Sur la conjecture de réarrangement de Graham

Huy Tuan Pham, Lisa Sauermann

Résumé

Graham a conjecturé en 1971 que pour tout nombre premier p, tout sous-ensemble $S \subseteq \mathbb{Z}_p \setminus \{0\}$ admet un ordonnancement $s_1, s_2, \dots, s_{|S|}$ tel que toutes les sommes partielles $s_1, s_1 + s_2, \dots, s_1 + s_2 + \cdots + s_{|S|}$ soient distinctes. Nous prouvons cette conjecture pour tous les sous-ensembles $S \subseteq \mathbb{Z}_p \setminus \{0\}$ avec $|S| \leq p^{1-\alpha}$ et $|S|$ suffisamment grand par rapport à α, pour tout $\alpha \in (0, 1)$. Combiné avec des résultats antérieurs, cela donne une résolution complète de la conjecture de réarrangement de Graham pour tous les nombres premiers p suffisamment grands.

1 Introduction

Étant donné un groupe abélien G et un sous-ensemble $S \subseteq G$, un *ordonnancement valide* de S est un ordonnancement $s_1, s_2, \dots, s_{|S|}$ des éléments de S tel que toutes les sommes partielles $s_1, s_1 + s_2, \dots, s_1 + s_2 + \cdots + s_{|S|}$ soient distinctes.

Les ordonnancements valides ont fait l'objet d'un certain nombre de travaux en combinatoire et en théorie des groupes. Le sujet principal de cet article est une conjecture, appelée la conjecture de réarrangement de Graham, qui a été posée par Graham [7, p. 36] en 1971 et ensuite réitérée par Erdős et Graham [6, p. 95].

Conjecture : Tout sous-ensemble $S \subseteq \mathbb{Z}_p \setminus \{0\}$ admet un ordonnancement valide.

La conjecture de réarrangement de Graham a suscité beaucoup d'intérêt ces dernières années. Bedert et Kravitz [3] ont montré que la conjecture est vraie pour les petits ensembles S, à savoir pour $|S| \leq \exp((\log p)^{1/4})$, améliorant un résultat antérieur de Kravitz [9] et une observation de Sawin [12]. Müyesser et Pokrovskiy [10] ont montré que la conjecture est vraie pour des S très grands de taille $|S| \geq (1 - o(1))p$. Bucić, Frederickson, Müyesser, Pokrovskiy et Yepremyan [4] ont montré une version approximative de la conjecture, où toutes les sommes partielles sauf $o(|S|)$ sont garanties d'être distinctes. Récemment, Bedert, Bucić, Kravitz, Montgomery et Müyesser [2] ont montré que la conjecture est vraie pour de grands ensembles S, à savoir pour $|S| \geq p^{1-c}$ pour une petite constante positive c.

Le résultat principal de cet article est le théorème suivant, qui montre que la conjecture de réarrangement de Graham est vraie pour tous les $S \subseteq \mathbb{Z}_p \setminus \{0\}$ avec $C_\alpha \leq |S| \leq p^{1-\alpha}$, pour tout $\alpha > 0$ (avec une constante appropriée $C_\alpha > 0$ dépendant de α).

Théorème 1. *Pour tout $0 < \alpha < 1$, il existe une constante $C_\alpha > 0$ telle que ce qui suit est vrai. Soit p un nombre premier et soit $S \subseteq \mathbb{Z}_p \setminus \{0\}$ un sous-ensemble avec $C_\alpha \leq |S| \leq p^{1-\alpha}$. Alors il*

H.T.P. : Département de mathématiques, California Institute of Technology, Pasadena, CA 91125. Recherche financée par une bourse de recherche Clay.
L.S. : Institut de mathématiques appliquées, Université de Bonn, Allemagne. Recherche financée par le programme Heisenberg de la DFG.

existe un ordonnancement valide de S, c'est-à-dire qu'il existe un ordonnancement $s_1, s_2, \dots, s_{|S|}$ des éléments de S tel que toutes les sommes partielles $s_1, s_1 + s_2, \dots, s_1 + s_2 + \cdots + s_{|S|}$ soient distinctes.

Conjointement avec les résultats antérieurs discutés ci-dessus, cela résout complètement la conjecture de réarrangement de Graham pour tous les nombres premiers p suffisamment grands.

Contrairement aux résultats précédents concernant la conjecture de réarrangement de Graham, employant des résultats structurels de combinatoire additive, ou des arguments de théorie des graphes reposant sur des notions appropriées d'expansion et la méthode d'absorption, notre preuve est intrinsèquement probabiliste, reposant sur des estimations d'anticoncentration sur les sommes de sous-ensembles aléatoires de S d'une taille donnée. Plus précisément, nous prouvons le résultat d'anticoncentration suivant, qui est une entrée importante pour notre preuve du Théorème 1.

Théorème 2. *Il existe une constante absolue $C > 0$ telle que ce qui suit est vrai. Soit p un nombre premier, soit $S \subseteq \mathbb{Z}_p$ un sous-ensemble de taille $|S| \geq 2$, et soit m un entier avec $C \log |S| \leq m \leq 10^{-3}|S|/\log |S|$. Maintenant, soit $R \subseteq S$ un sous-ensemble uniformément aléatoire de S de taille m, et soit $\Sigma(R) = \sum_{x \in R} x \in \mathbb{Z}_p$ la somme des éléments de R. Alors*

$$\max_{z \in \mathbb{Z}_p} \mathbb{P}[\Sigma(R) = z] \leq \frac{1}{p} + \frac{C}{|S|\sqrt{m}}.$$

Dans notre preuve du Théorème 2, nous représentons un sous-ensemble uniformément aléatoire R de taille m en partitionnant d'abord S aléatoirement en m parties de taille à peu près égale, puis en choisissant un élément uniformément aléatoire dans chaque partie. Pour comprendre l'anticoncentration, étant donné une partition fixe, nous employons des idées d'analyse de Fourier similaires au travail de Nguyen et Vu [11] sur le problème inverse de Littlewood-Offord. L'étape nouvelle clé dans la preuve est l'utilisation d'estimations de concentration appropriées pour relier certaines quantités impliquant la partition aléatoire de S à leurs analogues déterministes.

Afin de traiter également le cas où m est plus grand que la borne supérieure supposée dans le Théorème 2, nous utilisons le corollaire suivant du Théorème 2.

Corollaire 3. *Pour tout $0 < \varepsilon < 1$ Il existe une constante $C'_\varepsilon > 0$ telle que ce qui suit est vrai. Soit p un nombre premier, soit $S \subseteq \mathbb{Z}_p$ un sous-ensemble de taille $|S| \geq 2$, et considérons un entier positif $m \leq (1-\varepsilon)|S|$. Maintenant, soit $R \subseteq S$ un sous-ensemble uniformément aléatoire de S de taille m, et soit $\Sigma(R) = \sum_{x \in R} x \in \mathbb{Z}_p$ la somme des éléments de R. Alors*

$$\max_{z \in \mathbb{Z}_p} \mathbb{P}[\Sigma(R) = z] \leq \frac{1}{p} + \frac{C'_\varepsilon \sqrt{\log |S|}}{|S|\sqrt{m}}.$$

En gros, notre preuve du Théorème 1 se déroule comme suit. En partant d'un ordonnancement aléatoire de S, nous effectuons des ajustements locaux pour chaque segment de somme nulle (en échangeant l'extrémité du segment avec un autre élément ultérieur proche dans l'ordonnancement). En utilisant les bornes d'anticoncentration du Théorème 2 et du Corollaire 3, nous montrons que de cette manière nous pouvons obtenir un ordonnancement valide de S.

Outre le cadre du groupe cyclique dans la conjecture de réarrangement de Graham, les ordonnancements valides ont également été étudiés dans d'autres groupes. Alspach [1, 5] a conjecturé un analogue de la conjecture de réarrangement de Graham dans des groupes abéliens finis arbitraires. Nous pensons que notre argument peut se généraliser à d'autres groupes abéliens également, et prévoyons de revenir sur la conjecture d'Alspach dans des travaux futurs.

Notation. Pour un nombre premier p, et tout sous-ensemble $S \subseteq \mathbb{Z}_p$, nous écrivons $\Sigma(S) = \sum_{x \in S} x \in \mathbb{Z}_p$ pour la somme des éléments dans S. Tous les logarithmes sont en base e, sauf indication contraire.

Organisation. Après quelques préliminaires dans la Section 2, nous prouverons notre résultat d'anticoncentration, le Théorème 2, dans la Section 3. Dans la Section 4, nous déduisons quelques corollaires du résultat d'anticoncentration, en particulier le Corollaire 3 et un résultat d'anticoncentration pour une chaîne de sous-ensembles aléatoires de tailles données. Enfin, nous donnons la preuve de notre résultat principal, le Théorème 1, dans la Section 5, en utilisant les résultats d'anticoncentration de la Section 4.

2 Préliminaires

Pour $y \in \mathbb{R}$, définissons $\|y\|_{\mathbb{Z}} := \min_{z \in \mathbb{Z}} |y - z|$ comme la distance de y à l'entier le plus proche (et notons que $\|y\|_{\mathbb{Z}} \leq 1$ pour tout $y \in \mathbb{R}$).
Pour tous $y_1, \ldots, y_k \in \mathbb{R}$, nous avons

$$\|y_1 + \cdots + y_k\|_{\mathbb{Z}}^2 \leq k \cdot (\|y_1\|_{\mathbb{Z}}^2 + \cdots + \|y_k\|_{\mathbb{Z}}^2).$$

Démonstration. Soit $z_i \in \mathbb{Z}$ tel que $\|y_i\|_{\mathbb{Z}} = |y_i - z_i|$. Nous avons alors

$$\|y_1 + \cdots + y_k\|_{\mathbb{Z}} \leq |(y_1 + \cdots + y_k) - (z_1 + \cdots + z_k)| = \left| \sum_{i=1}^{k} (y_i - z_i) \right| \leq \sum_{i=1}^{k} |y_i - z_i| = \sum_{i=1}^{k} \|y_i\|_{\mathbb{Z}}.$$

Par l'inégalité de Cauchy-Schwarz, nous pouvons alors conclure que

$$\|y_1 + \cdots + y_k\|_{\mathbb{Z}}^2 \leq \left(\sum_{i=1}^{k} \|y_i\|_{\mathbb{Z}} \right)^2 \leq k \cdot (\|y_1\|_{\mathbb{Z}}^2 + \cdots + \|y_k\|_{\mathbb{Z}}^2). \qquad \square$$

Pour tout $y \in \mathbb{R}$, nous avons

$$1 - 20\|y\|_{\mathbb{Z}}^2 \leq \cos(2\pi y) \leq 1 - 2\|y\|_{\mathbb{Z}}^2.$$

Démonstration. Notons que tous les termes de l'inégalité sont des fonctions 1-périodiques de y, qui sont de plus symétriques autour de 0. Il suffit donc de vérifier l'inégalité pour $y \in [0, 1/2]$.

Pour $y \in [0, 1/2]$, nous avons $\|y\|_{\mathbb{Z}} = y$, et donc l'inégalité désirée se simplifie en

$$1 - 20y^2 \leq \cos(2\pi y) \leq 1 - 2y^2.$$

Par le théorème de Taylor (avec la forme de Lagrange du reste), pour tout $y \in [0, 1/2]$, nous avons

$$\cos(2\pi y) = 1 - \frac{(2\pi)^2}{2} y^2 + \frac{(2\pi)^3 \sin(2\pi\xi)}{6} y^3$$

pour un certain $\xi \in [0, y] \subseteq [0, 1/2]$. Puisque $\sin(2\pi\xi) \geq 0$ et $y \in [0, 1/2]$, nous pouvons conclure

$$\cos(2\pi y) \geq 1 - \frac{(2\pi)^2}{2} y^2 = 1 - (2\pi^2) y^2 \geq 1 - 20y^2.$$

De même, nous avons

$$\cos(2\pi y) = 1 - \frac{(2\pi)^2}{2} y^2 + \frac{(2\pi)^4 \cos(2\pi\xi)}{24} y^4,$$

pour un certain $\xi \in [0, y]$. En utilisant que $\cos(2\pi\xi) \leq 1$ et $y \in [0, 1/2]$, nous avons

$$\cos(2\pi y) \leq 1 - \frac{(2\pi)^2}{2} y^2 + \frac{(2\pi)^4}{24} \cdot \left(\frac{1}{2}\right)^2 y^2 \leq 1 - 2y^2. \qquad \square$$

Pour un nombre premier p, et $y \in \mathbb{Z}$, nous définissons de plus $\|y\|_p := \|y/p\|_{\mathbb{Z}} = \min_{z \in \mathbb{Z}} |y/p - z|$. Notant que $\|y\|_p$ est p-périodique, cela nous permet de définir $\|x\|_p$ pour tout $x \in \mathbb{Z}_p$ en posant $\|x\|_p := \|y\|_p$ pour tout représentant $y \in \mathbb{Z}$ de la classe de résidus $x \in \mathbb{Z}_p$.
Pour un nombre premier p, et $x_1, \ldots, x_k \in \mathbb{Z}_p$, nous avons

$$\|x_1 + \cdots + x_k\|_p^2 \leq k \cdot (\|x_1\|_p^2 + \cdots + \|x_k\|_p^2).$$

Démonstration. En choisissant des représentants $y_1, \ldots, y_k \in \mathbb{Z}$ pour $x_1, \ldots, x_k \in \mathbb{Z}_p$, il découle du Fait 2 que

$$\|x_1 + \cdots + x_k\|_p^2 = \|(y_1/p) + \cdots + (y_k/p)\|_{\mathbb{Z}}^2 \leq k \cdot (\|y_1/p\|_{\mathbb{Z}}^2 + \cdots + \|y_k/p\|_{\mathbb{Z}}^2) = k \cdot (\|x_1\|_p^2 + \cdots + \|x_k\|_p^2). \quad \square$$

Enfin, nous rappelons une conséquence facile du théorème de Cauchy-Davenport.
Pour un nombre premier p, un sous-ensemble $A \subseteq \mathbb{Z}_p$, et un entier positif k, considérons la k-ième somme itérée $kA = A + \cdots + A = \{a_1 + \cdots + a_k : a_1, \ldots, a_k \in A\}$. Si $kA \neq \mathbb{Z}_p$, nous avons

$$|kA| \geq 1 + k \cdot (|A| - 1).$$

Démonstration. Rappelons que le théorème de Cauchy-Davenport stipule que pour tous sous-ensembles $A, B \subseteq \mathbb{Z}_p$ avec $A + B \neq \mathbb{Z}_p$, nous avons $|A + B| \geq |A| + |B| - 1$, et donc $|A + B| - 1 \geq (|A| - 1) + (|B| - 1)$. En appliquant cela de manière répétée, pour tous sous-ensembles $A_1, \ldots, A_k$ avec $A_1 + \cdots + A_k \neq \mathbb{Z}_p$ (et donc en particulier $A_1 + \cdots + A_j \neq \mathbb{Z}_p$ pour $j = 1, \ldots, k$) nous pouvons conclure

$$|A_1 + \cdots + A_k| - 1 \geq (|A_1 + \cdots + A_{k-1}| - 1) + (|A_k| - 1) \geq \cdots \geq (|A_1| - 1) + \cdots + (|A_k| - 1)$$

En prenant $A_1 = \cdots = A_k = A$, on obtient $|kA| - 1 \geq k \cdot (|A| - 1)$, ce qui implique l'inégalité désirée. $\square$

Enfin, pour un nombre premier p et $y \in \mathbb{Z}$, nous définissons $e_p(y) = \exp(2\pi i y/p)$. Notant que cette fonction est p-périodique, nous pouvons maintenant définir $e_p(x)$ pour tout $x \in \mathbb{Z}_p$ en posant $e_p(x) = e_p(y) = \exp(2\pi i y/p)$ pour tout représentant $y \in \mathbb{Z}$ de la classe de résidus $x \in \mathbb{Z}_p$.
Pour un nombre premier p, et $x \in \mathbb{Z}_p$, nous avons

$$\mathrm{Re}(e_p(x)) \leq 1 - 2\|x\|_p^2.$$

Démonstration. Soit $y \in \mathbb{Z}$ un représentant de la classe de résidus $x \in \mathbb{Z}_p$, par le Fait 2 nous avons

$$\mathrm{Re}(e_p(x)) = \mathrm{Re}(e_p(y)) = \mathrm{Re}(\exp(2\pi i y/p)) = \cos(2\pi y/p) \leq 1 - 2\|y/p\|_{\mathbb{Z}}^2 = 1 - 2\|y\|_p^2 = 1 - 2\|x\|_p^2. \quad \square$$

3 Anticoncentration sur les tranches booléennes via l'analyse de Fourier

Dans cette section, nous prouvons le Théorème 1, en prenant $C = 2^{24}$. Soit donc p un nombre premier, et $S \subseteq \mathbb{Z}_p$ un sous-ensemble de taille $|S| \geq 2$. De plus, soit m un entier positif avec $2^{24} \log |S| = C \log |S| \leq m \leq 10^{-3}|S|/\log |S|$. Notons que cela implique en particulier $|S| \geq m \geq 2^{24} \geq 10^7$.

Soit $\widehat{\mathbb{Z}_p}$ l'ensemble des caractères de Fourier sur $\mathbb{Z}_p$ (rappelons que ce sont les homomorphismes de groupes $\chi : \mathbb{Z}_p \to \{z \in \mathbb{C} : |z| = 1\}$). Rappelons également que nous pouvons identifier un caractère $\chi : \mathbb{Z}_p \to \{z \in \mathbb{C} : |z| = 1\}$ avec un élément $\chi \in \mathbb{Z}_p$ via

$$\chi(x) = e_p(\chi x)$$

(rappelons que dans la Section 2, pour tout $x \in \mathbb{Z}_p$ nous avons défini $e_p(x) = \exp(2\pi i y/p)$ où $y \in \mathbb{Z}$ est un représentant de la classe de résidus $x \in \mathbb{Z}_p$).

Étant donné l'ensemble $S \subseteq \mathbb{Z}_p$, dans l'énoncé du Théorème 1 nous considérons un sous-ensemble uniformément aléatoire $R \subseteq S$ de taille m. Nous pouvons échantillonner un tel sous-ensemble de taille m uniformément aléatoire de la manière suivante, ce qui sera utile dans notre preuve.

