Diamètre et croissance dans les groupes de permutations

Thomas Budzinski et Jaouad Mourtada

Sous la direction de Harald Helfgott

Table des matières

1 Introduction

1.1 Objectif et définitions

Considérons un casse-tête de type Rubik's Cube, c'est-à-dire un ensemble de configurations d'un objet auquel on a le droit d'appliquer certaines transformations « élémentaires » et qu'on veut amener à une certaine position. On peut alors se demander quel est l'ordre de grandeur du nombre de permutation élémentaires nécessaires pour résoudre le casse-tête, dans le pire des cas.

Précisons cela. Étant donnés un groupe fini G et une partie génératrice A de G, on notera $\Gamma(G, A)$ le graphe de Cayley (non orienté) de G par rapport à A, c'est-à-dire le graphe (V, E) avec $V = G$ et $E = \{\{g, ag\} | g \in G, a \in A\}$.

Définition 1.1. Le *diamètre* d'un graphe $\Gamma = (V, E)$ est la quantité :

$$\operatorname{diam}(\Gamma) = \max_{v_1, v_2 \in V} \min_{\gamma \text{ chemin de } v_1 \text{ à } v_2} \operatorname{long}(\gamma)$$

Ainsi, le diamètre de $\Gamma(G, A)$ est le maximum sur $g \in G$ de la longueur l de la plus petite écriture de g sous la forme $a_1^{\varepsilon_1} \dots a_\ell^{\varepsilon_\ell}$ avec $a_1, \dots, a_\ell \in A$ et $\varepsilon_1, \dots, \varepsilon_\ell \in \{-1, 1\}$.

Définition 1.2. Si G est un groupe fini, le diamètre de G est la quantité :

$$\operatorname{diam}(G) = \max\{\operatorname{diam}(\Gamma(G, A)) | A \text{ partie génératrice de } G\}$$

Pour faire le lien avec le problème énoncé plus haut, si X est l'ensemble des configurations possibles, A est l'ensemble des permutations élémentaires, et $G = \langle A \rangle$ est le groupe – transitif – de toutes les permutations obtenues à partir des opérations élémentaires, le nombre maximal de mouvements nécessaires pour « dénouer » une position de X (*i.e.* la ramener à une configuration de référence) est majoré par $\operatorname{diam} \Gamma(G, A)$, donc par $\operatorname{diam}(G)$.

Le but de ce mémoire va donc être d'obtenir une majoration de $\operatorname{diam}(G)$ quand G est le groupe symétrique $\mathfrak{S}_n$ ou alterné $\mathfrak{A}_n$ (ou plus généralement un groupe de permutations transitif) de degré n pour n suffisamment grand. Il s'appuie sur l'article [HS13], qui fournit la meilleure majoration (asymptotique) du diamètre de ces groupes connue à ce jour [1].

1.2 Contexte et résultat principal

Le problème du diamètre dans un groupe est intimement relié à celui de la croissance de parties d'un groupe, *i.e.* au comportement du cardinal de $A \cdot A$, ou de $A^k = A \cdots A$, par rapport à celui de A. L'étude de la croissance dans groupe est un problème central de la combinatoire additive (cas où A est une partie d'un groupe abélien, typiquement $A \subset \mathbb{Z}$) et de la théorie géométrique des groupes où l'on s'intéresse, entre autres, au comportement asymptotique de $|A^n|$ lorsque $n \to \infty$, A étant une partie génératrice finie d'un groupe infini G. Dans le cas d'un groupe fini, l'étude asymptotique du cardinal $|A^n|$ ne présente aucun intérêt, c'est alors le diamètre qui mesure la croissance dans le groupe.

Dans le cas d'un groupe dont les éléments satisfont de nombreuses relations, on peut s'attendre à ce que de nombreux produits dans l'ensemble A^k soient égaux, donc que A croisse assez lentement, et donc que le diamètre soit assez grand : ainsi, le diamètre d'un groupe cyclique est linéaire en $|G|$ (de l'ordre de $\frac{|G|}{2}$) et celui d'un groupe abélien est polynomial en $|G|$.

La principale conjecture actuelle sur le diamètre des groupes, formulée pour la première fois par Babai, porte sur la situation opposée :

Conjecture. *Il existe une constante absolue $C > 0$ telle que pour tout groupe fini simple non abélien G,* $\operatorname{diam}(G) \leq (\ln |G|)^C$.

La première catégorie de groupes pour laquelle la conjecture a été établie est celle des groupes $\mathrm{SL}_2(\mathbb{F}_p)$, dans [Hel08]. Les seuls groupes pour lesquels elle a été montrée sont des groupes algébriques de rang borné [2]. Pour les groupes symétriques ou alternés, elle reviendrait à borner le diamètre polynomialement en n. Le résultat principal de ce mémoire est une majoration un peu moins bonne, dite « quasi-polynomiale », obtenue en 2011 par Helfgott et Seress dans [HS13] :

1. Il existe cependant de meilleures majorations, notamment polynomiales, du diamètre $\operatorname{diam}(\Gamma(G, A))$ lorsque l'on sait quelque chose sur la partie génératrice A (par exemple qu'elle contient un élément de petit support), cf. [BBS04].

2. Les majorations obtenues pour $\mathrm{SL}_n(\mathbb{F}_p)$ (cf. [GH11]) ou, plus généralement, pour tous les groupes simples de type de Lie (cf. [BGT11]) sont de la forme $(\ln |G|)^C$, où la constante C est indépendante du corps de base, mais dépend fortement du rang n.

Théorème 1.3. *Si $G = \mathfrak{A}_n$ ou $G = \mathfrak{S}_n$, on a :*

$$\mathrm{diam}(G) = e^{(\ln n)^{O(1)}}$$

Plus précisément, $\mathrm{diam}(G) = e^{O((\ln n)^4 \ln\ln n)}$.

L'intérêt de traiter les groupes symétriques et alternés vient du théorème suivant, qui remonte à [BS92] :

Théorème 1.4. *Soit G un sous-groupe de $\mathfrak{S}_n$. Si G est transitif, alors :*

$$\mathrm{diam}(G) \leq e^{O((\ln n)^3)} \mathrm{diam}(\mathfrak{A}_k)$$

où $\mathfrak{A}_k$ est le plus grand facteur alterné dans la suite de composition de G.

La majoration du théorème principal reste donc vraie pour n'importe quel sous-groupe transitif de $\mathfrak{S}_n$.

1.3 Notations et conventions

Si Δ est un ensemble fini, on note $\mathfrak{S}_\Delta$ le groupe des permutations de Δ, et $\mathfrak{A}_\Delta$ le sous-groupe formé des permutations paires ; on note également $\mathfrak{S}_n = \mathfrak{S}_{[\![1,n]\!]}$ et $\mathfrak{A}_n = \mathfrak{A}_{[\![1,n]\!]}$, où $[\![1,n]\!] = \{1,\dots,n\}$, les groupes symétriques et alternés de degré n. Par *groupe de permutations de degré n*, nous entendrons sous-groupe du groupe symétrique d'un ensemble à n éléments.

Si A, B sont des parties d'un groupe G, AB désigne l'ensemble $\{ab \mid a \in A, b \in B\}$; de plus, A^k désigne[3] $\underbrace{A \cdots A}_{k \text{ fois}}$. Si le groupe G agit sur l'ensemble Δ, on note pour $A \subset G$ et $\Sigma \subset \Delta$: $A \cdot \Sigma = \{g \cdot x \mid g \in A, s \in \Sigma\}$. Le *stabilisateur point par point* $A_{(\Sigma)}$ et le *stabilisateur global* A_Σ de Σ dans A sont respectivement :

$$A_{(\Sigma)} = \{g \in A \mid \forall s \in \Sigma,\ g \cdot s = s\} \quad \text{et} \quad A_\Sigma = \{g \in A \mid g \cdot \Sigma = \Sigma\}.$$

Comme le suggèrent les notations précédentes, nous avons choisi d'utiliser des actions **à gauche**, rompant avec une tradition bien établie dans le domaine des groupes de permutations. Lorsque l'on parlera de classes modulo un sous-groupe, on parlera donc toujours de classes à gauche. Ainsi si H est un sous-groupe de G, G/H désigne l'ensembles des classes à gauche modulo H, $[G : H] = |G|/|H|$ son cardinal, et $\pi_{G/H} : G \longrightarrow G/H$ désigne la projection canonique qui à un élément de G associe sa classe modulo H.

Tous les groupes et ensembles considérés dans ce texte seront, sans précision supplémentaire, supposés finis.

Nous dirons qu'une action d'un groupe G sur un ensemble X est *k-transitive* ($k \geq 1$) si pour tous k-uplets $(x_1,\dots,x_k), (y_1,\dots,y_k) \in X^k$ tels que pour $i \neq j$, $x_i \neq x_j$ et $y_i \neq y_j$, il existe $g \in G$ tel que $g \cdot x_i = y_i$ pour tout i.

Le point suivant a son importance : par partie *symétrique* d'un groupe G, nous entendrons partie de G stable par inverse **et** contenant l'identité. L'assertion « A est symétrique » équivaudra donc à « $A = A^{-1}$ et $e \in A$ ».

3. Nous nous permettrons parfois, pour alléger les notations, de noter A^t à la place de $A^{\lfloor t \rfloor}$ pour $t \in \mathbb{R}^+$.

1.4 Esquisse de la preuve ; idées récurrentes

Dans le cas des groupes linéaires algébriques comme dans [Hel08], la majoration du diamètre se déduit immédiatement d'un résultat de croissance :

Théorème 1.5. *Il existe k entier et $\delta > 0$ tels que pour tous p premier et A partie génératrice de $\mathrm{SL}_2(\mathbb{F}_p)$, on ait soit :*

$$|A^3| \geq |A|^{1+\delta},$$

soit $(A \cup A^{-1})^k = \mathrm{SL}_2(\mathbb{F}_p)$.

Malheureusement, ce résultat n'est plus vrai pour les groupes de permutation, des contre-exemples étant construits dans [PPSS12].

Ce qui va croître ici n'est donc pas le cardinal de A^k, mais la longueur de chaînes de stabilisateurs, c'est-à-dire de suites $(\alpha_1, \dots, \alpha_\ell)$ d'éléments de $[\![1, n]\!]$ telles que les orbites $A^k_{(\alpha_1,\dots,\alpha_{i-1})} \cdot \alpha_i$ soient toutes assez grandes (ici de taille supérieure à $\frac{9}{10}n$).

L'outil utilisé pour allonger de telles chaînes est le « lemme de séparation » (lemme 2.6), qui fait l'objet de la partie 2. Son utilisation nécessite la construction d'un grand nombre d'éléments dans le stabilisateur point par point d'une chaîne, obtenu en faisant agir le stabilisateur global sur le stabilisateur point par point par conjugaison : c'est l'étape de création, décrite dans la partie 4. Le résultat final de la partie 3 assure, lui, que l'action est « assez large », c'est-à-dire qu'on peut trouver $\Delta \subset \Sigma$ grand, tel que le stabilisateur point par point agisse sur Δ comme A_Δ. La partie 5 permet d'assembler ces différents morceaux et de conclure la preuve.

