

Conjugaison itérée par un cycle fixe : le graphe fonctionnel de $p \mapsto p s p^{-1}$ sur les n -cycles

Frédéric Lefebvre-Naré*

juillet 2026

Résumé

Fixons un n -cycle s et, en partant d'un n -cycle p quelconque, remplaçons-le de façon répétée par son conjugué $D(p) = p s p^{-1}$. De façon équivalente, D relit le mot des images en une ligne $(p(0), \dots, p(n-1))$ comme un cycle — un cousin par conjugaison de la transformation fondamentale classique. Itérer D organise les $(n-1)!$ n -cycles en un graphe fonctionnel, et cet article en dresse une première carte.

L'image a un centre net. Le cycle choisi s est l'unique point fixe, et conjuguer par s est une symétrie $\mathbb{Z}/n$ qui commute avec D ; le graphe tout entier est indépendant de s à réétiquetage près. Certains n -cycles sont finalement amenés jusqu'à s — ils forment l'*arbre entrant* de s — tandis que tous les autres se rangent dans d'autres orbites périodiques, de longueur au moins deux, chacune alimentée par son propre arbre entrant. Exactement $\varphi(n)$ cycles s'envoient directement sur s , et l'arbre entrant reste peu profond (profondeur 1) sauf si $8 \mid n$ ou $p^2 \mid n$ pour un premier impair, le seuil de Hull–Dobell ; au-delà l'arbre s'approfondit, et un article compagnon [2] en calcule la profondeur exacte (p^{e-1} pour p impair et $2^{e-1} - 1$ pour $p = 2$ lorsque $n = p^e$, et le plus grand de ces nombres sur les puissances de premiers divisant n en général).

La symétrie $\mathbb{Z}/n$ est le principe organisateur du reste du graphe. Elle impose des congruences sur les tailles des bassins, contraint quelles longueurs d'orbite et de queue peuvent apparaître (les deux contraintes s'avérant fines, avec des exceptions explicites pour de petits n), et fournit un décompte par crible cyclique des cycles fixés par la symétrie. Chemin faisant, la suite des tailles de bassins 1, 2, 2, 6, 7, 18, 17, 29, 56, 157 ($n \leq 12$) semble nouvelle. Nous concluons en opposant D à une application aléatoire uniforme : D dévie fortement de l'aléatoire, et le signe de l'écart suit lui-même l'arithmétique de n .

Classification MSC 2020 : 05A05, 20B30, 37P99. *Mots-clés* : n -cycles, conjugaison, graphe fonctionnel, bassins d'attraction, action de groupe cyclique, crible cyclique, indicatrice d'Euler, Hull–Dobell, motifs d'applications.

1 Introduction

Soit S_n le groupe symétrique sur $\mathbb{Z}/n = \{0, 1, \dots, n-1\}$, avec arithmétique modulo n partout. Soit $C(n) \subset S_n$ l'ensemble des n -cycles, de sorte que $|C(n)| = (n-1)!$. Fixons une fois pour toutes un n -cycle s ; le choix standard est $s_0 = (0\ 1 \cdots n-1)$, c'est-à-dire $s_0(i) = i+1 \bmod n$.

**Provenance et statut.* Les résultats ci-dessous ont été obtenus par des modèles d'intelligence artificielle (Claude, d'Anthropic) en dialogue interactif avec l'auteur, et les éléments de preuve ont ensuite été relus par des modèles d'OpenAI (principalement GPT-5.5) ; chaque affirmation numérique a été vérifiée par calcul fini exact. Le résultat de profondeur (§5) est démontré dans un article compagnon autonome [2]. Ceci demeure un rapport provisoire : une vérification de bout en bout de l'ensemble, ainsi qu'une relecture humaine par les pairs, restent à faire, et le texte doit être examiné de façon critique avant d'être utilisé.

Un n -cycle p peut se présenter de deux façons : par sa notation en cycle, par exemple $(0\ 2\ 4\ 3\ 1)$, ou par son mot d'images en une ligne $(p(0), p(1), \dots, p(n-1))$, ici $(2, 0, 4, 1, 3)$. La construction étudiée ici transforme la seconde présentation en la première : elle envoie $p = (0\ 2\ 4\ 3\ 1)$ sur $D(p) = (2\ 0\ 4\ 1\ 3)$.

Définition 1.1. La *dérivation* est l'application $D : C(n) \rightarrow C(n)$ qui envoie p sur le n -cycle écrit en notation de cycle $(p(0)\ p(1)\ \dots\ p(n-1))$; de façon équivalente, $D(p)$ est le n -cycle qui envoie $p(i)$ sur $p(i+1)$ pour tout i (indices modulo n).

Lemme 1.2. Avec $s = s_0$, on a $D(p) = p s p^{-1}$ pour tout $p \in C(n)$.

Démonstration. Par la Définition 1.1, $D(p)(p(i)) = p(i+1) = p(s(i))$ pour tout i , c'est-à-dire $D(p) \circ p = p \circ s$, d'où $D(p) = p s p^{-1}$. $\square$

Comme la conjugaison préserve le type de cycle, $p s p^{-1}$ est encore un n -cycle, donc D envoie $C(n)$ dans lui-même. Puisque $C(n)$ est fini, toute orbite avant $(D^k(p))_{k \geq 0}$ est finalement périodique : il existe $j < k$ minimaux avec $D^k(p) = D^j(p)$.

Définition 1.3. Le *graphe fonctionnel* de D a pour ensemble de sommets $C(n)$ et une arête orientée $p \rightarrow D(p)$ pour chaque p . Chaque composante faiblement connexe contient exactement un cycle orienté — une *orbite périodique* de D — auquel sont attachés des arbres entrants. Nous appelons ces composantes les *bassins*, et notons $P(n)$ la partition de $C(n)$ qui en résulte.

Une bijection classique identifie $C(n)$ à S_{n-1} . Écrivant le cycle de p comme $(0\ p(0)\ p^2(0)\ \dots\ p^{n-1}(0))$ et supprimant le 0 initial, on obtient la suite $(p(0), p^2(0), \dots, p^{n-1}(0))$, une permutation en une ligne de $\{1, \dots, n-1\}$; c'est une bijection $C(n) \rightarrow S_{n-1}$, une variante de la transformation fondamentale [6, 13]. Par elle, $C(n)$ s'identifie à l'ensemble des sommets du permutoèdre Π_{n-1} , que nous utilisons pour les figures.

Remarque 1.4. Le passage « relire le mot des images comme un cycle » est l'idée, par jeu de mots, derrière la transformation fondamentale de Foata [6], mais D n'est pas cette bijection. (Cette transformation écrit chaque cycle d'une permutation en commençant par son plus grand élément, ordonne les cycles par plus grand élément croissant, et efface les parenthèses pour lire le résultat comme un mot en une ligne, transformant le nombre de cycles en nombre de records de gauche à droite.) La transformation fondamentale est une bijection de S_n , ni équivariante par conjugaison ni un homomorphisme ; l'itérer partitionne S_n en les cycles purs (« circuits de Foata ») étudiés par Mason et Borghesan [11], qui observent qu'elle n'a pas de point fixe pour $n > 1$, de sorte que tout tel cycle est de longueur au moins deux. Notre D en diffère par deux aspects structurels. C'est une conjugaison par un cycle fixe, donc loin d'être injective (Proposition 3.2), si bien que son graphe fonctionnel porte de véritables arbres entrants et bassins plutôt que des cycles purs ; et c'est une endofonction de $C(n)$ ayant l'*unique* point fixe s (Proposition 3.1), alors que la transformation fondamentale n'en a aucun. Les deux applications ne partagent que le jeu de mots cycle/mot sous-jacent. Une autre famille non injective, les *opérateurs de tri* — le tri par pile de West et ses proches [14, 3] — porte de même des arbres entrants, mais draine toute permutation vers l'unique point fixe id en au plus $n-1$ itérations ; D scinde au contraire $C(n)$ en plusieurs bassins avec un spectre non trivial d'orbites périodiques.

La Figure 1 montre le plus petit cas intéressant, $n = 4$.

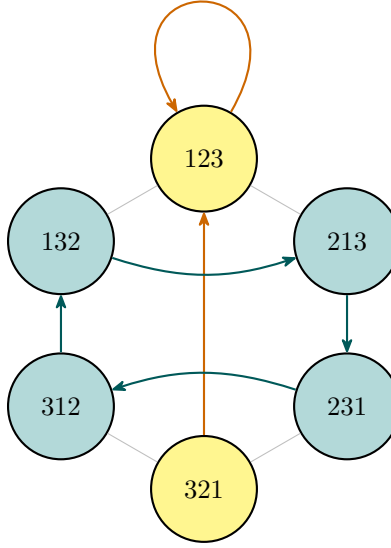


Figure 1: Le permutohédre Π_3 (hexagone), $n = 4$. Les sommets sont les six 4-cycles de $C(4)$, étiquetés par leurs mots de S_3 dans la coordonnée du §1 (par exemple $s = 123$ est le 4-cycle $(0\ 1\ 2\ 3)$ et 213 est $(0\ 2\ 1\ 3)$) ; les flèches sont D . Le point fixe $s = 123$ (boucle) et son unique prédécesseur 321 forment le bassin doré de taille 2 ; les quatre autres sommets forment un unique 4-cycle (sarcelle), de taille 4.