Nous partitionnons d'abord aléatoirement les éléments de S en m ensembles $S_1, \ldots, S_m$ avec $|S_1| \geq |S_2| \geq \cdots \geq |S_m| \geq |S_m| - 1$ (cela signifie que $S_1, \ldots, S_m$ ont chacun une taille $\lfloor |S|/m \rfloor + 1$ ou $\lfloor |S|/m \rfloor$, et exactement les premiers $|S| - m\lfloor |S|/m \rfloor$ des ensembles $S_1, \ldots, S_m$ ont une taille $\lceil |S|/m \rceil + 1$). Puisque $m \leq |S|/4$, tous les ensembles $S_1, \ldots, S_m$ ont une taille d'au moins 4. Nous choisissons ensuite indépendamment exactement un élément X_i dans chaque ensemble S_i pour former un ensemble $R = \{X_1, \ldots, X_m\}$. Il est facile de voir que R est distribué précisément comme un sous-ensemble uniformément aléatoire de S de taille m. Notons également que $\Sigma(R) = X_1 + \cdots + X_m$. Nous écrirons $\mathcal{S} = (S_1, \ldots, S_m)$ pour le m-uplet d'ensembles dans la partition de S, et $X = (X_1, \ldots, X_m)$ pour le m-uplet d'éléments choisis dans ces ensembles.

Nous écrivons $\mathbb{P}_{\mathcal{S}}$ et $\mathbb{E}_{\mathcal{S}}$ pour les probabilités et les espérances sur l'aléa de $\mathcal{S} = (S_1, \ldots, S_m)$, c'est-à-dire sur l'aléa de la partition $S = S_1 \cup \cdots \cup S_m$. Pour une réalisation fixe de $\mathcal{S} = (S_1, \ldots, S_m)$, nous écrivons $\mathbb{P}_X$ et $\mathbb{E}_X$ pour désigner les probabilités et les espérances sur l'aléa de $X = (X_1, \ldots, X_n)$, conditionnellement à $\mathcal{S} = (S_1, \ldots, S_m)$. Notons que conditionnellement à $\mathcal{S} = (S_1, \ldots, S_m)$, les éléments $X_i \in S_i$ sont des éléments aléatoires uniformément indépendants de S_i pour $i = 1, \ldots, m$.

Maintenant, nous avons

$$\mathbb{P}[\Sigma(R) = z] = \mathbb{E}_{\mathcal{S}}[\mathbb{P}_X[\Sigma(R) = z]],$$

où la probabilité $\mathbb{P}_X[\Sigma(R) = z]$ est conditionnelle à $\mathcal{S} = (S_1, \ldots, S_m)$, sur l'aléa de $X = (X_1, \ldots, X_n)$.

Fixons une réalisation de $\mathcal{S} = (S_1, \ldots, S_m)$. L'identité standard

$$\mathbb{P}_X[\Sigma(R) = z] = \mathbb{P}_X[X_1 + \cdots + X_m = z] = \frac{1}{p}\mathbb{E}_X\left[\sum_{\chi \in \widehat{\mathbb{Z}_p}} \chi(X_1 + \cdots + X_m - z)\right] = \frac{1}{p}\sum_{\chi \in \widehat{\mathbb{Z}_p}} \chi(-z) \prod_{i=1}^{m} \mathbb{E}_X[\chi(X_i)]$$

donne

$$\mathbb{P}_X[\Sigma(R)=z] \le \frac{1}{p}\sum_{\chi\in\widehat{\mathbb{Z}_p}}\left|\chi(-z)\prod_{i=1}^{m}\mathbb{E}[\chi(X_i)]\right| = \frac{1}{p}\sum_{\chi\in\widehat{\mathbb{Z}_p}}\prod_{i=1}^{m}|\mathbb{E}_X[\chi(X_i)]|. \tag{1}$$

Pour tout $\chi \in \widehat{\mathbb{Z}_p}$ et tout $i = 1, \dots, m$, nous avons

$$|\mathbb{E}_X[\chi(X_i)]| = \left|\frac{1}{|S_i|}\sum_{x\in S_i}\chi(X_i)\right| = \left|\frac{1}{|S_i|}\sum_{x\in S_i}e_p(\chi x)\right| = \left(\frac{1}{|S_i|^2}\sum_{x\in S_i}e_p(\chi x)\cdot\overline{\sum_{x\in S_i}e_p(\chi x)}\right)^{1/2}$$

Comme $\sum_{x\in S_i} e_p(\chi x)\cdot\overline{\sum_{x\in S_i} e_p(\chi x)} \in \mathbb{R}$ et $\overline{e_p(\chi x)} = e_p(-\chi x)$ pour tout $x \in \mathbb{Z}_p$, nous pouvons observer que

$$\begin{aligned}
\frac{1}{|S_i|^2}\sum_{x\in S_i}e_p(\chi x)\cdot\overline{\sum_{x\in S_i}e_p(\chi x)} &= \frac{1}{|S_i|^2}\operatorname{Re}\left(\sum_{x\in S_i}e_p(\chi x)\cdot\sum_{x\in S_i}\overline{e_p(\chi x)}\right)\\
&= \frac{1}{|S_i|^2}\operatorname{Re}\left(\sum_{x,x'\in S_i}e_p(\chi x-\chi x')\right)\\
&\le \frac{1}{|S_i|^2}\sum_{x,x'\in S_i}(1-2\|\chi x-\chi x'\|_p^2)\\
&= 1-\frac{2}{|S_i|^2}\sum_{x,x'\in S_i}\|\chi x-\chi x'\|_p^2,
\end{aligned}$$

où l'inégalité est due au Fait 2. Cela donne

$$|\mathbb{E}_X[\chi(X_i)]| \le \left(1-\frac{2}{|S_i|^2}\sum_{x,x'\in S_i}\|\chi x-\chi x'\|_p^2\right)^{1/2} \le \exp\left(-\frac{1}{|S_i|^2}\sum_{x,x'\in S_i}\|\chi x-\chi x'\|_p^2\right).$$

Ainsi, nous obtenons

$$\prod_{i=1}^{m}|\mathbb{E}_X[\chi(X_i)]| \le \exp\left(-\sum_{i=1}^{m}\frac{1}{|S_i|^2}\sum_{x,x'\in S_i}\|\chi x-\chi x'\|_p^2\right) = \exp(-\psi(\chi)), \tag{2}$$

où nous définissons

$$\psi(\chi) := \sum_{i=1}^{m}\frac{1}{|S_i|^2}\sum_{x,x'\in S_i}\|\chi x-\chi x'\|_p^2$$

pour tout $\chi \in \mathbb{Z}_p$.

Notons que la valeur de $\psi(\chi)$ dépend de la réalisation de $\mathcal{S} = (S_1, \dots, S_m)$, et que pour le caractère trivial correspondant à l'élément $\chi = 0 \in \mathbb{Z}_p$, nous avons toujours $\psi(\chi) = 0$. Notons également que pour tout $\chi \in \mathbb{Z}_p$, nous avons

$$\psi(\chi) \ge \frac{m^2}{2|S|^2}\sum_{i=1}^{m}\sum_{x,x'\in S_i}\|\chi x-\chi x'\|_p^2, \tag{3}$$

puisque pour $i = 1, \dots, m$ nous avons $|S_i| \le \lfloor |S|/m \rfloor + 1 \le \sqrt{2}|S|/m$. Enfin, puisque $\|\chi x - \chi x'\|_p^2 \le 1$ pour tous $x, x' \in S$, nous avons toujours $\psi(\chi) \le m$.

Maintenant, soit

$$A_0 := \left\{ \chi \in \mathbb{Z}_p : \psi(\chi) \in [0,1) \right\},$$

et pour tout entier positif t, soit

$$A_t := \left\{ \chi \in \mathbb{Z}_p : \psi(\chi) \in [t,2t) \right\}.$$

Nous obtenons alors une partition $\mathbb{Z}_p = A_0 \cup A_1 \cup A_2 \cup A_4 \cup A_8 \cup \dots \cup A_{2^{\lfloor \log_2 m \rfloor}}$ (notant que $A_t = \emptyset$ pour $t > m$). De plus, par (1) et (2) nous avons

$$\mathbb{P}_X[\Sigma(R) = z] \le \frac{1}{p} \sum_{\chi \in \widehat{\mathbb{Z}_p}} \prod_{i=1}^{m} |\mathbb{E}_X[\chi(X_i)]| \le \frac{1}{p} \sum_{\chi \in \mathbb{Z}_p} \exp(-\psi(\chi)) \le \frac{1}{p}|A_0| + \frac{1}{p} \sum_{\ell=0}^{\lfloor \log_2 m \rfloor} |A_{2^\ell}| \exp(-2^\ell).$$

Désormais, nous obtenons

$$\begin{aligned} \mathbb{P}[\Sigma(R) = z] &= \mathbb{E}_{\mathcal{S}}[\mathbb{P}_X[\Sigma(R) = z]] \\ &\le \mathbb{E}_{\mathcal{S}}\left[\frac{1}{p}|A_0| + \frac{1}{p} \sum_{\ell=0}^{\lfloor \log_2 m \rfloor} |A_{2^\ell}| \exp(-2^\ell) \right] \\ &= \frac{1}{p}\mathbb{E}_{\mathcal{S}}[|A_0|] + \frac{1}{p} \sum_{\ell=0}^{\lfloor \log_2 m \rfloor} \mathbb{E}_{\mathcal{S}}[|A_{2^\ell}|] \cdot \exp(-2^\ell). \end{aligned} \tag{4}$$

Dans la partie restante de la section, nous allons borner $\mathbb{E}_{\mathcal{S}}[|A_t|]$ pour $t \in \{0, 1, 2, 4, 8, \dots\}$. Pour $\chi \in \mathbb{Z}_p$, définissons

$$\Psi(\chi) = \frac{m}{|S|^2} \sum_{x,x' \in S} \|\chi x - \chi x'\|_p^2.$$

Pour tout entier positif t, soit

$$B_t = \{\chi \in \mathbb{Z}_p : \Psi(\chi) \le t\}.$$

De plus, soit D_t la collection des $\chi \in \mathbb{Z}_p \setminus \{0\}$ tels qu'il existe un $y \in \mathbb{Z}_p$ avec

$$\left| \left\{ x \in S : \|\chi x - y\|_p \le 8\sqrt{t/m} \right\} \right| \ge \frac{3}{4}|S|$$

(en d'autres termes, cela signifie qu'il existe un "intervalle" dans $\mathbb{Z}_p$ de longueur $16p\sqrt{t/m}$ contenant au moins une fraction $(3/4)$ des éléments de χS).

Notons que, pour tout entier positif t, les ensembles B_t et D_t ne dépendent pas de la réalisation de $\mathcal{S} = (S_1, \dots, S_m)$ (ils ne dépendent que de l'ensemble donné $S \subseteq \mathbb{Z}_p$). Notre prochain objectif est de relier les ensembles A_t, qui dépendent de la réalisation de $\mathcal{S} = (S_1, \dots, S_m)$, aux ensembles B_t et D_t. Plus précisément, nous allons montrer que tout $\chi \in \mathbb{Z}_p$ avec $\chi \notin D_t$ est contenu dans A_t avec une faible probabilité. De même, nous montrerons que tout $\chi \in D_t \setminus B_{32t}$ est contenu dans A_t avec une faible probabilité. Nous obtiendrons ensuite la borne désirée pour $\mathbb{E}_{\mathcal{S}}[|A_t|]$ en majorant $|B_{32t}|$.

Lemme 4. *Soit t un entier positif, et soit $\chi \in \mathbb{Z}_p \setminus \{0\}$ avec $\chi \notin D_t$. Alors nous avons*

$$\mathbb{P}_{\mathcal{S}}[\psi(\chi) < 2t] \leq \frac{1}{|S|^9}.$$

Démonstration. Pour un élément $x' \in S$, soit $i(x') \in \{1, \ldots, m\}$ l'indice tel que $x' \in S_{i(x')}$, c'est-à-dire l'indice de la partie de la partition aléatoire $S = S_1 \cup \cdots \cup S_m$ contenant x'. Puisque $\chi \notin D_t$, pour tout $x' \in S$ fixé nous avons $|\{x \in S : \|\chi x - \chi x'\|_p > 8\sqrt{t/m}\}| \geq |S|/4$. Notons que, en conditionnant sur $i(x')$ (c'est-à-dire en exposant et conditionnant sur la partie de la partition aléatoire à laquelle l'élément x' appartient), l'ensemble $S_{i(x')} \setminus \{x'\}$ est un sous-ensemble uniformément aléatoire de $S \setminus \{x'\}$ de taille soit $\lfloor |S|/m \rfloor$ (si $i(x') \leq |S| - m\lfloor |S|/m \rfloor$) soit $\lfloor |S|/m \rfloor - 1$ (si $i(x') > |S| - m\lfloor |S|/m \rfloor$). Ainsi, en conditionnant sur $i(x')$, l'ensemble $S_{i(x')} \setminus \{x'\}$ est un sous-ensemble uniformément aléatoire de $S \setminus \{x'\}$ d'une taille donnée $k \geq |S|/(2m)$. Rappelant qu'il y a au moins $|S|/4$ éléments $x \in S \setminus \{x'\}$ avec $\|\chi x - \chi x'\|_p > 8\sqrt{t/m}$, par la borne de Chernoff pour les distributions hypergéométriques (voir [8, Théorème 2.10 et Éq. (2.6)]), avec probabilité au moins $1 - e^{-k/32} \geq 1 - e^{-|S|/(64m)}$ il y a au moins $k/8 \geq |S|/(16m)$ éléments différents $x \in S_{i(x')} \setminus \{x'\}$ avec $\|\chi x - \chi x'\|_p > 8\sqrt{t/m}$.

Ainsi, par une borne d'union, avec probabilité au moins $1 - |S|e^{-|S|/(64m)}$ pour tout $x' \in S$ nous avons au moins $|S|/(16m)$ éléments différents $x \in S_{i(x')} \setminus \{x'\}$ avec $\|\chi x - \chi x'\|_p > 8\sqrt{t/m}$. Chaque fois que cela se produit, par (3) nous obtenons

$$\psi(\chi) \geq \frac{m^2}{2|S|^2} \sum_{i=1}^{m} \sum_{x,x' \in S_i} \|\chi x - \chi x'\|_p^2 = \frac{m^2}{2|S|^2} \sum_{x' \in S} \sum_{x \in S_{i(x')}} \|\chi x - \chi x'\|_p^2 \geq \frac{m^2}{2|S|^2} \cdot |S| \cdot \frac{|S|}{16m} \cdot \left(8\sqrt{t/m}\right)^2 = 2t.$$

Ainsi, nous pouvons conclure

$$\mathbb{P}_{\mathcal{S}}[\psi(\chi) < 2t] \leq |S| \cdot e^{-|S|/(64m)} \leq |S| \cdot e^{-10 \log |S|} = \frac{1}{|S|^9},$$

rappelant notre hypothèse $m \leq 10^{-3}|S|/\log|S|$. □

Notre prochain objectif est de montrer que tout $\chi \in D_t \setminus B_{32t}$ est contenu dans A_t avec une faible probabilité. Pour tout entier positif t, et tout $\chi \in D_t$, soit $y_\chi \in \mathbb{Z}_p$ tel que $|\{x \in S : \|\chi x - y_\chi\|_p \leq 8\sqrt{t/m}\}| \geq \frac{3}{4}|S|$ (c'est-à-dire tel qu'au moins une fraction (3/4) des éléments de χS soient contenus dans l'"intervalle" dans $\mathbb{Z}_p$ de longueur $16p\sqrt{t/m}$ autour de y_χ). Notons que nous pouvons choisir y_χ indépendant de t en considérant le plus petit entier positif t avec $\chi \in D_t$ (choisir un $y_\chi \in \mathbb{Z}_p$ valide pour cette plus petite valeur de t donnera automatiquement un y_χ valide pour toutes les valeurs plus grandes de t). Maintenant, soit

$$J_{\chi,t} = \{x \in \mathbb{Z}_p : \|\chi x - y_\chi\|_p \leq 16\sqrt{t/m}\}.$$

Lemme 5. *Pour tout entier positif t, et tout $\chi \in D_t \setminus B_{2000t}$, nous avons*

$$\sum_{x \in S \setminus J_{\chi,t}} \|\chi x - y_\chi\|_p^2 \geq \frac{200t}{m} \cdot |S|.$$

Démonstration. Par le Fait 2 nous avons

$$\|\chi x - \chi x'\|_p^2 \leq 2\|\chi x - y_\chi\|_p^2 + 2\|\chi x' - y_\chi\|_p^2,$$

d'où nous obtenons (rappelant que $\chi \notin B_{2000t}$ et donc $\Psi(\chi) \geq 2000t$)

$$\frac{2000t}{m} \leq \frac{\Psi(\chi)}{m} = \frac{1}{|S|^2}\sum_{x,x'\in S}\|\chi x - \chi x'\|_p^2 \leq \frac{2}{|S|^2}\sum_{x,x'\in S}(\|\chi x - y_\chi\|_p^2 + \|\chi x' - y_\chi\|_p^2) = \frac{4}{|S|}\sum_{x\in S}\|\chi x - y_\chi\|_p^2.$$

Notant que

$$\sum_{x\in S}\|\chi x - y_\chi\|_p^2 = \sum_{x\in S\setminus J_{\chi,t}}\|\chi x - y_\chi\|_p^2 + \sum_{x\in S\cap J_{\chi,t}}\|\chi x - y_\chi\|_p^2 \leq \sum_{x\in S\setminus J_{\chi,t}}\|\chi x - y_\chi\|_p^2 + |S\cap J_{\chi,t}|\cdot\frac{265t}{m},$$

nous pouvons conclure que

$$\frac{2000t}{m} \leq \frac{4}{|S|}\sum_{x\in S\setminus J_{\chi,t}}\|\chi x - y_\chi\|_p^2 + \frac{4|S\cap J_{\chi,t}|}{|S|}\cdot\frac{265t}{m} \leq \frac{4}{|S|}\sum_{x\in S\setminus J_{\chi,t}}\|\chi x - y_\chi\|_p^2 + \frac{1024t}{m}.$$

Ainsi, nous obtenons

$$\sum_{x\in S\setminus J_{\chi,t}}\|\chi x - y_\chi\|_p^2 \geq \frac{|S|}{4}\cdot\frac{976t}{m} \geq \frac{200t}{m}\cdot|S|.$$ □

Lemme 6. *Pour tout entier positif t, et tout $\chi \in D_t \setminus B_{2000t}$, nous avons*

$$\mathbb{P}_{\mathcal{S}}[\psi(\chi) < 2t] \leq \frac{1}{|S|^9}.$$

Démonstration. Pour un élément $x \in S$, écrivons à nouveau $i(x) \in \{1,\ldots,m\}$ pour l'indice tel que $x \in S_{i(x)}$. Rappelons que $|\{x' \in S : \|\chi x' - y_\chi\|_p \leq 8\sqrt{t/m}\}| \geq \frac{3}{4}|S|$, donc au moins $3|S|/4$ éléments $x' \in S$ satisfont $\|\chi x' - y_\chi\|_p \leq 8\sqrt{t/m}$.

