THÈSE DE DOCTORAT

présentée par

Benjamin Girard
Centre de Mathématiques Laurent Schwartz

pour obtenir le grade de

DOCTEUR DE L'ÉCOLE POLYTECHNIQUE
Spécialité : Mathématiques

Sur certains aspects combinatoires de la théorie de la factorisation non unique

Thèse présentée le 19 septembre 2008 devant le jury composé de :

Emmanuel Breuillard	Université Paris XI	Examinateur
Jean-Marc Deshouillers	Université Bordeaux II	Président du jury
Alfred Geroldinger	Université de Graz	Rapporteur
Yahya Ould Hamidoune	Université Paris VI, CNRS	Examinateur
François Hennecart	Université de Saint-Étienne	Examinateur
Ulrich Krause	Université de Brême	Rapporteur (excusé)
Alain Plagne	École polytechnique	Directeur de thèse

Remerciements

Tout d'abord, je tiens à remercier mon directeur de thèse, Alain Plagne, pour son cocktail savamment dosé d'écoute, de rigueur, de confiance et d'humour. J'ai beaucoup appris à son contact, et suis heureux d'avoir eu la chance de travailler trois années en sa compagnie.

Je voudrais aussi exprimer toute ma gratitude à Emmanuel Breuillard, Jean-Marc Deshouillers, Alfred Geroldinger, Yahya Ould Hamidoune, François Hennecart et Ulrich Krause, qui m'ont fait l'honneur, mais aussi l'amitié, d'accepter de faire partie de mon jury de thèse. Aussi vrai que l'on puisse écrire dans l'espoir d'être lu, je les remercie pour leur lecture attentive, et leur retour positif sur mon travail.

Bien sûr, un grand merci à Terence Tao, Melvyn Nathanson et Régis de la Bretèche, pour m'avoir invité à présenter les résultats de ma thèse dans leurs séminaires respectifs à Los Angeles, New York et Paris. J'ai aussi bénéficié de l'atmosphère conviviale et très enrichissante de plusieurs colloques à Luminy, Saint-Étienne et Barcelone, dont j'aimerais remercier ici les organisateurs. Encore merci à Melvyn Nathanson, qui m'accueille l'année prochaine pour un postdoctorat au Graduate Center de la City University de New York.

Je voudrais aussi remercier chaleureusement tous les membres, chercheurs et enseignants du Centre de Mathématiques Laurent Schwartz, et tout particulièrement Claude Viterbo, qui m'a accueilli en doctorat à l'École polytechnique, Yves Laszlo pour ses conseils éclairés, ainsi que mes collègues thésards. Je tiens aussi à remercier Claudine et Michèle, Carole et Alain, mais aussi Florence, Philippe et Stéphane pour la façon qu'ils ont eu de rendre ces trois années productives et agréables. Un merci particulier à Michèle, pour sa gentillesse presque maternelle et ses conseils judicieux dans les moments clés.

Je suis aussi très reconnaissant aux membres de l'Équipe Combinatoire de l'Université Paris 6 où j'ai commencé ma formation doctorale, parmi lesquels Yahya Ould Hamidoune, Jean Fonlupt, Sylvain Sorin et Éric Balandraud. Plus généralement, je remercie aussi tous ceux, professeurs, chercheurs, mais pas seulement, qui m'ont communiqué leur goût pour les mathématiques. Mille mercis à Aurélien Galateau, pour m'avoir tant de fois porté sur ses épaules ces dix dernières années, et à Wolfgang Schmid pour avoir constellé les trois dernières de ses remarques enrichissantes.

Les pages qui suivent ne sont en fait qu'un appendice de ce petit paragraphe en italique. Alors, à ma famille bien sûr, et à toute cette mythique bande d'ami(e)s, en compagnie desquel(le)s, que ce soit à Tokyo, Umeå, Barcelone, Joshua Tree, Greenwich Village, sur la pointe du Vert-Galant ou partout ailleurs, j'aurai savouré chaque goutte de ces trente-six mois d'authentique étudiant. A Emilie, dont le sourire et l'aide providentielle se cachent derrière chacune des lettres de ce mémoire.

*"La connaissance poétique naît dans le grand silence de la connaissance scientifique... la connaissance scientifique est sommaire. Il faut ajouter qu'elle est **pauvre et famélique**."*

Aimé Césaire.

Table des matières

INTRODUCTION

Factorisation non unique et théorie additive des groupes

Cette thèse est consacrée à l'étude de plusieurs problèmes combinatoires liés à la théorie de la factorisation non unique. Ce thème de recherche, qui tire son origine de la théorie algébrique des nombres, a pour but de décrire, dans un anneau d'entiers algébriques général, la variété des décompositions en facteurs irréductibles d'un élément de celui-ci. En effet, comme nous allons le voir dans cette introduction, il s'avère que ce type de problèmes, dont la nature est arithmétique, peut se "réduire" à l'étude d'invariants combinatoires liés au groupe des classes d'idéaux, comme par exemple la constante de Davenport ou le nombre de Krause (en anglais, cross number).

Une des propriétés fondamentales des anneaux principaux, comme $\mathbb{Z}$ ou $\mathbb{Z}[i]$, est qu'ils sont factoriels, c'est-à-dire que les théorèmes classiques de l'arithmétique - unicité de la décomposition en facteurs premiers, existence du pgcd, du ppcm, lemmes de Gauss et d'Euclide - y sont valables, facilitant ainsi la réduction de certains problèmes diophantiens.

Or, l'arithmétique dans les anneaux d'entiers des corps de nombres, qui ne sont en général ni principaux, ni factoriels, empêche d'avoir recours, en l'état, à ces théorèmes. La particularité des anneaux de Dedekind est justement de venir pallier cet inconvénient, par l'existence d'une décomposition unique, non plus d'un nombre en facteurs premiers, mais d'un idéal en produit d'idéaux premiers. La proposition suivante permet alors d'établir un pont entre la théorie de la factorisation non unique et la théorie additive des groupes.

Soit $\mathcal{O}_{\mathbf{K}}$ un anneau d'entiers algébriques, de groupe des classes d'idéaux G, noté additivement. Alors, un élément $x \in \mathcal{O}_{\mathbf{K}}$ est irréductible si et seulement si l'idéal $x\mathcal{O}_{\mathbf{K}}$ qu'il engendre se décompose en un produit $\mathfrak{p}_1 \cdots \mathfrak{p}_\ell$ d'idéaux premiers, vérifiant la propriété suivante dans le groupe des classes d'idéaux :

$$\sum_{i=1}^{\ell} [\mathfrak{p}_i] = 0, \ \textit{et} \ \sum_{i \in I} [\mathfrak{p}_i] \neq 0 \ \textit{pour tout} \ \emptyset \subsetneq I \subsetneq \{1, \ldots, \ell\}.$$

Par conséquent, l'unicité de la décomposition en produit d'idéaux premiers nous donne une bijection entre les irréductibles de $\mathcal{O}_{\mathbf{K}}$ et certaines suites remarquables du groupe G, dont la somme des éléments est nulle, mais telles qu'aucune sous-somme stricte ne le soit. C'est l'étude, dans le cadre des groupes abéliens finis, de problèmes liés à ces suites particulières qui fait l'objet du présent mémoire.

Dans cette partie, toute suite finie $S = (g_1, \ldots, g_\ell)$ de ℓ éléments de G sera appelée une *suite* de G de *longueur* $|S| = \ell$. Etant donnée une suite $S = (g_1, \ldots, g_\ell)$ de G, on dit que $s \in G$ est une *sous-somme* de S lorsque s appartient à l'ensemble suivant, appelé *ensemble des sous-sommes* de S :

$$\Sigma(S) = \left\{ \sum_{i \in I} g_i \mid \emptyset \subsetneq I \subseteq \{1, \ldots, \ell\} \right\}.$$

Si 0 n'est pas une sous-somme de S, on dit que S est une *suite sans sous-somme nulle.* Si $\sum_{i=1}^{\ell} g_i = 0$, alors S est appelée *suite de somme nulle*, et si de plus, on a $\sum_{i \in I} g_i \neq 0$ pour tout sous-ensemble propre $\emptyset \subsetneq I \subsetneq \{1, \dots, \ell\}$, S est alors appelée *suite minimale.*

Soit G un groupe abélien fini, noté additivement. Si G est cyclique d'ordre n, nous le noterons C_n. Dans le cas général, d'après le théorème de structure des groupes abéliens de type fini, G se décompose en somme directe de groupes cycliques $C_{n_1} \oplus \cdots \oplus C_{n_r}$, où $1 < n_1 \mid \dots \mid n_r \in \mathbb{N}$.

On parle de problème de somme nulle lorsque l'on s'intéresse aux différentes conditions qui garantissent qu'une suite S d'éléments d'un groupe abélien fini G contienne une sous-suite non vide $S' \subseteq S$ de somme nulle, et vérifiant éventuellement quelques propriétés additionnelles.

En général, cette étude se décompose en deux étapes. La première consiste à introduire une caractéristique numérique qui permette de mesurer la "taille" d'une suite d'éléments du groupe abélien fini considéré. La seconde étape consiste alors à essayer de trouver une valeur seuil pour cette caractéristique, au-delà de laquelle l'existence d'une sous-suite remarquable est garantie.

Les premières recherches dans ce domaine datent du début des années 1960, et le théorème suivant, démontré par Erdős, Ginzburg et Ziv en 1961 (voir [5]), est très souvent considéré comme un point de départ dans l'étude de ces questions : *Dans le groupe C_n, toute suite S de longueur $2n - 1$ contient une sous-suite S' de longueur n et de somme nulle.*

Constante de Davenport d'un groupe abélien fini

Supposons, dans un premier temps, que l'on choisisse de mesurer la "taille" d'une suite $S = (g_1, \dots, g_\ell)$ par sa longueur $|S| = \ell$. Dans ce cas, nous obtenons la question naturelle suivante.

Soit G un groupe abélien fini. Quel est le plus petit entier $\ell \in \mathbb{N}^*$ tel que toute suite S de G de longueur $|S| \geq \ell$ contienne une sous-suite non vide de somme nulle?