Résumé. La Section 2 montre que le système ne dépend que de n , et la Section 3 enregistre la structure élémentaire (s unique point fixe, D uniformément n -vers-1 comme $S_n \rightarrow C(n)$). La Section 4 introduit la symétrie $\mathbb{Z}/n$ commutante σ , calcule $\deg^-(s) = \varphi(n)$, et identifie la taille du bassin de s au critère de plein cycle de Hull–Dobell pour les applications affines — le pont principal de l'article vers une théorie classique. La Section 5 en développe les conséquences : σ -congruences sur les tailles de bassins (avec le théorème de Wilson comme cas premier), contraintes fines sur périodes et queues, une projection récursive $F_p \rightarrow C(n/p)$ réalisant le système comme une copie plus petite de lui-même, le collier d'attachement des arbres entrants, et — dans le régime de Hull–Dobell — la profondeur de l'arbre entrant de s , qu'une coordonnée de retenue linéarise sur une « fibre racine » réalisant les plus longues chaînes ; la profondeur exacte p^{e-1} (resp. $2^{e-1} - 1$) est démontrée dans le compagnon [2]. La Section 6 situe D face à une application aléatoire ; la Section 7 donne les décomptes de points σ -fixes (généralisant Wilson), qui ne réalisent un crible cyclique que tautologiquement, de sorte que le contenu est le décompte lui-même. La Section 8 liste des problèmes ouverts.

2 Indépendance du cycle choisi

Théorème 2.1. Soient s, s' deux n -cycles et écrivons $s' = g s g^{-1}$ (possible car tous les n -cycles sont conjugués). La conjugaison par g , $\sigma_g : C(n) \rightarrow C(n)$, $\sigma_g(p) = g p g^{-1}$, est une bijection avec

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

où $D_t(p) = p t p^{-1}$ (la seconde identité n'est que la loi d'homomorphisme $\sigma_g \sigma_s \sigma_g^{-1} = \sigma_{g s g^{-1}} = \sigma_{s'}$). Ainsi $(C(n), D_s, \sigma_s) \cong (C(n), D_{s'}, \sigma_{s'})$ comme systèmes dynamiques à symétrie ; g est déterminé à multiplication à droite par $\langle s \rangle$ près.

Démonstration. $D_{s'}(\sigma_g(p)) = (gpg^{-1})(gsg^{-1})(gp^{-1}g^{-1}) = g(psp^{-1})g^{-1} = \sigma_g(D_s(p))$, et $\sigma_g\sigma_s\sigma_g^{-1}(q) = g s (g^{-1}qg) s^{-1}g^{-1} = s'qs'^{-1} = \sigma_{s'}(q)$. Les solutions de $s' = gsg^{-1}$ forment la classe $gC_{S_n}(s) = g\langle s \rangle$. $\square$

Corollaire 2.2. *Tout invariant d'isomorphisme du graphe fonctionnel — le nombre de bassins, le multi-ensemble des paires (période, taille de bassin), la partition $P(n)$ entière, et la symétrie $\mathbb{Z}/n$ — ne dépend que de n . Le cycle standard s_0 n'est qu'une coordonnée commode ; aucun n -cycle n'est dynamiquement distingué.*

Nous l'avons vérifié numériquement : pour tout 6-cycle s la signature de bassins égale celle de la Table 1, et l'unique point fixe est toujours s lui-même. Désormais nous fixons $s = s_0$.

3 Structure élémentaire

Proposition 3.1. *s est l'unique point fixe de D dans $S_n : D(p) = p$ si et seulement si $p = s$.*

Démonstration. Multipliant $psp^{-1} = p$ à gauche par p^{-1} on obtient $sp^{-1} = e$, donc $p = s$; réciproquement $D(s) = s$. $\square$

Proposition 3.2. *Comme application $D : S_n \rightarrow S_n$, l'image de D est exactement $C(n)$, et D est uniformément n -vers-1 sur $C(n)$: chaque fibre $D^{-1}(q)$ est une classe de $\langle s \rangle$ de taille n . Toute permutation qui n'est pas un n -cycle a degré entrant 0 et s'envoie en un pas dans $C(n)$.*

Démonstration. $D(p) = D(p')$ ssi $(p'^{-1}p)s(p'^{-1}p)^{-1} = s$ ssi $p'^{-1}p \in C_{S_n}(s) = \langle s \rangle$; donc les fibres sont les classes $p\langle s \rangle$, de taille n , et l'image est la classe de conjugaison de s , à savoir $C(n)$. Toute préimage r de q vérifie $rsr^{-1} = q$, donc q n'a de préimage que si $q \in C(n)$; ainsi un non- n -cycle a degré entrant 0. $\square$

La description informelle des non- n -cycles comme feuilles greffées sur la structure périodique est rendue précise — et quantitative — par le résultat suivant, qui enregistre aussi comment se comportent les cardinaux de bassins sous l'extension du domaine à tout S_n .

Proposition 3.3. *Étendons D à S_n . Chaque $q \in C(n)$ a degré entrant exactement n dans S_n , portant $n - \deg_{C(n)}^-(q)$ feuilles pendantes (des non- n -cycles), où $\deg_{C(n)}^-(q)$ est son degré entrant au sein de $C(n)$. Par conséquent, pour chaque bassin $B \subseteq C(n)$ du système restreint, le bassin correspondant dans S_n a taille exactement $n|B|$: la partition $P(n)$ est préservée à un facteur de dilatation global n près, et le total devient $n(n-1)! = n!$.*

Démonstration. Le degré entrant n est la taille de fibre de la Proposition 3.2. Dans le graphe restreint chaque sommet a degré sortant 1 d'image dans B , donc le nombre d'arêtes internes à B égale $|B|$, c'est-à-dire $\sum_{q \in B} \deg_{C(n)}^-(q) = |B|$. Ainsi les feuilles sur B comptent $\sum_{q \in B} (n - \deg_{C(n)}^-(q)) = (n-1)|B|$, et le bassin dans S_n a taille $|B| + (n-1)|B| = n|B|$. $\square$

Remarque 3.4. Les feuilles s'attachent directement au n -cycle dont elles sont l'image, à toute profondeur de l'arbre (y compris sur des sommets périodiques) ; par exemple s lui-même porte $n - \varphi(n)$ feuilles. Les hauteurs d'arbre augmentent d'au plus un.

4 La symétrie cyclique

Théorème 4.1. *Soit $n \geq 3$ et $\sigma(p) = s p s^{-1}$. Alors $\sigma \circ D = D \circ \sigma$, et $\langle \sigma \rangle \cong \mathbb{Z}/n$ agit sur $C(n)$ par automorphismes du graphe fonctionnel. (À $n = 2$, $C(n) = \{s\}$ est un point unique et σ est triviale, s étant central dans S_2 .)*

Démonstration. $D(\sigma p) = (s p s^{-1}) s (s p^{-1} s^{-1}) = s (p s p^{-1}) s^{-1} = \sigma(Dp)$. Pour $n \geq 3$, $\sigma^k = \text{id}$ ssi $s^k \in Z(S_n) = \{e\}$ ssi $n \mid k$, donc σ est d'ordre n . $\square$

Corollaire 4.2. *$\langle \sigma \rangle$ permute les bassins ; les bassins d'une même σ -orbite sont isomorphes (même période, même taille), et les tailles de σ -orbites divisent n (orbite-stabilisateur, le stabilisateur de p étant $\langle s \rangle \cap \langle p \rangle$). Les points fixes de σ sont exactement les $\varphi(n)$ générateurs $\{s^a : \gcd(a, n) = 1\}$ de $\langle s \rangle$, et $\deg_{C(n)}^-(s) = \varphi(n)$.*

Démonstration. Les premières affirmations découlent du Théorème 4.1 et d'orbite-stabilisateur. $\sigma(p) = p$ ssi $s \in \langle p \rangle$; comme $|\langle s \rangle| = |\langle p \rangle| = n$, cela force $\langle p \rangle = \langle s \rangle$, c'est-à-dire p générateur. Enfin $D^{-1}(s) \cap C(n) = \langle s \rangle \cap C(n)$ a $\varphi(n)$ éléments. $\square$

Chaque générateur vérifie $D(s^a) = s^a s s^{-a} = s$, donc les $\varphi(n)$ rotations sont les prédécesseurs immédiats de s . Que le bassin de s consiste exactement en celles-ci, ou soit strictement plus grand, est un seuil de nature arithmétique.