Maintenant, pour tout $x \in S \setminus J_{\chi,t}$ fixé (c'est-à-dire tout $x \in S$ avec $\|\chi x - y_\chi\|_p > 16\sqrt{t/m}$), en conditionnant sur $i(x)$, l'ensemble $S_{i(x)}\setminus\{x\}$ est un sous-ensemble uniformément aléatoire de $S\setminus\{x\}$ de taille soit $\lfloor|S|/m\rfloor$ (si $i(x) \leq |S| - m\lfloor|S|/m\rfloor$) soit $\lfloor|S|/m\rfloor - 1$ (si $i(x) > |S| - m\lfloor|S|/m\rfloor$). Ainsi, en conditionnant sur $i(x)$, l'ensemble $S_{i(x)} \setminus \{x\}$ est un sous-ensemble uniformément aléatoire de $S\setminus\{x\}$ d'une taille donnée $k \geq |S|/(2m)$. Rappelant qu'il y a au moins $3|S|/4$ éléments $x' \in S\setminus\{x\}$ avec $\|\chi x' - y_\chi\|_p \leq 8\sqrt{t/m}$, par la borne de Chernoff pour les distributions hypergéométriques (voir [8, Théorème 2.10 et Éq. (2.6)]), avec probabilité au moins $1 - e^{-k/24} \geq 1 - e^{-|S|/(48m)}$ il y a au moins $k/2 \geq |S|/(4m)$ éléments différents $x' \in S_{i(x)} \setminus \{x\}$ avec $\|\chi x' - y_\chi\|_p \leq 8\sqrt{t/m} \leq \|\chi x - y_\chi\|_p/2$. Ces éléments $x' \in S_{i(x)}\setminus\{x\}$ satisfont alors $\|\chi x - \chi x'\|_p \geq \|\chi x - y_\chi\|_p - \|\chi x' - y_\chi\|_p \geq \|\chi x - y_\chi\|_p/2$.

Ainsi, par une borne d'union, avec probabilité au moins $1 - |S|e^{-|S|/(48m)}$ pour tout $x \in S \setminus J_{\chi,t}$ nous avons au moins $|S|/(4m)$ éléments différents $x' \in S_{i(x)}\setminus\{x\}$ avec $\|\chi x - \chi x'\|_p \geq \|\chi x - y_\chi\|_p/2$.

Chaque fois que cela se produit, par (3) nous obtenons

$$\begin{aligned}\psi(\chi) &\geq \frac{m^2}{2|S|^2}\sum_{i=1}^{m}\sum_{x,x'\in S_i}\|\chi x-\chi x'\|_p^2\\ &= \frac{m^2}{2|S|^2}\cdot\sum_{x\in S}\sum_{x'\in S_{i(x)}}\|\chi x-\chi x'\|_p^2\\ &\geq \frac{m^2}{2|S|^2}\cdot\sum_{x\in S\setminus J_{\chi,t}}\sum_{x'\in S_{i(x)}}\|\chi x-\chi x'\|_p^2\\ &\geq \frac{m^2}{2|S|^2}\cdot\sum_{x\in S\setminus J_{\chi,t}}\frac{|S|}{4m}\cdot(\|\chi x-y_\chi\|_p/2)^2\\ &= \frac{m}{32|S|}\cdot\sum_{x\in S\setminus J_{\chi,t}}\|\chi x-y_\chi\|_p^2 \geq \frac{m}{32|S|}\cdot\frac{200t}{m}\cdot|S|\geq 5t,\end{aligned}$$

où pour l'avant-dernière inégalité nous avons utilisé le Lemme 5. Ainsi, nous pouvons conclure

$$\mathbb{P}_{\mathcal{S}}[\psi(\chi)<2t]\leq\mathbb{P}_{\mathcal{S}}[\psi(\chi)<5t]\leq|S|\cdot e^{-|S|/(48m)}\leq|S|\cdot e^{-10\log|S|}=\frac{1}{|S|^9},$$

rappelant notre hypothèse $m\leq 10^{-3}|S|/\log|S|$. □

Notre dernier ingrédient pour la preuve du Théorème 2 est la borne supérieure suivante pour $|B_t|$.

Lemme 7. *Pour tout entier positif $t\leq m/2000$, nous avons*

$$|B_t|\leq 1+\frac{200p\sqrt{t}}{|S|\sqrt{m}}.$$

Nous aurons besoin de quelques lemmes auxiliaires pour la preuve du Lemme 7. Pour $\delta>0$, définissons

$$Q_{t,\delta}=\left\{x\in\mathbb{Z}_p:\sum_{\chi\in B_t}\|\chi x\|_p^2<\delta|B_t|\right\}.$$

Lemme 8. *Pour tout entier positif t, nous avons*

$$|Q_{t,10t/m}|\geq\frac{9}{10}|S|.$$

Démonstration. Soient $Y,Y'\in S$ deux éléments uniformément aléatoires indépendants de S. Notons qu'alors pour tout $\chi\in\mathbb{Z}_p$, nous avons

$$\mathbb{E}_{Y,Y'\in S}\left[\|\chi Y-\chi Y'\|_p^2\right]=\frac{1}{|S|^2}\sum_{x,x'\in S}\|\chi x-\chi x'\|_p^2=\frac{\Psi(\chi)}{m}.$$

Ainsi, nous obtenons

$$\mathbb{E}_{Y,Y'\in S}\left[\sum_{\chi\in B_t}\|\chi Y-\chi Y'\|_p^2\right]=\sum_{\chi\in B_t}\frac{\Psi(\chi)}{m}\leq|B_t|\cdot\frac{t}{m}.$$

Par conséquent, par l'inégalité de Markov, nous pouvons conclure

$$\mathbb{P}_{Y,Y'\in S}\Big[Y-Y'\notin Q_{t,10t/m}\Big]=\mathbb{P}_{Y,Y'\in S}\left[\sum_{\chi\in B_t}\|\chi Y-\chi Y'\|_p^2\geq\frac{10t}{m}|B_t|\right]\leq\frac{|B_t|\cdot\frac{t}{m}}{\frac{10t}{m}|B_t|}=\frac{1}{10}.$$

Ainsi, avec probabilité au moins 9/10, nous avons $Y-Y'\in Q_{t,10t/m}$. En particulier, cela signifie qu'il existe un certain $y'\in S$ fixé tel que pour $Y\in S$ uniformément aléatoire, avec probabilité au moins 9/10, nous avons $Y-y'\in Q_{t,10t/m}$. Cela signifie qu'il y a au moins $(9/10)|S|$ éléments $y\in S$ avec $y-y'\in Q_{t,10t/m}$. Notant que les éléments résultants $y-y'\in Q_{t,10t/m}$ sont distincts pour tous ces $y\in S$, nous pouvons conclure que $|Q_{t,10t/m}|\geq(9/10)|S|$. □

Lemme 9. *Pour tout entier positif t, nous avons*

$$|Q_{t,1/200}|\leq\frac{5}{4}\cdot\frac{p}{|B_t|}.$$

Démonstration. Notons que $\Psi(0)=0$ et $\Psi(\chi)=\Psi(-\chi)$ pour tout $\chi\in\mathbb{Z}_p$. Par conséquent, nous avons $0\in B_t$, et $-\chi\in B_t$ pour tout $\chi\in B_t$. Ainsi, nous obtenons

$$\sum_{x\in\mathbb{Z}_p}\left(\sum_{\chi\in B_t}e_p(\chi x)\right)^2=\sum_{x\in\mathbb{Z}_p}\left(\sum_{\chi\in B_t}e_p(\chi x)\right)\cdot\left(\sum_{\chi'\in B_t}e_p(\chi x)\right)=\sum_{\chi,\chi'\in B_t}\sum_{x\in\mathbb{Z}_p}e_p((\chi+\chi')x)=|B_t|\cdot p.$$

D'autre part, par le Fait 2, pour tout $z\in\mathbb{Z}$, nous avons

$$\frac{e_p(z)+e_p(-z)}{2}=\frac{\exp(2\pi iz/p)+\exp(-2\pi iz/p)}{2}=\cos(2\pi z/p)\geq1-20\|z/p\|_{\mathbb{Z}}^2=1-20\|z\|_p^2.$$

Par conséquent, pour tout $x\in Q_{t,1/200}$, nous avons

$$\sum_{\chi\in B_t}e_p(\chi x)=\sum_{\chi\in B_t}\frac{e_p(\chi x)+e_p(-\chi x)}{2}\geq\sum_{\chi\in B_t}(1-20\|\chi x\|_p^2)=|B_t|-20\sum_{\chi\in B_t}\|\chi x\|_p^2\geq|B_t|-20\cdot\frac{|B_t|}{200},$$

et donc

$$\left(\sum_{\chi\in B_t}e_p(\chi x)\right)^2\geq\left(|B_t|-20\cdot\frac{|B_t|}{200}\right)^2=\left(\frac{9}{10}|B_t|\right)^2=\frac{81}{100}|B_t|^2\geq\frac{4}{5}|B_t|^2.$$

Ainsi, nous pouvons conclure

$$p\cdot|B_t|=\sum_{x\in\mathbb{Z}_p}\left(\sum_{\chi\in B_t}e_p(\chi x)\right)^2\geq\sum_{x\in Q_{t,1/200}}\left(\sum_{\chi\in B_t}e_p(\chi x)\right)^2\geq|Q_{t,1/200}|\cdot\frac{4}{5}|B_t|^2.$$

Cela donne

$$|Q_{t,1/200}|\leq\frac{5}{4}\cdot\frac{p}{|B_t|}.$$ □

Lemme 10. *Soit t un entier positif, et soit $\delta>0$. Pour un entier positif k, nous considérons la k-ième somme $kQ_{t,\delta}=Q_{t,\delta}+\cdots+Q_{t,\delta}=\{x_1+\cdots+x_k:x_1,\ldots,x_k\in Q_{t,\delta}\}$. Alors nous avons $kQ_{t,\delta}\subseteq Q_{t,k^2\delta}$.*

Démonstration. Pour $x_1, \dots, x_k \in Q_{t,\delta}$, par le Fait 2 nous avons

$$\|\chi(x_1 + \cdots + x_k)\|_p^2 = \|\chi x_1 + \cdots + \chi x_k\|_p^2 \le k \cdot (\|\chi x_1\|_p^2 + \cdots + \|\chi x_k\|_p^2)$$

pour tout $\chi \in \mathbb{Z}_p$ et donc

$$\sum_{\chi \in B_t} \|\chi(x_1 + \cdots + x_k)\|_p^2 \le k \sum_{\chi \in B_t} \|\chi x_1\|_p^2 + \cdots + k \sum_{\chi \in B_t} \|\chi x_k\|_p^2 \le k \cdot k \cdot \delta |B_t| = k^2 \delta |B_t|.$$

Cela montre que $x_1 + \cdots + x_k \in Q_{t,k^2\delta}$ pour tous $x_1, \dots, x_k \in Q_{t,\delta}$. □

Nous sommes maintenant prêts à prouver le Lemme 7.

Preuve du Lemme 7. Nous pouvons supposer $|B_t| \ge 2$, sinon l'inégalité désirée est trivialement vraie. Notons qu'alors le Lemme 9 implique en particulier $|Q_{t,1/200}| \le (5/4) \cdot (p/2) = (5/8) \cdot p < p$.

Maintenant, soit $k = \lfloor \sqrt{m/(2000t)} \rfloor$. Rappelant notre hypothèse selon laquelle $t \le m/2000$, nous pouvons voir que $\sqrt{m/(2000t)} \ge 1$ et $k = \lfloor \sqrt{m/(2000t)} \rfloor \ge \frac{1}{2}\sqrt{m/(2000t)} \ge 10^{-2}\sqrt{m/t}$, et de plus aussi $k = \lfloor \sqrt{m/(2000t)} \rfloor \ge 1$. Nous avons $k^2(10t/m) \le 1/200$, et donc par le Lemme 10, la k-ième somme $kQ_{t,10t/m}$ de $Q_{t,10t/m}$ satisfait

$$kQ_{t,10t/m} \subseteq Q_{t,k^2(10t/m)} \subseteq Q_{t,1/200}.$$

En particulier, nous obtenons $|kQ_{t,10t/m}| \le |Q_{t,1/200}| < p$, et donc $kQ_{t,10t/m} \ne \mathbb{Z}_p$.

Maintenant, en combinant le Fait 2 et le Lemme 8 on obtient

$$|kQ_{t,10t/m}| \ge 1 + k \cdot (|Q_{t,10t/m}| - 1) \ge 1 + k \cdot \left(\frac{9}{10}|S| - 1\right) \ge k \cdot \frac{4}{5}|S| = \frac{4}{5} \cdot k \cdot |S|$$

(rappelant que $|S| \ge 10^7$). Ainsi, nous pouvons conclure

$$\frac{4}{5} \cdot k \cdot |S| \le |kQ_{t,10t/m}| \le |Q_{t,1/200}| \le \frac{5}{4} \cdot \frac{p}{|B_t|},$$

où dans la dernière étape nous avons utilisé le Lemme 9. Ainsi, nous obtenons

$$|B_t| \le \frac{25}{16} \cdot \frac{p}{k \cdot |S|} \le 2 \cdot \frac{p}{10^{-2}\sqrt{m/t} \cdot |S|} = \frac{200p\sqrt{t}}{|S|\sqrt{m}} \le 1 + \frac{200p\sqrt{t}}{|S|\sqrt{m}}.$$ □

Enfin, nous donnons la preuve du Théorème 2.

Preuve du Théorème 2. Soit $z \in \mathbb{Z}_p$. Rappelons de (4) que

$$\mathbb{P}[\Sigma(R) = z] \le \frac{1}{p}\mathbb{E}_{\mathcal{S}}[|A_0|] + \frac{1}{p}\sum_{\ell=0}^{\lfloor \log_2 m \rfloor} \mathbb{E}_{\mathcal{S}}[|A_{2^\ell}|] \cdot \exp(-2^\ell).$$

Pour tout entier positif t, par les Lemmes 4 et 6, nous avons

$$\mathbb{E}_{\mathcal{S}}\Big[|\{\chi \in \mathbb{Z}_p \setminus \{0\} : \psi(\chi) < 2t\}|\Big] \le \frac{|(\mathbb{Z}_p \setminus \{0\}) \setminus D_t|}{|S|^9} + \frac{|D_t \setminus B_{2000t}|}{|S|^9} + |B_{2000t} \setminus \{0\}| \le \frac{p}{|S|^9} + |B_{2000t} \setminus \{0\}|.$$

Puisque $0 \in B_{2000t}$ pour tout entier positif t, nous avons $|B_{2000t} \setminus \{0\}| = |B_{2000t}| - 1$, et donc pour tout entier positif $t \leq m/2000^2$ nous pouvons conclure

$$\mathbb{E}_{\mathcal{S}}\Big[|\{\chi \in \mathbb{Z}_p \setminus \{0\} : \psi(\chi) < 2t\}|\Big] \leq \frac{p}{|S|^9} + |B_{2000t}| - 1 \leq \frac{p}{|S|^9} + \frac{200p\sqrt{2000t}}{|S|\sqrt{m}} \leq \frac{10^4 p\sqrt{t}}{|S|\sqrt{m}},$$

où l'avant-dernière étape est due au Lemme 7 (et dans la dernière étape nous avons utilisé $\sqrt{m} \leq m \leq |S|$).

Rappelons que pour $\chi = 0 \in \mathbb{Z}_p$ nous avons toujours $\psi(\chi) = 0$, et donc $\chi \in A_0$ (et $\chi \notin A_t$ pour tout entier positif t). Ainsi, nous pouvons conclure (rappelant que $m \geq 10^7$)

$$\mathbb{E}_{\mathcal{S}}[|A_0|] \leq 1 + \mathbb{E}_{\mathcal{S}}\Big[|\{\chi \in \mathbb{Z}_p \setminus \{0\} : \psi(\chi) < 2\}|\Big] \leq 1 + \frac{10^4 p}{|S|\sqrt{m}}$$

et

$$\mathbb{E}_{\mathcal{S}}[|A_t|] = \mathbb{E}_{\mathcal{S}}\Big[|\{\chi \in \mathbb{Z}_p \setminus \{0\} : t \leq \psi(\chi) < 2t\}|\Big] \leq \mathbb{E}_{\mathcal{S}}\Big[|\{\chi \in \mathbb{Z}_p \setminus \{0\} : \psi(\chi) < 2t\}|\Big] \leq \frac{10^4 p\sqrt{t}}{|S|\sqrt{m}}$$

pour tout entier positif $t \leq m/2^{22} \leq m/2000^2$. Enfin, notons que pour tout entier positif t, nous avons aussi la borne triviale $\mathbb{E}_{\mathcal{S}}[|A_t|] \leq p$.

En insérant ces bornes, nous obtenons

$$\begin{aligned}
\mathbb{P}[\Sigma(R) = z] &\leq \frac{1}{p}\mathbb{E}_{\mathcal{S}}[|A_0|] + \frac{1}{p}\sum_{\ell=0}^{\lfloor \log_2 m \rfloor} \mathbb{E}_{\mathcal{S}}[|A_{2^\ell}|] \cdot \exp(-2^\ell) \\
&\leq \frac{1}{p}\left(1 + \frac{10^4 p}{|S|\sqrt{m}}\right) + \frac{1}{p}\sum_{\ell=0}^{\lfloor \log_2 m \rfloor - 22} \frac{10^4 p 2^{\ell/2}}{|S|\sqrt{m}} \cdot \exp(-2^\ell) + \frac{1}{p}\sum_{\ell=\lfloor \log_2 m \rfloor - 21}^{\lfloor \log_2 m \rfloor} p \cdot \exp(-2^\ell) \\
&\leq \frac{1}{p} + \frac{10^4}{|S|\sqrt{m}} + \frac{10^4}{|S|\sqrt{m}} \sum_{\ell=0}^{\infty} \exp(\ell/2 - 2^\ell) + 22 \cdot \exp(-m/2^{22}) \\
&\leq \frac{1}{p} + \frac{10^4}{|S|\sqrt{m}} + \frac{10^4}{|S|\sqrt{m}} \cdot 2 + \frac{22}{|S|^4} \leq \frac{1}{p} + \frac{30022}{|S|\sqrt{m}} \leq \frac{1}{p} + \frac{C}{|S|\sqrt{m}}.
\end{aligned}$$

Ici, pour l'inégalité au début de la dernière ligne, nous avons utilisé $\sum_{\ell=0}^{\infty} \exp(\ell/2 - 2^\ell) \leq \sum_{\ell=0}^{\infty} \exp(\ell/2 - 2\ell) \leq \sum_{\ell=0}^{\infty} \exp(-\ell) \leq \sum_{\ell=0}^{\infty} 2^{-\ell} = 2$, ainsi que notre hypothèse $m \geq C \log |S| = 2^{24} \log |S|$. Pour l'inégalité suivante, nous avons utilisé $\sqrt{m} \leq m \leq |S|$. □

4 Déductions combinatoires d'anticoncentration

Dans cette section, nous utilisons des arguments combinatoires pour déduire le Corollaire 3 du Théorème 2, et pour dériver également un autre corollaire dont nous aurons besoin dans notre preuve du Théorème 1.

Nous commençons par l'observation simple suivante.