Mentionnons l'un des principaux leitmotifs de l'article [HS13] : de nombreux résultats portant sur des sous-groupes H de G peuvent être adaptés au cas d'une partie quelconque $A \subset G$ (en remplaçant H parfois par A, d'autres fois par A, $A^{-1}A$ ou encore A^k, k relativement petit). Ceci peut être réalisé de plusieurs manières :

1. Dans le cas où la preuve du résultat original est algorithmique, constructive, il est possible de la reprendre sans trop de modifications, en gardant une trace du nombre de produits mis en jeu. Ce procédé est employé à plusieurs reprises dans la partie 3, le cas du lemme 3.5 adapté d'un résultat de Bochert étant très représentatif. Typiquement, ce procédé permet de transformer un énoncé du type « un sous-groupe H de G satisfaisant la propriété $(\mathcal{P})$ est assez grand » en « si une partie $A \subset G$ satisfait $(\mathcal{P})$, alors il existe un entier k relativement petit tel que A^k soit assez grand ».
2. Certains résultats, d'abord en combinatoire ou en théorie des nombres, puis en théorie des groupes, ont été établis en faisant appel à la *méthode probabiliste*. Le principe est le suivant : pour montrer qu'un objet satisfaisant une certaine propriété existe, on montre qu'un objet satisfait cette propriété avec une probabilité positive (pour une certaine distribution de probabilité, souvent uniforme). Pour adapter un énoncé portant sur des sous-groupes en énoncé portant sur des parties quelconques, on peut considérer non plus des distributions uniformes, mais des distributions issues de marches aléatoires de longueur contrôlée. Pour être bref, on remplace ainsi un argument *probabiliste* par un argument *stochastique*.

2 Le lemme de séparation

2.1 Le lemme de séparation pour les sous-groupes

La version originale du lemme est un résultat sur les sous-groupes 2-transitifs de $\mathfrak{S}_n$, qui apparaît dans [Bab82]. La motivation originale était d'obtenir des bornes sur la taille de tels groupes. Sa démonstration est une des nombreuses illustrations de la méthode probabiliste :

Lemme 2.1. *Soient $0 < \rho < 1$, H un sous-groupe 2-transitif de $\mathfrak{S}_n$ et $\Sigma \subset [\![1, n]\!]$. On suppose qu'il existe au moins $\rho n(n-1)$ paires (α, β) d'éléments de $[\![1, n]\!]$ telles qu'il n'y ait aucun $g \in H_{(\Sigma)}$ tel que $g \cdot \alpha = \beta$. Alors il existe $S \subset H$ tel que :*

$$H_{(S \cdot \Sigma)} = \{e\}$$

et $|S| \leq C_1(\rho) \ln n$, où $C_1(\rho)$ est une constante ne dépendant que de ρ.

Démonstration. Soient $\alpha \neq \beta$ dans $[\![1, n]\!]$ et $h \in H$. Si il existe $g' \in H_{(h.\Sigma)}$ tel que $g' \cdot \alpha = \beta$, alors $g = h^{-1}g'h$ est un élément de $H_{(\Sigma)}$ qui envoie $h^{-1} \cdot \alpha$ sur $h^{-1} \cdot \beta$. Or, l'ensemble des $h \in H$ qui envoient (α, β) sur un α', β' fixé est une classe à gauche de $H_{(\alpha,\beta)}$ dans H. Si h est choisi aléatoirement de manière uniforme sur H, tous les couples $(h^{-1} \cdot \alpha, h^{-1} \cdot \beta)$ sont équiprobables donc :

$$\mathbb{P}(\text{Il n'existe pas de } g \in H_{(\Sigma)} \text{ qui envoie } h^{-1} \cdot \alpha \text{ sur } h^{-1} \cdot \beta) \geq \rho$$

d'où :

$$\mathbb{P}(\text{Il n'existe pas de } g \in H_{(h \cdot \Sigma)} \text{ qui envoie } \alpha \text{ sur } \beta) \geq \rho$$

Soient donc $h_1, \ldots, h_r$ r variables aléatoires indépendantes uniformes sur H : pour (α, β) fixée avec $\alpha \neq \beta$, on a :

$$\mathbb{P}(\forall i \in [\![1, r]\!], \exists g \in H_{(h \cdot \Sigma)}, g \cdot \alpha = \beta) \leq (1 - \rho)^r$$

donc, si $S = \{h_1, \ldots, h_r\}$:

$$\mathbb{P}(\text{Il existe } \alpha \neq \beta \text{ et } g \in H_{(S \cdot \Sigma)} \text{ tels que } g \cdot \alpha = \beta) \leq n^2(1 - \rho)^r$$

d'où le résultat, car $n^2(1 - \rho)^r < 1$ pour $r > \frac{2 \ln n}{\ln(1/(1-\rho))}$. □

On veut maintenant adapter ce lemme à des sous-ensembles A de $\mathfrak{S}_n$. On veut pouvoir utiliser le même type d'argument que ci-dessus, donc s'approcher d'une distribution uniforme sur un sous-groupe, et ce par des éléments de A^k en contrôlant k. On commence donc par donner une estimation de la vitesse de convergence d'une marche aléatoire vers la distribution uniforme.

2.2 Marches aléatoires

Soit Γ un graphe (non orienté) fini pondéré à poids entiers, en notant $p(x, y)$ le poids de l'arête qui relie x à y. On va supposer Γ connexe et d-régulier, c'est-à-dire que pour tout x dans V, la somme des poids des arêtes issues de x vaut d. On considère des chaînes de Markov sur V de matrice de transition Q avec, pour x et y dans V :

$$Q(x, y) = \begin{cases} \frac{1}{2} & \text{si } x = y \\ \frac{p(x,y)}{2d} & \text{sinon} \end{cases}$$

Un tel processus est appelée « marche aléatoire paresseuse ». Il permet d'assurer l'apériodicité de la chaîne de Markov, et donc sa convergence vers la mesure uniforme.

Définition 2.2. Soit $\varepsilon > 0$. Le temps de mélange ℓ^∞ pour ε est le plus petit entier k tel que pour tous $x, y \in V$:

$$\frac{1 - \varepsilon}{|V|} \leq Q^k(x, y) \leq \frac{1 + \varepsilon}{|V|}$$

Lemme 2.3. *Soit Γ connexe et d-régulier à N sommets. Alors le temps de mélange ℓ^∞ pour ε de la marche aléatoire paresseuse est inférieur ou égal à $N^2 d \ln \frac{N}{\varepsilon}$.*

Démonstration. Q étant une matrice symétrique, elle est diagonalisable en base orthonormée. On note $1 = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0$ ses valeurs propres et $(v_1, \ldots, v_n)$ une base orthonormée de vecteurs propres correspondante. On a alors, comme $v_1 = (\frac{1}{\sqrt{N}}, \ldots, \frac{1}{\sqrt{N}})$:

$$\begin{aligned} Q^k(x,y) &= \langle Q^k e_x, e_y \rangle = \left\langle \sum_{i=1}^{N} \langle e_x, v_i \rangle Q^k v_i, e_y \right\rangle \\ &= \sum_{i=1}^{N} \lambda_i^k \langle e_x, v_i \rangle \langle v_i, e_y \rangle = \frac{1}{N} + \sum_{j=2}^{N} \lambda_i^k \langle e_x, v_i \rangle \langle v_i, e_y \rangle \end{aligned}$$

d'où :

$$|Q^k(x,y) - \frac{1}{N}| \leq \lambda_2^k \sum_{j=2}^{N} |\langle e_x, v_i \rangle \langle v_i, e_y \rangle| \leq \lambda_2^k$$

par l'inégalité de Cauchy-Schwarz.

Il reste donc à estimer la deuxième valeur propre de Q. Or, une telle estimation est obtenue dans [Fie72] : on a $\lambda_2 \leq 1 - 2\left(1 - \cos\frac{\pi}{N}\right)\mu(Q)$ où :

$$\mu(Q) = \min_{M \subset V, M \neq \emptyset, V} \sum_{x \in M, y \notin M} Q(x,y)$$

est une mesure quantitative de l'irréductibilité. Comme les poids sont entiers, les on a $Q(x,y) \geq \frac{1}{2d}$ dès que $Q(x,y) \neq 0$, donc $\mu(Q) \geq \frac{1}{2d}$ par connexité. De plus, $1 - \cos\frac{\pi}{N} \geq \frac{1}{N^2}$, donc $|Q^k(x,y) - \frac{1}{N}| \leq \left(1 - \frac{1}{N^2 d}\right)^k \leq e^{-k/N^2 d}$, d'où le résultat. □

Le lemme élémentaire suivant sera utilisé à de multiples reprises par la suite. Le premier énoncé permet d'utiliser au mieux la borne précédente du temps de mélange :

Lemme 2.4. *Soit G un groupe agissant transitivement sur un ensemble X, et $\ell = |X|$. Soit $A \subset G$ avec $e \in A$ et $\langle A \rangle = G$. Alors :*

1. *Il existe $A_0 \subset A$ avec $|A_0| < \ell$ telle que $\langle A_0 \rangle$ agisse transitivement sur X.*
2. *Pour tout $x \in X$, on a $A^\ell \cdot x = X$.*

Démonstration. Pour la première assertion, soit Γ le graphe dont les sommets sont les éléments de X et dont deux sommets x et y sont reliés si et seulement si il existe $g \in A$ avec $g \cdot x = y$: l'action étant transitive, Γ est connexe donc admet un arbre couvrant Γ_0, qui a $|X| - 1$ arêtes. Il suffit alors de prendre, pour toute arête $\{x, y\}$ de Γ_0, un $g_0 \in A$ tel que $g_0 \cdot x = y$.

La seconde se démontre de manière similaire. □

On peut maintenant montrer un résultat qui permettra d'approcher la distribution uniforme en faisant agir successivement un petit nombre d'éléments de A :

Lemme 2.5. *Soient $k \in \mathbb{N}^*$, H un sous-groupe k-transitif de $\mathfrak{S}_n$ et A une partie génératrice symétrique de H. Alors il existe $A' \subset A$ avec $A' = A'^{-1}$ tel que, pour tous $\varepsilon > 0$ et $\ell \geq 2n^{3k} \ln \frac{n^k}{\varepsilon}$, et pour tous k-uplets $\bar{x} = (x_1, \ldots, x_k)$ et $\bar{y} = (y_1, \ldots, y_n)$ d'éléments de $[\![1, n]\!]$ deux à deux distincts, on ait :*

$$(1 - \varepsilon)\frac{(n-k)!}{n!} \leq \mathbb{P}(g_1 \ldots g_\ell \cdot \bar{x} = \bar{y}) \leq (1 + \varepsilon)\frac{(n-k)!}{n!}$$

où $g_1, \ldots, g_\ell$ sont des variables aléatoires indépendantes et identiquement distribuées à valeur dans A' avec $\mathbb{P}(g_1 = e) = \frac{1}{2}$ et, pour tous $g, h \in A' \backslash \{e\}$: $\mathbb{P}(g_1 = g) = \mathbb{P}(g_1 = h)$.