Ce plus petit entier, que l'on note $\mathsf{D}(G)$, est appelé constante de Davenport du groupe abélien fini G. Même si cette définition est purement combinatoire, on peut remarquer que ce nombre a le sens arithmétique suivant. Imaginons que G soit le groupe des classes d'idéaux d'un certain anneau d'entiers $\mathcal{O}_{\mathbf{K}}$ d'un corps de nombres $\mathbf{K}$. D'après un théorème de Dirichlet, G est un groupe abélien fini. De plus, il est facile de voir que $\mathsf{D}(G)$ est égal à la longueur maximale d'une suite minimale d'éléments de G. Par conséquent, $\mathsf{D}(G)$ est égal au nombre maximal d'idéaux premiers dans la décomposition d'un élément irréductible de $\mathcal{O}_{\mathbf{K}}$.

Pour cette raison, la constante de Davenport joue un rôle important dans l'étude de l'arithmétique des anneaux d'entiers des corps de nombres. A titre d'exemple, cette quantité intervient dans la généralisation suivante du théorème des nombres premiers (voir [19], Theorem 9.15), portant sur la répartition des éléments irréductibles dans un anneau d'entiers algébriques général.

Soit $\mathcal{O}_{\mathbf{K}}$ un anneau d'entiers algébriques, de groupe des classes d'idéaux G. Soit $F(x)$ le nombre d'irréductibles de $\mathcal{O}_{\mathbf{K}}$ non associés deux à deux, dont la norme n'excède pas x en valeur absolue. Alors, il existe un réel $C > 0$ tel que l'on ait :

$$F(x) \sim C \frac{x}{\log x} (\log \log x)^{\mathsf{D}(G)-1}.$$

D'après un théorème de Claborn (voir [3]), tout groupe abélien fini est réalisable comme groupe des classes d'idéaux d'un certain anneau d'entiers algébriques. Le problème de la valeur exacte de la constante de Davenport se pose donc dans toute sa généralité. Or, encore aujourd'hui, ce problème reste très largement ouvert, et cette valeur exacte n'est connue que pour des classes très particulières de groupes abéliens finis.

Le théorème qui suit donne les meilleures bornes générales connues pour la constante de Davenport d'un groupe abélien fini. Le minorant est obtenu par la construction explicite d'une suite sans sous-somme nulle canonique (voir par exemple [11], Proposition 5.1.8). Le majorant, quant à lui, a d'abord été prouvé en 1969 par van Emde Boas (voir [4]), grâce à une méthode purement combinatoire. En 1993, Alford, Granville et Pomerance (voir [1]) ont trouvé une autre preuve élégante de cette majoration, qui utilise l'algèbre de groupe et la théorie des caractères, pour démontrer qu'il existe une infinité de nombres de Carmichael.

Soit $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, où $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, un groupe abélien fini. Alors, on a les deux inégalités suivantes :

$$\mathsf{D}^*(G) = \sum_{i=1}^{r} (n_i - 1) + 1 \leq \mathsf{D}(G) \leq n_r \left(1 + \log \frac{|G|}{n_r}\right).$$

Il est à noter que la valeur de la constante de Davenport des groupes cycliques découle directement de ce théorème. Ainsi, on obtient l'égalité $\mathsf{D}(C_n) = n$ pour tout $n \in \mathbb{N}^*$. De plus, deux résultats démontrés en 1969 par Olson (voir [20] et [21]), donnent la valeur exacte de la constante de Davenport dans le cas des p-groupes abéliens finis, et des groupes abéliens finis de rang inférieur ou égal à deux. Pour tous ces groupes, la constante de Davenport se trouve être égale au minorant dans l'encadrement ci-dessus, mais ceci n'est pas le cas en général. Par exemple, pour le groupe $G \simeq C_3^3 \oplus C_6$, on peut démontrer l'égalité $\mathsf{D}(G) = 13$, alors que $\mathsf{D}^*(G) = 12$. Néanmoins, il est conjecturé que le minorant $\mathsf{D}^*(G)$ reste la bonne valeur de la constante de Davenport pour tous les groupes abéliens finis de rang trois.

Une seconde conjecture classique en théorie additive des groupes affirme que le minorant $\mathsf{D}^*(G)$ est aussi la vraie valeur de la constante de Davenport pour les groupes de la forme C_n^r. Cette conjecture est clairement vraie lorsque n est la puissance d'un nombre premier, puisque dans ce cas, le groupe C_n^r est un p-groupe abélien fini et le théorème d'Olson s'applique. En dehors de ce cas particulier, aucun résultat exact n'a encore été prouvé pour les groupes abéliens finis de rang supérieur ou égal à trois. Par exemple, on ne sait pas si l'égalité $\mathsf{D}(C_n^3) = 3n - 2$ est vraie pour tout $n \in \mathbb{N}^*$. Le meilleur résultat connu concernant cette conjecture est le résultat qualitatif suivant, démontré en 1995 par Alon et Dubiner (voir [2]).

Pour tout $r \in \mathbb{N}^*$, il existe un réel $c_r > 0$ tel que, pour tout groupe abélien fini G de rang inférieur ou égal à r et d'exposant n, on ait :

$$\mathsf{D}(G) \leq c_r n.$$

Nombre de Krause d'un groupe abélien fini

Le nombre de Krause d'un groupe abélien fini G apparaît lorsque l'on choisit, pour mesurer la "taille" d'une suite d'éléments de G, une caractéristique qui prenne en compte les ordres dans G des éléments composant la suite. Plus précisément, le *nombre de Krause* d'une suite $S = (g_1, \dots, g_\ell)$ de G, noté $\mathsf{k}(S)$, est défini par :

$$\mathsf{k}(S) = \sum_{i=1}^{\ell} \frac{1}{\mathrm{ord}(g_i)}.$$

Comme pour la constante de Davenport, le problème naturel porte alors sur la valeur seuil du nombre de Krause d'une suite S, au-delà de laquelle l'existence d'une sous-suite non vide $S' \subseteq S$ de somme nulle est garantie.

Soit G un groupe abélien fini. Quelle est la valeur maximale du nombre de Krause d'une suite sans sous-somme nulle de G?

Cette valeur maximale, notée $\mathsf{k}(G)$, est appelée nombre de Krause du groupe abélien fini G (en anglais, cross number). Ce nombre, introduit par Krause en 1984 (voir [17] et [18]), joue lui aussi un rôle clé en théorie de la factorisation non unique. D'une part, il intervient dans l'étude des ensembles semi-factoriels des groupes abéliens finis (voir [22], [23], [24]), et d'autre part, il permet de progresser dans le sens d'une caractérisation arithmétique du groupe des classes d'idéaux (voir [26], [27], [28]).

Le problème de la valeur exacte du nombre de Krause d'un groupe abélien fini est lui aussi encore très largement ouvert, même dans le cas particulier des groupes cycliques (voir [12]). Le résultat suivant donne un minorant, obtenu par la construction explicite d'une suite sans sous-somme nulle canonique (voir [11], Proposition 5.1.8), ainsi qu'un majorant, démontré en 1996 par Geroldinger et Schneider (voir [13]), par une méthode utilisant l'algèbre de groupe et la théorie des caractères.

Soit G un groupe abélien fini, et $G \simeq C_{\nu_1} \oplus \cdots \oplus C_{\nu_s}$ sa plus longue décomposition en somme directe de groupes cycliques. Alors, on a les deux inégalités suivantes :

$$\mathsf{k}^*(G) = \sum_{i=1}^{s} \frac{\nu_i - 1}{\nu_i} \leq \mathsf{k}(G) \leq \log |G|.$$

Un théorème de Geroldinger (voir [10]), prouvé en 1994, donne la valeur exacte du nombre de Krause dans le cas des p-groupes abéliens finis, et dans tous les cas où la valeur de ce nombre est connue, celle-ci est égale au minorant dans l'encadrement ci-dessus. Contrairement à son équivalent pour la constante de Davenport, la conjecture suivante reste donc toujours à confirmer ou à infirmer.

Soit G un groupe abélien fini, et $G \simeq C_{\nu_1} \oplus \cdots \oplus C_{\nu_s}$ sa plus longue décomposition en somme directe de groupes cycliques. Alors, on a :

$$\mathsf{k}(G) = \sum_{i=1}^{s} \frac{\nu_i - 1}{\nu_i}.$$

Par ailleurs, et même si le majorant $\log |G|$ est simple et facile à calculer, il apparaît que celui-ci ne rend pas compte de ce qui est déjà connu du comportement du nombre de Krause. En effet, considérons le p-groupe élémentaire C_p^r, où $r \geq 1$. On sait, d'après le théorème de Geroldinger, que $\mathsf{k}\left(C_p^r\right) = r(p-1)/p \leq r$, alors que $\log\left(|C_p^r|/p\right) = (r-1)\log p$ diverge quand p tend vers l'infini. De ce point de vue, mais dans le cas particulier des groupes cycliques seulement, une majoration plus précise a été découverte en 1991 par Krause et Zahlten (voir [18]), qui ne dépend que du nombre $\omega(n)$ de diviseurs premiers distincts de l'ordre du groupe considéré. Ainsi, pour tout $n \in \mathbb{N}^*$, l'égalité suivante est vérifiée :

$$\mathsf{k}(C_n) \leq 2\omega(n).$$

C'est cette majoration plus précise que nous avons pu étendre au cas général de tous les groupes abéliens finis. Ainsi, nous avons pu établir, pour le nombre de Krause, l'analogue suivant du théorème d'Alon et Dubiner sur la constante de Davenport.

Pour tout $r \in \mathbb{N}^*$, il existe un réel $d_r > 0$ tel que, pour tout groupe abélien fini G de rang inférieur ou égal à r et d'exposant n, on ait :

$$\mathsf{k}(G) \leq d_r \omega(n).$$

L'intérêt principal de ce résultat est qu'il permet, pour un groupe abélien fini G quelconque, de remplacer la fonction régulière et croissante $\log |G|$ par la fonction arithmétique et irrégulière $\omega(n)$, qui peut prendre des valeurs arbitrairement petites, même pour des valeurs arbitrairement grandes de $|G|$.

De plus, nous obtenons pour les groupes abéliens finis de petit rang des bornes effectives significativement plus précises que le $\log |G|$ du théorème de Geroldinger et Schneider. Ces bornes, valables pour tous $m \mid n \in \mathbb{N}^*$, sont les suivantes :

$$\mathsf{k}(C_n) \leq 1.5237\omega(n),$$

$$\mathsf{k}(C_m \oplus C_n) \leq 3.7421\omega(n).$$

Enfin, la méthode utilisée pour démontrer ces résultats permet d'établir, dans deux directions particulières, que la valeur conjecturale du nombre de Krause d'un groupe abélien fini est asymptotiquement la bonne.