Lemme 11. *Soit p un nombre premier, soit $S \subseteq \mathbb{Z}_p$, et soit $m \leq |S|$ un entier positif. Maintenant, soit $R \subseteq S$ un sous-ensemble uniformément aléatoire de S de taille m. Alors nous avons*

$$\max_z \mathbb{P}[\Sigma(R) = z] \leq \frac{1}{|S| - m + 1},$$

Démonstration. Nous échantillonnons le sous-ensemble uniformément aléatoire $R \subseteq S$ de taille R en échantillonnant d'abord un sous-ensemble uniformément aléatoire $R' \subseteq S$ de taille $m-1$, puis en échantillonnant un élément uniformément aléatoire $r \in S \setminus R'$, en posant $R = R' \cup \{r\}$.

Conditionnellement à toute réalisation de R', pour tout $z \in \mathbb{Z}_p$, nous avons

$$\mathbb{P}[\Sigma(R) = z \mid R'] = \mathbb{P}[r = z - \Sigma(R') \mid R'] \leq \frac{1}{|S \setminus R'|} = \frac{1}{|S| - m + 1}.$$

Ainsi, pour tout $z \in \mathbb{Z}_p$, nous pouvons conclure

$$\mathbb{P}[\Sigma(R) = z] \leq \frac{1}{|S| - m + 1}.$$ □

Maintenant, nous sommes prêts à déduire le Corollaire 3 du Lemme 11 et du Théorème 2.

Preuve du Corollaire 3. Soit la constante $C > 0$ comme dans le Théorème 1. Nous pouvons supposer que $|S|$ est suffisamment grand par rapport à ε, puisque l'énoncé du Corollaire 3 est trivialement vrai pour les petits $|S|$ (en choisissant une grande constante $C'_\varepsilon > 0$). En particulier, nous pouvons supposer $|S| \geq (4000C/\varepsilon) \cdot (\log |S|)^2$ (et $|S| \geq 10$).

Si $m \leq C \log |S|$, l'assertion du Corollaire 3 découle directement du Lemme 11, puisque alors (notant que $m \leq C \log |S| \leq |S|/2$)

$$\max_z \mathbb{P}[\Sigma(R) = z] \leq \frac{1}{|S| - m + 1} \leq \frac{1}{|S|/2} \leq \frac{2\sqrt{C \log |S|}}{|S|\sqrt{m}} \leq \frac{1}{p} + \frac{2\sqrt{C} \cdot \sqrt{\log |S|}}{|S|\sqrt{m}}.$$

De plus, si $C \log |S| \leq m \leq 10^{-3}|S|/\log |S|$, l'assertion du Corollaire 3 découle directement du Théorème 2. Nous pouvons donc supposer que $m \geq 10^{-3}|S|/\log |S|$.

Soit $m_2 = \lfloor \varepsilon 10^{-3}|S|/\log |S| \rfloor \geq (\varepsilon/2)10^{-3}|S|/\log |S|$, et notons que $m_2 \leq m$. En posant $m_1 = m - m_2$, nous pouvons maintenant échantillonner le sous-ensemble uniformément aléatoire $R \subseteq S$ de taille m en échantillonnant d'abord un sous-ensemble uniformément aléatoire $R_1 \subseteq S$ de taille m_1, puis en échantillonnant un sous-ensemble uniformément aléatoire $R_2 \subseteq S \setminus R_1$ de taille m_2, en posant $R = R_1 \cup R_2$ (alors R a pour taille $m_1 + m_2 = m$).

Notons que pour toute réalisation de R_1, nous avons $|S \setminus R_1| \geq |S| - m \geq |S| - (1-\varepsilon)|S| = \varepsilon|S|$ et donc $m_2 \leq \varepsilon 10^{-3}|S|/\log |S| \leq 10^{-3}|S \setminus R_1|/\log |S \setminus R_1|$, ainsi que $m_2 \geq (\varepsilon/2)10^{-3}|S|/\log |S| \geq C \log |S| \geq C \log |S \setminus R_1|$. Par conséquent, conditionnellement à toute réalisation de R_1, par le Théorème 2, pour tout $z \in \mathbb{Z}_p$, nous avons

$$\mathbb{P}[\Sigma(R) = z \mid R_1] = \mathbb{P}[\Sigma(R_2) = z - \Sigma(R_1) \mid R_1] \leq \frac{1}{p} + \frac{C}{|S \setminus R_1|\sqrt{m_2}}.$$

Notant que $|S \setminus R_1|\sqrt{m_2} \geq \varepsilon|S| \cdot \sqrt{(\varepsilon/2)10^{-3}|S|/\log|S|} \geq \varepsilon^{3/2}|S|^{3/2}/(50\sqrt{\log|S|})$, nous pouvons conclure que

$$\mathbb{P}[\Sigma(R) = z \mid R_1] \leq \frac{1}{p} + \frac{50C\varepsilon^{-3/2}\sqrt{\log|S|}}{|S|^{3/2}} \leq \frac{1}{p} + \frac{50C\varepsilon^{-3/2}\sqrt{\log|S|}}{|S|\sqrt{m}}$$

pour toute réalisation de R_1 et tout $z \in \mathbb{Z}_p$. Cela montre que

$$\mathbb{P}[\Sigma(R) = z] \leq \frac{1}{p} + \frac{50C\varepsilon^{-3/2}\sqrt{\log|S|}}{|S|\sqrt{m}}$$

pour tout $z \in \mathbb{Z}_p$, ce qui termine la preuve. □

Dans la preuve de notre résultat principal dans le Théorème 1, nous utiliserons le corollaire suivant du Corollaire 3 plusieurs fois. Plutôt qu'avec un seul sous-ensemble aléatoire $R \subseteq S$ d'une taille donnée, ce corollaire concerne une chaîne uniformément aléatoire de sous-ensembles $R_1 \subseteq R_1 \subseteq \cdots \subseteq R_k \subseteq S$ de tailles données.

Corollaire 12. *Pour tout entier positif k, il existe une constante $C_k > 0$ telle que ce qui suit est vrai. Soit p un nombre premier, soit $S \subseteq \mathbb{Z}_p$ un sous-ensemble de taille $|S| \geq 2$, et considérons des entiers $1 \leq m_1 < \cdots < m_k < |S|$. Maintenant, soit $R_1 \subseteq \cdots \subseteq R_k \subseteq S$ une chaîne uniformément aléatoire de sous-ensembles de S satisfaisant $|R_i| = m_i$ pour $i = 1, \ldots, k$. Alors pour tous $z_1, \ldots, z_k \in \mathbb{Z}_p$, nous avons*

$$\mathbb{P}[\Sigma(R_i) = z_i \text{ pour } i = 1, \ldots, k] \leq \sum_{j=0}^{k} \prod_{i \in \{0,\ldots,k\} \setminus \{j\}} \left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1} - m_i}} \right),$$

où nous posons $m_0 = 0$ et $m_{k+1} = |S|$.

Démonstration. Soit $\varepsilon = 1/(k+1)$, et définissons $C_k = C'_\varepsilon/\varepsilon$ pour la constante C'_ε dans le Corollaire 3. Soient aussi $z_1, \ldots, z_k \in \mathbb{Z}_p$.

Comme $(m_1 - m_0) + (m_2 - m_1) + \cdots + (m_{k+1} - m_k) = m_{k+1} - m_0 = |S|$, nous pouvons fixer un indice $j \in \{0, \ldots, k\}$ avec $m_{j+1} - m_j \geq |S|/(k+1)$. Il suffit maintenant de prouver

$$\mathbb{P}[\Sigma(R_i) = z_i \text{ pour } i = 1, \ldots, k] \leq \prod_{i \in \{0,\ldots,k\} \setminus \{j\}} \left(\frac{1}{p} + \frac{(C'_\varepsilon/\varepsilon)\sqrt{\log|S|}}{|S|\sqrt{m_{i+1} - m_i}} \right).$$

Pour $i = j+1, \ldots, k$, soit $R'_i = S \setminus R_i$, et notons qu'alors nous avons $R'_k \subseteq R'_{k-1} \subseteq \cdots \subseteq R'_{j+1} \subseteq S \setminus R_j$ et $|R'_i| = |S| - m_i$ pour $i = j+1, \ldots, k$. De plus, conditionnellement à toute réalisation de $R_1, \ldots, R_j$, la chaîne d'ensembles $R'_k \subseteq R'_{k-1} \subseteq \cdots \subseteq R'_{j+1} \subseteq S \setminus R_j$ est uniformément aléatoire parmi toutes ces chaînes imbriquées dans $S \setminus R_j$ avec les tailles appropriées $|R'_i| = |S| - m_i$ pour $i = j+1, \ldots, k$.

Nous exposons la chaîne aléatoire $R_1 \subseteq R_1 \subseteq \cdots \subseteq R_k \subseteq S$ en exposant d'abord R_1 (c'est un sous-ensemble uniformément aléatoire de S de taille m_1), puis $R_2 \setminus R_1$ (c'est maintenant un sous-ensemble uniformément aléatoire de $S \setminus R_1$ de taille $m_2 - m_1$), et ainsi de suite jusqu'à ce que

nous exposions $R_j \setminus R_{j-1}$ (qui est un sous-ensemble uniformément aléatoire de $S \setminus R_{j-1}$ de taille $m_j - m_{j-1}$). À ce stade, nous avons déterminé $R_1, \ldots, R_j$. Maintenant, nous exposons R'_k (c'est un sous-ensemble uniformément aléatoire de $S \setminus R_j$ de taille $|S| - m_k$), puis $R'_{k-1} \setminus R'_k$ (c'est un sous-ensemble uniformément aléatoire de $S \setminus (R_j \cup R'_k)$ de taille $(|S| - m_{k-1}) - (|S| - m_k) = m_k - m_{k-1}$), et ainsi de suite jusqu'à ce que nous ayons également exposé toute la chaîne $R'_k \subseteq R'_{k-1} \subseteq \cdots \subseteq R'_{j+1}$. Cela détermine maintenant $R_1 \subseteq R_1 \subseteq \cdots \subseteq R_k$.

Observons que nous avons $\Sigma(R_i) = z_i$ pour $i = 1, \ldots, k$ si et seulement si toutes les conditions suivantes sont remplies : $\Sigma(R_1) = z_1$, et $\Sigma(R_i \setminus R_{i-1}) = z_i - z_{i-1}$ pour $i = 2, \ldots, j$, et $\Sigma(R'_k) = \Sigma(S) - z_k$, et $\Sigma(R'_i \setminus R'_{i+1}) = z_{i+1} - z_i$ pour $i = j+1, \ldots, k-1$. Cela signifie qu'à chaque étape de la procédure d'exposition ci-dessus, nous choisissons un sous-ensemble uniformément aléatoire des éléments non encore choisis d'une certaine taille prescrite, et nous devons borner la probabilité d'atteindre une certaine somme (conditionnellement à nos informations précédemment exposées). À chacune de ces étapes, nous pouvons utiliser le Corollaire 3 pour borner cette probabilité. Pour cela, nous utilisons de manière cruciale qu'à chaque étape nous choisissons au plus une fraction $(1 - \varepsilon)$ des éléments non encore choisis. En effet, cela est vrai puisque à la toute fin de la procédure, $m_{j+1} - m_j \geq |S|/(k+1) = \varepsilon|S|$ éléments restent non choisis (à savoir, les éléments de $R_{j+1} \setminus R_j$), et donc nous ne pouvons pas réduire le nombre d'éléments restants d'un facteur inférieur à ε à aucune étape. Notons également qu'à chaque étape, l'ensemble des éléments non encore choisis a une taille d'au moins $\varepsilon|S|$.

Ainsi, à chaque étape, conditionnellement aux informations précédemment exposées, la probabilité que notre sous-ensemble aléatoire atteigne la somme désirée peut effectivement être bornée par le Corollaire 3. Plus précisément, la probabilité d'avoir $\Sigma(R_1) = z_1$ est au plus

$$\frac{1}{p} + \frac{C'_\varepsilon \sqrt{\log |S|}}{\varepsilon |S| \sqrt{m_1}} = \frac{1}{p} + \frac{C'_\varepsilon \sqrt{\log |S|}}{\varepsilon |S| \sqrt{m_1 - m_0}}.$$

Pour tout $i = 2, \ldots, j$, la probabilité d'avoir $\Sigma(R_i \setminus R_{i-1}) = z_i - z_{i-1}$, conditionnellement aux informations précédemment exposées, est au plus

$$\frac{1}{p} + \frac{C'_\varepsilon \sqrt{\log |S|}}{\varepsilon |S| \sqrt{m_i - m_{i-1}}}.$$

La probabilité d'avoir $\Sigma(R'_k) = \Sigma(S) - z_k$, conditionnellement aux informations précédemment exposées déterminant $S \setminus R_j$, est au plus

$$\frac{1}{p} + \frac{C'_\varepsilon \sqrt{\log |S|}}{\varepsilon |S| \sqrt{|S| - m_k}} = \frac{1}{p} + \frac{C'_\varepsilon \sqrt{\log |S|}}{\varepsilon |S| \sqrt{m_{k+1} - m_k}}.$$

Et, enfin, pour $i = j+1, \ldots, k-1$, la probabilité d'avoir $\Sigma(R'_i \setminus R'_{i+1}) = z_{i+1} - z_i$, conditionnellement aux informations précédemment exposées, est au plus

$$\frac{1}{p} + \frac{C'_\varepsilon \sqrt{\log |S|}}{\varepsilon |S| \sqrt{m_{i+1} - m_i}}.$$

Au total, cela montre que

$$\begin{aligned}
&\mathbb{P}[\Sigma(R_i) = z_i \text{ pour } i = 1, \dots, k] \\
&\quad \le \left(\frac{1}{p} + \frac{C'_\varepsilon\sqrt{\log|S|}}{\varepsilon|S|\sqrt{m_1 - m_0}}\right) \cdot \prod_{i=2}^{j} \left(\frac{1}{p} + \frac{C'_\varepsilon\sqrt{\log|S|}}{\varepsilon|S|\sqrt{m_i - m_{i-1}}}\right) \cdot \left(\frac{1}{p} + \frac{C'_\varepsilon\sqrt{\log|S|}}{\varepsilon|S|\sqrt{m_{k+1} - m_k}}\right) \\
&\qquad\qquad \cdot \prod_{i=j+1}^{k} \left(\frac{1}{p} + \frac{C'_\varepsilon\sqrt{\log|S|}}{\varepsilon|S|\sqrt{m_{i+1} - m_i}}\right) \\
&\quad = \prod_{i \in \{0,\dots,k\}\setminus\{j\}} \left(\frac{1}{p} + \frac{(C'_\varepsilon/\varepsilon)\sqrt{\log|S|}}{|S|\sqrt{m_{i+1} - m_i}}\right). \qquad \square
\end{aligned}$$

Nous terminons cette section avec la borne suivante pour la somme des termes du membre de droite de l'inégalité du Corollaire 12 obtenue pour différents choix de $m_1 < \cdots < m_k$.

Lemme 13. *Soit k un entier positif, et soit $C_k > 0$ la constante dans le Corollaire 12. De plus, soit p un nombre premier, et soit $S \subseteq \mathbb{Z}_p$ un sous-ensemble de taille $|S| \ge 2$. Comme dans le Corollaire 12, posons $m_0 = 0$ et $m_{k+1} = |S|$. Alors, nous avons*

$$\sum_{1 \le m_1 < \cdots < m_k < |S|} \sum_{j=0}^{k} \prod_{i \in \{0,\dots,k\}\setminus\{j\}} \left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1} - m_i}}\right) \le (k+1) \cdot \left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right)^k,$$

où la somme du membre de gauche est prise sur tous les k-uplets $(m_1, \dots, m_k) \in \{1, \dots, |S|\}^k$ satisfaisant $1 \le m_1 < \cdots < m_k < |S|$.

Démonstration. Nous montrons d'abord par récurrence que pour $h = 0, \dots, k$ nous avons

$$\sum_{1 \le m_1 < \cdots < m_h < |S|} \prod_{i=0}^{h-1} \left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1} - m_i}}\right) \le \left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right)^h. \tag{5}$$

Pour $h = 0$, la somme du membre de droite de (5) comporte exactement un terme, correspondant à l'unique 0-uplet vide, et ce terme vaut 1 (comme produit vide). Ainsi, pour $h = 0$, l'inégalité s'écrit $1 \le 1$, ce qui est vrai. Supposons maintenant que nous ayons déjà montré (5) pour un certain $h \in \{0, \dots, k-1\}$. Maintenant, pour $h+1$, nous avons

$$\begin{aligned}
&\sum_{1 \le m_1 < \cdots < m_{h+1} < |S|} \prod_{i=0}^{h} \left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1} - m_i}}\right) \\
&\quad = \sum_{1 \le m_1 < \cdots < m_h < |S|} \left(\prod_{i=0}^{h-1} \left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1} - m_i}}\right) \cdot \sum_{m_{h+1} = m_h + 1}^{|S|-1} \left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{h+1} - m_h}}\right)\right) \\
&\quad \le \sum_{1 \le m_1 < \cdots < m_h < |S|} \left(\prod_{i=0}^{h-1} \left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1} - m_i}}\right) \cdot \left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right)\right) \\
&\quad = \left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right) \cdot \sum_{1 \le m_1 < \cdots < m_h < |S|} \prod_{i=0}^{h-1} \left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1} - m_i}}\right) \\
&\quad \le \left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right) \cdot \left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right)^h = \left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right)^{h+1},
\end{aligned}$$

où la deuxième inégalité découle de l'hypothèse de récurrence, et la première inégalité découle de

$$\sum_{m_{h+1}=m_h+1}^{|S|-1} \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{h+1}-m_h}} \le \sum_{t=1}^{|S|} \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{t}} \le \frac{C_k\sqrt{\log|S|}}{|S|}\cdot 2\sqrt{|S|} = \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}.$$

Cela prouve (5), comme affirmé.