Démonstration. Soit Δ l'ensemble des k-uplets d'éléments distincts de $[\![1,n]\!]$: H agit transitivement sur Δ, donc le lemme 3 donne un sous-ensemble A_0. Si on pose $A' = A_0 \cup A_0^{-1}$, alors on a bien $A' = A'^{-1}$, $\langle A' \rangle$ agit transitivement sur Δ, et $|A'| \leq 2|\Delta| \leq 2n^k$. On note alors Γ le graphe dont les sommets sont les éléments de Δ et où le poids de l'arête $\{\bar{x}, \bar{y}\}$ est le nombre de $g \in A'$ tels que $g \cdot \bar{x} = \bar{y}$: ce graphe est $|A'|$-régulier, d'où le résultat en appliquant le lemme 2 avec $N = |\Delta| \leq n^k$ et $d = |A'| \leq 2n^k$. □

2.3 Le lemme de séparation pour les ensembles et ses conséquences

On peut maintenant formuler et démontrer le lemme de séparation pour les ensembles :

Lemme 2.6. *Soient $0 < \rho < 1$, $A \subset \mathfrak{S}_n$ symétrique avec $\langle A \rangle$ 2-transitif et $\Sigma \subset [\![1,n]\!]$. On suppose qu'il existe au moins $\rho n(n-1)$ paires (α, β) d'éléments de $[\![1,n]\!]$ telles qu'il n'y ait aucun $g \in (A^{9n^6 \ln n})_{(\Sigma)}$ tel que $g \cdot \alpha = \beta$. Alors il existe $S \subset A^{5n^6 \ln n}$ tel que :*

$$(AA^{-1})_{(S \cdot \Sigma)} = \{e\}$$

et $|S| \leq C_2(\rho) \ln n$, où $C_2(\rho)$ est une constante ne dépendant que de ρ.

Démonstration. On adapte la preuve du lemme pour les sous-groupes : on choisit $h_1, \ldots, h_r$ aléatoirement comme résultats de marches aléatoires paresseuses indépendantes de longueur ℓ avec $\ell = \lceil 2n^6 \ln \frac{n^2}{1/3} \rceil \leq 5n^6 \ln n$: d'après le lemme 4, pour tous (α, β) et (α', β'), on a :

$$\mathbb{P}\left((h \cdot \alpha, h \cdot \beta) = (\alpha', \beta')\right) \geq \frac{2}{3n(n-1)}$$

Si il existe $g \in (AA^{-1})_{(h \cdot \Sigma)}$ tel que $g \cdot \alpha = \beta$, alors $g = h^{-1} g' h$ est un élément de $(A^{9n^6 \ln n})_{(\Sigma)}$ qui envoie $h^{-1} \cdot \alpha$ sur $h^{-1} \cdot \beta$, donc :

$$\mathbb{P}\left(\text{Il n'existe pas de } g \in (AA^{-1})_{(\Sigma)} \text{ qui envoie } h^{-1} \cdot \alpha \text{ sur } h^{-1} \cdot \beta\right) \geq \frac{2}{3}\rho$$

et on conclut de même que pour les sous-groupes. □

Le lemme suivant montre comment exploiter le lemme de séparation pour construire des chaînes de stabilisateurs :

Lemme 2.7. *Soient $A \subset \mathfrak{S}_n$ symétrique avec $\langle A \rangle$ 2-transitif. Soient $A' = A^{9n^6 \ln n}$, $0 < \rho < 1$ et $\Sigma \subset [\![1,n]\!]$ tel que pour tout α, $|A'_{(\Sigma)} \cdot \alpha| < (1-\rho)n$. Alors :*

$$|\Sigma| > C_3(\rho) \frac{\ln |A'|}{(\ln n)^2}$$

où $C_3(\rho) > 0$ ne dépend que de ρ.

Démonstration. L'hypothèse implique qu'il existe au moins $\rho n(n-1)$ paires (α, β) telles qu'il n'existe aucun $g \in A'_{(\Sigma)}$ envoyant α sur β. Le lemme de séparation fournit donc $S \subset \mathfrak{S}_n$ tel que $(AA^{-1})_{(S \cdot \Sigma)} = \{e\}$ et $|S| \leq C_2(\rho) \ln n$. Chaque classe à gauche de $(\mathfrak{S}_n)_{(S \cdot \Sigma)}$ dans $\mathfrak{S}_n$ contient donc au plus un élément de A, donc :

$$|S||\Sigma| \geq |S \cdot \Sigma| \geq \frac{\ln |A|}{\ln n}$$

d'où le résultat. □

Ce lemme permet donc de construire de grandes chaînes de stabilisateurs tant que la partie A est assez grande, ce qui jouera un rôle crucial à la fin de la preuve.

3 Action et croissance de grandes parties de $\mathfrak{S}_n$

3.1 Croissance et quotients

L'idée qui guide ce paragraphe est que l'on peut obtenir de la croissance dans un groupe en le faisant agir sur un certain ensemble.

Le résultat (assez simple) suivant généralise le fait que, dans le cadre d'une action de groupe, le cardinal de l'orbite d'un élément est égal à l'indice de son stabilisateur.

Lemme 3.1 (Théorème orbite-stabilisateur)**.** *Soit G un groupe agissant sur un ensemble X, $x \in X$ et A une partie non vide de G. Alors :*

$$|A^{-1}A \cap G_x| \geq \frac{|A|}{|A \cdot x|}\,.$$

De plus, pour tout $B \subset G$:

$$|AB| \geq |A \cdot x| \cdot |B \cap G_x|\,.$$

Dans le cours de la preuve, on sera amené à considérer une suite de trois groupes imbriqués : $(\mathfrak{S}_n)_{(\Sigma)} \subset (\mathfrak{S}_n)_\Sigma \subset \mathfrak{S}_n$ (où $\Sigma \subset [\![1, n]\!]$), et l'on voudra obtenir une partie A de $\mathfrak{S}_n$ telle que A_Σ rencontre beaucoup de classes à gauche modulo $(\mathfrak{S}_n)_{(\Sigma)}$. C'est précisément ce que permet le lemme suivant, qui généralise le lemme orbite-stabilisateur (rappelons que si $A \subset G$, $|\pi_{G/H}(A)|$ est le nombre de classes à gauche modulo H que rencontre A).

Lemme 3.2. *Soit G un groupe, et H, K deux sous-groupes de G avec $H \subset K$. Pour toute partie non vide A de G, on a*

$$|\pi_{K/H}(A^{-1}A \cap K)| \geq \frac{|\pi_{G/H}(A)|}{|\pi_{G/K}(A)|} \geq \frac{|\pi_{G/H}(A)|}{[G : K]}.$$

Ainsi, si A intersecte $r[G : H]$ classes modulo H, alors $A^{-1}A \cap K$ intersecte au moins $r[K : H]$ classes modulo H.

Démonstration. Soit $A' \subset A$ un système de représentants des classes de A modulo H (donc $|A'| = |\pi_{G/H}(A)|$). L'application $p : A' \to G/K$, $a \mapsto aK$ est à valeurs dans $\pi_{G/K}(A)$ et chaque élément de $\pi_{G/K}(A)$ admet au plus $|\pi_{K/H}(A^{-1}A \cap H)|$ antécédents. En effet, si $a_0 \in A$ est fixé et si $a \in A'$ vérifie $aK = a_0K$, $\pi_{G/H}(a_0^{-1}a) \in \pi_{K/H}(A^{-1}A \cap K)$ caractérise $a \in p^{-1}(a_0K)$ car $\pi_{G/H}(a_0^{-1}a) = \pi_{G/H}(a_0^{-1}a')$ implique $aH = a'H$ donc (par définition de A') $a = a'$. □

3.2 Grandes parties de $\mathfrak{S}_n$

Dans cette partie, on s'intéresse aux grandes parties du groupe symétrique, dont on cherche à montrer qu'elles contiennent le groupe alterné d'un grand ensemble $\Sigma \subset [\![1, n]\!]$. Il est assez remarquable qu'à l'exception du premier lemme, indépendant des autres, tous les résultats de cette section sont établis par des méthodes *purement quantitatives* : ils n'utilisent pas de propriétés algébriques fines du groupe symétrique, par exemple.

Les deux premiers résultats font appel à la notion de *primitivité* d'une action de groupe.

Définition 3.3. Soit G un groupe agissant sur un ensemble X. On dit que l'action de G est *primitive* (ou, si G est donné comme un groupe de permutations, que G est primitif) si elle est transitive et s'il n'existe pas de partition $\mathscr{B} = \{B_1, \ldots, B_p\}$ de X non triviale telle que pour tout $g \in G$ et tout i, il existe j tel que $g \cdot B_i = B_j$.

Dans le cas contraire, on dit que l'action est *imprimitive*, et la partition $\mathscr{B}$ est appelée *système d'imprimitivité*.

Notons qu'une action 2-transitive est primitive.

L'un des problèmes les plus importants de la théorie des groupes naissante du XIX^e siècle était l'étude de groupes de permutations primitifs. Le problème type était de montrer qu'un sous-groupe primitif G de $\mathfrak{S}_n$ distinct de $\mathfrak{S}_n$ et de $\mathfrak{A}_n$ ne peut pas être très grand. Pendant près d'un siècle, le meilleur résultat connu a été celui de Bochert – affirmant que $|G| \leq n!/(n/2)!$ – que nous allons démontrer en l'adaptant au cas de parties de $\mathfrak{S}_n$ (lemme 3.5). Par la suite, cette borne a été raffinée en : $|G| \leq 4^n$ (cf. [PS80]), et une borne presque optimale ($e^{4\sqrt{n}(\ln n)^2}$) a été obtenue par Babai dans [Bab81].

Pour la suite, nous admettrons seulement les deux résultats suivants (le premier ne sert que dans la preuve de 3.5, le second dans 3.4) :

Fait (Jordan). *Un groupe de permutations primitif contenant un 3-cycle est soit symétrique, soit alterné.*

Fait (Praeger-Saxl). *Si un sous-groupe G de $\mathfrak{S}_n$ est primitif, alors soit $\mathfrak{A}_n \subset G$, soit $|G| \leq 4^n$.*

Rappelons qu'une *section* de G est par définition un quotient d'un sous-groupe de G.

Lemme 3.4. *Soit G un sous-groupe transitif de $\mathfrak{S}_n$, qui admet une section isomorphe à $\mathfrak{A}_k$ avec $k > \frac{n}{2}$. Si $n \geq 84$, $G = \mathfrak{S}_n$ ou $\mathfrak{A}_n$.*

Démonstration. G est primitif : sinon, G admettrait un système d'imprimitivité, donc s'injecterait dans $\mathfrak{S}_m \times \mathfrak{S}_{n/m}$ avec m un diviseur non trivial de n. Donc $\mathfrak{A}_k$ serait une section de $\mathfrak{S}_m \times \mathfrak{S}_{n/m}$, donc (par simplicité de $\mathfrak{A}_k$) une section d'un des facteurs de composition de $\mathfrak{S}_m \times \mathfrak{S}_{n/m}$, ce qui est impossible car ces facteurs sont $\mathbb{Z}/2\mathbb{Z}$, $\mathfrak{A}_m$ et $\mathfrak{A}_{n/m}$, tous de cardinal plus petit que $\mathfrak{A}_k$ (car $k > \frac{n}{2}$).