Problèmes inverses en théorie additive des groupes

Soit G un groupe abélien fini. Que peut-on dire sur la structure d'une suite sans sous-somme nulle de G, et de longueur suffisamment grande? La réponse à cette question serait précieuse en théorie de la factorisation non unique. Néanmoins, la complexité du problème s'accroît avec le rang du groupe abélien fini étudié, et il semble difficile d'espérer, dans le cas général, qu'une telle caractérisation explicite soit possible.

A l'heure actuelle, seul le cas des groupes cycliques est véritablement compris. Le cas des groupes abéliens finis de rang deux repose, quant à lui, sur une conjecture classique concernant la propriété suivante, nommée Propriété B (voir [9], [25] et [8] par exemple). On dit que l'entier $n \geq 2$ a la Propriété B si, dans le groupe $C_n \oplus C_n$, toute suite minimale de longueur $2n-1$ contient un élément répété $n-1$ fois, et il est conjecturé que tous les entiers vérifient cette propriété.

Par ailleurs, un second axe de recherche consiste à établir, au lieu d'une caractérisation exacte des suites sans sous-somme nulle suffisamment longues, un faisceau de propriétés devant être vérifiées par celles-ci, ce quel que soit le groupe abélien fini considéré. Ce travail consiste par exemple à tenter de quantifier le type d'intuitions suivant : les idéaux premiers dans une longue décomposition d'un irréductible doivent être d'ordre élevé dans le groupe des classes d'idéaux.

Dans cette thèse, nous avons aussi étudié ces questions, et obtenu plusieurs résultats sur la distribution des ordres des éléments dans une suite sans sous-somme nulle de longueur suffisamment grande. Nous proposons notamment la conjecture générale suivante.

Soit $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, où $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, un groupe abélien fini, et S une suite sans sous-somme nulle de G. Alors,

$$|S| \geq \sum_{i=1}^{r} (n_i - 1) \text{ entraîne } \mathsf{k}(S) \leq \sum_{i=1}^{r} \left(\frac{n_i - 1}{n_i} \right).$$

Cette conjecture peut être vue comme une généralisation de la conjecture classique sur la constante de Davenport des groupes de la forme C_n^r. Nous avons pu démontrer qu'elle est vraie pour les p-groupes abéliens finis, les groupes cycliques et les groupes abéliens finis de rang deux. Par ailleurs, la méthode utilisée permet de démontrer les deux résultats suivants, qui viennent améliorer ceux déjà prouvés par Gao et Geroldinger (voir [6] et [7] par exemple).

Soit G un groupe abélien fini de rang deux et d'exposant n. Alors, toute suite sans sous-somme nulle de longueur maximale contient au moins $0.8n$ éléments d'ordre n.

Soit G un p-groupe abélien fini d'exposant n. Alors, toute suite sans sous-somme nulle de longueur maximale contient au moins $n-1$ éléments d'ordre n.

Enfin, dans le cas des p-groupes abéliens finis, la méthode utilisée pour démontrer ces résultats permet l'étude du nombre d'éléments d'ordre maximal dans une suite sans sous-somme nulle de longueur quelconque. Dans ce but, nous avons introduit un nouvel invariant, noté $\Gamma_\delta(G)$, pour lequel des bornes sont prouvées. L'encadrement obtenu s'avère alors être optimal dans certains cas particuliers.

Plan de la thèse

Ce travail est composé de trois parties indépendantes, organisées sous forme d'articles.

La première partie, dont le texte est à paraître dans l'*Israel Journal of Mathematics* (voir [14]), traite du nombre de Krause, dans le cas général des groupes abéliens finis. Dans cet article, nous établissons un analogue, pour le nombre de Krause, du théorème d'Alon et Dubiner pour la constante de Davenport. Pour cela, deux nouveaux invariants sont introduits, puis utilisés via une méthode d'optimisation en nombres entiers, permettant ainsi d'obtenir un nouveau majorant pour le nombre de Krause d'un groupe abélien fini quelconque, qui s'avère ne dépendre que du rang du groupe considéré et du nombre de diviseurs premiers distincts de son exposant. D'une part, ce résultat vient étendre les précédents résultats de Krause et Zahlten, obtenus en 1991 dans le cas particulier des groupes cycliques. D'autre part, il donne pour les groupes de petit rang des bornes effectives significativement plus précises que celles données par le majorant de Geroldinger et Schneider. Enfin, la méthode utilisée dans cet article permet de démontrer, dans deux directions différentes, que la valeur conjecturale du nombre de Krause d'un groupe abélien fini est asymptotiquement la bonne.

La deuxième partie, dont le texte est à paraître dans *Acta Arithmetica* (voir [15]), étudie plusieurs problèmes inverses en théorie additive des groupes, principalement dans le cas des groupes abéliens finis de rang deux. En utilisant les invariants définis et étudiés dans le premier chapitre, nous arrivons à démontrer qu'une généralisation de la conjecture classique sur la constante de Davenport des groupes de la forme C_n^r est vraie pour tous les groupes cycliques, les p-groupes abéliens finis et les groupes abéliens finis de rang deux. Par ailleurs, la méthode utilisée permet aussi, via la résolution d'une question d'optimisation en nombres entiers, d'améliorer significativement un résultat de Gao et Geroldinger, portant sur le nombre d'éléments d'ordre maximal dans une suite sans sous-somme nulle de longueur maximale.

La troisième partie, dont le texte est soumis à publication (voir [16]), étudie aussi plusieurs problèmes inverses en théorie additive des groupes, dans le cas particulier des p-groupes abéliens finis. Après avoir introduit un nouvel invariant, correspondant au nombre d'éléments d'ordre maximal contenus dans une suite sans sous-somme nulle de longueur quelconque, nous pouvons obtenir des bornes sur cet invariant, qui s'avèrent être optimales dans certains cas de figure. De plus, la méthode utilisée permet aussi d'améliorer significativement un résultat de Gao et Geroldinger sur le nombre d'éléments d'ordre maximal dans une suite sans sous-somme nulle de longueur maximale dans un p-groupe abélien fini.

Références

[1] W. R. Alford, A. Granville et C. Pomerance *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), 703-722.

[2] N. Alon et M. Dubiner *A lattice point problem and additive number theory*, Combinatorica **15** (1995), 301-309.

[3] L. Claborn *Every abelian group is a class group*, Pacific J. of Math. **18** (1966), 219-222.

[4] P. van Emde Boas *A combinatorial problem on finite abelian groups II*, Reports ZW-1969-007, Math. Centre, Amsterdam (1969).

[5] P. Erdős, A. Ginzburg et A. Ziv *Theorem in the additive number theory*, Bull. Research Council Israel **10** (1961), 41-43.

[6] W. Gao et A. Geroldinger *On long minimal zero sequences in finite abelian groups*, Period. Math. Hung. **38**(3) (1999), 179-211.

[7] W. Gao et A. Geroldinger *On the order of elements in long minimal zero-sum sequences*, Period. Math. Hung. **44**(1) (2002), 63-73.

[8] W. Gao, A. Geroldinger et D. Grynkiewicz *Inverse zero-sum problems III*, soumis.

[9] W. Gao, A. Geroldinger et W. Schmid *Inverse zero-sum problems*, Acta Arith. **128** (2007), 245-279.

[10] A. Geroldinger *The cross number of finite abelian groups*, J. Number Theory **48** (1994), 219-223.

[11] A. Geroldinger et F. Halter-Koch *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics **278**, Chapman & Hall/CRC (2006).

[12] A. Geroldinger et R. Schneider *The cross number of finite abelian groups II*, European J. Combin. **15** (1994), 399-405.

[13] A. Geroldinger et R. Schneider *The cross number of finite abelian groups III*, Discrete Math. **150** (1996), 123-130.

[14] B. Girard *A new upper bound for the cross number of finite Abelian groups*, Israel J. Math., à paraître.

[15] B. Girard *Inverse zero-sum problems and algebraic invariants*, Acta Arith., à paraître.

[16] B. Girard *Inverse zero-sum problems in finite Abelian p-groups*, soumis.

[17] U. Krause *A characterization of algebraic number fields with cyclic class group of prime power order*, Math. Z. **186** (1984), 143-148.

[18] U. Krause et C. Zahlten *Arithmetic in Krull monoids and the cross number of divisor class groups*, Mitt. Math. Ges. Hamburg **12** (1991), 681-696.

[19] W. Narkiewicz *Elementary and analytic theory of algebraic numbers*, 3rd edition, Springer (2004).

[20] J. E. Olson *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8-10.

[21] J. E. Olson *A combinatorial problem on finite abelian groups II*, J. Number Theory **1** (1969), 195-199.

[22] A. Plagne et W. A. Schmid *On large half-factorial sets in elementary p-groups : maximal cardinality and structural characterization*, Israel J. Math. **145** (2005), 285-310.

[23] A. Plagne et W. A. Schmid *On the maximal cardinality of half-factorial sets in cyclic groups*, Math. Ann. **333** (2005), 759-785.

[24] M. Radziejewski et W. A. Schmid *Weakly half-factorial sets in finite abelian groups*, Forum Math. **19** (2007), 727-747.

[25] W. Schmid *Inverse zero-sum problems II*, soumis.

[26] W. A. Schmid *Differences in sets of lengths of Krull monoids with finite class group*, J. Théor. Nombres Bordeaux, **17**(1) (2005), 323-345.

[27] W. Schmid *Arithmetical characterization of class groups of the form $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ via the system of sets of lengths*, soumis.

[28] W. Schmid *Characterization of class groups of Krull monoids via their systems of sets of lengths : a status report*, soumis.

A NEW UPPER BOUND FOR THE CROSS NUMBER OF FINITE ABELIAN GROUPS

by

Benjamin Girard

Abstract. — In this paper, building among others on earlier works by U. Krause and C. Zahlten (dealing with the case of cyclic groups), we obtain a new upper bound for the little cross number valid in the general case of arbitrary finite Abelian groups. Given a finite Abelian group, this upper bound appears to depend only on the rank and on the number of distinct prime divisors of the exponent. The main theorem of this paper allows us, among other consequences, to prove that a classical conjecture concerning the cross and little cross numbers of finite Abelian groups holds asymptotically in at least two different directions.