Passons maintenant à l'inégalité de l'énoncé du lemme. Pour montrer cette inégalité, il suffit clairement de montrer

$$\sum_{1\le m_1<\cdots<m_k<|S|} \prod_{i\in\{0,\dots,k\}\setminus\{j\}} \left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1}-m_i}}\right) \le \left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right)^k$$

pour tout $j = 0,\dots,k$. Fixons donc $j \in \{0,\dots,k\}$. Maintenant, nous avons

$$\begin{aligned}
&\sum_{1\le m_1<\cdots<m_k<|S|} \prod_{i\in\{0,\dots,k\}\setminus\{j\}} \left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1}-m_i}}\right)\\
&\quad\le \sum_{1\le m_1<\cdots<m_j<|S|}\ \sum_{1\le m_{j+1}<\cdots<m_k<|S|} \prod_{i=0}^{j-1}\left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1}-m_i}}\right)\cdot\prod_{i=j+1}^{k}\left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1}-m_i}}\right)\\
&\quad= \sum_{1\le m_1<\cdots<m_j<|S|} \prod_{i=0}^{j-1}\left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1}-m_i}}\right)\cdot \sum_{1\le m_{j+1}<\cdots<m_k<|S|} \prod_{i=j+1}^{k}\left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1}-m_i}}\right)\\
&\quad= \sum_{1\le m_1<\cdots<m_j<|S|} \prod_{i=0}^{j-1}\left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m_{i+1}-m_i}}\right)\cdot \sum_{1\le m'_1<\cdots<m'_{k-j}<|S|} \prod_{i=0}^{k-j-1}\left(\frac{1}{p} + \frac{C_k\sqrt{\log|S|}}{|S|\sqrt{m'_{i+1}-m'_i}}\right)\\
&\quad\le \left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right)^j\cdot\left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right)^{k-j} = \left(\frac{|S|}{p} + \frac{2C_k\sqrt{\log|S|}}{|S|^{1/2}}\right)^k,
\end{aligned}$$

en définissant $m'_0 = 0$. Ici, à la troisième étape, nous avons substitué $m'_1 = |S| - m_k$ et $m'_2 = |S| - m_{k-1}$, et ainsi de suite jusqu'à $m'_{k-j} = |S| - m_{j+1}$. De plus, à l'avant-dernière étape, nous avons utilisé (5). □

5 Conjecture de réarrangement

Dans cette section, nous prouvons le Théorème 1, en utilisant le Corollaire 3. Soit $0 < \alpha < 1/2$ (notons que dans le Théorème 1 nous pouvons supposer sans perte de généralité que $\alpha < 1/2$, puisque l'énoncé pour une certaine valeur de α implique automatiquement le même énoncé pour toutes les valeurs plus grandes de α). Soit $D = \lceil 3/\alpha\rceil$ et soit C_α suffisamment grand pour que $C_\alpha \ge (10^4\cdot 2^{40D})^{1/\alpha}$ et $C_\alpha \ge (D+1)\cdot 2^D\cdot D^{14D^2} \ge 100\cdot(5D)^{2D} \ge (40D)^D$ et tel que nous ayons $4\max(C_D, C_1)\sqrt{\log n}/n^{1/2} \le n^{-\alpha}$ pour tout $n \ge C_\alpha$ (où C_1 et C_D désignent les constantes du Corollaire 12 pour $k = 1$ et $k = D$).

Maintenant, soit $S \subseteq \mathbb{Z}_p \setminus \{0\}$ comme dans le Théorème 1, ce qui signifie que $C_\alpha \leq |S| \leq p^{1-\alpha}$. Alors en particulier nous avons $|S|/p \leq p^{-\alpha} \leq |S|^{-\alpha}$ ainsi que $4C_1\sqrt{\log|S|}/|S|^{1/2} \leq |S|^{-\alpha}$ et $4C_D\sqrt{\log|S|}/|S|^{1/2} \leq |S|^{-\alpha}$.

Nous devons montrer qu'il existe un ordonnancement $s_1, s_2, \ldots, s_{|S|}$ des éléments de S tel que toutes les sommes partielles $s_1, s_1 + s_2, \ldots, s_1 + s_2 + \cdots + s_{|S|}$ soient distinctes. En d'autres termes, cela signifie que toutes les sommes partielles $s_a + s_{a+1} + \cdots + s_b$ doivent être non nulles dans $\mathbb{Z}_p$ pour tous $2 \leq a \leq b \leq |S|$.

Un ordonnancement $s_1, s_2, \ldots, s_{|S|}$ des éléments de S correspond à une bijection $\sigma : \{1, \ldots, |S|\} \to S$, où $\sigma(a) = s_a$ pour tout $a \in \{1, \ldots, |S|\}$. Pour une bijection $\sigma : \{1, \ldots, |S|\} \to S$, nous définissons

$$\Sigma(\sigma, [a, b]) = \sum_{i=a}^{b} \sigma(i) = \sigma(a) + \sigma(a+1) + \cdots + \sigma(b)$$

pour tous $1 \leq a < b \leq |S|$. C'est précisément $s_a + s_{a+1} + \cdots + s_b$ pour l'ordonnancement correspondant $s_1, s_2, \ldots, s_{|S|}$ des éléments de S. Ainsi, pour prouver le Théorème 1, notre tâche est de trouver une bijection $\sigma : \{1, \ldots, |S|\} \to S$ telle que $\Sigma(\sigma, [a, b]) \neq 0$ pour tous $2 \leq a < b \leq |S|$.

Notre point de départ est de considérer une bijection uniformément aléatoire $\sigma : \{1, \ldots, |S|\} \to S$. Typiquement, pour une telle bijection aléatoire, il y aura quelques (mais seulement peu) paires (a, b) avec $2 \leq a < b \leq |S|$ et $\Sigma(\sigma, [a, b]) = 0$. Au lieu de σ elle-même, nous considérerons donc $\sigma \circ \pi$ pour une permutation appropriée $\pi : \{1, \ldots, |S|\} \to \{1, \ldots, |S|\}$ obtenue en composant certaines transpositions afin de modifier $\Sigma(\sigma, [a, b])$ pour les intervalles $[a, b]$ où nous avons $\Sigma(\sigma, [a, b]) = 0$.

Étant donné une bijection $\sigma : \{1, \ldots, |S|\} \to S$, soit $B(\sigma) \subseteq \{3, \ldots, |S|\}$ l'ensemble constitué des extrémités droites de tous les intervalles $[a, b]$ avec $2 \leq a < b \leq |S|$ et $\Sigma(\sigma, [a, b]) = 0$. Plus formellement, soit $B(\sigma) \subseteq \{1, \ldots, |S|\}$ l'ensemble de tous les $b \in \{1, \ldots, |S|\}$ tels qu'il existe $a \in \{2, \ldots, |S|\}$ avec $a < b$ et $\Sigma(\sigma, [a, b]) = 0$ (notons qu'alors automatiquement $b \geq 3$).

Nous allons maintenant considérer divers événements indésirables (à savoir les événements $\mathcal{B}_1$, $\mathcal{B}_2$ et $\mathcal{B}_3$ définis ci-dessous), et montrer via nos résultats d'anticoncentration du Corollaire 12 que pour une bijection uniformément aléatoire $\sigma : \{1, \ldots, |S|\} \to S$ ces événements indésirables se produisent avec une très faible probabilité. Afin de prouver le Théorème 1, nous pouvons alors fixer une bijection $\sigma : \{1, \ldots, |S|\} \to S$ telle qu'aucun de ces événements ne se produise, et la prendre comme point de départ pour construire l'ordonnancement désiré $s_1, \ldots, s_{|S|}$ des éléments de S.

Lemme 14. *Pour une bijection uniformément aléatoire $\sigma : \{1, \ldots, |S|\} \to S$, soit $\mathcal{B}_1$ l'événement qu'il existe un $b \in B(\sigma)$ avec $|S| - 30D \leq b \leq |S|$. Alors nous avons $\mathbb{P}[\mathcal{B}_1] \leq 1/100$.*

Lemme 15. *Pour une bijection uniformément aléatoire $\sigma : \{1, \ldots, |S|\} \to S$, soit $\mathcal{B}_2$ l'événement qu'il existe $z \in \{1, \ldots, |S|\}$ avec $|B(\sigma) \cap \{z - 10D, \ldots, z + 10D\}| > D$. Alors nous avons $\mathbb{P}[\mathcal{B}_2] \leq 3/100$.*

Nous prouverons les Lemmes 14 et 15 plus loin ci-dessous (vers la fin de cette section). Les preuves de ces lemmes reposent sur nos résultats d'anticoncentration établis dans les sections précédentes.

Pour une permutation $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$, soit $\mathrm{Fix}(\pi) = \{t \in \{1, \dots, |S|\} : \pi(t) = t\}$ l'ensemble des points fixes de π. Pour tous $x, y \in \{1, \dots, |S|\}$ avec $x < y$, soit $\pi_{x,y} : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$ la transposition échangeant x et y (c'est-à-dire $\pi_{x,y}(x) = y$, $\pi_{x,y}(y) = x$ et $\pi_{x,y}(t) = t$ pour tout $t \in \{1, \dots, |S|\} \setminus \{x, y\}$).

Disons qu'une collection P de paires (x, y) avec $x, y \in \{1, \dots, |S|\}$ et $x < y$ est *admissible* si tous les éléments de $\{1, \dots, |S|\}$ apparaissant dans les paires de P sont distincts, et nous avons $y - x \leq 5D$ pour tout $(x, y) \in P$. À toute telle P admissible, nous pouvons associer la bijection $\pi_P : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$ obtenue en composant les transpositions $\pi_{x,y}$ pour tout $(x, y) \in P$ (notons qu'ici l'ordre de ces transpositions n'a pas d'importance, car elles commutent toutes entre elles car leurs supports sont disjoints). Nous disons qu'une permutation $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$ est *admissible*, si $\pi = \pi_P$ pour un certain P admissible. Notons également que P peut être reconstruit de manière unique à partir de π_P, de sorte que les permutations admissibles sont en correspondance bijective avec les collections admissibles P de paires.

Intuitivement, les permutations admissibles sont précisément les permutations qui peuvent être obtenues en échangeant une collection de paires disjointes (x, y) avec $x < y \leq x + 5D$. Pour nous, de telles permutations sont pertinentes, car nous allons modifier la bijection $\sigma : \{1, \dots, |S|\} \to S$ avec laquelle nous commençons dans notre argument via une telle permutation π (voir aussi la discussion ci-dessus), en remplaçant σ par $\sigma \circ \pi$. Plus précisément, π sera obtenue en composant des transpositions soigneusement choisies $\pi_{b,y}$ (avec $b < y \leq b + 5D$) pour chacun des éléments $b \in B(\sigma)$. Nous choisirons ces transpositions $\pi_{b,y}$ une par une pour chaque $b \in B(\sigma)$.

Pour une bijection $\sigma : \{1, \dots, |S|\} \to S$, un élément $b \in B(\sigma)$, et une permutation admissible $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$, disons qu'un élément $y \in \{1, \dots, |S|\}$ avec $b < y \leq b + 5D$ est *bloqué* pour σ, b et π, si nous avons $\Sigma(\sigma \circ \pi \circ \pi_{b,y}, [s, t]) = 0$ pour un certain intervalle $[s, t]$ avec $s, t \in \{2, \dots, |S|\}$ et $s < t$, tel que $s \in \{b + 1, \dots, y\}$ ou $t \in \{b, \dots, y - 1\}$.

Heuristiquement, si y est bloqué pour σ, b et π, alors cela signifie que nous ne pouvons pas remplacer $\sigma \circ \pi$ par $\sigma \circ \pi \circ \pi_{b,y}$ lorsque nous essayons de choisir la transposition désirée $\pi_{b,y}$ pour l'élément donné $b \in B(\sigma)$, car sinon l'intervalle $[s, t]$ créerait un nouveau problème.

Lemme 16. *Pour une bijection uniformément aléatoire $\sigma : \{1, \dots, |S|\} \to S$, soit $\mathcal{B}_3$ l'événement qu'il existe $b \in B(\sigma)$ et une permutation admissible $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$ avec $\{1, \dots, b - 1\} \subseteq \mathrm{Fix}(\pi)$ tels qu'au moins $2D$ éléments différents $y \in \{b + 1, \dots, b + 5D\}$ soient bloqués pour σ, b et π. Alors nous avons $\mathbb{P}[\mathcal{B}_3] \leq 1/25$.*

Nous reportons également la preuve du Lemme 16 à plus tard (elle utilise à nouveau nos résultats d'anticoncentration), afin de voir d'abord comment le Théorème 1 découle des Lemmes 14 à 16.

Preuve du Théorème 1. Pour une bijection uniformément aléatoire $\sigma : \{1, \dots, |S|\} \to S$, la probabilité que l'un des événements $\mathcal{B}_1$, $\mathcal{B}_2$ et $\mathcal{B}_3$ des Lemmes 14 à 16 se produise est au plus $\mathbb{P}[\mathcal{B}_1] + \mathbb{P}[\mathcal{B}_2] + \mathbb{P}[\mathcal{B}_3] \leq 1/100 + 3/100 + 1/25 = 2/25 < 1$. En particulier, il existe une bijection $\sigma : \{1, \dots, |S|\} \to S$ telle qu'aucun des événements $\mathcal{B}_1$, $\mathcal{B}_2$ et $\mathcal{B}_3$ ne se produise. Fixons une telle bijection σ.

Maintenant, soit $B(\sigma) = \{b_1, \dots, b_\ell\}$ avec $b_1 > \cdots > b_\ell$. Puisque l'événement $\mathcal{B}_1$ ne se produit pas, nous avons $b_i < |S| - 30D$ pour $i = 1, \dots, \ell$. De plus, puisque l'événement $\mathcal{B}_2$ ne se produit pas, pour tout $z \in \{1, \dots, |S|\}$ il y a au plus D indices différents $i \in \{1, \dots, \ell\}$ avec $|b_i - z| \leq 10D$.

Nous allons maintenant construire des $y_1, \dots, y_\ell \in \{1, \dots, |S|\} \setminus \{b_1, \dots, b_\ell\}$ distincts tels que $b_i < y_i \leq b_i + 5D$ pour $i = 1, \dots, \ell$ et tels que la bijection $\sigma \circ \pi_{b_1,y_1} \circ \cdots \circ \pi_{b_\ell,y_\ell} : \{1, \dots, |S|\} \to S$ corresponde à un ordonnancement des éléments de S avec les conditions désirées. En d'autres termes, cela signifie que $\Sigma(\sigma \circ \pi_{b_1,y_1} \circ \cdots \circ \pi_{b_\ell,y_\ell}, [a, b]) \neq 0$ pour tous $2 \leq a < b \leq |S|$.

Nous allons construire $y_1, \dots, y_\ell$ un par un. À l'étape j, nous nous assurons que pour tous $2 \leq a < b \leq |S|$ avec $\Sigma(\sigma \circ \pi_{b_1,y_1} \circ \cdots \circ \pi_{b_j,y_j}, [a, b]) = 0$ nous avons $b \in \{b_{j+1}, \dots, b_\ell\}$. De plus, lors du choix de y_j, nous nous assurons également que $y_j \in \{1, \dots, |S|\} \setminus \{b_1, \dots, b_\ell, y_1, \dots, y_{j-1}\}$ et $b_j < y_j \leq b_j + 5D$.

Supposons maintenant que pour un certain $j \in \{1, \dots, \ell\}$ nous ayons déjà construit des $y_1, \dots, y_{j-1} \in \{1, \dots, |S|\} \setminus \{b_1, \dots, b_\ell\}$ distincts avec $b_i < y_i \leq b_i + 5D$ pour $i = 1, \dots, j-1$, tels que pour tous $2 \leq a < b \leq |S|$ avec $\Sigma(\sigma \circ \pi_{b_1,y_1} \circ \cdots \circ \pi_{b_{j-1},y_{j-1}}, [a, b]) = 0$ nous avons $b \in \{b_j, \dots, b_\ell\}$. Notons que dans le cas $j = 1$ cette dernière condition est trivialement vraie, puisque pour tous $2 \leq a < b \leq |S|$ avec $\Sigma(\sigma, [a, b]) = 0$ nous avons $b \in B(\sigma) = \{b_1, \dots, b_\ell\}$.

D'abord, rappelons que $b_j < |S| - 30D$, donc nous avons $\{b_j + 1, \dots, b_j + 5D\} \subseteq \{1, \dots, |S|\}$. Observant que la collection constituée des paires (b_i, y_i) pour $i = 1, \dots, j-1$ est admissible, nous pouvons considérer la permutation admissible $\pi^* = \pi_{b_1,y_1} \circ \cdots \circ \pi_{b_{j-1},y_{j-1}}$. Parce que $b_1, \dots, b_{j-1} > b_j$, et par conséquent $y_1, \dots, y_{j-1} > b_j$, nous avons $\{1, \dots, b_j\} \subseteq \mathrm{Fix}(\pi^*)$. Par conséquent, puisque σ ne satisfait pas l'événement $\mathcal{B}_3$ du Lemme 16, au plus $2D$ éléments $y \in \{b_j + 1, \dots, b_j + 5D\}$ sont bloqués pour σ, $b_j \in B(\sigma)$ et π^*.

Nous affirmons qu'il existe $y_j \in \{b_j + 1, \dots, b_j + 5D\}$ qui est distinct de $b_1, \dots, b_\ell, y_1, \dots, y_{j-1}$ et non bloqué pour σ, b_j et π^*. En effet, l'intervalle $\{b_j + 1, \dots, b_j + 5D\}$ peut contenir b_i pour au plus D indices $i \in \{1, \dots, \ell\}$ (puisque nous avons $|b_i - b_j| \leq 5D$ pour tous ces i). De plus, pour tout indice $i \in \{1, \dots, j-1\}$ avec $y_i \in \{b_j + 1, \dots, b_j + 5D\}$ nous avons $|b_i - b_j| \leq |b_i - y_i| + |y_i - b_j| \leq 5D + 5D = 10D$, et donc il peut aussi y avoir au plus D indices $i \in \{1, \dots, j-1\}$ avec $y_i \in \{b_j, \dots, b_j + 5D\}$. Ainsi, le nombre d'éléments $y \in \{b_j + 1, \dots, b_j + 5D\}$, tels que y soit distinct de $b_1, \dots, b_\ell, y_1, \dots, y_{j-1}$, et y ne soit pas bloqué pour σ, b_j et π^*, est d'au moins $5D - 2D - D - D = D > 0$. En particulier, nous pouvons choisir $y_j \in \{b_j + 1, \dots, b_j + 5D\} \subseteq \{1, \dots, |S|\}$ distinct de $b_1, \dots, b_\ell, y_1, \dots, y_{j-1}$, tel que y_j ne soit pas bloqué pour σ, b_j et π^*.