Comme de plus $|G| \geq |\mathfrak{A}_k| \geq \frac{1}{2}(\frac{n}{2})! \geq 4^n$ pour $n \geq 84$, on conclut par le lemme de Praeger-Saxl. □

Lemme 3.5. *Soit $n \geq 5$, $A \subset \mathfrak{S}_n$ symétrique. Si $\langle A \rangle$ est primitif et si $|A| > n!/\lfloor n/2 \rfloor !$, alors $A^{n^4} = \mathfrak{S}_n$ ou $\mathfrak{A}_n$.*

Démonstration. La preuve procède comme suit :

- en utilisant $|A| > n!/\lfloor n/2 \rfloor !$ et le principe des tiroirs, on montre qu'il existe $g, h \in A^2$ tels que $\mathrm{supp}\,(g) \cap \mathrm{supp}\,(h)$ est un singleton ;
- ceci implique que $x := [g, h] = ghg^{-1}h^{-1} \in A^8$ est un 3-cycle ;
- par le théorème de Jordan ($\langle A \rangle$ est primitif et contient un 3-cycle), $\langle A \rangle = \mathfrak{S}_n$ ou $\mathfrak{A}_n$ [4] ;
- on en déduit que l'action de $\langle A \rangle$ par conjugaison sur l'ensemble X des 3-cycles est transitive ($n \geq 5$), donc par 2.4 si $\ell = |X| \leq \frac{n^3}{3}$, $A^\ell \cdot x = X$. D'où $X \subset A^{n^3/3} A^8 A^{n^3/3} \subset A^{n^3-1}$;
- toute permutation paire est produit d'au plus n 3-cycles, donc $\mathfrak{A}_n \subset X^n \subset A^{n^4-1}$, et donc $A^{n^4} = \mathfrak{S}_n$ ou $\mathfrak{A}_n$. □

Les deux lemmes précédents comportent, au moins implicitement, une hypothèse de primitivité. Dans ce qui suit, on se place dans le cas général : que peut-on dire d'une grande partie A de $\mathfrak{S}_n$, sans faire d'hypothèse de primitivité, ni même de transitivité, sur $\langle A \rangle$?

Le lemme suivant est une adaptation d'un résultat déjà connu dû à Liebeck, portant sur les grands sous-groupes de $\mathfrak{S}_n$. Les arguments de [HS13] sont purement quantitatifs.

4. On pouvait aussi utiliser le résultat de Praeger-Saxl, qui n'utilise pas l'existence de 3-cycle. Mais de toute façon, nous aurons besoin de l'existence de ce 3-cycle engendré rapidement pour montrer que $\langle A \rangle$ est engendré rapidement. De plus, ceci permet de reprendre la preuve originale du théorème de Bochert.

Lemme 3.6. *Soit $\frac{1}{2} < d < 1$, et $A \subset \mathfrak{S}_n$ symétrique telle que $|A| \geq d^n n!$. Si n est plus grand qu'une constante ne dépendant que de d, il existe une orbite $\Delta \subset [\![1, n]\!]$ sous l'action de $\langle A \rangle$ telle que $|\Delta| \geq dn$ et $(A^{n^4})|_\Delta = \mathfrak{S}_\Delta$ ou $\mathfrak{A}_\Delta$.*

Démonstration. Voici les grandes étapes de la preuve :

- l'hypothèse $|A| \geq d^n n!$ implique que, pour n assez grand, $\langle A \rangle$ admet une orbite Δ de cardinal $k \geq dn$: dans le cas contraire, $|A| \leq (dn)!((1-d)n)! = o(d^n n!)$;
- de plus, $A|_\Delta$ est assez grand car A l'est : $|A|_\Delta| \geq \frac{|A|}{(\mathfrak{S}_n)_{(\Delta)}} \geq \frac{d^n n!}{(n-k)!}$;
- le groupe transitif $G = \langle A|_\Delta \rangle$ est donc primitif : sinon G admet un système d'imprimitivité de m blocs, d'où $|G| \leq m! \left((\frac{k}{m})!\right)^m \leq 2\left((\frac{k}{2})!\right)^2$; cette majoration, combinée à la minoration précédente, donne $\frac{d^n n!}{(n-k)!} \leq 2\left((\frac{k}{2})!\right)^2 \leq 2k!$, d'où (par Stirling) $2 \geq d^n \binom{n}{k} \geq d^n \binom{n}{\lfloor dn \rfloor} = d^n\, n^{O(1)} (d^{-d}(1-d)^{-(1-d)})^n = n^{O(1)} \left(\frac{1}{d(1-d)}\right)^{(1-d)n}$, ce qui est faux pour n assez grand ;
- la minoration du deuxième point donne $|A|_\Delta| \geq \frac{k!}{\lfloor k/2 \rfloor!}$, et on a vu que $\langle A|_\Delta \rangle$ est transitif, donc par 3.5 $(A|_\Delta)^{k^4} = \mathfrak{S}_\Delta$ ou $\mathfrak{A}_\Delta$, ce qui conclut. □

Avec un peu de travail, on peut renforcer la conclusion de ce lemme pour obtenir l'énoncé sur les grandes parties de $\mathfrak{S}_n$ dont nous aurons besoin. La différence avec le lemme précédent est que A^k, k contrôlé, « contient » $\mathfrak{A}_\Delta$ en un sens plus fort, précisément : avec des permutations qui fixent $[\![1, n]\!] \setminus \Delta$ point par point.

Lemme 3.7. *Soit $\frac{1}{2} < d < 1$, et $A \subset \mathfrak{S}_n$ symétrique telle que $|A| \geq d^n n!$. Si n est plus grand qu'une constante ne dépendant que de d, il existe une orbite $\Delta \subset [\![1, n]\!]$ sous l'action de $\langle A \rangle$ avec $|\Delta| \geq dn$ telle que $(A^{8n^5})_{([\![1,n]\!] \setminus \Delta)}|_\Delta$ contienne $\mathfrak{A}_\Delta$.*

Démonstration. Il nous suffit de montrer que, pour $|\Delta| > \frac{n}{2}$, si $A' \subset (\mathfrak{S}_n)_\Delta$ symétrique vérifie $A'|_\Delta = \mathfrak{S}_\Delta$ ou $\mathfrak{A}_\Delta$, alors $(A'^{8n})_{([\![1,n]\!] \setminus \Delta)}|_\Delta$ contient $\mathfrak{A}_\Delta$ (puis de prendre $A' = A^{n^4}$). Soit $\Omega = [\![1, n]\!] \setminus \Delta$. Nous donnons une nouvelle fois un schéma de la preuve :

- comme $A'|_\Delta = \mathfrak{S}_\Delta$ ou $\mathfrak{A}_\Delta$, $|A'| \geq \frac{1}{2}|\Delta|! > |\Omega|!$, donc il existe deux éléments de A' dont l'action sur Ω (qui est stable par A') est la même, donc il existe $g \in A'^2 \setminus \{e\}$ tel que $g|_\Omega = \mathrm{Id}_\Omega$;
- on utilise le fait suivant, qui se montre par disjonction de cas : si $\sigma \in \mathfrak{S}_m$, $m \geq 6$, est distincte de l'identité, alors soit il existe $\tau \in \mathfrak{A}_m$ tel que $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ soit un 3-cycle, soit il existe $\tau, \tau' \in \mathfrak{A}_m$ tels que $[[\sigma, \tau], \tau']$ soit un 3-cycle ;
- en l'appliquant à $\sigma = g|_\Delta$, et en utilisant que $A' \geq \mathfrak{A}_\Delta$, on obtient qu'ou bien il existe $h \in A'$ tel que $[g, h] \in A^6$ soit un 3-cycle à support dans Δ, ou bien il existe $h, h' \in A'$ tels que $[[g, h], h'] \in A'^{14}$ soit un 3-cycle à support dans Δ ; dans tous les cas, A'^{14} contient un tel 3-cycle ;
- en conjuguant par les éléments de A', comme $A'|_\Delta$ est 3-transitif, il vient que A'^{16} contient tous les 3-cycles à support dans Δ ;
- toute permutation paire de Δ étant produit d'au plus $\frac{|\Delta|}{2} \leq \frac{n}{2}$ 3-cycles (par récurrence sur la taille du support, qu'on peut faire diminuer de 2 après chaque composition par un 3-cycle convenable), on en déduit que $(\mathfrak{A}_n)_{(\Omega)} \subset (A'^{16})^{n/2} \subset A'^{8n}$. □

3.3 Chaînes de stabilisateurs

Le lemme suivant montre comment occuper beaucoup de classes modulo $(\mathfrak{S}_n)_{(\Sigma)}$ à partir de la donnée d'une chaîne de stabilisateurs.

Lemme 3.8. *Soit $\Sigma = \{\alpha_1, \dots, \alpha_m\} \subset [\![1, n]\!]$ et $A \subset \mathfrak{S}_n$. Supposons que, pour $1 \leq i \leq m$, on ait :*

$$|A_{(\alpha_1,\dots,\alpha_{i-1})} \cdot \alpha_i| \geq r_i$$

Alors A^m occupe au moins $\prod_{i=1}^m r_i$ classes à gauche modulo $(\mathfrak{S}_n)_{(\Sigma)}$.

Démonstration. Considérons l'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]^m$: le stabilisateur de $(\alpha_1, \dots, \alpha_m)$ est $(\mathfrak{S}_n)_{(\Sigma)}$, et donc le nombre de classes à gauche modulo $(\mathfrak{S}_n)_{(\Sigma)}$ que rencontre A^m est égal à $|A^m \cdot (\alpha_1, \dots, \alpha_m)|$. Pour $i = 1, \dots, m$, soit $B_i \subset A_{(\alpha_1,\dots,\alpha_{i-1})}$ telle que les $b \cdot \alpha_i$, $b \in B_i$, soient deux à deux distincts et au nombre de r_i, *i.e.* $|B_i| = r_i$.

Maintenant si $b_1 \dots b_m \cdot (\alpha_1, \dots, \alpha_m) = b'_1 \dots b'_m \cdot (\alpha_1, \dots, \alpha_m)$, on a $b_1 = b'_1$ (en regardant la première coordonnée, qui est $b_1 \cdot \alpha_1 = b'_1 \cdot \alpha_1$), puis (en regardant la deuxième coordonnée) $b_2 = b'_2$ et ainsi de suite : $(b_1, \dots, b_m) = (b'_1, \dots, b'_m)$. D'où $|A^m \cdot (\alpha_1, \dots, \alpha_m)| \geq r_1 \dots r_m$ comme voulu. □

Ainsi, en choisissant $\alpha_1, \dots, \alpha_m$, m assez grand, tels que les orbites $A_{(\alpha_1,\dots,\alpha_{i-1})} \cdot \alpha_i$ soient toutes grandes – ce que permet de faire le lemme de séparation, cf. lemme 2.6 – on obtient que A^m occupe beaucoup de classes modulo $(\mathfrak{S}_n)_{(\Sigma)}$ par le lemme précédent. Le lemme 3.2 montre alors que $(A^m)_\Sigma$ occupe beaucoup de classes modulo $(\mathfrak{S}_n)_{(\Sigma)}$, *i.e.* que $(A^m)_\Sigma|_\Sigma$ est grand. On peut alors appliquer le lemme de Liebeck 3.7. C'est de cette manière que l'on établit l'énoncé :

Lemme 3.9. *Soient $d > \frac{1}{2}$, $A \subset \mathfrak{S}_n$ symétrique. Soit $\Sigma = \{\alpha_1, \dots, \alpha_m\}$ une partie de $[\![1, n]\!]$ telle que pour $i = 1, \dots, m$:*

$$|A_{(\alpha_1,\dots,\alpha_{i-1})} \cdot \alpha_i| \geq dn$$

Si m est plus grand qu'une constante ne dépendant que de d, il existe une partie $\Delta \subset \Sigma$ telle que $|\Delta| \geq d|\Sigma|$ et

$$\mathfrak{A}_\Delta \subset ((A^{16m^6})_\Sigma)_{(\Sigma\setminus\Delta)}|_\Delta$$

i.e. pour toute permutation paire h de Δ, il existe un élément de A^{16m^6} qui agit comme h sur Δ et qui agit trivialement sur $\Sigma \setminus \Delta$.

4 Petites parties génératrices et étape de création

4.1 Petites parties génératrices

Le but de cette section est de répondre à la question suivante : étant donnée une partie génératrice du groupe symétrique ou alterné, en combien d'étapes peut-on engendrer un petit ensemble de générateurs (précisément : de taille bornée par une constante absolue) d'un groupe transitif ?