1. Introduction

Let G be a finite Abelian group, written additively. By $\mathrm{r}(G)$ and $\exp(G)$ we denote respectively the rank and the exponent of G. If G is cyclic of order n, it will be denoted by C_n. In the general case, we can decompose G (see for instance [27]) as a direct product of cyclic groups $C_{n_1} \oplus \cdots \oplus C_{n_r}$ where $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, so that every element g of G can be written $g = [a_1, \ldots, a_r]$ (this notation will be used freely along this paper), with $a_i \in C_{n_i}$ for all $i \in [\![1, r]\!] = \{1, \ldots, r\}$.

In this paper, any finite sequence $S = (g_1, \ldots, g_l)$ of l elements from G will be called a *sequence* of G with *length* l. Given a sequence $S = (g_1, \ldots, g_l)$ of G, we say that $s \in G$ is a *subsum* of S when it lies in the following set, called the *set of subsums* of S:

$$\Sigma(S) = \left\{ \sum_{i \in I} g_i \mid \emptyset \subsetneq I \subseteq \{1, \ldots, l\} \right\}.$$

If 0 is not a subsum of S, we say that S is a *zero-sumfree sequence*. If $\sum_{i=1}^{l} g_i = 0$, then S is said to be a *zero-sum sequence*. If moreover one has $\sum_{i \in I} g_i \neq 0$ for all proper subsets $\emptyset \subsetneq I \subsetneq \{1, \ldots, l\}$, S is called a *minimal zero-sum sequence*.

In a finite Abelian group G, the order of an element g will be written $\mathrm{ord}(g)$ and for every divisor d of the exponent of G, we denote by G_d the subgroup of G consisting of all the elements of order dividing d:

$$G_d = \{x \in G \mid dx = 0\}.$$

Mathematics Subject Classification (2000): 11R27, 11B75, 11P99, 20D60, 20K01, 05E99, 13F05.

In a sequence S of elements of G, we denote by S_d the subsequence of S consisting of all the elements of order d contained in S.

Let $\mathcal{P} = \{p_1 = 2 < p_2 = 3 < \dots\}$ be the set of prime numbers. Given a positive integer $n \in \mathbb{N}^* = \mathbb{N} \backslash \{0\}$, we denote by $\mathcal{D}_n$ the set of its positive divisors. If $n > 1$, we denote by $P^-(n)$ the smallest prime element of $\mathcal{D}_n$, and we put by convention $P^-(1) = 1$. By $\tau(n)$ and $\omega(n)$ we denote respectively the number of positive divisors of n and the number of distinct prime divisors of n.

By $\mathsf{D}(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G with length $|S| \geq t$ contains a zero-sum subsequence. The constant $\mathsf{D}(G)$ is called the *Davenport constant* of the group G.

By $\eta(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G with length $|S| \geq t$ contains a zero-sum subsequence $S' \subseteq S$ with length $|S'| \leq \exp(G)$. Such a subsequence is called a *short zero-sum subsequence*.

The constants $\mathsf{D}(.)$ and $\eta(.)$ have been extensively studied during last decades and even if numerous results were proved (see Chapter 5 of the book [13] or [9] for a survey and many references on the subject), their exact values are known for very special types of groups only. In the sequel, we shall need some results on some of the groups for which we know the exact values, so we gather what is known concerning them in the following theorem.

Theorem 1.1. — *The two following statements hold:*

(*i*) *Let $p \in \mathcal{P}$, $r \in \mathbb{N}^*$ and $\alpha_1 \leq \dots \leq \alpha_r$, where $\alpha_i \in \mathbb{N}^*$ for all $i \in [\![1, r]\!]$. Then, for the p-group $G \simeq C_{p^{\alpha_1}} \oplus \dots \oplus C_{p^{\alpha_r}}$, we have:*

$$\mathsf{D}(G) = \sum_{i=1}^{r} (p^{\alpha_i} - 1) + 1.$$

(*ii*) *For every $m, n \in \mathbb{N}^*$ with $m|n$, we have:*

$$\mathsf{D}(C_m \oplus C_n) = m + n - 1 \quad \text{and} \quad \eta(C_m \oplus C_n) = 2m + n - 2.$$

In particular, we have $\mathsf{D}(C_n) = \eta(C_n) = n$.

Proof. — (*i*) This result was proved by J. Olson in [21] using the notion of group algebra. The special case of elementary p-groups, which says that $\mathsf{D}(C_p^r) = r(p-1)+1$, can be easily deduced from the Chevalley-Warning theorem (see [7] for example).

(*ii*) The value of $\mathsf{D}(.)$ for groups with rank 2 is also due to J. Olson (see [22]), and uses the special case $\eta(C_p^2) = 3p - 2$ with p prime. The complete statement for $\eta(.)$ has been proved by A. Geroldinger and F. Halter-Koch (see [13], Theorem 5.8.3).

□

The value of $\eta(.)$ for Abelian p-groups with rank $r \geq 3$ is not known in general, even in the special case of elementary p-groups. It is only known that for every $r \in \mathbb{N}^*$, we have $\eta(C_2^r) = 2^r$, and it is conjectured that for every odd $p \in \mathcal{P}$, we have $\eta(C_p^3) = 8p - 7$ and $\eta(C_p^4) = 19p - 18$. The interested reader is for instance referred to [5] and [10], for a complete account on this topic.

Yet, N. Alon and M. Dubiner showed in [1] an important theorem related to the constant $\eta(.)$ of elementary p-groups. We will use the following corollary of this result.

Theorem 1.2. — *For every $r \in \mathbb{N}^*$, there exists a constant $c_r > 0$ such that for every $p \in \mathcal{P}$, the following holds:*

$$\eta\left(C_p^r\right) \leq c_r(p-1)+1.$$

In this paper, we will study the *cross number* of finite Abelian groups. For this purpose, we recall some definitions and also the results known so far, to the best of our knowledge, concerning this constant. Let G be a finite Abelian group. If $G \simeq C_{\nu_1} \oplus \cdots \oplus C_{\nu_s}$, with $\nu_i > 1$ for all $i \in [\![1, s]\!]$, is the longest possible decomposition of G into a direct product of cyclic groups, then we set:

$$\mathsf{k}^*(G) = \sum_{i=1}^{s} \frac{\nu_i - 1}{\nu_i},$$

and

$$\mathsf{K}^*(G) = \sum_{i=1}^{s} \frac{\nu_i - 1}{\nu_i} + \frac{1}{\exp(G)} = \mathsf{k}^*(G) + \frac{1}{\exp(G)}.$$

The *cross number* of a sequence $S = (g_1, \ldots, g_l)$, denoted by $\mathsf{k}(S)$, is defined by:

$$\mathsf{k}(S) = \sum_{i=1}^{l} \frac{1}{\operatorname{ord}(g_i)}.$$

Then, we define the *little cross number* $\mathsf{k}(G)$ of G:

$$\mathsf{k}(G) = \max\{\mathsf{k}(S) | S \text{ zero-sumfree sequence of } G\},$$

as well as the *cross number* of G, denoted by $\mathsf{K}(G)$:

$$\mathsf{K}(G) = \max\{\mathsf{k}(S) | S \text{ minimal zero-sum sequence of } G\}.$$

The cross number was introduced by U. Krause in [19] in order to clarify the relationship between the arithmetic of a Krull monoid and the properties of its ideal class group. For this reason, the cross number plays a key rôle in the theory of non-unique factorization (see [19], [8], [15], [28], [23], [24] and [25] for some applications of the cross number, the surveys [3], [14] and the book [13] which presents exhaustively the different aspects of the theory).

For the sake of completeness, we mention that the cross number has been studied in other directions also (see for example [4], [18] and [2]), and that this concept arose in a natural way in combinatorial number theory (see for instance [11] and [6]).

Given a finite Abelian group G, a natural construction (see [19] or [13], Proposition 5.1.8) gives the following lower bounds:

$$\mathsf{k}^*(G) \leq \mathsf{k}(G) \quad \text{and} \quad \mathsf{K}^*(G) \leq \mathsf{K}(G),$$

yet, except for Abelian p-groups (see [12]) and other special cases (see [16]), the exact values of the cross and little cross numbers are also unknown in general, even for cyclic groups. In addition, still no counterexample is known for which equality does not hold in the previous inequalities, which would allow us to disprove the following conjecture.

Conjecture 1.3. — *For every finite Abelian group G, one has the following:*

$$\mathsf{k}^*(G) = \mathsf{k}(G) \quad \text{and} \quad \mathsf{K}^*(G) = \mathsf{K}(G).$$

Regarding upper bounds, and since the constants $\mathsf{k}(.)$ and $\mathsf{K}(.)$ are closely related to each other, it suffices, according to the following proposition (see [13], Proposition 5.1.8), to bound from above the little cross number so as to bound from above the cross number, but also the Davenport constant. Since $\mathsf{k}(.)$ is easier to handle, one usually prefers to study the cross number via the little cross number, and we will do so in this paper.

Proposition 1.1. — *Let G be a finite Abelian group with $\exp(G) = n$. Then, the two following statements hold:*

(*i*)

$$\mathsf{k}(G) + \frac{1}{n} \leq \mathsf{K}(G) \leq \mathsf{k}(G) + \frac{1}{P^-(n)},$$

(*ii*)

$$\mathsf{D}(G) \leq n\mathsf{k}(G) + 1.$$

Two types of upper bounds are currently known for $\mathsf{k}(.)$. The first one holds for any finite Abelian group, and was obtained by A. Geroldinger and R. Schneider in [17] and in [13], Theorem 5.5.5, using character theory and the notion of group algebra.

Theorem 1.4. — *Let G be a finite Abelian group with $\exp(G) = n$. Then, for every $d \in \mathcal{D}_n$, one has the following:*

$$\mathsf{k}(G) \leq \frac{d-1}{P^-(n)} + \log\left(\frac{|G|}{d}\right).$$

In particular $\mathsf{k}(G) \leq \log|G|$.

Eventhough this upper bound is general and easy to compute, it does not really fit what we know about the behaviour of the cross number. For example, let $r > 1$ be an integer. If we consider an elementary p-group with rank r, it is known that $\mathsf{k}\left(C_p^r\right) = \mathsf{k}^*\left(C_p^r\right) \leq r$, yet $\log\left(|C_p^r|/p\right) = (r-1)\log p$ diverges when p tends to infinity.