Cette dernière condition signifie qu'il n'y a pas d'intervalle $[a, b]$ avec $a, b \in \{2, \dots, |S|\}$ et $a < b$ et $\Sigma(\sigma \circ \pi^* \circ \pi_{b_j,y_j}, [a, b]) = 0$, tel que $a \in \{b_j + 1, \dots, y_j\}$ ou $b \in \{b_j, \dots, y_j - 1\}$. Cela signifie que pour tout $2 \leq a < b \leq |S|$ avec $\Sigma(\sigma \circ \pi^* \circ \pi_{b_j,y_j}, [a, b]) = 0$ nous avons $a \notin \{b_j + 1, \dots, y_j\}$ et $b \notin \{b_j, \dots, y_j - 1\}$. Nous affirmons qu'alors soit b_j et y_j appartiennent tous deux à l'intervalle $[a, b]$, soit aucun des deux. En effet, si $b_j \in [a, b]$, alors nous avons $a \leq b_j < y_j$ ainsi que $b \geq b_j$ et donc $b \geq y_j$ (comme $b \notin \{b_j, \dots, y_j - 1\}$), ce qui implique que $y_j \in [a, b]$. Si $y_j \in [a, b]$, alors nous avons $b \geq y_j > b_j$ ainsi que $a \leq y_j$ et donc $a \leq b_j$ (comme $a \notin \{b_j + 1, \dots, y_j\}$), ce qui implique $b_j \in [a, b]$. Ainsi, pour tout $2 \leq a < b \leq |S|$ avec $\Sigma(\sigma \circ \pi^* \circ \pi_{b_j,y_j}, [a, b]) = 0$, soit b_j et y_j appartiennent tous

deux à l'intervalle $[a,b]$, soit aucun des deux, et donc dans la somme

$$\Sigma(\sigma\circ\pi^*\circ\pi_{b_j,y_j},[a,b])=\sigma(\pi^*(\pi_{b_j,y_j}(a)))+\sigma(\pi^*(\pi_{b_j,y_j}(a+1)))+\cdots+\sigma(\pi^*(\pi_{b_j,y_j}(b)))$$

soit les deux termes $\sigma(\pi^*(\pi_{b_j,y_j}(b_j)))=\sigma(\pi^*(y_j))$ et $\sigma(\pi^*(\pi_{b_j,y_j}(y_j)))=\sigma(\pi^*(b_j))$ apparaissent, soit aucun. Cela signifie que nous avons

$$\Sigma(\sigma\circ\pi^*\circ\pi_{b_j,y_j},[a,b])=\sigma(\pi^*(a)))+\sigma(\pi^*(a+1))+\cdots+\sigma(\pi^*(b))=\Sigma(\sigma\circ\pi^*,[a,b]).$$

Nous obtenons donc

$$\Sigma(\sigma\circ\pi_{b_1,y_1}\circ\cdots\circ\pi_{b_{j-1},y_{j-1}},[a,b])=\Sigma(\sigma\circ\pi^*,[a,b])=\Sigma(\sigma\circ\pi^*\circ\pi_{b_j,y_j},[a,b])=0,$$

et donc nous devons avoir $b\in\{b_j,\dots,b_\ell\}$. Comme $b\notin\{b_j,b_j+1,\dots,y_j-1\}$, nous avons $b\neq b_j$ et par conséquent $b\in\{b_{j+1},\dots,b_\ell\}$.

Ainsi, pour tout $2\leq a<b\leq|S|$ avec $\Sigma(\sigma\circ\pi^*\circ\pi_{b_j,y_j},[a,b])=0$ nous avons $b\in\{b_{j+1},\dots,b_\ell\}$. Notant que $\sigma\circ\pi^*\circ\pi_{b_j,y_j}=\sigma\circ\pi_{b_1,y_1}\circ\cdots\circ\pi_{b_j,y_j}$, cela montre que notre y_j choisi satisfait toutes les conditions désirées.

Après ℓ étapes, nous avons construit des $y_1,\dots,y_\ell\in\{1,\dots,|S|\}\setminus\{b_1,\dots,b_\ell\}$ distincts avec $b_i<y_i\leq b_i+5D$ pour $i=1,\dots,\ell$, tels que pour tous $2\leq a<b\leq|S|$ avec $\Sigma(\sigma\circ\pi_{b_1,y_1}\circ\cdots\circ\pi_{b_\ell,y_\ell},[a,b])=0$ nous avons $b\in\emptyset$. Cela signifie qu'il ne peut y avoir aucun $2\leq a<b\leq|S|$ avec $\Sigma(\sigma\circ\pi_{b_1,y_1}\circ\cdots\circ\pi_{b_\ell,y_\ell},[a,b])=0$. Ainsi, $\sigma\circ\pi_{b_1,y_1}\circ\cdots\circ\pi_{b_\ell,y_\ell}:\{1,\dots,|S|\}\to S$ est une bijection satisfaisant $\Sigma(\sigma\circ\pi_{b_1,y_1}\circ\cdots\circ\pi_{b_\ell,y_\ell},[a,b])\neq0$ pour tous $2\leq a<b\leq|S|$. Ainsi, en définissant $s_i=(\sigma\circ\pi_{b_1,y_1}\circ\cdots\circ\pi_{b_\ell,y_\ell})(i)$ pour $i=1,\dots,|S|$, nous avons

$$s_a+\cdots+s_b=(\sigma\circ\pi_{b_1,y_1}\circ\cdots\circ\pi_{b_\ell,y_\ell})(a)+\cdots+(\sigma\circ\pi_{b_1,y_1}\circ\cdots\circ\pi_{b_\ell,y_\ell})(b)=\Sigma(\sigma\circ\pi_{b_1,y_1}\circ\cdots\circ\pi_{b_\ell,y_\ell},[a,b])\neq0$$

pour tous $2\leq a<b\leq|S|$. Ainsi, les sommes partielles $s_1,s_1+s_2,\dots,s_1+\cdots+s_{|S|}$ sont toutes distinctes. □

Il reste à prouver les Lemmes 14 à 16. Nous commençons par prouver le Lemme 14.

Preuve du Lemme 14. Il suffit de montrer que pour chaque $b\in\{|S|-30D,\dots,|S|\}$ nous avons

$$\mathbb{P}[b\in B(\sigma)]\leq\frac{3}{|S|^\alpha}.$$

En effet, par une borne d'union, cela impliquerait (rappelant $(C_\alpha)^\alpha\geq10^4\cdot2^{40D}\geq10^4D$)

$$\mathbb{P}[\mathcal{B}_1]\leq\sum_{b=|S|-30D}^{|S|}\mathbb{P}[b\in B(\sigma)]\leq\frac{(30D+1)\cdot3}{|S|^\alpha}\leq\frac{100D}{(C_\alpha)^\alpha}\leq\frac{1}{100},$$

comme désiré. Soit donc $b\in\{|S|-30D,\dots,|S|\}$, alors nous avons

$$\mathbb{P}[b\in B(\sigma)]\leq\sum_{a=2}^{b-1}\mathbb{P}[\Sigma(\sigma,[a,b])=0]=\sum_{a=2}^{b-1}\mathbb{P}[\sigma(a)+\cdots+\sigma(b)=0].$$

Pour tout $2 \le a < b \le |S|$, l'ensemble $\{\sigma(a), \dots, \sigma(b)\}$ est un sous-ensemble uniformément aléatoire de S de taille $b-a+1$. Ainsi, par le Corollaire 12 (appliqué avec $k=1$ et $m_1 = b-a+1$, notant que $2 \le m_1 \le |S|-1$), nous avons

$$\mathbb{P}[\sigma(a)+\cdots+\sigma(b)=0] \le \left(\frac{1}{p} + \frac{C_1\sqrt{\log|S|}}{|S|\sqrt{b-a+1}}\right) + \left(\frac{1}{p} + \frac{C_1\sqrt{\log|S|}}{|S|\sqrt{|S|-b-1+a}}\right).$$

Ainsi, nous obtenons effectivement (rappelant que $|S|/p \le |S|^{-\alpha}$ et $4C_1\sqrt{\log|S|}/|S|^{1/2} \le |S|^{-\alpha}$)

$$\begin{aligned}
\mathbb{P}[b \in B(\sigma)] &\le \sum_{a=2}^{b-1}\left(\frac{2}{p} + \frac{C_1\sqrt{\log|S|}}{|S|\sqrt{b-a+1}} + \frac{C_1\sqrt{\log|S|}}{|S|\sqrt{|S|-b-1+a}}\right) \\
&\le \frac{2|S|}{p} + \sum_{i=2}^{b-1}\frac{C_1\sqrt{\log|S|}}{|S|\sqrt{i}} + \sum_{i=|S|-b+1}^{|S|-2}\frac{C_1\sqrt{\log|S|}}{|S|\sqrt{i}} \\
&\le 2|S|^{-\alpha} + \frac{2C_1\sqrt{\log|S|}}{|S|}\sum_{i=1}^{|S|}\frac{1}{\sqrt{i}} \le 2|S|^{-\alpha} + \frac{4C_1\sqrt{\log|S|}}{|S|^{1/2}} \le 3|S|^{-\alpha}. \qquad \square
\end{aligned}$$

Avant de prouver les Lemmes 15 et 16, nous prouvons d'abord le lemme auxiliaire suivant.

Lemme 17. *Pour une bijection uniformément aléatoire $\sigma : \{1, \dots, |S|\} \to S$, soit $\mathcal{B}_0$ l'événement que pour un certain $b \in B(\sigma)$ avec $b \le |S| - 30D$ il existe des sous-ensembles distincts $J, J' \subseteq \{b, b+1, \dots, b+20D\}$ tels que $\Sigma(\sigma(J)) = \Sigma(\sigma(J'))$. Alors nous avons $\mathbb{P}[\mathcal{B}_0] \le 1/100$.*

Démonstration. Il suffit de montrer que pour tout $b \in \{1, \dots, |S| - 30D\}$ et tous deux sous-ensembles distincts $J, J' \subseteq \{b, b+1, \dots, b+20D\}$ nous avons

$$\mathbb{P}[b \in B(\sigma) \text{ et } \Sigma(\sigma(J)) = \Sigma(\sigma(J'))] \le \frac{8}{|S|^{1+\alpha}}. \tag{6}$$

En effet, étant donné (6), en prenant une borne d'union sur les au plus $(|S|-30D)\cdot 2^{20D+1}\cdot 2^{20D+1} \le |S|\cdot 2^{40D+2}$ possibilités pour b, J et J' on obtient

$$\mathbb{P}[\mathcal{B}_0] \le |S|\cdot 2^{40D+2}\cdot\frac{8}{|S|^{1+\alpha}} = \frac{2^{40D+5}}{|S|^{\alpha}} \le \frac{2^{40D+5}}{(C_\alpha)^{\alpha}} \le \frac{1}{100}.$$

Soit donc $b \in \{1, \dots, |S| - 30D\}$, et considérons des sous-ensembles distincts $J, J' \subseteq \{b, b+1, \dots, b+20D\}$. Notons que l'événement $\Sigma(\sigma(J)) = \Sigma(\sigma(J'))$ (c'est-à-dire l'événement $\sum_{j\in J}\sigma(j) = \sum_{j'\in J'}\sigma(j')$) est déterminé par les réalisations de $\sigma(b), \dots, \sigma(b+20D)$. De plus, en choisissant un indice $i \in J \Delta J'$ et en conditionnant sur toutes les réalisations de $\sigma(b), \dots, \sigma(i-1), \sigma(i+1), \dots, \sigma(b+20D)$, nous pouvons voir qu'il y a au plus une réalisation pour $\sigma(i)$ (parmi les $|S| - 20D$ éléments restants dans S) telle que $\Sigma(\sigma(J)) = \Sigma(\sigma(J'))$ soit satisfaite. Ainsi, nous pouvons conclure

$$\mathbb{P}[\Sigma(\sigma(J)) = \Sigma(\sigma(J'))] \le \frac{1}{|S|-20D} \le \frac{2}{|S|},$$

puisque $|S| \geq C_\alpha \geq 50D$. Maintenant, en conditionnant sur toutes réalisations fixées de $\sigma(b), \ldots, \sigma(b+20D)$ telles que $\Sigma(\sigma(J)) = \Sigma(\sigma(J'))$ soit vraie, nous avons

$$\begin{aligned}
&\mathbb{P}[b \in B(\sigma) \mid \sigma(b), \ldots, \sigma(b+20D)] \\
&\quad \leq \sum_{a=2}^{b-1} \mathbb{P}[\Sigma(\sigma, [a,b]) = 0 \mid \sigma(b), \ldots, \sigma(b+20D)] \\
&\quad = \sum_{a=2}^{b-1} \mathbb{P}[\sigma(a) + \cdots + \sigma(b-1) = -\sigma(b) \mid \sigma(b), \ldots, \sigma(b+20D)] \\
&\quad \leq \sum_{a=2}^{b-1} \left(\frac{1}{p} + \frac{C_1\sqrt{\log(|S|-20D-1)}}{(|S|-20D-1)\sqrt{b-a}} + \frac{1}{p} + \frac{C_1\sqrt{\log(|S|-20D-1)}}{(|S|-20D-1)\sqrt{|S|-20D-1-b+a}} \right),
\end{aligned}$$

où dans la dernière étape nous avons appliqué le Corollaire 12 avec $k = 1$, notant que conditionnellement à nos réalisations fixées de $\sigma(b), \ldots, \sigma(b+20D)$, l'ensemble $\{\sigma(a), \ldots, \sigma(b-1)\}$ est un sous-ensemble uniformément aléatoire de taille $b-a$ dans $S \setminus \{\sigma(b), \ldots, \sigma(b+20D)\}$. Par conséquent nous pouvons conclure (rappelant que $|S| \geq C_\alpha \geq 50D$ ainsi que $|S|/p \leq |S|^{1-\alpha}$ et $4C_1\sqrt{\log|S|}/|S|^{1/2} \leq |S|^{-\alpha}$)

$$\mathbb{P}[b \in B(\sigma) \mid \sigma(b), \ldots, \sigma(b+20D)] \leq \frac{2|S|}{p} + 2 \cdot \frac{C_1\sqrt{\log|S|}}{(|S|/2)} \sum_{i=1}^{|S|} \frac{1}{\sqrt{i}} \leq 2|S|^{-\alpha} + \frac{8C_1\sqrt{\log|S|}}{|S|^{1/2}} \leq 4|S|^{-\alpha}$$

pour toutes réalisations fixées de $\sigma(b), \ldots, \sigma(b+20D)$. Ainsi, globalement nous obtenons effectivement

$$\mathbb{P}[b \in B(\sigma) \text{ et } \Sigma(\sigma(J)) = \Sigma(\sigma(J'))] \leq \frac{2}{|S|} \cdot 4|S|^{-\alpha} = \frac{8}{|S|^{1+\alpha}},$$

prouvant (6) □

Maintenant, nous sommes prêts à prouver le Lemme 15.

Preuve du Lemme 15. Pour les événements $\mathcal{B}_0$ et $\mathcal{B}_1$ des Lemmes 17 et 14, nous avons $\mathbb{P}[\mathcal{B}_0] \leq 1/100$ et $\mathbb{P}[\mathcal{B}_1] \leq 1/100$. Il suffit donc de prouver que $\mathbb{P}[\mathcal{B}_2 \setminus (\mathcal{B}_0 \cup \mathcal{B}_1)] \leq 1/100$.

Si $\mathcal{B}_2 \setminus (\mathcal{B}_0 \cup \mathcal{B}_1)$ (et donc $\mathcal{B}_2$) se produit, il existe $z \in \{1, \ldots, |S|\}$ avec $|B(\sigma) \cap \{z-10D, \ldots, z+10D\}| > D$. En prenant b_0 comme l'élément minimal de $B(\sigma) \cap \{z-10D, \ldots, z+10D\}$, cela signifie qu'il y a des $b_0, \ldots, b_D \in B(\sigma)$ distincts avec $b_1, \ldots, b_D \in \{b_0+1, \ldots, b_0+20D\}$. Comme $b_1, \ldots, b_D \in B(\sigma)$, il y a de plus $a_1, \ldots, a_D \in \{2, \ldots, |S|\}$ avec $a_i < b_i$ et $\Sigma(\sigma, [a_i, b_i]) = 0$ pour $i = 1, \ldots, D$. Puisque $\mathcal{B}_1$ ne se produit pas, nous devons avoir $b_0 \leq |S| - 30D$.

Nous affirmons que $a_1, \ldots, a_D$ doivent être distincts. En effet, supposons que $a_i = a_h$ pour deux indices distincts $i, h \in \{1, \ldots, D\}$, et supposons sans perte de généralité que $b_i < b_h$. Maintenant nous avons

$$\Sigma(\sigma(\{b_i+1, \ldots, b_h\})) = \Sigma(\sigma, [b_i+1, b_h]) = \Sigma(\sigma, [a_h, b_h]) - \Sigma(\sigma, [a_i, b_i]) = 0 - 0 = 0.$$

Ainsi, nous avons trouvé $b_0 \in B(\sigma)$ avec $b_0 \leq |S| - 30D$ tel que pour le sous-ensemble $J = \{b_i+1, \ldots, b_h\} \subseteq \{b_0, \ldots, b_0+20D\}$ nous avons $J \neq \emptyset$, mais $\Sigma(\sigma(J)) = 0 = \Sigma(\sigma(\emptyset))$. Cela signifie

que $\mathcal{B}_0$ se produit, ce qui est une contradiction. Par conséquent $a_1, \dots, a_D$ doivent effectivement être distincts.

Nous pouvons maintenant supposer sans perte de généralité que $a_1 < \cdots < a_D$. Nous affirmons également que $a_D < b_0$. En effet, si $a_D \geq b_0$ nous aurions $b_0 \leq a_D < b_D \leq b_0 + 20D$ et de plus $\Sigma(\sigma(\{a_D, \dots, b_D\})) = \Sigma(\sigma, [a_D, b_D]) = 0$. Ainsi, en considérant $b_0 \in B(\sigma)$ et $J = \{a_D, \dots, b_D\} \subseteq \{b_0, \dots, b_0 + 20D\}$ nous aurions à nouveau $J \neq \emptyset$, mais $\Sigma(\sigma(J)) = 0 = \Sigma(\sigma(\emptyset))$. Donc à nouveau $\mathcal{B}_0$ se produirait, contredisant notre hypothèse selon laquelle $\mathcal{B}_2 \setminus (\mathcal{B}_0 \cup \mathcal{B}_1)$ se produit.

Par conséquent nous devons avoir $a_D < b_0$ et donc $a_1 < \cdots < a_D < b_0$. En résumé, nous avons trouvé que si $\mathcal{B}_2 \setminus (\mathcal{B}_0 \cup \mathcal{B}_1)$ se produit, il doit exister $b_0 \in \{1, \dots, |S| - 30D\}$ et $b_1, \dots, b_D \in \{b_0 + 1, \dots, b_0 + 20D\}$ ainsi que $a_1, \dots, a_D \in \{1, \dots, |S|\}$ avec $a_1 < \cdots < a_D < b_0$ tels que $\Sigma(\sigma, [a_i, b_i]) = 0$ pour $i = 1, \dots, D$.