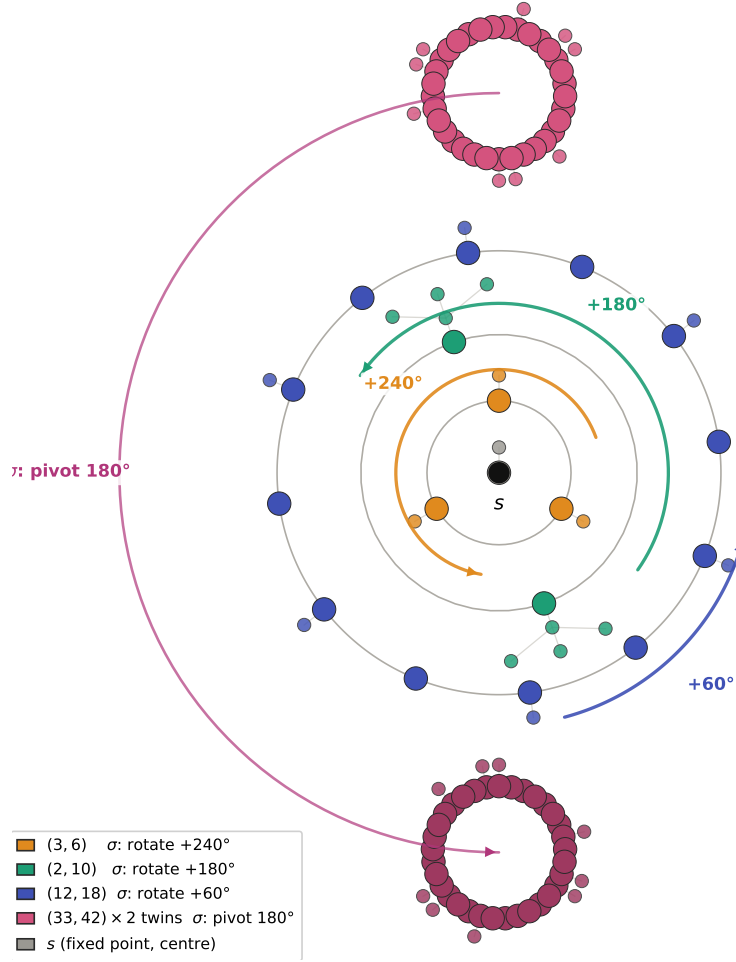


Figure 2: Le système de bassins à $n = 6$ dessiné en diagramme polaire centré sur s , choisi de sorte que σ agisse par rotation (Théorème 4.1, Corollaire 4.2). Le point fixe s est au centre ; chaque bassin σ -invariant est un anneau concentrique de ses n -cycles périodiques (reliés par D , dessinés dans le sens antihoraire), avec les arbres entrants attachés en pendentifs clairs. Un pas de σ fait tourner rigidelement chaque anneau autour de s de sa propre quantité, marquée par une flèche en arc : $+60^\circ$ sur (12, 18), $+180^\circ$ sur (2, 10), $+240^\circ$ sur (3, 6). Ces angles valent $2\pi r/P$ où $\sigma|_O = (D|_O)^r$; dès que $P \mid n$ on a $r \equiv -1$, c'est-à-dire σ agit comme D^{-1} — un pas en arrière, donc $2\pi(P-1)/P$. Les deux bassins isomorphes (33, 42) forment une σ -orbite de taille deux : placés en antipodes, ils sont échangés par un pivot de 180° . La couleur code la classe d'isomorphisme $(P, |B|)$. Ce que l'image fixe, c'est l'action rotationnelle de σ (chaque anneau, et l'amas, tournant rigidelement autour de s) ; les rayons, l'ordre des bassins et les phases initiales sont des conventions de dessin. Produit par `code/viz_polarN.py`.

Proposition 4.3. $|\text{basin}(s)| = \varphi(n)$ si et seulement si aucune application affine $x \mapsto ax + b$ sur $\mathbb{Z}/n$ avec $a \not\equiv 1$ n'est un n -cycle unique. Par le théorème de Hull–Dobell [7], une telle application affine non-translation de plein cycle existe si et seulement si $8 \mid n$ ou $p^2 \mid n$ pour un premier impair p . Dans ce cas les rotations acquièrent des préimages n -cycliques et le bassin est strictement plus grand.

Démonstration. Les D -préimages d'une rotation s^a dans $C(n)$ sont les n -cycles parmi les conjuga-

teurs de s vers s^a , qui sont précisément les applications affines $x \mapsto ax + b$. Pour $a = 1$ ce sont les translations, de plein cycle ssi $\gcd(b, n) = 1$ — les rotations elles-mêmes. Pour $a \not\equiv 1 \pmod{p}$, Hull–Dobell affirme que $x \mapsto ax + b$ est un n -cycle plein ssi $\gcd(b, n) = 1$, $a \equiv 1 \pmod{p}$ pour tout premier $p \mid n$, et $a \equiv 1 \pmod{4}$ quand $4 \mid n$. Une unité $a \not\equiv 1$ satisfaisant ces conditions existe ssi $p^2 \mid n$ pour un premier impair, ou $8 \mid n$. En l’absence d’un tel a , les rotations $s^a \neq s$ sont des sources, chacune s’envoyant en un pas sur le point fixe s (qui a donc degré entrant $\varphi(n)$ et n’est lui-même pas une source), et le bassin est simplement les $\varphi(n)$ rotations ; sinon l’arbre entrant s’approfondit. $\square$

La Proposition 4.3 compte les préimages d’une rotation ; l’application avant sur les cycles affines est tout aussi explicite et fixe leur place dans l’arbre.

Lemme 4.4 (Applications affines et multiplicateur). *Si $p: x \mapsto ax + b$ est une application affine sur $\mathbb{Z}/n$ qui est un n -cycle unique, alors*

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

Ainsi D ramène le multiplicateur à 1 : un n -cycle affine atteint s en au plus deux pas, $p \rightarrow s^a \rightarrow s$, de sorte que les n -cycles affines n’occupent que les deux couches supérieures de l’arbre entrant de s . Par Hull–Dobell les multiplicateurs admissibles sont les unités $a \equiv 1 \pmod{q}$ pour tout premier $q \mid n$ (et $a \equiv 1 \pmod{4}$ quand $4 \mid n$). Pour $n = p^e$ avec p impair ils forment le p -sous-groupe de Sylow de $(\mathbb{Z}/n)^\times$, cyclique d’ordre p^{e-1} . Pour $n = 2^e$ ($e \geq 2$) ils forment $\{a \equiv 1 \pmod{4}\} = \langle 5 \rangle$, cyclique d’ordre 2^{e-2} ; pour $e \geq 3$ c’est un sous-groupe propre d’indice 2 du 2-groupe non cyclique $(\mathbb{Z}/2^e)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{e-2}$, et pas son 2-Sylow (qui est le groupe des unités tout entier, d’ordre 2^{e-1}).

Démonstration. De $p^{-1}(x) = a^{-1}(x - b)$ on obtient $D(p)(x) = p s p^{-1}(x) = a(a^{-1}(x - b) + 1) + b = x + a$, c’est-à-dire $D(p) = s^a$. Appliqué à la rotation s^a (l’application affine de multiplicateur 1) cela donne $D(s^a) = s$. La condition d’admissibilité sur a est exactement le critère de Hull–Dobell de la Proposition 4.3 ; pour une puissance de premier impair il découpe le p -Sylow du groupe des unités, tandis que pour $n = 2^e$ il découpe le sous-groupe cyclique d’indice 2 $\langle 5 \rangle$ des unités $\equiv 1 \pmod{4}$. $\square$

Le même critère de plein cycle sous-tend les générateurs congruents linéaires de pleine période [10] et les T -fonctions à cycle unique [8]. Numériquement, $|\text{basin}(s)| = \varphi(n)$ pour $n \leq 7$ et $n = 10, \dots, 15$, tandis que $|\text{basin}(s)| = 16, 36, 2048, 36, 32, 10000, 472392$ pour $n = 8, 9, 16, 18, 24, 25, 27$ — exactement les n divisibles par 8 ou par un carré impair. L’invariant $\deg_{C(n)}^-(s) = \varphi(n)$ vaut pour tout n .

La Figure 3 présente les bassins sur Π_4 et Π_5 .

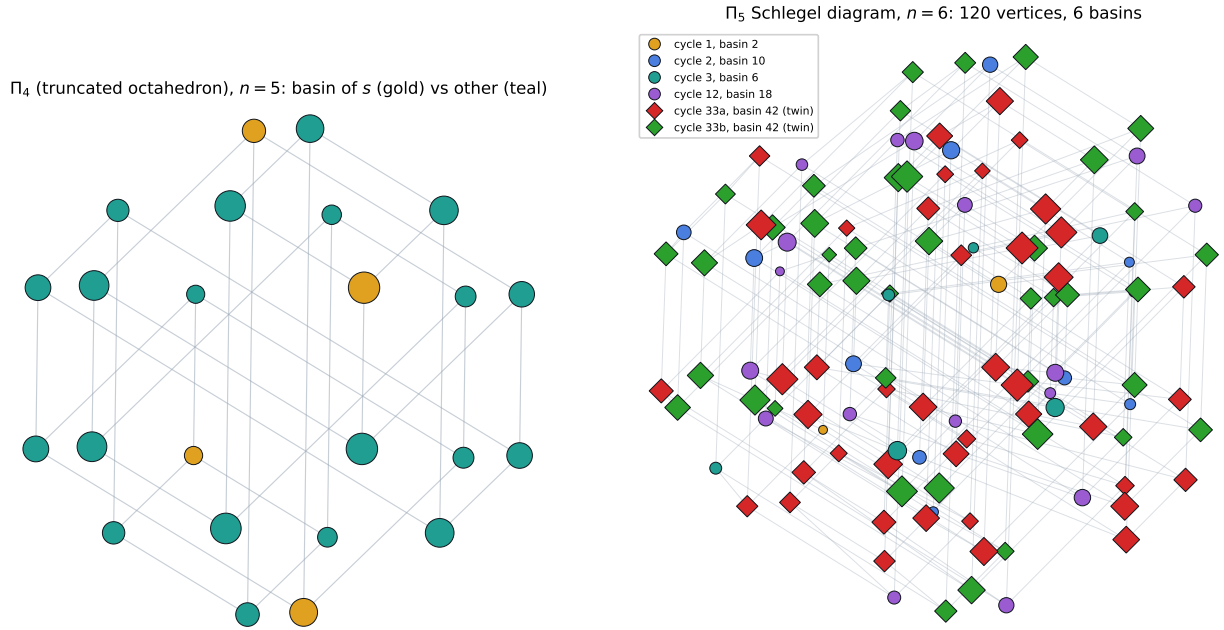


Figure 3: À gauche : le permutoèdre Π_4 (octaèdre tronqué), $n = 5$, colorié par bassin (doré : le bassin de s , taille 4 ; sarcelle : l'autre bassin, taille 20). À droite : un diagramme de Schlegel du permutoèdre de dimension 4, Π_5 , $n = 6$, avec 120 sommets coloriés selon les six bassins ; les deux bassins de taille 42 (les losanges rouge et vert) sont échangés par σ .