Tout comme dans la preuve du lemme de séparation (2.6), on fera dans cette partie un usage extensif de la méthode probabiliste et de sa variante stochastique. Le lemme de convergence des distributions des marches aléatoires sur un graphe vers la distribution uniforme (lemme 2.3) sera au centre de la démarche suivie.

Lemme 4.1. *Soit A une partie de $\mathfrak{S}_n$ contenant l'identité et qui engendre un sous-groupe transitif de $\mathfrak{S}_n$. Il existe $g \in A^n$ tel que $|\mathrm{supp}\,(g)| \geq \frac{n}{2}$.*

Démonstration. On va montrer que, pour une certaine loi de probabilité sur A^n, pour tout $\alpha \in [\![1, n]\!]$ on a $g \cdot \alpha \neq \alpha$ avec une probabilité supérieure à $\frac{1}{2}$.

Soit $i \in [\![1, n]\!]$; comme $\langle A \rangle$ est transitif, A ne fixe pas i (sinon $\langle A \rangle$ fixerait i), donc il existe $g_i \in A$ tel que $g_i \cdot i \neq i$. Considérons les éléments de A^n de la forme $g = g(\vec{a}) = g_1^{a_1} \cdots g_n^{a_n}$ où $\vec{a} = (a_1, \dots, a_n)$ est choisi avec probabilité uniforme dans $\{0, 1\}^n$.

Soit $\alpha \in [\![1,n]\!]$, et soit i minimal tel que $g_i \cdot \alpha \neq \alpha$, de sorte que $g \cdot \alpha = g_i^{a_i} h \cdot \alpha$, où $h := g_{i+1}^{a_{i+1}} \dots g_n^{a_n}$. Si $h \cdot \alpha = \alpha$, alors g déplace α si et seulement si $a_i = 1$, ce qui se produit avec probabilité $\frac{1}{2}$. Si $h\alpha \neq \alpha$, alors pour que g déplace α il suffit que $a_i = 0$, ce qui a lieu avec probabilité $\frac{1}{2}$. Donc g déplace α avec une probabilité supérieure à $\frac{1}{2}$.

Soit $N = N(g) = |\mathrm{supp}\,(g)|$ le nombre d'éléments déplacés par l'élément $g \in A^n$. On a :

$$\mathbb{E}[N] = \mathbb{E}\Big[\sum_{\alpha\in[\![1,n]\!]} \mathbb{1}_{\{g\cdot\alpha\neq\alpha\}}\Big] = \sum_{\alpha\in[\![1,n]\!]} \mathbb{P}(g\cdot\alpha\neq\alpha) \geq \sum_{\alpha\in[\![1,n]\!]} \frac{1}{2} = \frac{n}{2}\,,$$

donc il existe $g \in A^n$ tel que $N(g) = |\mathrm{supp}\,(g)| \geq \frac{n}{2}$. □

Le fait suivant sera utilisé dans la preuve du lemme 4.3 : le raisonnement utilisé est assez classique dans des problèmes d'empilement de sphères. Sur $U = \{0,1\}^k$, on définit la distance de Hamming par :

$$d(\vec{x},\vec{y}) = \sum_{i=1}^{k} |x_i - y_i| = \mathrm{card}\{i \in [\![1,k]\!] | x_i \neq y_i\}$$

Lemme 4.2. *Soit $n \geq 1$, $k \geq 5\log_2 n$ et $U = \{0,1\}^k$. Si n est plus grand qu'une certaine constante, il existe n éléments de U qui diffèrent deux à deux d'au moins $\log_2 n$ coordonnées.*

Démonstration. Il suffit de le montrer pour $k = 5\lfloor\log_2 n\rfloor$. Choisissons $v_1 \in U$ quelconque, puis, si $v_1, \dots, v_i$ sont choisis, choisissons un v_{i+1} à distance $\geq \log_2 n$ de $v_1, \dots, v_i$. Soit r l'entier où ce procédé s'arrête, donc $U = \bigcup_{i=1}^{r} B(v_i, \log_2 n)$. Le fait que $r \geq n$ résulte du fait que le cardinal d'une boule de rayon $p = \lfloor\log_2 n\rfloor$ est

$$\sum_{0\leq j\leq p} \binom{5p}{p} < (p+1)\frac{(5p)!}{(4p)!p!} \sim \sqrt{\frac{5p}{8\pi}}\left(\frac{5^5}{4^4}\right)^p = o(2^{4p})$$

donc, pour n plus grand qu'une certaine constante, le cardinal d'une boule de rayon p est $< 2^{4p-1}$, d'où $r \geq \frac{n}{2^{4p-1}} \geq 2^{p+1} \geq n$. □

Lemme 4.3. *Soit A une partie symétrique de $\mathfrak{S}_n$ qui engendre $\mathfrak{S}_n$ ou $\mathfrak{A}_n$. Si n est assez grand, il existe $g \in A^n$ et $h \in A^{n^{44\ln n}}$ tels que $[\![1,n]\!]$ admette au plus $417(\ln n)^2$ orbites sous l'action de $\langle g,h\rangle$.*

Preuve abrégée. D'après 4.1, il existe $g \in A^n$ tel que $|\mathrm{supp}\,(g)| \geq \frac{n}{2}$. Soit $k = 5\lceil\log_2 n\rceil$, $\varepsilon = \frac{1}{n}$ et $\ell = 2n^{6k}\ln\left(\frac{n^{2k}}{\varepsilon}\right) = n^{\left(\frac{6\times5}{\ln 2}+o(1)\right)\ln n} = o(n^{44\ln n})$ lorsque $n \to \infty$, donc pour n assez grand $\ell < n^{44\ln n}$. Soit $h \in A^\ell$ le résultat une marche aléatoire paresseuse sur une partie $A' \subset A$ symétrique de cardinal $|A'| \leq 2n^{2k}$ avec $\langle A'\rangle$ $2k$-transitif ; d'après le lemme 2.5, h agit de manière uniforme (à un facteur $1 \pm \frac{1}{n}$ près) sur les $2k$-uplets d'éléments distincts de $[\![1,n]\!]$.

Nous allons montrer qu'en moyenne, pour h pris aléatoirement selon le procédé décrit plus haut, l'action de $\langle g,h\rangle$ admet peu d'orbites. Pour cela, commençons par fixer $\beta \in [\![1,n]\!]$, et montrons que $|\langle g,h\rangle \cdot \beta|$ est assez grand. Pour $\vec{a} = (a_1, \dots, a_k) \in U := \{0,1\}^k$, on pose :

$$f(\vec{a}) = g^{a_k} h \cdots g^{a_1} h \quad \text{et} \quad f_\beta(\vec{a}) = f(\vec{a}) \cdot \beta\,.$$

On gardera à l'esprit que $f(\vec{a})$ et $f_\beta(\vec{a})$ dépendent de h et sont donc des variables aléatoires. Nous allons montrer que, lorsque $\vec{a}$ parcourt U, il y a beaucoup de résultats possibles pour $f_\beta(\vec{a})$, et

pour cela nous chercherons à minorer $\mathbb{P}(f_\beta(\vec{a}) = f_\beta(\vec{a}'))$ pour $\vec{a}, \vec{a}' \in U$ distants pour la distance de Hamming. C'est à une telle minoration que le premier point (le plus long [5]) est consacré.

• Considérons $V \subset U$ de cardinal n dont les éléments diffèrent deux à deux d'au moins $\log_2 n$ coordonnées (qui existe grâce à 4.2). Soient $\vec{a}, \vec{a}' \in V$ distincts. On pose :

$$\beta_0 = \beta\,,\ \beta_1 = g^{a_1}h \cdot \beta\,,\ \ldots\,,\ \beta_k = g^{a_k}h \cdot \beta_{k-1}$$

et on définit de même β'_i en remplaçant $\vec{a}$ par $\vec{a}'$. Comme h agit de manière aléatoire sur $[\![1, n]\!]$, $\mathbb{P}(\beta_1 = \beta) = \mathbb{P}(h \cdot \beta = g^{-a_1}\beta) \sim \frac{1}{n}$, et $\mathbb{P}(h \cdot \beta = \beta_1) \sim \frac{1}{n}$ (pour être précis, cette probabilité est majorée par $\frac{1}{n}(1 + \frac{1}{n})$), donc la probabilité pour que $\beta = h \cdot \beta$ ou $\beta = \beta_1$ est majorée par un terme de l'ordre de $\frac{2}{n}$. De même, si les β_i et leurs images sont deux-à-deux distincts pour $i \leq i_0$ (ce qui, par récurrence, est presque certain modulo une probabilité de l'ordre de $\sum_{i=0}^{i_0-1} \frac{2i}{n} \sim \frac{i_0^2}{n}$), la probabilité pour que β_{i_0+1} ou $h \cdot \beta_{i_0+1}$ soit égal à un β_i ou $h \cdot \beta_i$ avec $i \leq i_0$ est de l'ordre de $\frac{2i_0}{n}$.

En procédant ainsi (et en utilisant que h agit aléatoirement sur les $2k$-uplets composés d'éléments deux-à-deux distincts), on obtient que la probabilité pour que les β_i et leurs images par h soient deux à deux distincts est au moins $1 - O(\frac{k^2}{n})$. Il en va donc de même pour les β'_i. Par un argument similaire (en travaillant toujours avec des suites à composantes deux-à-deux distinctes, sur lesquelles l'action de h est aléatoire), il est presque certain (probabilité $1 - O(\frac{k}{n})$) que, si les trajectoires se séparent, *i.e.* $\beta_i \neq \beta'_i$ pour un certain i, alors les trajectoires se séparent définitivement, *i.e.* $\beta_j \neq \beta'_j$ pour $j > i$. En particulier, pour $j = k$, $f_\beta(\vec{a}) \neq f_\beta(\vec{a}')$.

Il reste donc à minorer la probabilité que les trajectoires se séparent. Déjà, elles ne peuvent se séparer (pour la première fois) qu'en un indice i tel que $a_i \neq a'_i$, et alors elles se séparent si et seulement si $h \cdot \beta_{i-1} \in \mathrm{supp}\,(g)$, ce qui a lieu avec une probabilité supérieure à $\frac{|\mathrm{supp}\,(g)|}{n}(1 - \frac{1}{n}) \geq \frac{1}{2}(1 - \frac{1}{n})$. Comme $\vec{a}$ et $\vec{a}'$ diffèrent d'au moins $\log_2 n$ coordonnées, la probabilité que l'on ait $h \cdot \beta_{i-1} \notin \mathrm{supp}\,(g)$ pour tout i tel que $a_i \neq a'_i$ est inférieure à (chaque événement « $h \cdot \beta_{i-1} \notin \mathrm{supp}\,(g)$ » étant presque indépendant des autres car, h agissant de manière aléatoire, β_{i-1} est presque indépendant de β_{j-1} si $i \neq j$) : $(\frac{1}{2}(1 + \frac{1}{n}))^{\log_2 n} = O(\frac{1}{n})$.