From this point of view, and in the special case of cyclic groups, a more precise upper bound was found by U. Krause and C. Zahlten in [20] which, expressed with our notations, gives the following.

Theorem 1.5. — *For every $n \in \mathbb{N}^*$, one has the following:*

$$\mathsf{k}(C_n) \leq 2\omega(n).$$

It should be underlined that this upper bound has the right order of magnitude, since one has $\mathsf{k}(C_n) \geq \mathsf{k}^*(C_n) \geq \omega(n)/2$ by definition.

2. New results and plan of the paper

In this paper, we generalize the work of [20] to every finite Abelian group so as to obtain a new upper bound for the little cross number in the general case, which no longer depends on the cardinality of the group considered, and which supports the conjecture that the little cross number of a finite Abelian group G with rank r and exponent n is less than $r\omega(n)$.

For this purpose, we introduce the two following constants. Let G be a finite Abelian group and $d', d \in \mathbb{N}^*$ be two integers such that $d \in \mathcal{D}_{\exp(G)}$ and $d' \in \mathcal{D}_d$.

By $\mathsf{D}_{(d',d)}(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G_d with length $|S| \geq t$ contains a subsequence of sum in $G_{d/d'}$.

By $\eta_{(d',d)}(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G_d with length $|S| \geq t$ contains a subsequence $S' \subseteq S$ of length $|S'| \leq d'$ and of sum in $G_{d/d'}$.

To start with, we will prove in Section 3 (Proposition 3.1), that for any finite Abelian group G and every $1 \leq d' \mid d \mid \exp(G)$, $\mathsf{D}_{(d',d)}(G)$ and $\eta_{(d',d)}(G)$ are linked to the constants $\mathsf{D}(.)$ and $\eta(.)$ of a particular subgroup $G_{\upsilon(d',d)}$ of G.

In Section 4, we will prove the main theorem (Theorem 2.1). This result will be stated at the end of this section. Before giving this general and technical theorem, we emphasize the many consequences it has.

To obtain these results, we introduce the two following arithmetic functions:

$$\alpha(n) = \sum_{d \in \mathcal{D}_n} \frac{P^-(d) - 1}{d} \quad \text{and} \quad \beta(n) = \sum_{d \in \mathcal{D}_n \cap \mathcal{P}} \frac{P^-(d) - 1}{d},$$

which will be investigated in Section 5. In particular, simple upper bounds for these functions lead, by applying the main theorem, to the following qualitative result, proved in Section 6.

Proposition 2.1. — *For every $r \in \mathbb{N}^*$ there exists a constant $d_r > 0$ such that, for every finite Abelian group G with $r(G) \leq r$ and $\exp(G) = n$, the following holds:*

$$\mathsf{k}(G) \leq d_r \omega(n).$$

Consequently, when considering the cross number of a finite Abelian group G with fixed or bounded rank, Proposition 2.1 gives a qualitative upper bound which depends only on the number of distinct prime divisors $\omega(n)$ of $\exp(G) = n$, and which improves, at least asymptotically, the one stated in Theorem 1.4, since the function ω can have arbitrary small values in $\mathbb{N}^*$ even for arbitrary large n, but mainly since it is known (see for instance Chapter I.5 of the book [30]) that one has:

$$\omega(n) \lesssim \frac{\log n}{\log \log n}.$$

In addition, more accurate upper bounds for some sequences built with $\alpha(n)$ and $\beta(n)$, obtained in Lemma 5.1 (see Section 5), enable us to prove the following quantitative result (see Section 6) which states that when $r = 1$ or 2, one can choose d_r in the following way:

$$d_1 = \frac{166822111}{109486080} \approx 1.5237 \qquad \text{and} \qquad d_2 = \frac{1784073894563}{476759162880} \approx 3.7421.$$

Once d_1 and d_2 are defined in such a way, one can state the following proposition.

Proposition 2.2. — *(i) For every cyclic group $G \simeq C_n$, $n \in \mathbb{N}^*$, we have:*

$$\mathsf{k}(G) \leq \alpha(n) \leq d_1 \omega(n).$$

(ii) For every finite Abelian group $G \simeq C_m \oplus C_n$, with $1 < m \mid n \in \mathbb{N}^*$, we have:

$$\mathsf{k}(G) \leq 3\alpha(n) - \beta(n) \leq d_2 \omega(n).$$

Moreover, the asymptotical behaviours of $\alpha(n)$ and $\beta(n)$, studied in Lemma 5.2, imply several asymptotical results, some of them being sharp, concerning the cross and little cross numbers as well as the Davenport constant. In particular, these results show that Conjecture 1.3 holds asymptotically in at least two different directions. These results will be proved in Section 7, and in order to state them, we will need the following notation. For every $r \in \mathbb{N}^*$ and $l_1, \ldots, l_r \in \mathbb{N}^*$, we set:

$$\mathcal{E}_{(l_1,\ldots,l_r)} = \left\{ \bigoplus_{i=1}^{r} C_{n_i},\ 1 < n_1 | \ldots | n_r \in \mathbb{N} \mid \forall i \in [\![1,r]\!],\ \omega(n_i) = l_i \text{ and } \gcd\left(n_i, \frac{n_r}{n_i}\right) = 1 \right\}.$$

Proposition 2.3. — *For every $r \in \mathbb{N}^*$ and $l_1, \ldots, l_r \in \mathbb{N}^*$, the following statements hold:*

(i)

$$\lim_{\substack{P^-(n_r) \to +\infty \\ C_{n_1} \oplus \cdots \oplus C_{n_r} \in \mathcal{E}_{(l_1,\ldots,l_r)}}} \mathsf{k}(C_{n_1} \oplus \cdots \oplus C_{n_r}) = \sum_{i=1}^{r} l_i,$$

(ii)

$$\lim_{\substack{P^-(n_r) \to +\infty \\ C_{n_1} \oplus \cdots \oplus C_{n_r} \in \mathcal{E}_{(l_1,\ldots,l_r)}}} \mathsf{K}(C_{n_1} \oplus \cdots \oplus C_{n_r}) = \sum_{i=1}^{r} l_i,$$

(iii)

$$\limsup_{\substack{P^-(n_r) \to +\infty \\ C_{n_1} \oplus \cdots \oplus C_{n_r} \in \mathcal{E}_{(l_1,\ldots,l_r)}}} \frac{\mathsf{D}(C_{n_1} \oplus \cdots \oplus C_{n_r})}{n_r} \leq \sum_{i=1}^{r} l_i.$$

Concerning the groups of the form C_n^r, we obtain the following corollary by specifying $n_1 = \cdots = n_r$ in Proposition 2.3.

Proposition 2.4. — *For all integers $r, l \in \mathbb{N}^*$ the three following statements hold:*

(i)

$$\lim_{\substack{P^-(n) \to +\infty \\ \omega(n) = l}} \mathsf{k}(C_n^r) = rl,$$

(ii)

$$\lim_{\substack{P^-(n) \to +\infty \\ \omega(n) = l}} \mathsf{K}(C_n^r) = rl,$$

(iii)

$$\limsup_{\substack{P^-(n) \to +\infty \\ \omega(n) = l}} \frac{\mathsf{D}(C_n^r)}{n} \leq rl.$$

It may be observed that Proposition 2.3 and Proposition 2.4 are somehow reminiscent of [17], Theorem 2(b), since this result and our Proposition 2.3 give the value of the cross number of "large" groups. However, a more precise look at both results shows that they are of a different nature. Indeed, while A. Geroldinger and R. Schneider's result is not asymptotical but valid only for special groups satisfying some restrictive conditions, ours, although of asymptotical nature, is valid in a wider framework.

The following proposition will also be proved in Section 7.

Proposition 2.5. — *For all $r \in \mathbb{N}^*$, the two following statements hold:*

(*i*)

$$\lim_{\omega(n) \to +\infty} \frac{\mathsf{k}(C_n^r)}{\omega(n)} = r,$$

(*ii*)

$$\lim_{\omega(n) \to +\infty} \frac{\mathsf{K}(C_n^r)}{\omega(n)} = r.$$

All these results are deduced from the following proposition, proved in Section 6 under the stronger form of Proposition 6.1, and which is a somewhat rough corollary of the main theorem (Theorem 2.1). For the sake of clarity, we recall that the constant c_r is the one which has been introduced in Theorem 1.2.

Proposition 2.6. — *Let G be a finite Abelian group with $r(G) = r$ and $\exp(G) = n$. We set $H = C_n^r$ and also:*

$$\varphi(G, H) = \begin{cases} \mathsf{k}^*(H/G) & \text{if } G \text{ is a direct summand of } H, \\ \mathsf{k}^*(H/G)/n & \text{otherwise.} \end{cases}$$

Then, one has the following upper bound for the little cross number $\mathsf{k}(G)$:

$$\mathsf{k}(G) \leq c_r\big(\alpha(n) - \beta(n)\big) + r\beta(n) - \varphi(G, H).$$

The main theorem of this paper (Theorem 2.1) will be proved in Section 4. In order to state it, we will need the following definitions and notations which will be extensively used in Sections 3 and 4.

Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group with $\exp(G) = n$, $\tau(n) = m$ and $d', d \in \mathbb{N}^*$ be such that $d \in \mathcal{D}_n$ and $d' \in \mathcal{D}_d$. For all $i \in [\![1, r]\!]$, we set:

$$A_i = \gcd(d', n_i),\ B_i = \frac{\operatorname{lcm}(d, n_i)}{\operatorname{lcm}(d', n_i)},$$

$$v_i(d', d) = \frac{A_i}{\gcd(A_i, B_i)},$$

and

$$G_{v(d',d)} = C_{v_1(d',d)} \oplus \cdots \oplus C_{v_r(d',d)}.$$

Then, for every $d \in \mathcal{D}_n = \{d_1, \ldots, d_m\}$ and $x = (x_{d_1}, \ldots, x_{d_m}) \in \mathbb{N}^m$, we set:

$$f_d(x) = \min_{d' \in \mathcal{D}_d \setminus \{1\}} \big(\eta(G_{v(d',d)})\big) - 1 - x_d,$$

$$g_d(x) = \mathsf{D}(G_{\upsilon(d,d)}) - 1 - \sum_{d' \in \mathcal{D}_d} x_{d'},$$

and

$$h(x) = \sum_{d \in \mathcal{D}_n} \frac{x_d}{d} - \mathsf{k}^*(G).$$

We can now state the main theorem.