5 Périodes, queues, et forme des bassins

Les structures globales qui suivent — l'action de σ sur les bassins, les congruences modulo p sur leurs tailles, les contraintes sur périodes et queues, les colliers d'attachement, et le crible cyclique — sont toutes des facettes d'une seule propriété : la symétrie $\mathbb{Z}/n$ commutant avec D (Théorème 4.1). La projection récursive $F_p \rightarrow C(n/p)$ est la seule structure véritablement plus fine, faisant intervenir la structure de blocs emboîtés (produit en couronne) des puissances de s .

Par le Corollaire 4.2, les bassins d'un type d'isomorphisme commun qui ne sont pas σ -fixes apparaissent avec une multiplicité divisible par leur taille de σ -orbite, un diviseur de n supérieur à 1 ; par exemple les deux bassins de taille 42 à $n = 6$ (Table 1) forment une σ -orbite de taille 2. Nous montrons maintenant que σ contraint aussi les tailles de bassins elles-mêmes.

Pour un premier $p \mid n$, posons $g = s^{n/p}$ (un élément d'ordre p , produit de n/p p -cycles disjoints) et

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

Théorème 5.1. F_p est invariant sous σ et sous D . Pour tout bassin σ -invariant B ,

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

Un bassin rencontre F_p seulement si son orbite périodique est dans F_p ; donc un bassin σ -invariant dont l'orbite périodique n'est pas $\sigma^{n/p}$ -symétrique a une taille divisible par p . Pour un bassin non σ -invariant, la congruence s'applique à sa σ -orbite entière, pas au bassin seul.

Démonstration. Pour $q \in F_p$, $\sigma^{n/p}(Dq) = D(\sigma^{n/p}q) = Dq$ par le Théorème 4.1, donc $Dq \in F_p$; ainsi F_p est invariant vers l'avant par D (et visiblement σ -invariant). Le groupe $\langle \sigma^{n/p} \rangle \cong \mathbb{Z}/p$ agit

sur l'ensemble σ -invariant B avec des orbites de taille 1 ou p , les orbites de taille 1 étant $B \cap F_p$; le décompte donne la congruence. Si $B \cap F_p \neq \emptyset$, l'orbite avant d'un point de $B \cap F_p$ reste dans F_p et atteint l'unique orbite périodique de B , qui est donc dans F_p . $\square$

Théorème 5.2. *Pour chaque premier $p \mid n$,*

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

Démonstration. Comme $\langle g \rangle$ est cyclique d'ordre n il a un unique sous-groupe d'ordre p , à savoir $\langle g^{n/p} \rangle$; ainsi $g \in \langle g \rangle$ ssi $q^{n/p} \in \{g, g^2, \dots, g^{p-1}\}$, donc $|F_p| = \sum_{m=1}^{p-1} \#\{q \in C(n) : q^{n/p} = g^m\}$. Les cibles g^m ont un même type de cycle, donc les sommes sont égales ; notons A la valeur commune, d'où $|F_p| = (p-1)A$.

Posons $d = n/p$. Tout q avec $q^d = g$ commute avec g , donc appartient à $C_{S_n}(g) \cong \mathbb{Z}/p \wr S_d = (\mathbb{Z}/p)^d \rtimes S_d$. Identifions chaque bloc (un p -cycle de g) à $\mathbb{Z}/p$ de sorte que g agisse par $+1$; un élément $(\vec{a}, \tau)$ envoie le résidu i du bloc j sur le résidu $i + a_j$ du bloc $\tau(j)$. Si τ est un d -cycle unique alors $(\vec{a}, \tau)^d$ fixe chaque bloc et y agit par $+T$ avec $T = \sum_j a_j$; donc $(\vec{a}, \tau)^d = g^T$, et $(\vec{a}, \tau)$ est un n -cycle unique ssi $T \not\equiv 0 \pmod{p}$. Ainsi $q^d = g$ ssi τ est un d -cycle et $T \equiv 1 \pmod{p}$ (ce qui force aussi la condition de cycle unique). Il y a $(d-1)!$ tels τ et p^{d-1} vecteurs $\vec{a}$ avec $\sum a_j \equiv 1$, donc $A = (d-1)! p^{d-1}$. $\square$

Corollaire 5.3 (Cas premier et Wilson). *Si $n = p$ est premier alors F_p est l'ensemble des $p-1$ rotations, toutes dans $\text{basin}(s)$ (de taille $p-1$) ; donc tout bassin σ -invariant autre que $\text{basin}(s)$ a une taille divisible par p . Un bassin non invariant n'y est pas tenu — à $n = 11$ la σ -orbite $(P, |B|) = (3, 56)$, répétée 11 fois, a $56 \not\equiv 0 \pmod{11}$ — mais une telle orbite consiste en p bassins isomorphes, donc sa réunion est divisible par p . De plus le décompte de Burnside pour l'action $\mathbb{Z}/p$ de $\sigma^{n/p}$ sur $C(n)$ donne $(n-1)! \equiv |F_p| \pmod{p}$; pour $n = p$ c'est $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$, le théorème de Wilson.*

Les valeurs $|F_p|$ (Table 2) ont été confirmées par énumération directe. Pour les bassins σ -invariants elles fixent le résidu modulo $\text{rad}(n)$ et confinent la rupture de divisibilité à ceux ayant des orbites périodiques symétriques ; les bassins non invariants ne sont contraints qu'à travers leur σ -orbite, et la distribution précise reste véritablement dynamique.

Proposition 5.4 (Périodes pour n premier). *Soit $n = p$ premier. Parmi les points périodiques de D , le seul σ -fixe est s ; par conséquent le nombre de points périodiques non fixes est un multiple de p . Si σ envoie une orbite périodique non fixe sur elle-même, alors p divise sa longueur ; donc toute période non fixe est un multiple de p , à une exception près : une période non divisible par p est nécessairement partagée par un multiple de p orbites, aucune d'elles n'étant σ -stable.*

Démonstration. Pour $n = p$ l'application σ est d'ordre p , et ses points fixes sont les $p-1$ rotations s^a (Corollaire 4.2). Parmi celles-ci seule s est périodique : $D(s^a) = s$ pour tout a , donc s^a avec $a \neq 1$ quitte sa position sous D et n'y revient jamais. Ainsi l'action $\mathbb{Z}/p$ de σ sur l'ensemble U des points périodiques a l'unique point fixe s ; comme p est premier toutes les autres σ -orbites de U ont taille p , donc $|U| \equiv 1 \pmod{p}$ et $|U| - 1$ est un multiple de p .

Soit maintenant O une orbite périodique non fixe avec $\sigma(O) = O$ et $|O| = \ell$. Alors $\sigma|_O$ commute avec le ℓ -cycle $D|_O$, donc en est une puissance (le centralisateur d'un ℓ -cycle est le groupe cyclique qu'il engendre). Cette puissance est non triviale, sinon tout point de O serait σ -fixe, forçant $O = \{s\}$; elle a donc un ordre > 1 divisant p , c'est-à-dire d'ordre p , et $p \mid \ell$. Enfin, σ permute les orbites périodiques de toute longueur fixée ℓ en orbites de taille 1 ou p ; une orbite de taille 1 est une orbite périodique σ -stable, pour laquelle le paragraphe précédent donne $p \mid \ell$. Ainsi si $p \nmid \ell$ alors toute

orbite de longueur ℓ est σ -instable, donc ces orbites tombent dans des σ -orbites de taille p , et leur nombre est un multiple de p . $\square$

Par exemple les périodes non fixes sont $\{5\}$ à $n = 5$ et $\{7, 7, 14, 14, 35, 49\}$ à $n = 7$, toutes multiples de n , aucune longueur n'étant partagée par un multiple de n orbites.

L'argument de la Proposition 5.4 s'étend à n composé et se passe de la réserve « longueur partagée » dès qu'on le mène sur le stabilisateur ensembliste d'une seule orbite.

Proposition 5.5 (Les périodes rencontrent n). *Soit O une orbite périodique non fixe de D sur $C(n)$, de longueur ℓ , et soit $\langle \sigma^t \rangle$ avec $t \mid n$ son stabilisateur ensembliste dans $\langle \sigma \rangle$ (donc t est la taille de la $\langle \sigma \rangle$ -orbite de O parmi les orbites périodiques). Si σ^t n'agit pas comme l'identité sur O , alors $\gcd(\ell, n) > 1$; c'est-à-dire ℓ partage un facteur premier avec n .*

Démonstration. Par construction σ^t stabilise O ensemblistement, et commute avec D ; donc $\sigma^t|_O$ appartient au centralisateur du ℓ -cycle $D|_O$ dans $\text{Sym}(O)$, qui est $\langle D|_O \rangle$. Ainsi $\sigma^t|_O$ est une puissance d'un ℓ -cycle, et étant non trivial par hypothèse son ordre $e > 1$ divise ℓ . Le même élément a un ordre divisant celui de σ^t , à savoir $n/\gcd(t, n) = n/t$. Donc $e \mid \gcd(\ell, n/t)$, d'où $\gcd(\ell, n) \geq \gcd(\ell, n/t) \geq e > 1$. $\square$

Ceci contient la Proposition 5.4 : pour n premier une orbite non fixe σ -stable a $t = 1$, sur laquelle σ agit non trivialement (l'unique point périodique σ -fixe étant s), donnant $p \mid \ell$; une orbite dans une σ -orbite de taille p a au contraire $t = p$, où $\sigma^t = \sigma^p = \text{id}$ agit trivialement — le cas exclu « longueur partagée », où la conclusion peut échouer (Remarque 5.6). Quand l'hypothèse tient, écrire $\ell = dm$ avec $d = \gcd(\ell, n) > 1$ un diviseur de n exhibe toute période non fixe comme une « graine » forcée d fois un cofacteur libre m portant la croissance irrégulière ($m = 11$ dans $33 = 3 \cdot 11$ à $n = 6$, $m = 7$ dans 49 à $n = 7$, $m = 6$ dans 54 à $n = 9$). L'unique hypothèse est que le stabilisateur ensembliste agisse non trivialement sur O ; de façon équivalente $s^t \notin \bigcap_{q \in O} \langle q \rangle$ pour $O \neq \{s\}$. Elle vaut pour toute orbite non fixe à $n \leq 9$ — la seule orbite sur laquelle le stabilisateur ensembliste agit trivialement est alors $\{s\}$ lui-même (déjà à $n = 10$ les cinq orbites de période 15 forment une σ -orbite sur laquelle σ^5 agit trivialement) — mais, comme son hypothèse, la conclusion n'est *pas* universelle.