En sommant les probabilités de tous les cas négligés, on obtient que pour tous $\vec{a}, \vec{a}' \in V$ distincts, $\mathbb{P}(f_\beta(\vec{a}) \neq f_\beta(\vec{a}')) \geq 1 - O(\frac{k^2}{n}) - O(\frac{k}{n}) - O(\frac{1}{n}) = 1 - O(\frac{k^2}{n})$, les constantes en jeu dans les O étant absolues. En effectuant un décompte des couples de trajectoires décrits précédemment comme dans [HS13], on obtient pour n assez grand :

$$\mathbb{P}(f_\beta(\vec{a}) \neq f_\beta(\vec{a}')) \geq 1 - \frac{8k^2}{n} \tag{1}$$

• Soit $\gamma_1, \ldots, \gamma_r$ les images de l'application $\vec{a} \mapsto f_\beta(\vec{a})$ de V dans $\langle g, h\rangle \cdot \beta$, et k_i le nombre d'antécédents de γ_i. On a par l'inégalité de Cauchy-Schwarz :

$$\frac{1}{r} \leq \frac{\sum_{i=1}^r k_i^2}{\left(\sum_{i=1}^r k_i\right)^2} = \frac{|\{(\vec{a}, \vec{a}') \in V^2 | f_\beta(\vec{a}) = f_\beta(\vec{a}')\}|}{|V|^2} \tag{2}$$

• Enfin, soit $N = N(h)$ le nombre d'orbites sous l'action de $\langle g, h\rangle$. On a $N = \sum_{\beta \in [\![1,n]\!]} \frac{1}{|\langle g,h\rangle \cdot \beta|}$

5. C'est sur ce point que la preuve est abrégée : pour obtenir une justification rigoureuse de la majoration de $\mathbb{P}(f_\beta(\vec{a}) = f_\beta(\vec{a}'))$, [HS13] procède en considérant l'ensemble des couples de trajectoires (qui ne reviennent pas sur leur pas) $(\beta_i), (\beta'_i)$ qui coïncident puis deviennent disjointes à partir d'un certain indice r (nécessairement tel que $a_r \neq a'_r$), puis estime la probabilité de suivre de telles trajectoires, ce qui donne une minoration de $\mathbb{P}(f_\beta(\vec{a}) \neq f_\beta(\vec{a}'))$. Pour ne pas trop alourdir la preuve, nous avons préféré en donner l'idée plutôt que le détail.

(car la contribution de chaque orbite $\langle g,h\rangle\cdot\beta$ est : $|\langle g,h\rangle\cdot\beta|\times\frac{1}{|\langle g,h\rangle\cdot\beta|}=1$) d'où :

$$\begin{aligned}\mathbb{E}[N] &= \sum_{\beta\in[\![1,n]\!]}\mathbb{E}\left[\frac{1}{|\langle g,h\rangle\cdot\beta|}\right]\overset{(2)}{\leq}\frac{1}{|V|^2}\sum_{\beta\in[\![1,n]\!]}\mathbb{E}\Big[\sum_{(\vec{a},\vec{a}')\in V^2}\mathbb{1}_{\{f_\beta(\vec{a})=f_\beta(\vec{a}')\}}\Big]\\ &= \frac{1}{|V|^2}\sum_{\beta\in[\![1,n]\!]}\sum_{(\vec{a},\vec{a}')\in V^2}\mathbb{P}(f_\beta(\vec{a})=f_\beta(\vec{a}'))\overset{(1)}{\leq}\frac{1}{|V|^2}n\times\left(|V|^2\frac{8k^2}{n}+|V|\right)\leq 417(\ln n)^2\end{aligned}$$

pour n grand, donc il existe $h\in A^{n^{44\ln n}}$ tel que $\langle g,h\rangle$ admette au plus $417(\ln n)^2$ orbites. □

Lemme 4.4. *Soit A une partie symétrique de $\mathfrak{S}_n$ qui engendre $\mathfrak{S}_n$ ou $\mathfrak{A}_n$. Si n est plus grand qu'une constante absolue, il existe $g_1,g_2,g_3\in A^{n^{44\ln n}}$ tels que $\langle g_1,g_2,g_3\rangle$ soit transitif.*

Démonstration. Soient $g\in A^n$ et $h\in A^{n^{44\ln n}}$ tels que l'action de $\langle g,h\rangle$ sur $[\![1,n]\!]$ admette au plus $C_4(\ln n)^2$ orbites ($C_4=417$) comme dans le lemme 4.3. Soit $\ell=\lceil 2n^6\ln(\frac{n^2}{\varepsilon})\rceil$, où $\varepsilon=\frac{1}{n}$, et soit $\gamma\in A^\ell$ le résultat d'une marche aléatoire comme dans 2.5 (de sorte que la variable aléatoire γ agit de manière presque uniforme sur les *couples* d'éléments distincts de $[\![1,n]\!]$). Nous allons montrer qu'avec une probabilité positive $\langle g,h,\gamma\rangle$ est transitif.

Soit Δ la réunion des orbites sous $\langle g,h\rangle$ de taille strictement inférieure à $\sqrt{n}$, et S un système de représentants de ces orbites. Alors, comme $|\Delta|\leq C_4(\ln n)^2\sqrt{n}$ (en tant que réunion d'au plus $C_4(\ln n)^2$ orbites de cardinal inférieur à $\sqrt{n}$), on a pour tout $\alpha\in S$: $\mathbb{P}(\gamma\cdot\alpha\in\Delta)\leq\frac{C_4(\ln n)^2\sqrt{n}}{n}\cdot(1+\frac{1}{n})$, d'où

$$\mathbb{P}(\exists\alpha\in S,\gamma\cdot\alpha\in\Delta)\leq\frac{2C_4^2(\ln n)^4}{\sqrt{n}}\,. \tag{3}$$

Soit maintenant κ_0 une orbite sous $\langle g,h\rangle$ de cardinal maximal (donc $|\kappa_0|\geq\frac{n}{C_4(\ln n)^2}$) fixée une fois pour toutes, et κ une orbite de cardinal supérieur ou égal à $\sqrt{n}$. On a d'une part :

$$\mathbb{E}[|\gamma\cdot\kappa\cap\kappa_0|]=\mathbb{E}\Big[\sum_{\alpha\in\kappa}\mathbb{1}_{\{\gamma\cdot\alpha\in\kappa_0\}}\Big]=\sum_{\alpha\in\kappa}\mathbb{P}(\gamma\cdot\alpha\in\kappa_0)\geq\frac{|\kappa|\cdot|\kappa_0|}{n}\cdot\left(1-\frac{1}{n}\right)$$

et d'autre part :

$$\begin{aligned}\mathbb{E}[|\gamma\cdot\kappa\cap\kappa_0|^2] &= \mathbb{E}\Big[\sum_{(\alpha,\alpha')\in\kappa^2}\mathbb{1}_{\{\gamma\cdot\alpha\in\kappa_0\}}\mathbb{1}_{\{\gamma\cdot\alpha'\in\kappa_0\}}\Big]=\sum_{(\alpha,\alpha')\in\kappa^2}\mathbb{P}(\gamma\cdot(\alpha,\alpha')\in\kappa_0^2)\\ &= \sum_{\alpha\in\kappa}\mathbb{P}(\gamma\cdot\alpha\in\kappa_0)+\sum_{(\alpha,\alpha')\in\kappa^2,\alpha\neq\alpha'}\mathbb{P}(\gamma\cdot(\alpha,\alpha')\in\kappa_0^2)\\ &\leq \frac{|\kappa|\cdot|\kappa_0|}{n}\cdot\left(1+\frac{1}{n}\right)+\frac{|\kappa|(|\kappa|-1)\cdot|\kappa_0|(|\kappa_0|-1)}{n(n-1)}\cdot\left(1+\frac{1}{n}\right)\\ &\leq \left(\frac{|\kappa|\cdot|\kappa_0|}{n}+\frac{|\kappa|^2\cdot|\kappa_0|^2}{n^2}\right)\cdot\left(1+\frac{1}{n}\right)\end{aligned}$$

D'où si $X(\gamma)=|\gamma\cdot\kappa\cap\kappa_0|$, on a par l'inégalité de Bienaymé-Tchebychev :

$$\begin{aligned}\mathbb{P}(\gamma\cdot\kappa\cap\kappa_0=\varnothing) &\leq \mathbb{P}(|X-\mathbb{E}[X]|\geq\mathbb{E}[X])\leq\frac{\mathrm{var}(X)}{\mathbb{E}[X]^2}=\frac{\mathbb{E}[|\gamma\cdot\kappa\cap\kappa_0|^2]}{\mathbb{E}[|\gamma\cdot\kappa\cap\kappa_0|]^2}-1\\ &\leq \left(1+\frac{n}{|\kappa|\cdot|\kappa_0|}\right)\cdot\left(1+\frac{1}{n}\right)\cdot\left(1-\frac{1}{n}\right)^{-2}-1\\ &\leq \left(1+\frac{C_4(\ln n)^2}{\sqrt{n}}\right)\cdot\left(1+\frac{1}{n}\right)\cdot\left(1-\frac{1}{n}\right)^{-2}-1\\ &\leq \frac{2C_4(\ln n)^2}{\sqrt{n}}\end{aligned}$$

pour n plus grand qu'une constante absolue. En sommant sur les orbites de cardinal supérieur à $\sqrt{n}$:

$$\mathbb{P}(\text{il existe une orbite } \kappa \text{ sous } \langle g,h\rangle \text{ telle que } |\kappa| \geq \sqrt{n} \text{ et } \gamma\cdot\kappa\cap\kappa_0 = \varnothing) \leq \frac{2C_4^2(\ln n)^4}{\sqrt{n}} \qquad (4)$$

En combinant (3) et (4), la probabilité que toute orbite (sous $\langle g,h\rangle$) de cardinal $< \sqrt{n}$ soit reliée par γ à une orbite de cardinal $\geq \sqrt{n}$ et que toute orbite de cardinal $\geq \sqrt{n}$ soit reliée par γ à κ_0 (ce qui entraîne que $\langle g,h,\gamma\rangle$ est transitif) est supérieure à $1 - \frac{4C_4^2(\ln n)^4}{\sqrt{n}}$, donc positive si n est assez grand. Ainsi pour n grand, il existe $\gamma \in A^{n^7}$ tel que $\langle g,h,\gamma\rangle$ soit transitif. □

Nous venons de répondre à la question posée au début de cette partie. Mais il est possible de renforcer la conclusion de l'énoncé précédent, et c'est à cela que nous allons dédier la fin de cette section.

4.2 Étape de création

Lemme 4.5 (Schreier)**.** *Soit G un groupe, H un sous-groupe et A une partie symétrique de G. On suppose que A intersecte toutes les classes à gauche de G modulo H. Alors : $\langle A\rangle\cap H = \langle A^3\cap H\rangle$ et $\langle A\rangle = A\langle A^3\cap H\rangle$.*

Démonstration. Il suffit de montrer que $\langle A\rangle = A\langle A^3\cap H\rangle$ (car alors, comme $\langle A^3\cap H\rangle \subset H$, $\langle A\rangle\cap H = (A\cap H)\langle A^3\cap H\rangle = \langle A^3\cap H\rangle$). Comme $B := A\langle A^3\cap H\rangle$ est clairement contenu dans $\langle A\rangle$, et que $e\in B$, il suffit de montrer que $AB\subset B$ (car alors $\langle A\rangle\subset B$).

Soit donc $g = ah \in B$, avec $a\in A$ et $h\in\langle A^3\cap H\rangle$, et $a'\in A$. Comme A rencontre toutes les classes à gauche modulo H, il existe $a''\in A$ tel que $a'aH = a''H$, d'où : $a'g = a''(a''^{-1}a'a)h \in A(A^3\cap H)\langle A^3\cap H\rangle \subset B$. Ceci conclut la preuve. □

Comme annoncé, le corollaire qui suit renforce le lemme 4.4. Nous ne nous en servirons que dans le cas $k=2$, où il permet d'obtenir un ensemble de 6 générateurs d'un groupe 2-transitif en « temps » $e^{O((\ln n)^2)}$.

