ_i is the length of the q_i -orbit of x_i ; this equals n for every point iff $\ell_i = n_i$ for every point. (b) Products compose coordinatewise. (c) Write $D_n(q) = t_1 \times t_2$; by (a), $t_i \in C(n_i)$. Since n_1 is invertible modulo n_2 , the orbits of $s^{n_1} = \text{id} \times s_{n_2}^{n_1}$ are the rows, and so are those of $D_n(q)^{n_1} = \text{id} \times t_2^{n_1}$. By Lemma 2.1(b), 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 . $\square$

Theorem 6.2. Let n_1, n_2 be coprime. Then $\text{basin}_n = \{q_1 \times q_2 : q_i \in \text{basin}_{n_i}\}$, and

$$\text{dist}(q_1 \times q_2) = \max(\text{dist } q_1, \text{dist } q_2).$$

Hence $|\text{basin}_n| = |\text{basin}_{n_1}| |\text{basin}_{n_2}|$ and $\text{depth}(n) = \max(\text{depth } n_1, \text{depth } n_2)$.

Proof. By Lemma 6.1(b), $D^t(q_1 \times q_2) = D^t(q_1) \times D^t(q_2)$, which equals s iff $t \geq \text{dist } q_1$ and $t \geq \text{dist } q_2$; this gives “ $\supseteq$ ” and the formula for dist . Conversely, if $q \in \text{basin}_n$ with $D^t(q) = s$, then s is a product, so by Lemma 6.1(c) applied repeatedly, $D^{t-1}(q), \dots, D(q), q$ are products; writing $q = q_1 \times q_2$, we have $q_i \in C(n_i)$ by Lemma 6.1(a), and $D^t(q_i) = s_{n_i}$. $\square$

Proof of Theorem 1.2. Theorem 5.1 gives the prime-power case, and Theorem 6.2, applied to the factorisation of n into prime powers, gives $\text{depth}(n) = \max_p \text{depth}(p^{e_p})$. Finally $\text{depth}(p^e) \geq 2$ iff p is odd and $e \geq 2$, or $p = 2$ and $e \geq 3$. $\square$

7 Discussion

The threshold. By Example 2.2, $\text{depth}(n) \geq 2$ iff some affine map $x \mapsto ax + b$ with $a \neq 1$ is an n -cycle. By Hull–Dobell [5] (see [8, §3.2.1.2]), $x \mapsto ax + b$ is an n -cycle iff $\gcd(b, n) = 1$, $a \equiv 1$ modulo every prime dividing n , and $a \equiv 1 \pmod{4}$ if $4 \mid n$; such an $a \neq 1$ exists iff $8 \mid n$ or $p^2 \mid n$ for an odd prime p , in accordance with Theorem 1.2. The threshold is not “non-squarefree”: for $n = 4$ or $n = 12$ the tree is flat.

What the proof gives beyond the depth. For $n = p^k$ it identifies the whole in-tree with the cycles of the Sylow subgroup P_k (Corollary 4.7), and bounds the distance of each vertex by the position of its defect in the filtration: $\text{dist}(q) \leq c + 1 - t$ when $\delta(q) \in \Gamma_t$ (Corollary 4.6). The bound need not be attained: $\text{dist}(q)$ is the Engel length of $\delta(q)$ relative to the particular element s , which depends on more than the filtration level.

Relation to the first version. The first version [11] proved the theorem by an explicit analysis in “carry coordinates”. In the present language, its main objects are as follows.

- The carry coordinates $\theta = (\bar{\theta}, a)$ are the factorisation of P_k as $A_k \rtimes P_{k-1}$ (reduction modulo p^{k-1} , with a the top increment); its “cocycle” is the formula for D in these coordinates.
- The “binomial flag” and its “flag characterisation of the basin” are the degree filtration (Remark 4.1), Lemma 4.3 with $t = 1$, and Corollary 4.7.
- The “root fibre” and its nilpotent map $I - S$ are the coset $A_k s$ and Lemma 5.3.
- The key statement (L2) of [11] — after m steps of the base, the carry lies in $\text{Im } N^m$ — says that the defect has reached $\Gamma_{m+1} \cap A_k$ (for $p = 2$, $\Gamma_{m+2} \cap A_k$). There it required a transport of functionals along the base path, an “obstruction law” and a “master identity”; here it is the one-line Corollary 4.6, because $[\Gamma_t, P_k] \subseteq \Gamma_{t+1}$.
- The “single carry that odd primes absorb and $p = 2$ cannot” is Remark 5.2: the abelianisation of P_k is $\mathbb{F}_p^k$, and $\mathbb{F}_2^\times$ is trivial.