Remarque 5.6 ($\gcd(\ell, n) > 1$ peut échouer). Au premier $n = 11$ la dérivation a des orbites périodiques non fixes de longueurs $\ell = 3, 9, 72$, chacune *première* avec 11. (Vérifié sur le graphe fonctionnel complet ; les périodes 3 et 9 ont été revérifiées directement, $D^3 = \text{id}$ et $D^9 = \text{id}$ sur les 11-cycles respectifs.) Chaque telle longueur apparaît avec multiplicité 11 : les onze orbites forment une seule $\langle \sigma \rangle$ -orbite, donc le stabilisateur ensembliste de l'une quelconque d'elles est trivial ($t = n = 11$, $\sigma^t = \text{id}$) et agit trivialement — exactement la configuration exclue, le « cas B » anticipé pour n premier dans la Proposition 5.4. Ainsi la lecture inconditionnelle « toute période non fixe partage un premier avec n » est fausse ; l'hypothèse de la Proposition 5.5 est essentielle. Les composés $n = 10, 12$ n'exhibent aucune période première avec n , donc le phénomène n'est pas qu'une affaire de taille.

La même rotation gouverne la façon dont les arbres entrants s'attachent à un cycle périodique.

Proposition 5.7 (Collier d'attachement). *Soit B un bassin de cycle périodique O de longueur P et de stabilisateur ensembliste $\langle \sigma^t \rangle$ dans $\langle \sigma \rangle$. Alors $\sigma^t|_O = (D|_O)^r$ est une rotation de O d'un pas r , d'ordre $P/\gcd(r, P)$ divisant n/t . Comme σ^t est un automorphisme du graphe fonctionnel il préserve le degré entrant, donc la suite $(\deg_{C(n)}^-(q))_{q \in O}$ — de façon équivalente les décomptes d'attachement d'arbres $\deg_{C(n)}^-(q) - 1$, l'unique préimage restante étant le prédécesseur cyclique — est un collier*

invariant sous cette rotation : sa période divise $\gcd(r, P)$. En particulier, quand r est premier avec P le degré entrant est constant autour de O .

Démonstration. σ^t stabilise O et commute avec D , donc $\sigma^t|_O$ centralise le P -cycle $D|_O$, d'où égal à $(D|_O)^r$ pour un certain r , d'ordre $P/\gcd(r, P)$ divisant $\text{ord}(\sigma^t) = n/t$. Étant un automorphisme de graphe, σ^t vérifie $\deg^-(\sigma^t q) = \deg^-(q)$, donc le degré entrant est constant sur les orbites de rotation-par- r de O , et sa période divise $\gcd(r, P)$. $\square$

Par exemple à $n = 7$ le bassin $(P, |B|) = (35, 119)$ a un collier de degré entrant de période 5 et $(49, 511)$ de période 7 (leurs cofacteurs $\ell/\gcd(\ell, n)$), tandis que les bassins de période 7 et 14 ont degré entrant constant 2 ; la borne a été vérifiée pour les 52 bassins à $n \leq 9$ (8 sont encore plus symétriques, à degré entrant constant). Le bassin de s est le cas dégénéré $P = 1$, $\deg^-(s) = \varphi(n)$ (Corollaire 4.2).

Pour un bassin σ -invariant cela fixe la période du collier au cofacteur de la période, donnant au cofacteur un sens géométrique.

Observation 5.8 (Le cofacteur est la période du collier). Pour tout bassin σ -invariant à $n \leq 9$, $\sigma|_O$ est une rotation d'ordre exactement $d = \gcd(P, n)$ (la graine) ; le cycle se scinde donc en $m = P/d = \ell/\gcd(\ell, n)$ σ -orbites, de taille d , sur chacune desquelles le degré entrant est constant. Le collier d'attachement a ainsi une période divisant le cofacteur m , avec égalité dans le cas générique ; de façon équivalente l'anneau des degrés entrants porte une symétrie de rotation d'ordre d construite à partir d'un motif de longueur m (donc $P = dm$). L'ordre de symétrie est n exactement quand $n \mid P$. Ainsi le cofacteur de la période, autrement inexplicable (Proposition 5.5), se réalise comme le nombre de σ -orbites de points périodiques du bassin — la période de son collier d'attachement. (Pour les σ -jumeaux, $t > 1$, l'analogue utilise σ^t : par exemple les deux bassins $(33, 42)$ à $n = 6$ montrent une symétrie d'ordre 3 sur un motif de longueur 11, leur cofacteur sauvage.) Voir la Figure 4.

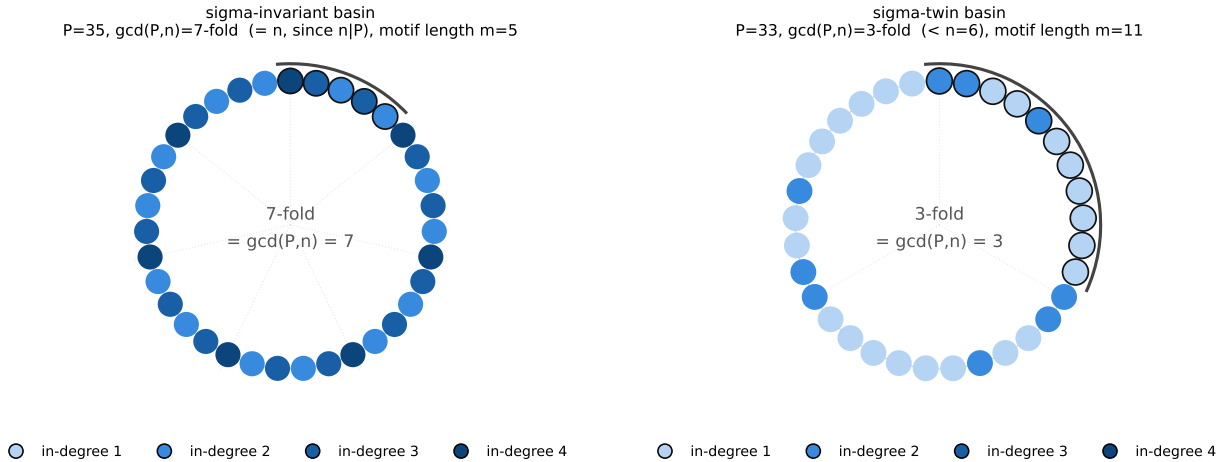


Figure 4: Colliers d'attachement (Observation 5.8). Chaque point est un n -cycle périodique sur l'attracteur d'un bassin, placé dans l'ordre de D autour de l'anneau et colorié par degré entrant (le nombre d'arbres attachés est $\deg_{C(n)}^- - 1$) ; un motif est encadré et les répétitions sont séparées par des rayons. À gauche : le bassin σ -invariant $(P, |B|) = (35, 119)$ à $n = 7$; $\sigma|_O$ est d'ordre $\gcd(35, 7) = 7$, donc l'anneau a une symétrie d'ordre 7 ($= n$ ici, puisque $7 \mid 35$) construite à partir d'un motif de longueur $m = 5$. À droite : un σ -jumeau $(33, 42)$ à $n = 6$, de symétrie d'ordre $\gcd(33, 6) = 3$ ($< n$) sur un motif de longueur 11 — son cofacteur sauvage.

Nous nous tournons vers la population hors orbite d'un bassin. Écrivons $P = |O|$ pour la période d'un bassin B d'attracteur O , et $T = |B| - P$ pour sa *queue* (les sommets non périodiques). Les σ -congruences du Théorème 5.1 contraignent P et T *conjointement*.

Proposition 5.9 (La queue reflète la période). *Soit B un bassin $\sigma^{n/p}$ -invariant d'attracteur O , de période P et queue T , pour un premier $p \mid n$. Si $O \not\subseteq F_p$, alors $p \mid P$ et $p \mid T$.*

Démonstration. En tant qu'automorphisme de graphe σ préserve l'ensemble des sommets périodiques et son complémentaire ; comme $\sigma^{n/p}(B) = B$ il s'ensuit que O et la queue $B \setminus O$ sont chacun $\sigma^{n/p}$ -invariants. Le groupe $\langle \sigma^{n/p} \rangle \cong \mathbb{Z}/p$ agit sur chacun avec des orbites de taille 1 ou p , les singletons étant les points fixés par $\sigma^{n/p}$, c'est-à-dire l'intersection avec F_p ; le décompte modulo p donne

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

Par le Théorème 5.1 un bassin rencontre F_p seulement si son attracteur est dans F_p ; comme $O \not\subseteq F_p$ on a $B \cap F_p = \emptyset$, donc les deux membres de droite s'annulent et $p \mid P, p \mid T$. $\square$

L'hypothèse $O \not\subseteq F_p$ est exactement $\sigma^{n/p}|_O \neq \text{id}$, et force à elle seule $p \mid P$ (une puissance non triviale du P -cycle $D|_O$ a ordre p) ; le contenu de la proposition est qu'elle force aussi $p \mid T$, de sorte que période et queue d'un tel bassin portent les *mêmes* diviseurs premiers de n . À $n \leq 9$ cela couvre tous les bassins sauf deux sortes : ceux à attracteur $\sigma^{n/p}$ -symétrique ($O \subseteq F_p$), qui sont précisément les bassins où la divisibilité du Théorème 5.1 échoue, et le rare σ -jumeau non individuellement $\sigma^{n/p}$ -invariant (les deux bassins (33, 42) à $n = 6$, échangés par σ^3). Sur les deux sortes la loi $p \mid P \Leftrightarrow p \mid T$ se trouve valoir pour $n \leq 9$, mais — contrairement à la proposition — ce n'est *pas* un théorème : elle échoue à partir de $n = 12$ (Remarque 5.13 ci-dessous). L'hypothèse $O \not\subseteq F_p$ est donc essentielle, et une projection de F_p sur une copie plus petite du même système, que nous précisons maintenant, atteint à la fois ces plus grands n à peu de frais et explique l'échec.