Une petite remarque sur ce résultat : on pourrait être tenté de l'appliquer avec k très grand, de manière à engendrer des groupes à fort degré de transitivité, donc potentiellement de plus en plus grands. Mais ceci n'est pas nécessaire : la classification des groupes finis simples implique qu'un groupe de permutations 6-transitif est symétrique ou alterné. Notons que ce constat permet de remplacer « constante ne dépendant que de k » par « constante absolue » dans l'énoncé ci-dessus.

Corollaire 4.6. *Soit A une partie symétrique de $\mathfrak{S}_n$ qui engendre $\mathfrak{S}_n$ ou $\mathfrak{A}_n$. Soit $k\geq 1$. Si n est plus grand qu'une constante ne dépendant que de k, il existe une partie $B\subset A^{n^{45\ln n}}$ de cardinal inférieur ou égal à $3k$ telle que $\langle B\rangle$ soit k-transitif.*

Démonstration. Soient $\alpha_1,\dots,\alpha_{k-1}\in[\![1,n]\!]$ deux-à-deux distincts.

On pose $A_0 = A$, et pour $1\leq i<k$, $A_i = (A_{i-1}^{3n})_{(\alpha_1,\dots,\alpha_i)}$. Montrons que $\langle A_i\rangle \geq (\mathfrak{A}_n)_{(\alpha_1,\dots,\alpha_i)}$. Pour $i=0$ c'est vrai, et si $\langle A_i\rangle \geq (\mathfrak{A}_n)_{(\alpha_1,\dots,\alpha_i)}$, alors par le lemme 2.4 $A_i^n\cdot\alpha_{i+1} = [\![1,n]\!]\setminus\{\alpha_1,\dots,\alpha_i\}$ donc A_i^n rencontre toutes les classes à gauche modulo $(\mathfrak{S}_n)_{(\alpha_1,\dots,\alpha_{i+1})}$. Par le lemme de Schreier 4.5, $\langle((A_i^n)^3)_{(\alpha_1,\dots,\alpha_{i+1})}\rangle = \langle A_i^n\rangle\cap(\mathfrak{S}_n)_{(\alpha_1,\dots,\alpha_{i+1})}$ donc $\langle A_{i+1}\rangle \geq (\mathfrak{A}_n)_{(\alpha_1,\dots,\alpha_{i+1})}$ comme voulu.

Comme $\langle A_i\rangle \geq (\mathfrak{A}_n)_{(\alpha_1,\dots,\alpha_i)}$ pour $0\leq i\leq k-1$, en identifiant par restriction $(\mathfrak{S}_n)_{(\alpha_1,\dots,\alpha_i)}$ à $\mathfrak{S}_{[\![1,n]\!]\setminus\{\alpha_1,\dots,\alpha_i\}}$ il existe par 4.4 $g_{1,i},g_{2,i},g_{3,i}\in A_i^{n^{44\ln n}}$ tels que $\langle g_{1,i},g_{2,i},g_{3,i}\rangle$ agisse transitivement sur $[\![1,n]\!]\setminus\{\alpha_1,\dots,\alpha_i\}$. Soit $S = \{g_{1,0},g_{2,0},g_{3,0},\dots,g_{1,k-1},g_{2,k-1},g_{3,k-1}\}$; comme $A_{i+1}\subset A_i^{3n}$, $S\subset A^{(3n)^k\cdot n^{44\ln n}}\subset A^{n^{45\ln n}}$ si n est plus grand qu'un constante ne dépendant que

de n, et $|S| \leq 3k$. Le fait que $\langle S \rangle$ soit k-transitif résulte de ce que pour $0 \leq i \leq k-1$, $\langle S \rangle_{(\alpha_1,\dots,\alpha_i)}$ agit transitivement sur $[\![1,n]\!] \setminus \{\alpha_1,\dots,\alpha_i\}$. □

L'intérêt de construire une petite partie qui engendre un sous-groupe 2-transitif réside dans le lemme suivant, qu'on pourra appliquer dans la dernière partie avec $k = 6$ pour obtenir beaucoup d'éléments dans un stabilisateur point par point : c'est l'étape de *création*, qui précède l'utilisation du lemme de séparation. Elle consiste à obtenir de la croissance en faisant agir le stabilisateur global par conjugaison sur le stabilisateur point par point.

Lemme 4.7. *Soient $G = \mathfrak{A}_n$ ou $\mathfrak{S}_n$, H^+ un sous-groupe de G, H^- un sous-groupe distingué de H^+ et Γ une orbite à la fois de H^+ et de H^-. Soient $Y \subset H^-$ de cardinal r telle que $\langle Y \rangle|_\Gamma$ soit 2-transitif sur Γ et $B \subset H^+$. Alors :*

- *soit il existe $b \in B^{-1}B$ tel que $b|_\Gamma = e$;*
- *soit $|BYB^{-1} \cap H^-| \geq |B|^{1/r}$.*

Démonstration. B agit sur $\bar{y} = (y_1,\dots,y_r)$ par conjugaison, où $Y = \{y_1,\dots,y_r\}$. S'il existe $b_1, b_2 \in B$ distincts tels que $b_1 \cdot \bar{y} = b_2 \cdot \bar{y}$, *i.e.* $b_1 y_i b_1^{-1} = b_2 y_i b_2^{-1}$ pour tout i, alors $b_1^{-1}b_2|_\Gamma$ commute avec tous les $y_i|_\Gamma$, donc avec tous les éléments de $\langle Y \rangle|_\Gamma$, d'où, comme ce groupe est 2-transitif : $b_1^{-1}b_2|_\Gamma = e$.

Si les $(by_1b^{-1},\dots,by_rb^{-1})$ sont deux à deux distincts, alors comme H^- est distingué dans H^+, ce sont tous des r-uplets de $BYB^{-1} \cap H^-$, donc :

$$|BYB^{-1} \cap H^-|^r \geq |B|$$

d'où le résultat. □

5 Démonstration du théorème

L'idée de la preuve consiste à construire par récurrence des chaînes de stabilisateurs de plus en plus grandes. Pour traiter les cas de sortie de la récurrence, on aura besoin du théorème 1.4 de l'introduction, et du théorème suivant, montré dans [BBS04].

Théorème 5.1. *Soit $0 < \varepsilon < \frac{1}{3}$. Il existe $C_5(\varepsilon)$ telle que si $G = \mathfrak{S}_n$ ou $\mathfrak{A}_n$ et A est une partie génératrice de G contenant un élément h tel que $1 < |\mathrm{supp}\,(h)| \leq \varepsilon n$, alors :*

$$\mathrm{diam}\,(\Gamma(G,A)) \leq C_5(\varepsilon) n^8$$

5.1 Cas de sortie de la récurrence

Le lemme suivant permettra de construire des éléments de petite orbite pour pouvoir utiliser ce dernier théorème :

Lemme 5.2. *Soient $\Delta \subset [\![1,n]\!]$ avec $|\Delta| \geq (\ln n)^2$ et H un sous-groupe de $\mathfrak{S}_n$ tel que $H|_\Delta$ soit $\mathfrak{S}_\Delta$ ou $\mathfrak{A}_\Delta$. Soit enfin Γ une orbite de H.*

Alors, si n est plus grand qu'une certaine constante absolue, il existe $g \in H \setminus \{e\}$ tel que $\mathrm{supp}\,(g|_\Gamma) < \frac{|\Gamma|}{4}$.

Démonstration. On note $p_1, p_2, \dots$ la suite des nombres premiers. Soit k maximal tel que $p_1 \dots p_k > n^4$. Le théorème des nombres premiers assure que $2p_1 + p_2 + \dots + p_k < (\ln n)^2$ pour n assez grand, donc il existe $h \in H$ tel que $h|_\Delta$ soit la composée de cycles à supports disjoints de longueur $p_1, p_1, p_2, p_3, \dots, p_k$.

Un argument de double-comptage montre alors qu'il existe p tel que le nombre de $\alpha \in [\![1,n]\!]$ tels que p divise la longueur du cycle de h contenant α soit inférieur à $\frac{|\Gamma|}{4}$. On note alors d l'ordre de h et on prend $g = h^{d/p}$. □

On aura besoin du lemme suivant, conséquence de 4.5 :

Lemme 5.3. *Soient $\Delta \subset [\![1,n]\!]$ et $B^+ \subset (\mathfrak{S}_n)_\Delta$ symétrique, tels que $B^+|_\Delta = \mathfrak{A}_\Delta$ ou $\mathfrak{S}_\Delta$. Soit $B^- = \big((B^+)^3\big)_{(\Delta)}$.*

Alors $\langle B^-\rangle = \langle B^+\rangle_{(\Delta)}$, et c'est donc un sous-groupe distingué de $\langle B^+\rangle$. De plus, si $\langle B^-\rangle$ admet une orbite Γ de taille supérieure à $\frac{n}{2}$, alors Γ est aussi une orbite de $\langle B^+\rangle$.

Démonstration. La première partie de l'énoncé est une conséquence immédiate du lemme 4.5. De plus, $\langle B^-\rangle$ étant distingué, on vérifie facilement que ses orbites forment un système d'imprimitivité de $\langle B^+\rangle$. Or, on ne peut pas avoir deux éléments d'une partition de $[\![1,n]\!]$ tous deux de taille supérieure à $\frac{n}{2}$, donc Γ est une orbite de $\langle B^+\rangle$. □

Le lemme suivant montre comment utiliser les théorèmes 1.4 et 5.1 pour se ramener au diamètre de groupes plus petits :

Lemme 5.4. *Soient $G = \mathfrak{S}_n$ ou $\mathfrak{A}_n$, $\Delta \subset [\![1,n]\!]$ avec $\Delta \geq (\ln n)^2$ et A partie génératrice symétrique de G. Soient $B^+ = (A^\ell)_\Delta$ avec $\ell \geq 1$ et $B^- = \big((B^+)^3\big)_{(\Delta)}$. On suppose que $B^+|_\Delta$ est $\mathfrak{A}_\Delta$ ou $\mathfrak{S}_\Delta$ et que $\langle B^-\rangle$ admet une orbite Γ de taille supérieure à ρn avec $\rho > \frac{8}{9}$.*

Si tous les facteurs de composition de $\langle B^-\rangle$ de la forme $\mathfrak{A}_k$ vérifient $k \leq \delta n$, on pose :

$$D = \max_{k \leq \delta n} \operatorname{diam}(\mathfrak{A}_k)$$

Alors si n est plus grand qu'une constante absolue, on a :

$$\mathfrak{A}_n \subset A^{\ell D e^{C_6(\rho)(\ln n)^3}}$$

où $C_6(\rho)$ ne dépend que de ρ.

Démonstration. Le groupe $\langle B^-\rangle|_\Gamma$ est transitif et est un quotient de $\langle B^-\rangle$, donc d'après le théorème 1.4, on a $(B^-)^u|_\Gamma = \langle B^-\rangle|_\Gamma$ avec $u = \lfloor e^{C_7(\ln n)^3} D \rfloor$ où C_7 est une constante absolue.