Theorem 2.1. — *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group with $\exp(G) = n$ and $\tau(n) = m$. For every zero-sumfree sequence S of G reaching the maximum $\mathsf{k}(S) = \mathsf{k}(G)$, and being of minimal length regarding this property, the m-tuple $x = (|S_{d_1}|, \ldots, |S_{d_m}|)$ is an element of the polytope $\mathbb{P}_G \cap \mathbb{H}_G$ where:*

$$\mathbb{P}_G = \{x \in \mathbb{N}^m \mid f_d(x) \geq 0,\ g_d(x) \geq 0,\ d \in \mathcal{D}_n\},$$

and

$$\mathbb{H}_G = \{x \in \mathbb{N}^m \mid h(x) \geq 0\}.$$

Keeping the notations of Theorem 2.1, we obtain the following immediate corollary, which gives a general upper bound for the little cross number of a finite Abelian group, expressed as the solution of an integer linear program.

Corollary 2.2. — *For every finite Abelian group G, one has the following upper bound:*

$$\mathsf{k}(G) \leq \max_{x \in \mathbb{P}_G} \left(\sum_{i=1}^{m} \frac{x_{d_i}}{d_i} \right).$$

In principle, the wide generality of Theorem 2.1 and Corollary 2.2 leaves a good hope that it could lead to new - and maybe optimal - upper bounds for $\mathsf{k}(G)$ in the general case. However, such improvements will require a precise study of the polytope $\mathbb{P}_G$, which is certainly a complicated, but not hopeless, task.

3. On the quantities $\mathsf{D}_{(d',d)}(G)$ and $\eta_{(d',d)}(G)$

In this section, we will denote by π_i, for all $i \in [\![1, r]\!]$, the canonical epimorphism from C_{n_i} to $C_{\upsilon_i(d',d)}$. Although this epimorphism clearly depends on d' and d, we do not emphasize this dependence here since there is no risk of ambiguity. Moreover, one can notice that whenever d divides n_i, we have $\upsilon_i(d', d) = \gcd(d', n_i) = d'$, and in particular $\upsilon_r(d', d) = d'$. In the sequel, when $d' = d$, we will write $\upsilon_i(d)$ instead of $\upsilon_i(d, d)$.

Lemma 3.1. — *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group and $d', d \in \mathbb{N}^*$ be such that $d \in \mathcal{D}_{\exp(G)}$ and $d' \in \mathcal{D}_d$. Then, for every $g = [a_1, \ldots, a_r] \in G$, we have:*

$$\frac{d}{d'} \left[\frac{n_1}{\gcd(d, n_1)} a_1, \ldots, \frac{n_r}{\gcd(d, n_r)} a_r \right] = 0 \text{ if and only if } \pi_i(a_i) = 0 \text{ for all } i \in [\![1, r]\!].$$

Proof. — First, we have the following equalities:

$$\begin{aligned}\frac{d}{d'}\frac{n_i}{\gcd(d,n_i)} &= \frac{\operatorname{lcm}(d,n_i)}{d'}\\ &= \frac{\operatorname{lcm}(d,n_i)n_i}{d'n_i}\\ &= \frac{\operatorname{lcm}(d,n_i)n_i}{\gcd(d',n_i)\operatorname{lcm}(d',n_i)}\\ &= B_i\frac{n_i}{A_i}\in\mathbb{N}.\end{aligned}$$

Let $[a_1,\dots,a_r]\in G$ be such that:

$$\frac{d}{d'}\left[\frac{n_1}{\gcd(d,n_1)}a_1,\dots,\frac{n_r}{\gcd(d,n_r)}a_r\right]=0.$$

For all $i\in[\![1,r]\!]$, one has:

$$\frac{d}{d'}\frac{n_i}{\gcd(d,n_i)}a_i=B_i\frac{n_i}{A_i}a_i=0,$$

which is equivalent, considering a_i as an integer, to the following relation:

$$A_i|B_ia_i,$$

that is to say, dividing each side by $\gcd(A_i,B_i)$, that one has:

$$\upsilon_i(d',d)\ \Big|\ \frac{B_i}{\gcd(A_i,B_i)}a_i,$$

which, since:

$$\gcd\left(\frac{A_i}{\gcd(A_i,B_i)},\frac{B_i}{\gcd(A_i,B_i)}\right)=1,$$

is equivalent to:

$$\upsilon_i(d',d)|a_i,$$

and the desired result is proved. □

Proposition 3.1. — *Let $G\simeq C_{n_1}\oplus\cdots\oplus C_{n_r}$, with $1<n_1\mid\dots\mid n_r\in\mathbb{N}$, be a finite Abelian group and $d',d\in\mathbb{N}^*$ be such that $d\in\mathcal{D}_{\exp(G)}$ and $d'\in\mathcal{D}_d$. Then, we have the two following equalities:*

$$\begin{cases}\mathsf{D}_{(d',d)}(G)=\mathsf{D}\left(C_{\upsilon_1(d',d)}\oplus\cdots\oplus C_{\upsilon_r(d',d)}\right),\\ \eta_{(d',d)}(G)=\eta\left(C_{\upsilon_1(d',d)}\oplus\cdots\oplus C_{\upsilon_r(d',d)}\right).\end{cases}$$

Proof. — Let $[a_1,\dots,a_r]\in G_d$. We know that $\operatorname{ord}([a_1,\dots,a_r])=\operatorname{lcm}(\operatorname{ord}(a_1),\dots,\operatorname{ord}(a_r))$, and so $\operatorname{ord}([a_1,\dots,a_r])|d$ implies $\operatorname{ord}(a_i)|d$ for all $i\in[\![1,r]\!]$.

By Lagrange theorem, we also have $\operatorname{ord}(a_i)|n_i$, which implies that:

$$\operatorname{ord}(a_i)|\gcd(d,n_i)\text{ for all }i\in[\![1,r]\!],$$

and since any cyclic group C_{n_i} contains a unique subgroup of order $\gcd(d,n_i)$, we can write:

$$a_i=\frac{n_i}{\gcd(d,n_i)}a_i'\text{ with }a_i'\in C_{n_i}.$$

We now consider a sequence $S = (g_1, \dots, g_m)$ of G_d with $m \in \mathbb{N}^*$. According to the previous argument, the elements of S have the following form:

$$\begin{array}{lllll} g_1 & = & [a_{1,1}, \dots, a_{1,r}] & = & \left[\frac{n_1}{\gcd(d,n_1)} a'_{1,1}, \dots, \frac{n_r}{\gcd(d,n_r)} a'_{1,r}\right], \\ \vdots & & \vdots & & \vdots \\ g_m & = & [a_{m,1}, \dots, a_{m,r}] & = & \left[\frac{n_1}{\gcd(d,n_1)} a'_{m,1}, \dots, \frac{n_r}{\gcd(d,n_r)} a'_{m,r}\right]. \end{array}$$

Let K be a nonempty subset of $\{1, \dots, m\}$. Then, the sum $\sum_{k \in K} [a_{k,1}, \dots, a_{k,r}]$ is an element of $G_{d/d'}$ if and only if:

$$\frac{d}{d'} \sum_{k \in K} [a_{k,1}, \dots, a_{k,r}] = \frac{d}{d'} \left[\frac{n_1}{\gcd(d,n_1)} \sum_{k \in K} a'_{k,1}, \dots, \frac{n_r}{\gcd(d,n_r)} \sum_{k \in K} a'_{k,r} \right] = 0,$$

and by Lemma 3.1, this relation is equivalent to:

$$\sum_{k \in K} \left[\pi_1(a'_{k,1}), \dots, \pi_r(a'_{k,r})\right] = 0 \text{ in } \bigoplus_{i=1}^{r} C_{\upsilon_i(d',d)}.$$

Therefore, from the definition of the constant $\mathsf{D}(.)$, one can deduce that the smallest integer $m \in \mathbb{N}^*$ such that for every sequence $S = (g_1, \dots, g_m)$ of G_d with length $|S| \geq m$, there exists a nonempty subset $K \subseteq \{1, \dots, m\}$ such that $\sum_{k \in K} [a_{k,1}, \dots, a_{k,r}]$ is an element of $G_{d/d'}$ is exactly $\mathsf{D}\left(C_{\upsilon_1(d',d)} \oplus \dots \oplus C_{\upsilon_r(d',d)}\right)$. This proves the first equality.

If moreover, one expects the additional condition $|K| \leq \upsilon_r(d',d) = d'$ to be verified, then, by the definition of $\eta(.)$, the corresponding smallest possible integer $m \in \mathbb{N}^*$ is exactly $\eta\left(C_{\upsilon_1(d',d)} \oplus \dots \oplus C_{\upsilon_r(d',d)}\right)$, which proves the second equality. □

4. Proof of the main theorem

Proof of Theorem 2.1. — Let S be a zero-sumfree sequence of G verifying $\mathsf{k}(S) = \mathsf{k}(G)$, and being of minimal length regarding this property. For every $d \in \mathcal{D}_n$, we set $x_d = |S_d|$, and we suppose that the m-tuple $x = (x_{d_1}, \dots, x_{d_m})$ is not an element of the polytope $\mathbb{P}_G \cap \mathbb{H}_G$. Thus, one has the three following cases.

Case 1. There exists $d_0 \in \mathcal{D}_n$ such that $f_{d_0}(x) < 0$. Therefore, it exists $d'_0 \in \mathcal{D}_{d_0} \backslash \{1\}$ verifying $x_{d_0} \geq \eta\left(C_{\upsilon_1(d'_0,d_0)} \oplus \dots \oplus C_{\upsilon_r(d'_0,d_0)}\right)$ which means, by Proposition 3.1, that $x_{d_0} \geq \eta_{(d'_0,d_0)}(G)$. So, the sequence S contains X elements of order d_0, with $1 < X \leq d'_0$, the sum of which is an element of order $\tilde{d}_0$ dividing d_0/d'_0.