Une projection récursive du réservoir symétrique

Fixons un premier $p \mid n$, posons $d = n/p$ et $g = s^{n/p}$. Comme dans le Théorème 5.2, g est un produit de d p -cycles disjoints — ses orbites sont les classes de résidus $B_r = \{r, r + d, \dots, r + (p - 1)d\}$, $0 \leq r < d$ — et $C_{S_n}(g) \cong \mathbb{Z}/p \wr S_d$. Tout $q \in F_p$ commute avec g et permute donc les blocs ; soit $\pi(q) \in S_d$ la permutation de blocs induite, $\pi(q)(r) = q(r) \bmod d$.

Proposition 5.10 (Projection récursive). *L'application $\pi: F_p \rightarrow S_d$ prend ses valeurs dans $C(d)$, est surjective, et a toute fibre de taille $(p - 1)p^{d-1}$. De plus $\pi(s) = s_d$ (le d -cycle standard), et*

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

où D_d, σ_d sont la dérivation et la symétrie cyclique sur $C(d)$. Ainsi π est une semiconjugaison (une application-facteur de systèmes dynamiques), envoyant le graphe fonctionnel de D sur F_p sur celui de D_d sur $C(d)$, de façon équivariante pour $\langle \sigma \rangle \twoheadrightarrow \langle \sigma_d \rangle$ (avec $\sigma^d \mapsto \text{id}$).

Démonstration. Puisque $g \in \langle q \rangle$, q commute avec g et permute donc ses orbites ; de $q(r + jd) = q(g^j r) = g^j q(r) = q(r) + jd$ la valeur $q(r) \bmod d$ est indépendante du représentant, donc $\pi(q)$ est la véritable permutation de blocs et π est la restriction de l'homomorphisme quotient $C_{S_n}(g) = \mathbb{Z}/p \wr S_d \twoheadrightarrow S_d$. Écrivant $q = (\vec{a}, \tau)$ avec $\tau = \pi(q)$, le calcul du Théorème 5.2 montre que q est un n -cycle unique ssi τ est un d -cycle et $\sum_j a_j \not\equiv 0 \pmod{p}$, ce qui est aussi la condition $g \in \langle q \rangle$; donc $\pi(F_p) \subseteq C(d)$, et sur chaque d -cycle la fibre $\{\vec{a} : \sum a_j \not\equiv 0\}$ a $p^d - p^{d-1} = (p - 1)p^{d-1}$ éléments, donc π est surjective et uniformément $(p - 1)p^{d-1}$ -vers-un. (Ceci retrouve $|F_p| = (d - 1)!(p - 1)p^{d-1}$.) Étant

un homomorphisme restreint aux éléments de $C_{S_n}(g)$, π vérifie $\pi(s) = s_d$ (car s envoie $r \mapsto r + 1$ sur les blocs), $\pi(Dq) = \pi(q)\pi(s)\pi(q)^{-1} = D_d(\pi q)$ et de même $\pi(\sigma q) = \sigma_d(\pi q)$. $\square$

Corollaire 5.11 (Les attracteurs symétriques sont des relèvements). *Si une orbite périodique O de D vérifie $O \subseteq F_p$, alors $\bar{O} = \pi(O)$ est une orbite périodique de D_d , et $|O| = k|\bar{O}|$ où k est le nombre de points de O dans une seule π -fibre ; $D^{|\bar{O}|}$ fait cycler ces k points. En particulier toute période $\sigma^{n/p}$ -symétrique au niveau n est un multiple entier d'une période au niveau n/p .*

Démonstration. π est D -équivalente, donc $\bar{O} = \pi(O)$ est D_d -invariante ; comme $\pi|_O$ semiconjugué le $|O|$ -cycle $D|_O$ à l'action cyclique $D_d|_{\bar{O}}$, l'image est une seule D_d -orbite, $|\bar{O}|$ divise $|O|$, et les fibres de $\pi|_O$ ont toutes taille $k = |O|/|\bar{O}|$, permutées en un k -cycle par $D^{|\bar{O}|}$. $\square$

Réciproquement la projection atteint *toute* orbite inférieure.

Corollaire 5.12 (Surjectivité sur les orbites périodiques). *π est surjective sur les orbites périodiques : chaque orbite périodique $\bar{O}$ de D_d sur $C(d)$ est $\pi(O)$ pour une certaine orbite périodique O de D contenue dans F_p .*

Démonstration. Choisissons $\bar{q} \in \bar{O}$; par la Proposition 5.10, $\bar{q} = \pi(q)$ pour un $q \in F_p$. L'orbite avant $(D^k q)_{k \geq 0}$ reste dans F_p , qui est invariant vers l'avant par D (Théorème 5.1), et est finalement périodique, atteignant une orbite périodique $O \subseteq F_p$. Par équivalence $\pi(D^k q) = D_d^k(\bar{q})$ parcourt tout $\bar{O}$; donc $\pi(O)$, une seule D_d -orbite rencontrant $\bar{O}$, égale $\bar{O}$. $\square$

Le nombre d'orbites périodiques de D dans F_p au-dessus d'une $\bar{O}$ donnée n'est cependant pas constant — il vaut déjà 1 ou 2 à $n = 8$ — de sorte que le Corollaire 5.12 ne compte pas à lui seul les bassins de $C(n)$.

Par exemple l'attracteur symétrique $(P, |B|) = (4, 16)$ à $n = 8$, $p = 2$ relève l'attracteur de période 4 de D_4 sur $C(4)$ avec $k = 1$; les bassins $(3, 6)$ à $n = 6$, $p = 2$ et $(2, 10)$ à $n = 6$, $p = 3$ relèvent le *point fixe* s_d de D_d avec $k = 3$ et $k = 2$. Comme $|F_p| = (d-1)!(p-1)p^{d-1}$ est bien plus petit que $(n-1)!$, la projection permet d'énumérer tout attracteur symétrique — et son relèvement — bien au-delà de la portée d'un graphe complet ; c'est ainsi qu'a été trouvée la remarque suivante.

Remarque 5.13 (La loi résiduelle de la Proposition 5.9 est fausse). Pour un attracteur $\sigma^{n/p}$ -symétrique ($O \subseteq F_p$) la conclusion $p \mid P \Leftrightarrow p \mid T$ peut échouer. À $n = 14$, $p = 2$ le bassin $(P, |B|) = (35, 119)$, queue $T = 84$, a $2 \mid T$ mais $2 \nmid P$; à $n = 12$, $p = 3$ le bassin $(2, 20)$, queue $T = 18$, a $3 \mid T$ mais $3 \nmid P$. Les deux bassins sont $\sigma^{n/p}$ -invariants (leurs attracteurs sont point par point $\sigma^{n/p}$ -fixes), et les deux tailles ont été confirmées par une recherche en largeur arrière dans le $C(n)$ complet. Le Corollaire 5.11 les explique : le bassin à $n = 14$ est le relèvement $k = 1$ du bassin $(35, 119)$ de $C(7)$, dont la queue $84 = 2^2 \cdot 3 \cdot 7$ porte déjà le nouveau premier $p = 2$ tandis que sa période $35 = 5 \cdot 7$ ne le porte pas, et le relèvement copie les deux mot pour mot. Ainsi un attracteur symétrique hérite de la période et de la queue d'un bassin à n plus petit, sur lequel le premier fraîchement introduit $p \mid n$ n'a pas besoin de diviser la période même quand il divise la queue. La divisibilité concordante de la Proposition 5.9 est propre au lieu non symétrique $O \not\subseteq F_p$.

La projection compagne $\text{Fix}(\sigma^t) \rightarrow C(t)$ reformule de la même façon l'hypothèse résiduelle de la Proposition 5.5 ; si elle admet elle aussi des contre-exemples symétriques, et une récursion close pour les périodes en n , nous le laissons ouvert.

Table 1: Bassins de D sur $C(n)$ pour de petits n : le nombre de bassins et les paires (période, taille de bassin). Un exposant k dénote une multiplicité de k bassins isomorphes de même période et taille ; ceux-ci forment une seule σ -orbite (Cor. 4.2) *sauf* pour $(4, 16)^2$ à $n = 8$, où les deux bassins isomorphes sont chacun individuellement σ -invariant (comme les paires à $n = 7$ ci-dessous), non σ -conjugués. Aucun exposant n'est utilisé pour les paires répétées à $n = 7$: $(7, 14)$ et $(14, 28)$ sont isomorphes mais *non* σ -conjugués — une σ -orbite de bassins a une taille divisant n , et $2 \nmid 7$ — donc chacun est un bassin σ -invariant séparé. Montré jusqu'à $n = 9$; pour $n = 10, 11, 12$ les nombres de bassins sont 29, 56, 157 (Section 8), et les signatures complètes jusqu'à $n = 12$ sont fournies comme données annexes.

n	#bassins	bassins (période, taille)
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)

Table 2: Le réservoir symétrique $|F_p| = (p-1)(n/p-1)!p^{n/p-1}$.