Pour tout $b_0 \in \{1, \dots, |S| - 30D\}$ donné et $b_1, \dots, b_D \in \{b_0 + 1, \dots, b_0 + 20D\}$, en conditionnant sur toutes réalisations fixées de $\sigma(b_0), \dots, \sigma(b_0 + 20D)$, nous avons

$$\begin{aligned}
&\mathbb{P}\Big[\text{il existe } a_1 < \cdots < a_D < b_0 \text{ avec } \Sigma(\sigma, [a_i, b_i]) = 0 \text{ pour } i = 1, \dots, D \,\Big|\, \sigma(b_0), \dots, \sigma(b_0 + 20D)\Big] \\
&\quad \leq \sum_{1 \leq a_1 < \cdots < a_D < b_0} \mathbb{P}\Big[\Sigma(\sigma, [a_i, b_i]) = 0 \text{ pour } i = 1, \dots, D \,\Big|\, \sigma(b_0), \dots, \sigma(b_0 + 20D)\Big] \\
&\quad = \sum_{1 \leq a_1 < \cdots < a_D < b_0} \mathbb{P}\Big[\Sigma(\sigma, [a_i, b_0 - 1]) = -\Sigma(\sigma, [b_0, b_i]) \text{ pour } i = 1, \dots, D \,\Big|\, \sigma(b_0), \dots, \sigma(b_0 + 20D)\Big].
\end{aligned}$$

Chaque terme du membre de droite peut être borné par le Corollaire 12, notant que $\Sigma(\sigma, [a_i, b_0 - 1]) = \Sigma(\{\sigma(a_i), \dots, \sigma(b_0 - 1)\})$ pour $i = 1, \dots, D$, et que $\{\sigma(a_D), \dots, \sigma(b_0 - 1)\} \subseteq \cdots \subseteq \{\sigma(a_1), \dots, \sigma(b_0 - 1)\}$ (conditionnellement à nos réalisations fixées de $\sigma(b_0), \dots, \sigma(b_0 + 20D)$) est une chaîne uniformément aléatoire de sous-ensembles de $S \setminus \{\sigma(b_0), \dots, \sigma(b_0 + 20D)\}$ de tailles $b_0 - a_D, \dots, b_0 - a_1$, où $1 \leq b_0 - a_D < \cdots < b_0 - a_1 < |S| - 20D - 1$. Ainsi, en appliquant le Corollaire 12 et le Lemme 13 nous pouvons conclure (rappelant également que $|S|/p \leq |S|^{-\alpha}$ et $4C_D\sqrt{\log|S|}/|S|^{1/2} \leq |S|^{-\alpha}$ ainsi que $D = \lceil 3/\alpha \rceil$)

$$\begin{aligned}
&\mathbb{P}\Big[\text{il existe } a_1 < \cdots < a_D < b_0 \text{ avec } \Sigma(\sigma, [a_i, b_i]) = 0 \text{ pour } i = 1, \dots, D \,\Big|\, \sigma(b_0), \dots, \sigma(b_0 + 20D)\Big] \\
&\quad \leq (D+1) \cdot \left(\frac{|S| - 20D - 1}{p} + \frac{2C_D\sqrt{\log(|S| - 20D - 1)}}{(|S| - 20D - 1)^{1/2}} \right)^D \\
&\quad \leq (D+1) \cdot \left(\frac{|S|}{p} + \frac{4C_D\sqrt{\log|S|}}{|S|^{1/2}} \right)^D \leq (D+1) \cdot (2|S|^{-\alpha})^D = (D+1)2^D \cdot |S|^{-\alpha D} \leq \frac{(D+1)2^D}{|S|^3}
\end{aligned}$$

pour tout $b_0 \in \{1, \dots, |S| - 30D\}$ donné et $b_1, \dots, b_D \in \{b_0 + 1, \dots, b_0 + 20D\}$, et toutes réalisations fixées de $\sigma(b_0), \dots, \sigma(b_0 + 20D)$. Cela montre que

$$\mathbb{P}\Big[\text{il existe } a_1 < \cdots < a_D < b_0 \text{ et } \Sigma(\sigma, [a_i, b_i]) = 0 \text{ pour } i = 1, \dots, D\Big] \leq \frac{(D+1)2^D}{|S|^3}$$

pour tout $b_0 \in \{1, \ldots, |S|-30D\}$ et $b_1, \ldots, b_D \in \{b_0+1, \ldots, b_0+20D\}$. En prenant la borne d'union sur tous les choix possibles de $b_0 \in \{1, \ldots, |S| - 30D\}$ et $b_1, \ldots, b_D \in \{b_0 + 1, \ldots, b_0 + 20D\}$, nous pouvons conclure que

$$\mathbb{P}[\mathcal{B}_2 \setminus (\mathcal{B}_0 \cup \mathcal{B}_1)] \leq |S| \cdot (20D)^D \cdot \frac{(D+1)2^D}{|S|^3} = \frac{(D+1)(40D)^D}{|S|^2} \leq \frac{(D+1)(40D)^D}{(C_\alpha)^2} \leq \frac{1}{100}. \quad \square$$

Pour prouver le Lemme 16, nous avons également besoin d'un autre lemme auxiliaire.

Lemme 18. *Soient $b, b' \in \{2, \ldots |S|-2\}$ avec $b'-b = 5D$, soient $u_1, \ldots, u_D \in \{b, \ldots, b'\}$, et considérons des permutations $\pi_1, \ldots, \pi_D : \{1, \ldots, |S|\} \to \{1, \ldots, |S|\}$ avec $\{1, \ldots, b-1\} \cup \{b'+1, \ldots, |S|\} \subseteq \mathrm{Fix}(\pi_i)$ pour $i = 1, \ldots, D$. Alors, pour une bijection uniformément aléatoire $\sigma : \{1, \ldots, |S|\} \to S$, il se produit avec probabilité au plus $1/|S|^2$ qu'il existe $x_1, \ldots, x_D \in \{b' + 1, \ldots, |S|\}$ avec $x_1 < \cdots < x_D$, ainsi qu'une permutation admissible $\pi : \{1, \ldots, |S|\} \to \{1, \ldots, |S|\}$, telles que $\Sigma(\sigma \circ \pi \circ \pi_i, [u_i, x_i]) = 0$ pour $i = 1, \ldots, D$.*

En inversant l'ordre de $\{1, \ldots, |S|\}$, nous obtenons l'énoncé analogue suivant à partir du Lemme 18.

Lemme 19. *Soient $b, b' \in \{2, \ldots |S| - 2\}$ avec $b' - b = 5D$, soient $u_1, \ldots, u_D \in \{b, \ldots, b'\}$, et considérons des permutations $\pi_1, \ldots, \pi_D : \{1, \ldots, |S|\} \to \{1, \ldots, |S|\}$ avec $\{1, \ldots, b-1\} \cup \{b' + 1, \ldots, |S|\} \subseteq \mathrm{Fix}(\pi_i)$ pour $i = 1, \ldots, D$. Alors, pour une bijection uniformément aléatoire $\sigma : \{1, \ldots, |S|\} \to S$, il se produit avec probabilité au plus $1/|S|^2$ qu'il existe $x_1, \ldots, x_D \in \{1, \ldots, b-1\}$ avec $x_1 < \cdots < x_D$, ainsi qu'une permutation admissible $\pi : \{1, \ldots, |S|\} \to \{1, \ldots, |S|\}$, telles que $\Sigma(\sigma \circ \pi \circ \pi_i, [x_i, u_i]) = 0$ pour $i = 1, \ldots, D$.*

Comme le Lemme 19 est complètement analogue au Lemme 18, nous ne prouvons que le Lemme 18.

Preuve du Lemme 18. Pour $x_1, \ldots, x_D \in \{b' + 1, \ldots, |S|\}$ avec $x_1 < \cdots < x_D$, disons qu'une permutation admissible $\pi : \{1, \ldots, |S|\} \to \{1, \ldots, |S|\}$ est *intéressante* pour $(x_1, \ldots, x_D)$ si pour toute paire $(q, r) \in P$ nous avons $|\{q, r\} \cap \pi_i(\{u_i, \ldots, x_i\})| = 1$ pour un certain $i \in \{1, \ldots, D\}$ (ici, par P nous désignons la collection admissible de paires correspondant à π).

Pour toute réalisation de $\sigma : \{1, \ldots, |S|\} \to S$, et tous $x_1, \ldots, x_D \in \{b' + 1, \ldots, |S|\}$ avec $x_1 < \cdots < x_D$, nous affirmons ce qui suit : S'il existe une permutation admissible $\pi : \{1, \ldots, |S|\} \to \{1, \ldots, |S|\}$ avec $\Sigma(\sigma \circ \pi \circ \pi_i, [u_i, x_i]) = 0$ pour $i = 1, \ldots, D$, alors il existe aussi une telle permutation admissible qui est intéressante pour $(x_1, \ldots, x_D)$. En effet, soit P la collection admissible de paires correspondant à π (c'est-à-dire soit $\pi = \pi_P$), et soit $P' \subseteq P$ le sous-ensemble des paires $(q, r) \in P$ satisfaisant $|\{q, r\} \cap \pi_i(\{u_i, \ldots, x_i\})| = 1$ pour un certain $i \in \{1, \ldots, D\}$. Maintenant, en prenant $\pi' = \pi_{P'}$ comme la permutation admissible correspondant à P', la permutation π' est par définition intéressante pour $(x_1, \ldots, x_D)$. De plus, pour $i = 1, \ldots, D$, nous avons $\pi_{q,r}(\pi_i(\{u_i, \ldots, x_i\})) = \pi_i(\{u_i, \ldots, x_i\})$ pour tout $(q, r) \in P \setminus P'$, et donc $\pi_{P \setminus P'}(\pi_i(\{u_i, \ldots, x_i\})) = \pi_i(\{u_i, \ldots, x_i\})$. Cela montre que $\pi(\pi_i(\{u_i, \ldots, x_i\})) = \pi'(\pi_i(\{u_i, \ldots, x_i\}))$ et donc

$$\Sigma(\sigma \circ \pi' \circ \pi_i, [u_i, x_i]) = \Sigma(\sigma(\pi'(\pi_i(\{u_i, \ldots, x_i\})))) = \Sigma(\sigma(\pi(\pi_i(\{u_i, \ldots, x_i\})))) = \Sigma(\sigma \circ \pi \circ \pi_i, [u_i, x_i]) = 0$$

pour $i = 1, \ldots, D$. Ainsi, il existe une permutation admissible π', qui est intéressante pour $(x_1, \ldots, x_D)$, et satisfait $\Sigma(\sigma \circ \pi' \circ \pi_i, [u_i, x_i]) = 0$ pour $i = 1, \ldots, D$.

Ainsi, l'événement décrit dans l'énoncé du lemme est équivalent à l'événement qu'il existe $x_1, \dots, x_D \in \{b'+1, \dots, |S|\}$ avec $x_1 < \cdots < x_D$, ainsi qu'une permutation admissible $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$ qui est intéressante pour $(x_1, \dots, x_D)$, telle que $\Sigma(\sigma \circ \pi \circ \pi_i, [u_i, x_i]) = 0$ pour $i = 1, \dots, D$. Il suffit donc de montrer que la probabilité de cet événement est au plus $1/|S|^2$.

Fixons tous $x_1, \dots, x_D \in \{b'+1, \dots, |S|\}$ avec $x_1 < \cdots < x_D$. Nous affirmons que le nombre de permutations admissibles $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$ qui sont intéressantes pour $(x_1, \dots, x_D)$ est au plus D^{14D^2}. En effet, soit P la collection admissible de paires correspondant à π, pour toute paire $(q, r) \in P$ nous avons $|\{q, r\} \cap \pi_i(\{u_i, \dots, x_i\})| = 1$ pour un certain $i \in \{1, \dots, D\}$. Ainsi, pour toute paire $(q, r) \in P$ nous avons $q \in \{b, \dots, b'\}$ ou $r \in \{b, \dots, b'\}$ ou $|\{q, r\} \cap \pi_i(\{b'+1, \dots, x_i\})| = 1$. Puisque $\pi_i(\{b'+1, \dots, x_i\}) = \{b'+1, \dots, x_i\}$ et $1 \le r - q \le 5D = b' - b$, cela signifie que $q \in \{b - 5D, \dots, b'\} = \{b - 5D, \dots, b + 5D\}$ ou $q \in \{x_i - 5D + 1, \dots, x_i\}$ pour un certain $i \in \{1, \dots, D\}$. Ainsi, nous avons $q \in \{b - 5D, \dots, b + 5D\} \cup \bigcup_{i=1}^{D} \{x_i - 5D + 1, \dots, x_i\}$ pour tout $(q, r) \in P$. Rappelons que deux paires dans P ne peuvent pas commencer par le même élément q, et que $r \in \{q+1, \dots, q+5D\}$ pour tout $(q, r) \in P$. Ainsi, pour choisir P, pour chaque élément $q \in \{b-5D, \dots, b+5D\} \cup \bigcup_{i=1}^{D} \{x_i - 5D + 1, \dots, x_i\}$ on a au plus $5D$ options pour choisir un élément correspondant r pour prendre $(q, r) \in P$, en plus de l'option de n'avoir aucune paire dans P commençant par q. Notant que $|\{b-5D, \dots, b+5D\} \cup \bigcup_{i=1}^{D} \{x_i - 5D + 1, \dots, x_i\}| \le 10D + 1 + D \cdot 5D \le 7D^2$, nous pouvons conclure que le nombre de possibilités pour P et donc pour π est au plus $(5D+1)^{7D^2} \le (D^2)^{7D^2} = D^{14D^2}$.

Maintenant, pour tous $x_1, \dots, x_D \in \{b'+1, \dots, |S|\}$ avec $x_1 < \cdots < x_D$ et pour chacune des au plus D^{14D^2} permutations admissibles $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$ qui sont intéressantes pour $(x_1, \dots, x_D)$, nous avons

$$\begin{aligned}
&\mathbb{P}[\Sigma(\sigma \circ \pi \circ \pi_i, [u_i, x_i]) = 0 \text{ pour } i = 1, \dots, D] \\
&\quad = \mathbb{P}[\Sigma((\sigma \circ \pi)(\pi_i(\{u_i, \dots, x_i\}))) = 0 \text{ pour } i = 1, \dots, D] \\
&\quad = \mathbb{P}[\Sigma((\sigma \circ \pi)(\{b'+1, \dots, x_i\})) = -\Sigma((\sigma \circ \pi)(\pi_i(\{u_i, \dots, b'\}))) \text{ pour } i = 1, \dots, D],
\end{aligned}$$

rappelant que $\pi_i(\{b'+1, \dots, x_i\}) = \{b'+1, \dots, x_i\}$. Notons que, pour notre π fixé, la composition $\sigma \circ \pi : \{1, \dots, |S|\} \to S$ est une bijection uniformément aléatoire. En conditionnant sur toutes réalisations fixées de $(\sigma \circ \pi)(b), \dots, (\sigma \circ \pi)(b')$ (qui déterminent alors la valeur de $\Sigma((\sigma \circ \pi)(\pi_i(\{u_i, \dots, b'\})))$ pour tout $i = 1, \dots, D$), nous avons

$$\begin{aligned}
&\mathbb{P}[\Sigma((\sigma \circ \pi)(\{b'+1, \dots, x_i\})) = -\Sigma((\sigma \circ \pi)(\pi_i(\{u_i, \dots, b'\}))) \text{ pour } i = 1, \dots, D | (\sigma \circ \pi)(b), \dots, (\sigma \circ \pi)(b')] \\
&\quad \le \sum_{j=0}^{D} \prod_{i \in \{0, \dots, D\} \setminus \{j\}} \left(\frac{1}{p} + \frac{C_D \sqrt{\log s}}{s \sqrt{m_{i+1}(x_1, \dots, x_D) - m_i(x_1, \dots, x_D)}} \right)
\end{aligned}$$

par le Corollaire 12, notant que $(\sigma \circ \pi)(\{b'+1, \dots, x_1\}) \subseteq \cdots \subseteq (\sigma \circ \pi)(\{b'+1, \dots, x_D\})$ est une chaîne uniformément aléatoire de sous-ensembles de $S \setminus \{(\sigma \circ \pi)(b), \dots, (\sigma \circ \pi)(b')\}$ de tailles $x_1 - b', \dots, x_D - b'$, où $1 \le x_1 - b' < \cdots < x_D - b' < |S| - (b' - b + 1)$. Ici, par commodité nous définissons

$$s = |S \setminus \{(\sigma \circ \pi)(b), \dots, (\sigma \circ \pi)(b')\}| = |S| - (b' - b + 1) = |S| - 5D - 1,$$

et $m_i(x_1, \dots, x_D) = x_i - b'$ pour $i = 1, \dots, D$ ainsi que $m_0(x_1, \dots, x_D) = 0$ et $m_{D+1}(x_1, \dots, x_D) = s$ (alors $m_1(x_1, \dots, x_D), \dots, m_D(x_1, \dots, x_D)$ sont précisément les tailles des sous-ensembles dans la

chaîne).

Puisque cela est vrai pour toutes réalisations fixées de $(\sigma \circ \pi)(b), \dots, (\sigma \circ \pi)(b')$, nous pouvons conclure que

$$\begin{aligned}
&\mathbb{P}[\Sigma(\sigma \circ \pi \circ \pi_i, [u_i, x_i]) = 0 \text{ pour } i = 1, \dots, D] \\
&\quad = \mathbb{P}[\Sigma((\sigma \circ \pi)(\{b'+1, \dots, x_i\})) = -\Sigma((\sigma \circ \pi)(\pi_i(\{u_i, \dots, b'\}))) \text{ pour } i = 1, \dots, D] \\
&\quad \leq \sum_{j=0}^{D} \prod_{i \in \{0,\dots,D\} \setminus \{j\}} \left(\frac{1}{p} + \frac{C_D \sqrt{\log s}}{s \sqrt{m_{i+1}(x_1, \dots, x_D) - m_i(x_1, \dots, x_D)}} \right)
\end{aligned}$$

pour tous $x_1, \dots, x_D \in \{b'+1, \dots, |S|\}$ avec $x_1 < \cdots < x_D$ et pour chacune des au plus D^{14D^2} permutations admissibles $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$ qui sont intéressantes pour $(x_1, \dots, x_D)$.