Let S' be the sequence obtained from S by replacing these X elements by their sum. In particular, we have $|S'| = |S| - X + 1 < |S|$. Moreover, S' is a zero-sumfree sequence and verifies the following equalities:

$$\begin{cases} |S'_{d_0}| = |S_{d_0}| - X, \\ |S'_{\tilde{d}_0}| = |S_{\tilde{d}_0}| + 1, \\ |S'_d| = |S_d| \ \forall d \neq d_0, \tilde{d}_0. \end{cases}$$

Since

$$\frac{1}{\tilde{d_0}} - \frac{X}{d_0} \geq 0,$$

one has the following inequalities:

$$\begin{aligned}\mathsf{k}(S) &= \sum_{d \in \mathcal{D}_{\exp(G)}} \frac{x_d}{d} \\ &\leq \sum_{d \in \mathcal{D}_{\exp(G)} \setminus \{d_0, \tilde{d_0}\}} \frac{x_d}{d} + \frac{x_{\tilde{d_0}} + 1}{\tilde{d_0}} + \frac{x_{d_0} - X}{d_0} \\ &= \mathsf{k}(S').\end{aligned}$$

So, we obtain $\mathsf{k}(S') = \mathsf{k}(G)$ and $|S'| < |S|$, which is a contradiction.

Case 2. There exists $d_0 \in \mathcal{D}_n$ such that $g_{d_0}(x) < 0$. As a consequence, we have $\sum_{d \in \mathcal{D}_{d_0}} x_d \geq \mathsf{D}(C_{\upsilon_1(d_0)} \oplus \cdots \oplus C_{\upsilon_r(d_0)})$ and Proposition 3.1 gives the existence of a zero-sum subsequence, which is a contradiction.

Case 3. One has $h(x) < 0$, that is to say $\mathsf{k}(S) = \mathsf{k}(G) < \mathsf{k}^*(G)$ which is a contradiction. □

An interesting special case is the one of finite Abelian groups with rank 2. Indeed, for such groups, all the parameters used to define the polytope $\mathbb{P}_G$ in the main theorem are known by Theorem 1.1:

$$\mathsf{D}_{(d,d)}(G) = \upsilon_1(d) + \upsilon_2(d) - 1 \quad \text{and} \quad \eta_{(d',d)}(G) = 2\upsilon_1(d',d) + \upsilon_2(d',d) - 2,$$

and therefore allow us to compute an explicit upper bound for the little cross number $\mathsf{k}(G)$ by linear programming methods (see for instance the book [29] for an exhaustive presentation of these methods).

5. Some sequences related to the exponent of a finite Abelian group

Let $(\alpha_l)_{l \geq 1}$ and $(\beta_l)_{l \geq 1}$ be the two following sequences of integers, built from the set of prime numbers:

$$\alpha_1 = 1 \text{ and } \alpha_l = 1 + \frac{p_l}{p_l - 1}\alpha_{l-1} \text{ for all } l \geq 2,$$

as well as

$$\beta_l = \sum_{i=1}^{l} \frac{p_i - 1}{p_i} \text{ for all } l \geq 1.$$

Finally, we define a third sequence $(\gamma_l)_{l \geq 1}$ in the following fashion:

$$\gamma_l = 3\alpha_l - \beta_l \text{ for all } l \geq 1.$$

The first values of $(\alpha_l)_{l \geq 1}$ are the following:

$$\alpha_1 = 1, \alpha_2 = 2.5, \alpha_3 = 4.125, \alpha_4 = 5.8125, \alpha_5 = 7.39375 \text{ etc.}$$

Since $2l - 1 \leq p_l$, we can already show, by induction on l, the following statement:

$$\alpha_l \leq 2l, \text{ for all } l \geq 1.$$

Indeed, one has $\alpha_1 = 1 \leq 2$, and if the statement is true for $l-1$, we obtain:

$$\alpha_l = 1 + \alpha_{l-1} + \frac{\alpha_{l-1}}{p_l - 1} \leq 1 + 2(l-1) + \frac{2(l-1)}{p_l - 1} \leq 2l.$$

In order to study more precisely the behaviours of $\alpha(n)$ and $\beta(n)$, we will extensively use a classical lower bound for the l-th prime number, proved by Rosser in [26], and which is the following:

$$l \log l \leq p_l \text{ for all } l \geq 1.$$

We can now prove Lemma 5.1, which gives accurate upper bounds for the sequences $(\alpha_l)_{l\geq 1}$ and $(\gamma_l)_{l\geq 1}$, and Lemma 5.2, which states on the one hand that α_l and β_l are both equivalent to l when l tends to infinity, and on the other hand that when $\omega(n) = l$ is fixed, then both $\alpha(n)$ and $\beta(n)$ tends to l when $P^-(n)$ tends to infinity.

Lemma 5.1. — *The following statements hold:*

(*i*) *For every integer $n \in \mathbb{N}^*$, with $\omega(n) = l$, we have:*

$$\beta_l \leq \beta(n) \leq \alpha(n) \leq \alpha_l.$$

(*ii*) *For every integer $l \geq 1$, we have:*

$$l \leq \alpha_l \leq \frac{\alpha_9}{9} l, \text{ where } \frac{\alpha_9}{9} = \frac{166822111}{109486080} \approx 1.5237.$$

(*iii*) *For every integer $l \geq 1$, we have:*

$$\frac{5}{2} l \leq \gamma_l \leq \frac{\gamma_8}{8} l, \text{ where } \frac{\gamma_8}{8} = \frac{1784073894563}{476759162880} \approx 3.7421.$$

Proof. — (*i*) Let $n = q_1^{m_1} \dots q_l^{m_l}$ be an integer with $q_1 < \cdots < q_l$. Since for all $i \in [\![1, l]\!]$, one has $p_i \leq q_i$, we obtain the first inequality:

$$\beta_l = l - \sum_{i=1}^{l} \frac{1}{p_i} \leq l - \sum_{i=1}^{l} \frac{1}{q_i} = \beta(n).$$

The second inequality follows directly from:

$$\beta(n) = \sum_{d \in \mathcal{D}_n \cap \mathcal{P}} \frac{P^-(d) - 1}{d} \leq \sum_{d \in \mathcal{D}_n} \frac{P^-(d) - 1}{d} = \alpha(n).$$

We prove the third inequality by induction on the number of distinct prime divisors $\omega(n) = l$ of n. For $l = 1$, the integer n is of the form $q_1^{m_1}$ and we obtain:

$$\alpha(q_1^{m_1}) = \sum_{i=1}^{m_1} \frac{q_1 - 1}{q_1^i} = \frac{q_1^{m_1} - 1}{q_1^{m_1}} \leq 1 = \alpha_1.$$

Assume now that the statement is valid for $l-1$. Therefore, we have:

$$\begin{aligned}\alpha(q_1^{m_1}\dots q_l^{m_l}) &= \frac{q_l^{m_l}-1}{q_l^{m_l}} + \left(\sum_{i=0}^{m_l}\frac{1}{q_l^i}\right)\alpha(q_1^{m_1}\dots q_{l-1}^{m_{l-1}}) \\ &\le \frac{q_l^{m_l}-1}{q_l^{m_l}} + \left(\sum_{i=0}^{m_l}\frac{1}{q_l^i}\right)\alpha_{l-1} \\ &\le 1 + \left(\sum_{i=0}^{+\infty}\frac{1}{p_l^i}\right)\alpha_{l-1} \\ &= 1 + \frac{p_l}{p_l-1}\alpha_{l-1} = \alpha_l,\end{aligned}$$

which proves the result.

(ii) To start with, it is straightforward that the first inequality $l \le \alpha_l$ always holds. Concerning the second inequality, one has the following:

$$\alpha_{l+1} - \alpha_l = 1 + \frac{\alpha_l}{p_{l+1}-1} \text{ for all } l \ge 1,$$

from which we deduce the two following relations:

$$\alpha_l = \alpha_1 + \sum_{k=1}^{l-1}(\alpha_{k+1}-\alpha_k) = l + \sum_{k=1}^{l-1}\frac{\alpha_k}{p_{k+1}-1},$$

as well as

$$\frac{\alpha_{l+1}}{l+1} - \frac{\alpha_l}{l} = \frac{1}{l+1} + \alpha_l\left(\frac{1}{l+1}\left(1+\frac{1}{p_{l+1}-1}\right) - \frac{1}{l}\right).$$

In the remainder of this proof, we will set $\varepsilon(l) = \alpha_l - l = \sum_{k=1}^{l-1}\frac{\alpha_k}{p_{k+1}-1}$, for all $l \ge 1$.

Using this notation, we obtain the following:

$$\begin{aligned}\frac{\alpha_l}{l} - \frac{\alpha_9}{9} &= \sum_{k=9}^{l-1}\frac{1}{k+1} + \sum_{k=9}^{l-1}\alpha_k\left(\frac{1}{k+1}\left(1+\frac{1}{p_{k+1}-1}\right)-\frac{1}{k}\right) \\ &= \sum_{k=9}^{l-1}\frac{1}{k+1} - \sum_{k=9}^{l-1}\frac{k+\varepsilon(k)}{k(k+1)} + \sum_{k=9}^{l-1}\frac{\alpha_k}{(p_{k+1}-1)(k+1)} \\ &= \sum_{k=9}^{l-1}\frac{1}{k+1}\left(\frac{\alpha_k}{(p_{k+1}-1)} - \frac{\varepsilon(k)}{k}\right) \\ &= \sum_{k=9}^{l-1}\left(\frac{\varepsilon(k+1)}{k+1} - \frac{\varepsilon(k)}{k}\right) \\ &= \frac{\varepsilon(l)}{l} - \frac{\varepsilon(9)}{9}.\end{aligned}$$

Moreover, using Rosser's lower bound, we obtain for all $l \ge 2$:

$$\varepsilon(l) = \sum_{k=1}^{l-1}\frac{\alpha_k}{p_{k+1}-1} \le \sum_{k=1}^{l-1}\frac{2k}{(k+1)\log(k+1)-1} \le 7 + \int_2^l \frac{2\mathrm{d}t}{\log t} = lf(l),$$

where we set for all $x \in \mathbb{R}$, $x \geq 2$:

$$f(x) = \frac{1}{x}\left(7 + \int_2^x \frac{2\mathrm{d}t}{\log t}\right).$$

It is readily seen that this function is non-increasing. Moreover, since:

$$\frac{\varepsilon(9)}{9} = \left(\frac{\alpha_9 - 9}{9}\right) > \frac{1}{2},$$

and since $f(l) \leq 1/2$ for all $l \geq 241$, we obtain:

$$\frac{\alpha_l}{l} \leq \frac{\alpha_9}{9}, \text{ for all } l \geq 241.$$

On the other hand, an easy computation allows us to verify that $\alpha_9/9$ is also the maximum value taken by $(\alpha_l/l)_{l\geq 1}$ on $1 \leq l \leq 240$, which proves the desired result.