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

L'arbre entrant de s : une coordonnée linéaire sur la fibre racine

La profondeur de cet arbre entrant — le plus grand nombre de pas de D qu'un n -cycle doit faire pour atteindre s — est l'analogue, pour D , du *temps de tri* du tri par pile (le plus petit t avec $s^t = \text{id}$, au plus $n-1$ pour l'application de West [14]) ; ici il est gouverné par l'arithmétique de n plutôt que par l'évitement de motifs.

Fixons un premier $p \mid n$, posons $d = n/p$, et considérons la fibre $R = \pi^{-1}(s_d) \subseteq F_p$ de la projection de la Proposition 5.10 au-dessus de la racine s_d : elle consiste en les n -cycles q avec $q(x) \equiv x+1 \pmod{d}$. Écrivant $q(x) = x+1 + da_{x \bmod d}$ on définit une *coordonnée de retenue* $a = a(q) \in (\mathbb{Z}/p)^d$, avec $a(s) = 0$.

Lemme 5.14. *R est invariant vers l'avant par D , et dans la coordonnée de retenue D agit linéairement :*

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

De plus q est un n -cycle unique ssi $\sum_r a_r \not\equiv -1 \pmod{p}$.

Démonstration. Posons $\alpha(x) = a_{x \bmod d}$ et $u = q^{-1}(x)$. Alors $D(q)(x) = q(u+1) = (u+1) + 1 + d\alpha(u+1)$, tandis que $x = u+1 + d\alpha(u)$, donc $D(q)(x) = x + 1 + d(\alpha(u+1) - \alpha(u))$; comme $x \equiv u+1 \pmod{d}$ la retenue de Dq en x est $a_{x \bmod d} - a_{(x-1) \bmod d}$, c'est-à-dire $(I-S)a$. Puisque S préserve $\sum_r a_r$, l'image est de somme nulle, donc $D(R) \subseteq R$. Pour le critère de cycle, itérer depuis 0 donne $q^d(0) = d(1 + \sum a)$, donc q^d permute le bloc $\{0, d, \dots, (p-1)d\}$ comme la translation $m \mapsto m+1 + \sum a$ de $\mathbb{Z}/p$; c'est un p -cycle unique — de façon équivalente q est un n -cycle unique — ssi $1 + \sum a \not\equiv 0$. $\square$

Proposition 5.15. *Pour $n = p^e$ dans le régime de Hull–Dobell l'arbre entrant de s a profondeur au moins*

$$p^{e-1} \text{ (} p \text{ impair)}, \quad 2^{e-1} - 1 \text{ (} p = 2),$$

et ce nombre est exactement la profondeur de l'arbre entrant restreint à R .

Démonstration. Par le Lemme 5.14 la distance de $q \in R$ à s est la hauteur de nilpotence de $a(q)$ sous $I-S$. Comme $d = p^{e-1}$ est une puissance de p , $X^d - 1 = (X-1)^d$ sur $\mathbb{F}_p$, donc $I-S$ est nilpotent d'indice exactement d ; et $(I-S)^{d-1}a = (\sum_r a_r)v$ pour un v non nul fixé, donc la hauteur égale d ssi $\sum a \neq 0$. Par le Lemme 5.14 les retenues admissibles sont celles avec $\sum a \not\equiv -1$. Pour p impair on peut prendre $\sum a = 1$, donnant la hauteur $d = p^{e-1}$; pour $p = 2$ le critère force $\sum a = 0$, donc la hauteur est au plus $d-1 = 2^{e-1} - 1$, atteinte (par exemple à $a = (1, 1, 0, \dots, 0)$). Comme $R \subseteq \text{basin}(s)$ (toute retenue est annulée par une puissance de $I-S$), cela borne la profondeur de l'arbre entrant complet par le bas. $\square$

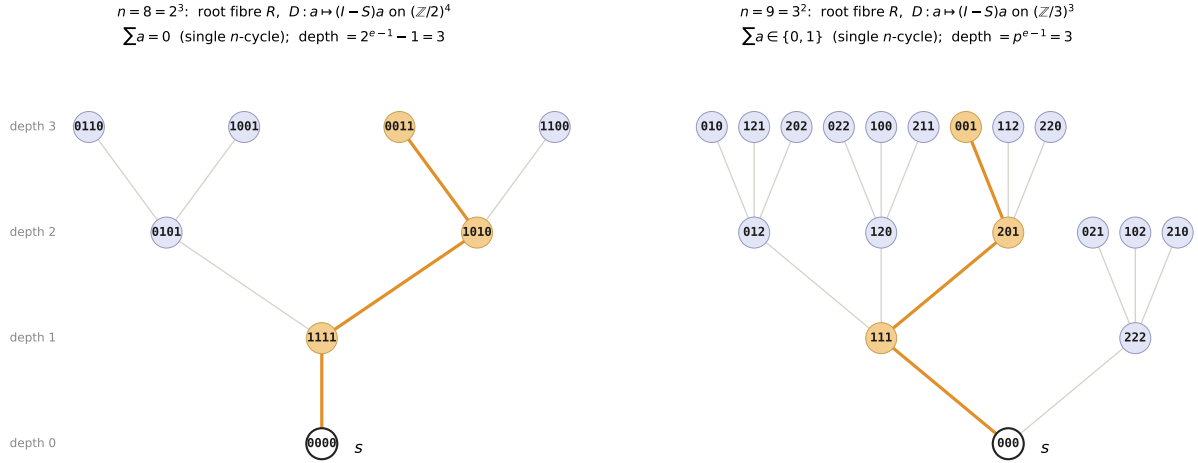


Figure 5: La fibre racine $R \subseteq \text{basin}(s)$ de l'arbre entrant de s — la partie invariante vers l'avant par D qui porte sa plus longue chaîne jusqu'à s — dans le régime de Hull–Dobell, $n = 8 = 2^3$ et $n = 9 = 3^2$, dessinée dans sa coordonnée de retenue (Lemme 5.14). Chaque sommet est son vecteur de retenue $a \in (\mathbb{Z}/p)^d$ ($d = p^{e-1}$, avec $s = \mathbf{0}$ en bas) ; chaque arête est un pas de D , qui sur R agit comme l'application linéaire $a \mapsto (I - S)a$ (la retenue moins son décalage cyclique). La figure est donc la tour de nilpotence de $I - S$ sur $\mathbb{F}_p$: les retenues admissibles sont celles avec $\sum a \neq -1$ (la condition d'unique n -cycle — $\sum a = 0$ pour $p = 2$, $\sum a \in \{0, 1\}$ pour $p = 3$), et la plus longue chaîne vers $\mathbf{0}$ (mise en évidence) réalise la profondeur de la Proposition 5.15 : $2^{e-1} - 1 = 3$ pour $n = 8$ et $p^{e-1} = 3$ pour $n = 9$. Les deux puissances de premier donnent ici la profondeur 3 ; les deux branches de la formule ne se séparent que pour e plus grand (profondeur 7 à $n = 16$, 9 à $n = 27$, dont les bassins — de 2048 et 472392 nœuds — sont trop grands pour être dessinés). Produit par `code/gen_fig_stree.py`.

Cette profondeur de fibre racine est en fait la profondeur *entière*. Le bassin ne peut quitter F_p :

Lemme 5.16. *Pour $n = p^e$ le bassin de s tout entier est dans F_p .*

Démonstration. Écrivons $g = s^{n/p}$, d'ordre p . Pour un n -cycle q le centralisateur est $\langle q \rangle$, donc $q \in F_p$ ssi $g \in \langle q \rangle$. Comme $\langle D(q) \rangle = q \langle s \rangle q^{-1}$, on a $D(q) \in F_p$ ssi $q^{-1} g q \in \langle s \rangle$; comme $q^{-1} g q$ a ordre p et le groupe cyclique $\langle s \rangle$ a un unique sous-groupe d'ordre p — à savoir $\langle g \rangle$ — cela dit exactement que q normalise $\langle g \rangle$. Mais un n -cycle normalisant $\langle g \rangle$ agit sur $\langle g \rangle \cong \mathbb{Z}/p$ par un automorphisme, et l'homomorphisme résultant $\langle q \rangle \rightarrow \text{Aut}(\mathbb{Z}/p)$ a une image d'ordre divisant à la fois $\text{ord}(q) = p^e$ et $|\text{Aut}(\mathbb{Z}/p)| = p - 1$; comme $\gcd(p^e, p - 1) = 1$ l'image est triviale, c'est-à-dire q centralise g et $q \in F_p$. Donc $D(q) \in F_p \Rightarrow q \in F_p$: F_p est clos par D -préimages, et comme $s \in F_p$ le bassin tout entier est dans F_p . $\square$

Ainsi tout $q \in \text{basin}(s)$ a $\pi(q) \in \text{basin}(s_d)$, et sa distance à s se scinde en $m + h$ avec m la distance de $\pi(q)$ dans $C(d)$ et h la hauteur à l'intérieur de R . L'article compagnon [2] démontre que cette borne est atteinte avec égalité à chaque niveau, de sorte que $\text{depth}(p^e) = \rho$ exactement : *les plus longues chaînes sont celles de la fibre racine de la Proposition 5.15*, aucune à travers le reste du bassin n'étant plus longue. La subtilité qu'il doit surmonter est que *hors* de R l'application de retenue n'est plus linéaire mais affine, $a(Dq) = L_{\pi(q)} a(q) + w_{\pi(q)}$ avec L_τ une copie permutée de

$I - S$, de sorte que la profondeur globale n'est pas celle d'un seul opérateur nilpotent — le bassin, de taille $2^3 \cdot 3^{10}$ à $n = 27$, n'est pas un arbre entrant $\mathbb{Z}/p$ -linéaire.