Related work. The Sylow subgroups of symmetric groups and their central series go back to Kaloujnine [6]; for a modern treatment of the polynomial model see [2]. For $p = 2$, P_k is the group of invertible T -functions on k bits, and Lemma 3.3(b) is the familiar criterion for single-cycle T -functions [7], part of Anashin’s non-Archimedean ergodic theory [1]; the affine cycles of Example 2.2 are the full-period linear congruential generators [8]. The linear dynamics on the root fibre is the purely nilpotent case of the additive cellular automata of Martin–Odlyzko–Wolfram [9]. Carries of base- p addition appear in other roles in the combinatorics of permutations, e.g. as a Markov chain related to riffle shuffles [4, 3]; here they are simply the increments ϵ_i of the shift.

Open questions. (i) *The distance profile.* The size of the in-tree is known in closed form (Corollary 4.7, Theorem 6.2), and now its height; how many cycles lie at each distance from s ? For $n = p^k$ this asks for the distribution of the Engel length relative to s on the set of defects $\{qs^{-1} : q \in \text{basin}_{p^k}\}$. For general n the answer reduces to prime powers: by Theorem 6.2, the number of vertices at distance $\leq t$ is multiplicative in n . (ii) *The rest of the functional graph.* Cycles that never reach s fall into other periodic orbits of D ; their structure is surveyed, but not explained, in [10]. Note that the commutator form (1) holds on all of $\text{Sym}(\mathbb{Z}/n)$.

A Computer verification

All statements were checked by exact computation, with the Python script `code/verify_companion_v2.py`, which runs in a few minutes on a laptop. These checks are falsification attempts, not part of the proof.

- *Depth and size of the in-tree* (Theorem 5.1, Corollary 4.7): by exhaustive backward search from s (the D -preimages of an n -cycle t are the maps $i \mapsto t^i(x_0)$, $x_0 \in \mathbb{Z}/n$) for

- $n = 2, 4, 8, 16, 3, 9, 27, 5, 25, 7$; the values of Table 1. The first version [11] independently confirmed $\text{depth}(32) = 15$, $\text{depth}(49) = 7$ and $\text{depth}(81) = 27$.
- *The in-tree is $C(p^k) \cap P_k$* (Proposition 3.4, Corollary 4.7): every vertex found lies in P_k , and, for $n = 2, 4, 8, 16, 3, 9, 5, 7$, every n -cycle of P_k was found.
 - *Commutator form* (Lemma 2.1(a)): for every vertex, $\text{dist}(q)$ equals the least t with $[qs^{-1}, {}_ts] = 1$, and $\text{dist}(q) \leq c + 1 - t$ whenever $qs^{-1} \in \Gamma_t$.
 - *Filtration* (Lemma 4.3, Proposition 4.4): $[g, s] \in \Gamma_{t+1}$ for every $g \in \Gamma_t$, on all of P_k for $n = 2, 4, 8, 16, 3, 9, 5, 7$, and on random samples for $n = 25, 27, 32, 49$; the degree inequality of Lemma 4.3 on random samples for the same n ; and the agreement of the weighted degree with the Newton degree (Remark 4.1).
 - *Extremal examples* (§5) and the chains of Example 5.4.

References

- [1] V. Anashin and A. Khrennikov, *Applied Algebraic Dynamics*, de Gruyter Expositions in Mathematics **49**, de Gruyter (2009).
- [2] R. Aragona, N. Gavioli and G. Nozzi, *Normality conditions in the Sylow p -subgroup of $\text{Sym}(p^n)$ and its associated Lie algebra*, arXiv:2504.05256 (2025).
- [3] P. Diaconis and J. Fulman, *Carries, shuffling, and an amazing matrix*, Amer. Math. Monthly **116** (2009), 788–803.
- [4] J. M. Holte, *Carries, combinatorics, and an amazing matrix*, Amer. Math. Monthly **104** (1997), 138–149.
- [5] T. E. Hull and A. R. Dobell, *Random number generators*, SIAM Review **4** (1962), 230–254.
- [6] L. Kaloujnine, *La structure des p -groupes de Sylow des groupes symétriques finis*, Ann. Sci. École Norm. Sup. (3) **65** (1948), 239–276.
- [7] A. Klimov and A. Shamir, *A new class of invertible mappings*, CHES 2002, LNCS **2523**, Springer (2003), 470–483.
- [8] D. E. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 3rd ed., Addison–Wesley (1997).
- [9] O. Martin, A. M. Odlyzko and S. Wolfram, *Algebraic properties of cellular automata*, Comm. Math. Phys. **93** (1984), 219–258.
- [10] F. Lefebvre-Naré, *Iterated conjugation by a fixed cycle: the functional graph of $p \mapsto p s p^{-1}$ on n -cycles*, survey (2026).
- [11] 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 $p = 2$* , first version (2026).