D'après le lemme précédent, Γ est une orbite de $\langle B^+\rangle$. Le lemme 5.2 avec $H = \langle B^+\rangle$ nous fournit un $g \in \langle B^+\rangle$ avec $|\operatorname{supp}(g|_\Gamma)| \leq \frac{|\Gamma|}{4}$. Soit $h \in B^+$ tel que $h|_\Delta = g|_\Delta$: on a alors $gh^{-1} \in \langle B^+\rangle_{(\Delta)} = \langle B^-\rangle$ donc il existe $b \in (B^-)^u$ tel que $b|_\Gamma = gh^{-1}|_\Gamma$, donc $bh \in (B^+)^{3u+1}$ vérifie $bh|_\Gamma = g|_\Gamma$, et est donc un élément d'assez petite orbite pour conclure par le théorème 5.1. □

5.2 Fin de la preuve

Pour montrer le théorème par un argument de récurrence, on va établir les deux propositions suivantes qui lient des majorations du diamètre à la construction de grandes chaînes de stabilisateurs. Comme dans [HS13], elles s'expriment en fonction de deux fonctions $F_1(n)$ et $F_2(n)$ vérifiant certaines conditions, et on déterminera après coup deux fonctions vérifiant ces conditions.

Proposition 5.5. *Il existe des constantes absolues $n_0, C_8, C_9, C_{10}, C_{11}$ telles que l'énoncé suivant soit vrai :*

Soient $n \geq n_0$, $G = \mathfrak{S}_n$ ou $\mathfrak{A}_n$ et A partie génératrice symétrique de G. Soient $\alpha_1, \ldots, \alpha_{m+1} \in [\![1,n]\!]$ avec $m \geq (\ln n)^2$ telle que pour tout $i \in [\![1, m+1]\!]$:

$$|A_{(\alpha_1,\ldots,\alpha_{i-1})} \cdot \alpha_i| \geq \frac{9}{10} n$$

alors si la conclusion de la proposition 5.6 est vérifiée pour tout $n' < n$ par rapport à une certaine fonction croissante $F_2(n)$, on a, pour toute $F_1(n)$ vérifiant :

$$F_1(n) \geq \max(n^{C_8 \ln n} e^{C_9 (\ln n)^3} F_2(0.95n), C_{10} n^{C_8 \ln n + 8})$$

soit $A^{F_1(n)}$ est égal à $\mathfrak{S}_n$ ou $\mathfrak{A}_n$, soit il existe $\alpha_{m+2}, \ldots, \alpha_{m+\ell+1}$ avec $\ell \geq C_{11} \frac{m \ln m}{(\ln n)^2}$ tels que pour tout $i \in [\![1, m+\ell+1]\!]$:

$$|A'_{(\alpha_1,\ldots,\alpha_{i-1})} \cdot \alpha_i| \geq \frac{9}{10} n$$

où $A' = A^{n^{C_8 \ln n}}$.

Proposition 5.6. *Soient C_8 et n_0 les constantes de la proposition précédente. Il existe C_{12} telle que l'énoncé suivant soit vrai :*

Soient $n \geq n_0$, $G = \mathfrak{S}_n$ ou $\mathfrak{A}_n$ et Y partie génératrice symétrique de G. Si la conclusion de la proposition 5.5 est vérifiée pour $n' \leq n$ par rapport à une fonction F_1 et si F_2 est telle que :

$$F_2(n) \geq \max(e^{(\ln n)^3 + 2 \ln n + C_{12} C_8 (\ln n)^5} F_1(n) + 1, n_0!)$$

alors on a :

$$\operatorname{diam}(\Gamma(G, Y)) \leq F_2(n)$$

On commence par montrer le second énoncé :

Démonstration. Soit $m_0 = \lfloor (\ln n)^2 \rfloor + 1$: on peut supposer n assez grand pour que $m_0 \leq \frac{1}{10} n \leq n-3$, de sorte que G agit transitivement sur l'ensemble X des (m_0+1)-uplets d'éléments distincts de $[\![1, n]\!]$. D'après le lemme 2.4. $A_0 = Y^{n^{m_0+1}}$ agit transitivement sur X, donc on a une chaîne de stabilisateurs vérifiant l'hypothèse de la proposition 5.5.

On peut alors itérer la proposition 5.5 : on note ℓ_0 le ℓ fourni par la proposition, on pose $m_1 = m_0 + \ell_0$ et $A_1 = A_0^r$ avec $r = \lfloor n^{C_8 \ln n} \rfloor$ et ainsi de suite, jusqu'à ce qu'on soit dans le premier cas de la proposition 5.5, ce qui arrive forcément car la longueur des chaînes est majorée par n.

Soit k tel que l'itération s'arrête en appliquant la proposition à A_k : on veut majorer k. Or, on a, si n est assez grand, $m_{i+1} \geq \left(1 + \frac{1}{(\ln n)^2}\right) m_i$ donc $\left(1 + \frac{1}{(\ln n)^2}\right)^k m_0 \leq n$, d'où $k \leq C_{12} (\ln n)^3$ où C_{12} est une constante absolue.

On a donc :

$$Y^{n^{m_0+1} r^{1 + C_{12} (\ln n)^3}} = G$$

d'où le résultat. □

Il reste maintenant à montrer la première :

Démonstration. On peut supposer n assez grand pour que m soit plus grand que la constante obtenue dans 3.9 pour $d = 0.9$. En posant $\Sigma = \{\alpha_1, \ldots, \alpha_m\}$, on a alors $\Delta \subset \Sigma$ avec $|\Delta| \geq \frac{9}{10} |\Sigma|$ tel que $\mathfrak{A}_\Delta$ soit contenu dans $\left(\left(A^{16m^6}\right)_\Sigma\right)_{(\Sigma \setminus \Delta)} |_\Delta$. On pose :

$$B^+ = \left\{ g \in \left(\left(A^{16m^6}\right)_\Sigma\right)_{(\Sigma \setminus \Delta)}, g|_\Delta \in \mathfrak{A}_\Delta \right\}$$

et $B^- = \left((B^+)^3\right)_{(\Delta)}$: B^+ est un grand sous-ensemble de G_Σ et B^- un sous-ensemble de $G_{(\Sigma)}$, qui vont permettre d'utiliser 4.7. Pour pouvoir appliquer le lemme 4.6 et réaliser l'étape de création, il faut montrer que $\langle B^- \rangle$ agit comme un groupe symétrique sur un grand ensemble Γ.

Or, comme $|B^- \cdot \alpha_{m+1}| \geq \frac{9}{10}n$, $\langle B^- \rangle$ admet une orbite Γ avec $|\Gamma| \geq \frac{9}{10}n$. D'après 5.3, Γ est une orbite de B^+. Si $\langle B^- \rangle$ n'a pas de facteur de composition A_k avec $k \geq 0.95n$, alors le lemme 5.4 permet de conclure par descente. Sinon, comme $\langle B^- \rangle|_\Gamma$ est le quotient de $\langle B^- \rangle$ par $(\langle B^- \rangle)_{(\Gamma)}$, A_k est un facteur de composition d'un des deux groupes. Comme $|(\langle B^- \rangle)_{(\Gamma)}| \leq \lceil 0.1n \rceil !$, c'est un facteur de composition de $\langle B^- \rangle|_\Gamma$ donc ce groupe contient $\mathfrak{A}_\Gamma$ d'après 3.4.

Le lemme 4.6 donne alors $Y = \{y_1, \ldots, y_6\} \subset (B^-)^{n^{45 \ln n}}$ tel que $\langle Y \rangle|_\Gamma$ soit 2-transitif sur Γ, et on applique le lemme 4.7 : si la première conclusion est vérifiée, on obtient un élément d'orbite assez petite pour pouvoir conclure par le théorème 5.1, en prenant $C_{10} = C_5(0.1) \geq C_5(0.05)$.

Si la seconde conclusion est vérifiée, en posant $W = B^+ Y (B^+)^{-1} \cap \langle B^- \rangle$, on a $W \subset A^{n^{46 \ln n}}$ et $|W| \geq |B^+|^{1/6} \geq m^{C_{13} m}$ où C_{13} est une constante absolue, car $|B^+| \geq |\mathfrak{A}_\Delta| \geq \frac{(9m/10)!}{2}$.

Maintenant qu'on a beaucoup d'éléments dans le stabilisateur point par point de Σ, on peut appliquer le lemme de séparation. Le lemme 2.7 en remplaçant A par $A^{\lceil n^{46 \ln n} \rceil} \cup \langle B^- \rangle$ et $\mathfrak{S}_n$ par $\mathfrak{S}_\Gamma$ montre que, si $(\alpha_{m+2}, \ldots, \alpha_{m+\ell+1})$ est une chaîne de stabilisateurs maximale, alors :

$$\ell \geq C_3(0.9) \frac{\ln |A^{\lceil n^{46 \ln n} \rceil} \cup \langle B^- \rangle|}{(\ln n)^2} \geq C_3(0.9) C_{13} \frac{m \ln m}{(\ln n)^2}$$

d'où la proposition. □

Pour terminer la preuve du théorème principal, il ne reste plus qu'à trouver des fonctions F_1 et F_2 vérifiant les hypothèses des deux dernières propositions : l'hypothèse de la seconde est satisfaite pour $F_2(n) = e^{C_{14}(\ln n)^5} F_1(n)$ si C_{14} est une constante assez grande. Il faut alors :

$$F_1(n) \geq e^{C_{15}(\ln n)^5} F_1(0.95n)$$

où C_{15} est une autre constante, et on vérifie aisément qu'il existe C telle que cette condition est vérifiée pour :

$$F_1(n) = e^{C(\ln n)^6}$$

d'où le théorème.

Remarque. *La borne qu'on obtient est un peu moins bonne que celle obtenue dans [HS13] : on obtient dans l'exponentielle un $O\left((\ln n)^6\right)$ au lieu d'un $O\left((\ln n)^4 \ln \ln n\right)$. Cela est dû au fait que l'on a repris des versions moins techniques des preuves des deux propositions. Pour améliorer la borne, il faut appliquer plusieurs fois le lemme de séparation dans la preuve de la première, et obtenir une majoration plus fine de k dans la preuve de la seconde.*

Références

[Bab81] L. Babai. On the orders of uniprimitive permutation groups. *Ann. of Math. 113*, pp. 553-568, 1981.

[Bab82] L. Babai. On the order of doubly transitive permutation groups. *Invent. Math., 65(3)*, pp. 473–484, 1981/82.

[BBS04] L. Babai, R. Beals, Á. Seress. On the diameter of the symmetric group : polynomial bounds, dans *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 1108–1112, New York, 2004 ;

[BGT11] E. Breuillard, B. Green, T. Tao. Approximate subgroups of linear groups. *Geom. Funct. Anal.*, 21(4), pp. 774–819, 2011 ;

[BS92] L. Babai, Á. Seress. On the diameter of permutation groups, dans *European J. Combin.*, 13(4), pp. 231–243, 1992 ;

[Fie72] M. Fiedler. Bounds for eigenvalues of doubly stochastic matrices. *Linear Algebra and Appl., 5*, pp. 299–310, 1972.

[GH11] N. Gill, H. A. Helfgott. Growth of small generating sets in $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$. *Int. Math. Res. Not. IMRN*, (18) pp. 4226–4251, 2011.

[Hel08] H. A. Helfgott. Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, dans *Ann. of Math. (2)*, 167(2), pp. 601–623, 2008 ;

[HS13] H. A. Helfgott, Á. Seress. On the diameter of permutation groups, à paraître dans *Annals of Math.* ;

[PS80] C. Praeger, J. Saxl. On the order of primitive permutation groups, dans *Bull. London Math. Soc. 12*, pp. 303-308, 1980.

[PPSS12] C. E. Praeger, L. Pyber, P. Spiga, et E. Szabo. Graphs with automorphism groups admitting composition factors of bounded rank. *Proc. Amer. Math. Soc., 140(7)*, pp.2307–2318, 2012.