Ainsi, pour tous $x_1, \dots, x_D \in \{b'+1, \dots, |S|\}$ avec $x_1 < \cdots < x_D$, nous pouvons conclure

$$\begin{aligned}
&\mathbb{P}[\exists \text{ admissible } \pi \text{ t.q. } \Sigma(\sigma \circ \pi \circ \pi_i, [u_i, x_i]) = 0 \text{ pour } i = 1, \dots, D] \\
&\quad = \mathbb{P}[\exists \text{ admissible } \pi, \text{ intéressante pour } (x_1, \dots, x_D), \text{ t.q. } \Sigma(\sigma \circ \pi \circ \pi_i, [u_i, x_i]) = 0 \text{ pour } i = 1, \dots, D] \\
&\quad \leq D^{14D^2} \cdot \sum_{j=0}^{D} \prod_{i \in \{0,\dots,D\} \setminus \{j\}} \left(\frac{1}{p} + \frac{C_D \sqrt{\log s}}{s \sqrt{m_{i+1}(x_1, \dots, x_D) - m_i(x_1, \dots, x_D)}} \right).
\end{aligned}$$

Ainsi, la probabilité qu'il existe $x_1, \dots, x_D \in \{b'+1, \dots, |S|\}$ avec $x_1 < \cdots < x_D$ et une permutation admissible $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$, telle que $\Sigma(\sigma \circ \pi \circ \pi_i, [u_i, x_i]) = 0$ pour $i = 1, \dots, D$, est au plus

$$\begin{aligned}
&\sum_{b'+1 \leq x_1 < \cdots < x_D \leq |S|} D^{14D^2} \cdot \sum_{j=0}^{D} \prod_{i \in \{0,\dots,D\} \setminus \{j\}} \left(\frac{1}{p} + \frac{C_D \sqrt{\log s}}{s \sqrt{m_{i+1}(x_1, \dots, x_D) - m_i(x_1, \dots, x_D)}} \right) \\
&\quad = D^{14D^2} \sum_{1 \leq m_1 < \cdots < m_D \leq |S| - b'} \sum_{j=0}^{D} \prod_{i \in \{0,\dots,D\} \setminus \{j\}} \left(\frac{1}{p} + \frac{2C_D \sqrt{\log s}}{s \sqrt{m_{i+1} - m_i}} \right) \\
&\quad \leq D^{14D^2} \sum_{1 \leq m_1 < \cdots < m_D < s} \sum_{j=0}^{D} \prod_{i \in \{0,\dots,D\} \setminus \{j\}} \left(\frac{1}{p} + \frac{2C_D \sqrt{\log s}}{s \sqrt{m_{i+1} - m_i}} \right) \\
&\quad \leq D^{14D^2} \cdot (D+1) \cdot \left(\frac{s}{p} + \frac{2C_D \sqrt{\log s}}{s^{1/2}} \right)^D \\
&\quad \leq D^{14D^2} \cdot (D+1) \cdot \left(\frac{|S|}{p} + \frac{4C_D \sqrt{\log |S|}}{|S|^{1/2}} \right)^D \\
&\quad \leq D^{14D^2} \cdot (D+1) \cdot (2|S|^{-\alpha})^D = D^{14D^2} (D+1) 2^D \cdot |S|^{-\alpha D} \leq \frac{(D+1) 2^D D^{14D^2}}{|S|^3} \leq \frac{1}{|S|^2}
\end{aligned}$$

en définissant $m_0 = 0$ et $m_{D+1} = s$. Ici, à la première étape nous avons utilisé le changement de variables $m_i = x_i - b'$ pour $i = 1, \dots, D$ (notant qu'alors m_i coïncide précisément avec $m_i(x_1, \dots, x_D)$ défini ci-dessus), à la troisième étape nous avons utilisé le Lemme 13, à la quatrième étape nous avons utilisé que $|S|/2 \leq s \leq |S|$, à la cinquième étape nous avons utilisé $|S|/p \leq |S|^{-\alpha}$ et $4C_D\sqrt{\log|S|}/|S|^{1/2} \leq |S|^{-\alpha}$, à l'avant-dernière étape $D = \lceil 3/\alpha \rceil$, et à la dernière étape $|S| \geq C_\alpha \geq (D+1)2^D D^{14D^2}$. □

Enfin, nous prouvons maintenant le Lemme 16, ce qui conclut la preuve du Théorème 1.

Preuve du Lemme 16. Pour les événements $\mathcal{B}_0$ et $\mathcal{B}_1$ des Lemmes 17 et 14, nous avons $\mathbb{P}[\mathcal{B}_0] \leq 1/100$ et $\mathbb{P}[\mathcal{B}_1] \leq 1/100$. Il suffit donc de prouver que $\mathbb{P}[\mathcal{B}_3 \setminus (\mathcal{B}_0 \cup \mathcal{B}_1)] \leq 2/100$.

Si l'événement $\mathcal{B}_3 \setminus (\mathcal{B}_0 \cup \mathcal{B}_1)$ se produit, il existe $b \in B(\sigma)$, et une permutation admissible $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$ avec $\{1, \dots, b-1\} \subseteq \mathrm{Fix}(\pi)$, et $2D$ éléments différents $y \in \{b+1, \dots, b+5D\}$ qui sont bloqués pour σ, b et π. Comme $\mathcal{B}_1$ ne se produit pas, nous devons avoir $b < |S| - 30D$ (et nous devons aussi avoir $b \geq 3$). De plus, comme $\mathcal{B}_0$ ne se produit pas, pour tous sous-ensembles distincts $J, J' \subseteq \{b, b+1, \dots, b+20D\}$ nous avons $\Sigma(\sigma(J)) \neq \Sigma(\sigma(J'))$. Ainsi, pour tous sous-ensembles distincts $J, J' \subseteq \{b, b+1, \dots, b+5D\}$ nous devons avoir $\Sigma(\sigma(\pi(J))) \neq \Sigma(\sigma(\pi(J')))$, puisque $\pi(J), \pi(J') \subseteq \{b, b+1, \dots, b+10D\}$ sont des sous-ensembles distincts (rappelant que π est admissible et $\{1, \dots, b-1\} \subseteq \mathrm{Fix}(\pi)$).

Ceci implique en particulier que $\Sigma(\sigma \circ \pi \circ \pi_{b,y}, [s,t]) \neq 0$ pour tout $y \in \{b+1, \dots, b+5D\}$ et tous $s, t \in \{b, \dots, b+5D\}$ avec $s < t$. En effet, nous avons $\Sigma(\sigma \circ \pi \circ \pi_{b,y}, [s,t]) = \Sigma(\sigma(\pi(\pi_{b,y}(\{s, \dots, t\})))) \neq \Sigma(\sigma(\pi(\emptyset))) = 0$ puisque $\pi_{b,y}(\{s, \dots, t\}) \subseteq \{b, \dots, b+5D\}$ est distinct de $\emptyset$. Par conséquent, pour tout $y \in \{b+1, \dots, b+5D\}$ et tout intervalle $[s,t]$ avec $\Sigma(\sigma \circ \pi \circ \pi_{b,y}, [s,t]) = 0$ nous devons avoir $s < b$ ou $t > b+5D$.

Rappelons qu'un élément $y \in \{b+1, \dots, b+5D\}$ est bloqué pour σ, b et π si nous avons $\Sigma(\sigma \circ \pi \circ \pi_{b,y}, [s,t]) = 0$ pour un certain intervalle $[s,t]$ avec $s \in \{b+1, \dots, y\}$ (et donc $t > b+5D$) ou $t \in \{b, \dots, y-1\}$ (et donc $s < b$). Puisqu'au total au moins $2D$ éléments $y \in \{b+1, \dots, b+5D\}$ sont bloqués, l'une de ces deux options doit se produire pour au moins D éléments différents $y \in \{b+1, \dots, b+5D\}$.

Soit donc $\mathcal{E}_1$ l'événement qu'il existe $b \in \{2, \dots, |S| - 30D\}$ et une permutation admissible $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$, tels que pour tous sous-ensembles distincts $J, J' \subseteq \{b, \dots, b+5D\}$ nous ayons $\Sigma(\sigma(\pi(J))) \neq \Sigma(\sigma(\pi(J')))$, et tels qu'il existe des $y_1, \dots, y_D \in \{b+1, \dots, b+5D\}$ distincts ainsi que $s_1, \dots, s_D \in \{b+1, \dots, b+5D\}$ et $t_1, \dots, t_D \in \{b+5D+1, \dots, |S|\}$ avec $s_i \leq y_i$ tels que $\Sigma(\sigma \circ \pi \circ \pi_{b,y_i}, [s_i, t_i]) = 0$ pour $i = 1, \dots, D$.

De même, soit $\mathcal{E}_2$ l'événement qu'il existe $b \in \{2, \dots, |S| - 30D\}$ et une permutation admissible $\pi : \{1, \dots, |S|\} \to \{1, \dots, |S|\}$, tels que pour tous sous-ensembles distincts $J, J' \subseteq \{b, \dots, b+5D\}$ nous ayons $\Sigma(\sigma(\pi(J))) \neq \Sigma(\sigma(\pi(J')))$, et tels qu'il existe des $y_1, \dots, y_D \in \{b+1, \dots, b+5D\}$ distincts ainsi que $s_1, \dots, s_D \in \{1, \dots, b-1\}$ et $t_1, \dots, t_D \in \{b, \dots, b+5D-1\}$ avec $t_i < y_i$ et $\Sigma(\sigma \circ \pi \circ \pi_{b,y_i}, [s_i, t_i]) = 0$ pour $i = 1, \dots, D$.

Alors nous avons $\mathbb{P}[\mathcal{B}_3 \setminus (\mathcal{B}_0 \cup \mathcal{B}_1)] \leq \mathbb{P}[\mathcal{E}_1] + \mathbb{P}[\mathcal{E}_2]$, et il suffit donc de prouver $\mathbb{P}[\mathcal{E}_1] \leq 1/100$ et $\mathbb{P}[\mathcal{E}_2] \leq 1/100$.

Nous commençons par borner la probabilité de l'événement $\mathcal{E}_1$. Pour $b, \pi, y_1 \ldots, y_D, s_1 \ldots, s_D, t_1 \ldots, t_D$ comme dans la définition de l'événement $\mathcal{E}_1$, nous affirmons que $t_1, \ldots, t_D$ doivent être distincts. En effet, supposons que $t_i = t_j$ pour deux indices distincts $i, j \in \{1, \ldots, D\}$, et supposons sans perte de généralité que $y_i < y_j$. Alors nous avons

$$\begin{aligned}
0 &= \Sigma(\sigma \circ \pi \circ \pi_{b,y_i}, [s_i, t_i]) \\
&= \Sigma(\sigma(\pi(\pi_{b,y_i}(\{s_i, \ldots, t_i\})))) \\
&= \Sigma(\sigma(\pi(\pi_{b,y_i}(\{s_i, \ldots, b + 5D\})))) + \Sigma(\sigma(\pi(\pi_{b,y_i}(\{b + 5D + 1, \ldots, t_i\})))) \\
&= \Sigma(\sigma(\pi(\pi_{b,y_i}(\{s_i, \ldots, b + 5D\})))) + \Sigma(\sigma(\pi(\{b + 5D, \ldots, t_i\}))),
\end{aligned}$$

ce qui signifie que $\Sigma(\sigma(\pi(\pi_{b,y_i}(\{s_i, \ldots, b + 5D\})))) = -\Sigma(\sigma(\pi(\{b + 5D, \ldots, t_i\})))$. De façon analogue nous avons $\Sigma(\sigma(\pi(\pi_{b,y_j}(\{s_j, \ldots, b+5D\})))) = -\Sigma(\sigma(\pi(\{b+5D, \ldots, t_j\})))$, et donc par notre hypothèse $t_i = t_j$ nous pouvons conclure

$$\Sigma(\sigma(\pi(\pi_{b,y_i}(\{s_i, \ldots, b + 5D\})))) = \Sigma(\sigma(\pi(\pi_{b,y_j}(\{s_j, \ldots, b + 5D\}))))$$

Mais cela contredit les conditions de la définition de l'événement $\mathcal{E}_1$, puisque $\pi_{b,y_i}(\{s_i, \ldots, b+5D\})$ et $\pi_{b,y_j}(\{s_j, \ldots, b + 5D\})$ sont deux sous-ensembles distincts de $\{b, \ldots, b + 5D\}$ (puisque $s_i \leq y_i < y_j \leq b + 5D$, nous avons $y_j \in \pi_{b,y_i}(\{s_i, \ldots, b + 5D\})$, mais puisque $s_j > b$, nous avons $y_j \notin \pi_{b,y_j}(\{s_j, \ldots, b + 5D\})$). Ainsi $t_1, \ldots, t_D$ doivent effectivement être distincts. En réétiquetant les indices nous pouvons donc supposer $t_1 < \cdots < t_D$.

Ainsi, chaque fois que l'événement $\mathcal{E}_1$ se produit, il existe $b \in \{2, \ldots, |S|-30D\}$ et $y_1, \ldots, y_D, s_1, \ldots, s_D \in \{b+1, \ldots, b+5D\}$ ainsi que $t_1, \ldots, t_D \in \{b+5D+1, \ldots, |S|\}$ avec $t_1 < \cdots < t_D$ et une permutation admissible $\pi : \{1, \ldots, |S|\} \to \{1, \ldots, |S|\}$, telle que $\Sigma(\sigma \circ \pi \circ \pi_{b,y_i}, [s_i, t_i]) = 0$ pour $i = 1, \ldots, D$. Pour tout $b \in \{2, \ldots, |S| - 30D\}$ donné et $y_1, \ldots, y_D, s_1, \ldots, s_D \in \{b+1, \ldots, b+5D\}$, la probabilité que cela se produise est au plus $1/|S|^2$ par le Lemme 18 (appliqué avec $b' = b+5D$, ainsi que $u_i = s_i$ et $\pi_i = \pi_{b,y_i}$ pour $i = 1, \ldots, D$). Ainsi, par une borne d'union, nous obtenons

$$\mathbb{P}[\mathcal{E}_1] \leq (|S| - 30D - 1) \cdot (5D)^{2D} \cdot \frac{1}{|S|^2} \leq \frac{(5D)^{2D}}{|S|} \leq \frac{(5D)^{2D}}{C_\alpha} \leq \frac{1}{100}.$$

Il reste à borner la probabilité de l'événement $\mathcal{E}_2$. Pour $b, \pi, y_1 \ldots, y_D, s_1 \ldots, s_D, t_1 \ldots, t_D$ comme dans la définition de l'événement $\mathcal{E}_2$, nous affirmons que $s_1, \ldots, s_D$ doivent être distincts. En effet, supposons que $s_i = s_j$ pour deux indices distincts $i, j \in \{1, \ldots, D\}$, et supposons sans perte de généralité que $y_i < y_j$. Alors nous avons

$$\begin{aligned}
0 &= \Sigma(\sigma \circ \pi \circ \pi_{b,y_i}, [s_i, t_i]) \\
&= \Sigma(\sigma(\pi(\pi_{b,y_i}(\{s_i, \ldots, t_i\})))) \\
&= \Sigma(\sigma(\pi(\pi_{b,y_i}(\{s_i, \ldots, b - 1\})))) + \Sigma(\sigma(\pi(\pi_{b,y_i}(\{b, \ldots, t_i\})))) \\
&= \Sigma(\sigma(\pi(\{s_i, \ldots, b - 1\}))) + \Sigma(\sigma(\pi(\pi_{b,y_i}(\{b, \ldots, t_i\})))),
\end{aligned}$$

donc nous obtenons que $\Sigma(\sigma(\pi(\pi_{b,y_i}(\{b, \ldots, t_i\})))) = -\Sigma(\sigma(\pi(\{s_i, \ldots, b - 1\})))$. De façon analogue nous avons aussi $\Sigma(\sigma(\pi(\pi_{b,y_j}(\{b, \ldots, t_j\})))) = -\Sigma(\sigma(\pi(\{s_j, \ldots, b-1\}))))$, et donc par notre hypothèse

$s_i = s_j$ nous pouvons conclure

$$\Sigma(\sigma(\pi(\pi_{b,y_i}(\{b,\dots,t_i\})))) = \Sigma(\sigma(\pi(\pi_{b,y_j}(\{b,\dots,t_j\}))))$$

Mais cela contredit les conditions de la définition de $\mathcal{E}_2$, puisque $\pi_{b,y_i}(\{b,\dots,t_i\})$ et $\pi_{b,y_j}(\{b,\dots,t_j\})$ sont deux sous-ensembles distincts de $\{b,\dots,b+5D\}$ (car nous avons $y_j = \pi_{b,y_j}(b) \in \pi_{b,y_j}(\{b,\dots,t_j\})$, mais $y_j \notin \pi_{b,y_i}(\{b,\dots,t_i\})$ puisque $t_i < y_i < y_j$). Ainsi $s_1,\dots,s_D$ doivent effectivement être distincts. En réétiquetant les indices nous pouvons donc supposer $s_1 < \cdots < s_D$.

Ainsi, lorsque l'événement $\mathcal{E}_2$ se produit, il existe $b \in \{2,\dots,|S|-30D\}$ et $y_1,\dots,y_D \in \{b+1,\dots,b+5D\}$ et $t_1,\dots,t_D \in \{b,\dots,b+5D-1\}$, ainsi que $s_1,\dots,s_D \in \{1,\dots,b-1\}$ avec $s_1 < \cdots < s_D$ et une permutation admissible $\pi : \{1,\dots,|S|\} \to \{1,\dots,|S|\}$, telle que $\Sigma(\sigma \circ \pi \circ \pi_{b,y_i}, [s_i,t_i]) = 0$ pour $i = 1,\dots,D$. Pour tout $b \in \{2,\dots,|S|-30D\}$ donné et $y_1,\dots,y_D \in \{b+1,\dots,b+5D\}$ et $t_1,\dots,t_D \in \{b,\dots,b+5D-1\}$, la probabilité que cela se produise est au plus $1/|S|^2$ par le Lemme 19 (appliqué avec $b' = b+5D$, ainsi que $u_i = t_i$ et $\pi_i = \pi_{b,y_i}$ pour $i = 1,\dots,D$). Ainsi, par une borne d'union, nous obtenons

$$\mathbb{P}[\mathcal{E}_2] \le (|S|-30D-1)\cdot(5D)^D \cdot (5D)^D \cdot \frac{1}{|S|^2} \le \frac{(5D)^{2D}}{|S|} \le \frac{(5D)^{2D}}{C_\alpha} \le \frac{1}{100}. \qquad \square$$

Références

[1] B. Alspach and G. Liversidge, On strongly sequenceable abelian groups, Art Discrete Appl. Math. (2020).

[2] B. Bedert, M. Bucić, N. Kravitz, R. Montgomery and A. Müyesser, On Graham's rearrangement conjecture over $\mathbb{F}_2^n$, arXiv preprint 2508.18254.

[3] B. Bedert and N. Kravitz, Graham's rearrangement conjecture beyond the rectification barrier, Isr. J. Math. (to appear), arXiv preprint 2409.07403.

[4] M. Bucić, B. Frederickson, A. Müyesser, A. Pokrovskiy, and L. Yepremyan, Towards Graham's rearrangement conjecture via rainbow paths, arXiv preprint 2503.01825 (2025).

[5] S. Costa and M. A. Pellegrini, Some new results about a conjecture by Brian Alspach, Arch. Math. 115 (2020), no. 5, 479-488.

[6] P. Erdős and R. L. Graham, Old and new problems and results in combinatorial number theory, Université de Genève, L'Enseignement Mathématique, Geneva, 1980.

[7] R. L. Graham, On sums of integers taken from a fixed sequence, Proceedings of the Washington State University Conference on Number Theory (Washington State Univ., Pullman, Wash., 1971), Washington State University, Department of Mathematics, Pi Mu Epsilon, Pullman, WA, 1971, pp. 22-40.

[8] S. Janson, T. Łuczak, and A. Rucinski, Random graphs, John Wiley & Sons, 2011.

[9] N. Kravitz, Rearranging small sets for distinct partial sums. Preprint arXiv :2407.01835v2 (2024).

[10] A. Müyesser and A. Pokrovskiy, A random Hall-Paige conjecture, Inventiones mathematicae 240 (2025), 779-867.

[11] H. Nguyen and V. Vu, Optimal inverse Littlewood-Offord theorems, Adv. Math. 226 (2011), 5298-5319.

[12] W. Sawin, comment on the post "Ordering subsets of the cyclic group to give distinct partial sums". MathOverflow (2015), https ://mathoverflow.net/q/202857.