Remarque 5.17 (Le bassin comme T -fonctions à cycle unique). Les n -cycles affines occupant les deux couches supérieures (Lemme 4.4) sont exactement les générateurs congruentiels linéaires de pleine période de Hull–Dobell [7, 10] ; et pour $n = 2^e$ le bassin tout entier coïncide avec les T -fonctions à cycle unique de Klimov–Shamir [8] — les permutations de $\mathbb{Z}/2^e$ dont le bit i ne dépend que des bits $\leq i$, de façon équivalente celles triangulaires pour le drapeau binomial —, dont la transitivité est l'objet de la théorie ergodique non archimédienne d'Anashin [9]. La dérivation se déploie donc dans l'arithmétique même des générateurs de pleine période. Sa profondeur, en revanche, est *orthogonale* à la force cryptographique : le caractère de cycle unique sature uniformément les mesures standard sur tout le bassin. La condition de cyclicité $\sum a \not\equiv 0$ est exactement « la retenue à le degré algébrique maximal », donc tout élément du bassin atteint le degré maximal ; et les bits de poids faible affines forcent partout une non-linéarité de map nulle et une uniformité différentielle au pire cas (vérifié exhaustivement sur $C(16)$ et par échantillonnage sur $C(32)$). Aucune de ces mesures ne varie avec la position dans l'arbre ; seule la dichotomie $\text{dist} \leq 2 \Leftrightarrow \text{affine}$ a un sens, de sorte que $\text{dist} \geq 3$ certifie « véritablement non affine (pas un générateur congruentiel linéaire déguisé) » et rien de plus fin. La calculabilité même de dist en forme close (§5) — une vertu ici — est, dans tout cadre clavetée fondé sur la conjugaison, exactement ce qu'une attaque par longueur descendrait.

6 Comparaison avec une application aléatoire

Pour situer combien D est structuré, nous le comparons à une endofonction aléatoire uniforme sur $N = (n - 1)!$ nœuds, dont le nombre attendu de composantes est $\sim \frac{1}{2} \ln N$ et de points périodiques $\sim \sqrt{\pi N/2}$ [4, 5]. L'écart est grand et son signe suit l'arithmétique de n (Table 3) : les n arithmétiquement simples ont bien plus de points périodiques que l'aléatoire, tandis que $8 \mid n$ ou $p^2 \mid n$ donnent des arbres profonds et bien moins (le régime de Hull–Dobell de la Proposition 4.3). C'est un diagnostic, pas un théorème.

Table 3: D contre une application aléatoire uniforme sur $N = (n - 1)!$ nœuds.

n	N	#bassins	$\frac{1}{2} \ln N$	#périodiques	$\sqrt{\pi N/2}$	% périodiques
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 Crible cyclique

Les n -cycles σ^k -fixes ont un décompte clos qui généralise à la fois le Théorème 5.2 et le corollaire de Wilson.

Proposition 7.1 (Décomptes de points fixes). *Pour $0 \leq k < n$, avec $g = \gcd(k, n)$ et $m = n/g$,*

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

Démonstration. $\langle s^k \rangle = \langle s^g \rangle$ est le sous-groupe d'ordre m de $\langle s \rangle$; écrivons $h = s^g$, un produit de g m -cycles disjoints, avec $C_{S_n}(h) = \mathbb{Z}/m \wr S_g$. Comme dans le Théorème 5.2, $q \in C(n)$ contient h dans $\langle q \rangle$ ssi $q \in C_{S_n}(h)$, sa permutation de blocs τ est un g -cycle, et $q^g = h^t$ avec $\gcd(t, m) = 1$; il y a $\varphi(m)$ t admissibles, $(g-1)!$ tels τ , et m^{g-1} vecteurs de blocs réalisant chacun, donnant le produit. Le cas $g = n/p$, $m = p$ retrouve $|F_p|$ (Théorème 5.2) ; $\#\text{Fix}(\sigma^k)$ ne dépend que de $\gcd(k, n)$. $\square$

Remarque 7.2. Ces décomptes réalisent un phénomène de crible cyclique [12] : le polynôme d'orbites $X(t) = \sum_O [|O|]_t^{n/|O|}$ (somme sur les σ -orbites $O \subseteq C(n)$, $[d]_u = 1 + u + \dots + u^{d-1}$) est dans $\mathbb{Z}_{\geq 0}[t]$ avec $\deg X < n$, $X(1) = (n-1)!$, et $X(\zeta^k) = \#\text{Fix}(\sigma^k)$ pour $\zeta = e^{2\pi i/n}$ et tout k . Mais c'est le crible *tautologique* porté par tout $\mathbb{Z}/n$ -ensemble — la positivité est automatique — de sorte que le contenu est le décompte de la Proposition 7.1, pas le phénomène. Le polynôme ne fait qu'empaqueter les données de tailles de σ -orbites ; son terme constant $c_0 = \frac{1}{n} \sum_k \#\text{Fix}(\sigma^k)$ est le nombre de σ -orbites, la suite 2, 3, 8, 24, 108, 640, 4492, $\dots = \text{A002619}$ (permutations circulaires à rotation près [16]), que X raffine par taille d'orbite. Le même décompte apparaît pour les classes de σ -équivalence de Yordzhev — le « factor set » de S_n sous l'action bilatère $\alpha \mapsto s^k \alpha s^{-l}$ avec k, l indépendants [15] ; nos σ -orbites sont le cas couplé $k = l$ (conjugaison) restreint aux n -cycles, en même nombre bien que relation différente. Ce qui serait substantiel — une statistique *intrinsèque* réalisant X , lue depuis q plutôt que depuis son orbite — est ouvert (Section 8).

8 Problèmes ouverts

Question 8.1. Par la Proposition 5.5 chaque période non fixe ℓ porte une graine forcée $d = \gcd(\ell, n) > 1$; le cofacteur $m = \ell/d$ est la part erratique ($m = 11$ dans $33 = 3 \cdot 11$ à $n = 6$, $m = 7$ dans 49 à $n = 7$), réalisée géométriquement comme la période du collier d'attachement (Observation 5.8), de façon équivalente comme le nombre de σ -orbites sur le cycle. Existe-t-il une description du multi-ensemble des cofacteurs à travers les bassins de $C(n)$? La projection récursive (Corollaire 5.12) organise ces orbites — chacune est héritée le long d'un relèvement — mais sa fibre est irrégulière (Section 5), et nous n'avons trouvé aucune forme close.

Question 8.2. Les nombres de bassins 1, 2, 2, 6, 7, 18, 17, 29, 56, 157 pour $n = 3, \dots, 12$ sont absents de l'OEIS [16] (contrairement au décompte d'orbites $c_0 = \text{A002619}$), de sorte que la partition en bassins $P(n)$ est une suite véritablement nouvelle. (Les valeurs pour $n = 10, 11, 12$ ont été obtenues en codant chaque n -cycle comme le rang de Lehmer de son mot de permutoèdre et en calculant le graphe fonctionnel sur des tableaux d'entiers ; les multi-ensembles de périodes et les données de la Remarque 5.6 viennent du même calcul.) Existe-t-il une formule ou une série génératrice ? Scinder les orbites périodiques entre celles dans un F_p (relèvements, Corollaire 5.12) et le reste réduit le décompte d'un niveau, mais le nombre d'orbites au-dessus d'une orbite inférieure donnée n'est pas constant — déjà 1 ou 2 à $n = 8$ — donc aucune récursion propre par diviseurs n'en découle, et la suite pourrait être véritablement irrégulière.

Question 8.3. Le crible cyclique de la Remarque 7.2 vaut pour tout n via les σ -orbites, mais seulement tautologiquement. Existe-t-il une statistique *intrinsèque* $\text{stat} : C(n) \rightarrow \mathbb{Z}/n$ — définie depuis q directement, non depuis sa σ -orbite, et idéalement compatible avec D — avec $\sum_q t^{\text{stat}(q)} = X(t)$? Elle doit être σ -équivariante, $\text{stat}(\sigma q) \equiv \text{stat}(q) + n/|O_q| \pmod{n}$, ce qui exclut déjà les statistiques de permutation usuelles.

Question 8.4. Sur quel espace les symétries $\mathbb{Z}/n$ deviennent-elles géométriques ? Le permutoèdre Π_{n-1} porte les sommets mais pas σ comme isométrie ; le cycloèdre de Bott–Taubes [1] porte la symétrie cyclique mais son ensemble de sommets, de taille $\binom{2d}{d}$, n’est pas $C(n)$. Existe-t-il un polytope ou un complexe cellulaire portant les deux ?

Remerciements

Les résultats ont été obtenus par le modèle d’IA Claude Opus 4.8 (Anthropic) en dialogue avec l’auteur ; les calculs de support sont courts et reproductibles. Ils restent à étudier et à vérifier de façon indépendante.

Références

- [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] V. Anashin and A. Khrennikov, *Applied Algebraic Dynamics*, de Gruyter Expositions in Mathematics **49**, Walter de Gruyter (2009).
- [10] D. E. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 3rd ed., Addison-Wesley (1997).
- [11] 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.
- [12] V. Reiner, D. Stanton and D. White, *The cyclic sieving phenomenon*, J. Combin. Theory Ser. A **108** (2004), 17–50.
- [13] R. P. Stanley, *Enumerative Combinatorics, Vol. 1*, 2nd ed., Cambridge Univ. Press (2012).
- [14] J. West, *Permutations with forbidden subsequences and stack-sortable permutations*, Ph.D. thesis, Massachusetts Institute of Technology (1990).

- [15] K. Yordzhev, *On the cardinality of a factor set in the symmetric group*, Asian-Eur. J. Math. **7** (2014), no. 2, 1450027.
- [16] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, sequence **A002619**, <https://oeis.org>.