(iii) The fact that the first inequality $5l/2 \leq \gamma_l$ always holds is straightforward. Moreover, for all $l \geq 1$, one has the following equality:

$$\begin{aligned}
\gamma_{l+1} &= 3\alpha_{l+1} - \beta_{l+1} \\
&= 3 + 3\alpha_l + \frac{3\alpha_l}{p_{l+1} - 1} - \beta_l - 1 + \frac{1}{p_{l+1}} \\
&= 2 + \gamma_l + \frac{3\alpha_l}{p_{l+1} - 1} + \frac{1}{p_{l+1}}.
\end{aligned}$$

Using the inequalities $5l/2 \leq \gamma_l$ and $\alpha_l \leq \alpha_9 l/9$, one can deduce that:

$$\begin{aligned}
\frac{\gamma_{l+1}}{l+1} - \frac{\gamma_l}{l} &= \frac{2}{l+1} + \gamma_l\left(\frac{1}{l+1} - \frac{1}{l}\right) + \frac{3\alpha_l}{(l+1)(p_{l+1} - 1)} + \frac{1}{p_{l+1}(l+1)} \\
&\leq \frac{1}{p_{l+1}(l+1)}\left(-\frac{p_{l+1}}{2} + \frac{\alpha_9 l}{3}\left(1 + \frac{1}{p_{l+1} - 1}\right) + 1\right).
\end{aligned}$$

We set, for all $x \in \mathbb{R}$, $x \geq 1$:

$$g(x) = -\frac{(x+1)\log(x+1)}{2} + \frac{\alpha_9 x}{3}\left(1 + \frac{1}{(x+1)\log(x+1) - 1}\right) + 1.$$

It is easily seen that this function is non-increasing. Moreover, since a study of g shows that $g(l) \leq 0$ for all $l \geq 9333$, we obtain:

$$\frac{\gamma_{l+1}}{l+1} - \frac{\gamma_l}{l} \leq 0, \text{ for all } l \geq 9333.$$

On the other hand, an easy computation allows us to verify that $(\gamma_l)_{l\geq 1}$ is increasing from $l = 1$ to $l = 8$ and decreasing from $l = 8$ to $l = 9333$, which proves the desired result.

□

Lemma 5.2. — *The two following statements hold:*

(i)

$$\lim_{l \to +\infty} \frac{\alpha_l}{l} = 1 \quad \textit{and} \quad \lim_{l \to +\infty} \frac{\beta_l}{l} = 1,$$

(ii)

$$\lim_{\substack{P^-(n)\to+\infty\\ \omega(n)=l}} \alpha(n) = l \qquad \textit{and} \qquad \lim_{\substack{P^-(n)\to+\infty\\ \omega(n)=l}} \beta(n) = l.$$

Proof. — (i) Firstly, for all $l \geq 1$, one has the following inequality:

$$l \leq \alpha_l \leq l + \sum_{k=1}^{l-1} \frac{2k}{p_{k+1}-1},$$

and since the prime number theorem reads as $p_k \sim k \log k$, we can deduce that:

$$\sum_{k=1}^{l-1} \frac{k}{p_{k+1}-1} \sim \sum_{k=2}^{l} \frac{1}{\log k} \sim \frac{l}{\log l}.$$

Therefore, when l tends to infinity, we obtain $\lim_{l\to+\infty} (\alpha_l/l) = 1$.

Secondly, we can deduce from Rosser's lower bound that for every $l \geq 3$, one has:

$$\begin{aligned} \beta_l &\geq l - \frac{5}{6} - \sum_{i=3}^{l} \frac{1}{i \log i} \\ &\geq l - 2 - \log\log l. \end{aligned}$$

Since, on the other hand, one always has $\beta_l \leq l$, we obtain $\lim_{l\to+\infty} (\beta_l/l) = 1$, which is the desired result.

(ii) The result follows from the very definition of $\alpha(n)$ and $\beta(n)$.

□

6. Upper bounds for the little cross number

As previously stated, the upper bound implied by Theorem 2.1, and given in Corollary 2.2, is expressed as the solution of an integer linear program. Even if this formulation is more precise than any explicit formula derived from Theorem 2.1, one may still like to obtain such a formula in order to interprete the behaviour of the cross number. In the present section, we obtain such a formula in Proposition 6.1. For the proof of this result, we will use the following lemma, which can be found in [13], Proposition 5.1.11.

Lemma 6.1. — *Let H be a finite Abelian group and $G \subseteq H$ a subgroup. Then, one has:*

(i)

$$\mathsf{k}(G) + \frac{\mathsf{k}(H/G)}{\exp(G)} \leq \mathsf{k}(H).$$

(ii) *If G is a direct summand of H, then:*

$$\mathsf{k}(G) + \mathsf{k}(H/G) \leq \mathsf{k}(H).$$

We are now ready to prove the following proposition.

Proposition 6.1. — *Let G be a finite Abelian group with $r(G) = r$ and $\exp(G) = n$. We set $H = C_n^r$ and also:*

$$\varphi(G,H) = \begin{cases} \mathsf{k}^*(H/G) & \text{if } G \text{ is a direct summand of } H, \\ \mathsf{k}^*(H/G)/n & \text{otherwise.} \end{cases}$$

Then, one has the following upper bound for the little cross number $\mathsf{k}(G)$:

$$\mathsf{k}(G) \leq \sum_{d \in \mathcal{D}_n} \frac{\min\Big(\eta\big(C^r_{P^-(d)}\big), \mathsf{D}(C_d^r)\Big) - 1}{d} - \varphi(G,H).$$

Proof. — Since the group G can be injected in the group $H = C_n^r$, one obtains, applying Lemma 6.1, the relation $\mathsf{k}(G) + \varphi(G,H) \leq \mathsf{k}(H)$. Then, the desired result follows from Theorem 2.1 applied to H. □

One can notice that for all $r \in \mathbb{N}^*$ and every $p \in \mathcal{P}$, one always has $\mathsf{D}(C_p^r) \leq \eta\big(C_p^r\big)$, by definition. Therefore, if we consider an elementary p-group with rank r, we obtain:

$$\mathsf{k}\left(C_p^r\right) \leq \sum_{d \in \mathcal{D}_p} \frac{\mathsf{D}(C_d^r) - 1}{d} = \frac{r(p-1)}{p} = \mathsf{k}^*\left(C_p^r\right).$$

Let G be a finite Abelian group with $r(G) = r$ and $\exp(G) = n$. Using Theorem 1.1, one obtains that if $r = 1$, then for all $d \in \mathcal{D}_n \backslash \mathcal{P}$, we have $\mathsf{D}(C_d) \geq \eta\big(C_{P^-(d)}\big)$. Moreover, when $r = 2$, then for all $d \in \mathcal{D}_n \backslash \mathcal{P}$, one has the following inequality:

$$\mathsf{D}(C_d^2) = 2d - 1 \geq 3P^-(d) - 2 = \eta\big(C^2_{P^-(d)}\big).$$

Yet, as soon as $r \geq 3$, and except for special types groups, it becomes more complicated to know exactly, for a given d in $\mathcal{D}_n \backslash \mathcal{P}$, what is the minimum of $\eta\big(C^r_{P^-(d)}\big)$ and $\mathsf{D}(C_d^r)$. For this reason, Theorem 2.1 and Proposition 6.1 remain, in general, really stronger than Proposition 2.6, which we are going to prove now. Even so, we will see in the next section that Proposition 2.6 implies sharp asymptotical results on the little cross number and the cross number.

Proof of Proposition 2.6. — Applying Proposition 6.1 and Theorem 1.2, we obtain the desired result in the following manner:

$$\begin{aligned} \mathsf{k}(G) + \varphi(G,H) &\leq \sum_{d \in \mathcal{D}_n} \frac{\min\Big(\eta\big(C^r_{P^-(d)}\big), \mathsf{D}(C_d^r)\Big) - 1}{d} \\ &\leq \sum_{d \in \mathcal{D}_n \cap \mathcal{P}} \frac{r(P^-(d) - 1)}{d} + \sum_{d \in \mathcal{D}_n \backslash \mathcal{P}} \frac{c_r(P^-(d) - 1)}{d} \\ &= c_r\big(\alpha(n) - \beta(n)\big) + r\beta(n). \end{aligned}$$

□

We can now prove the announced qualitative upper bound.

Proof of Proposition 2.1. — Since, by the definitions of Section 5, one always has the following straightforward inequalities:

$$\frac{\omega(n)}{2} \leq \beta(n) \quad \text{and} \quad \alpha(n) \leq 2\omega(n),$$

we can deduce, by Proposition 2.6 and the inequality $r \leq c_r$, the following relation:

$$\mathsf{k}(G) \leq c_r\big(\alpha(n) - \beta(n)\big) + r\beta(n) \leq \left(\frac{3c_r + r}{2}\right)\omega(n),$$

which gives the desired result. □

According to the previous remark, and in the case of $r = 1$ or 2, $\eta\big(C^r_{P^-(d)}\big)$ and $\mathsf{D}(C^r_d)$ are known and easy to compare. Therefore, we can prove Proposition 2.2.

Proof of Proposition 2.2. — Applying Theorem 1.1, one can choose $c_1 = 1$ and $c_2 = 3$.

(i) For every $n \in \mathbb{N}^*$, one has by Proposition 2.6 and Lemma 5.1 (i), (ii):

$$\mathsf{k}(C_n) \leq \alpha(n) \leq \alpha_{\omega(n)} \leq \frac{\alpha_9}{9}\omega(n),$$

which proves that one can take $d_1 = \alpha_9/9$.

(ii) For all $m, n \in \mathbb{N}^*$ with $1 < m|n$, one has by Proposition 2.6 applied to $G \simeq C_m \oplus C_n$ and Lemma 5.1 (i), (iii):

$$\mathsf{k}(G) \leq 3\alpha(n) - \beta(n) - \varphi(G, C_n^2) \leq \gamma_{\omega(n)} \leq \frac{\gamma_8}{8}\omega(n),$$

which proves that one can take $d_2 = \gamma_8/8$.

□

7. Asymptotical results

In the present section, we will apply the results obtained in Section 6 in order to prove that Conjecture 1.3 holds asymptotically in the two directions of Proposition 2.3 and Proposition 2.5.

Proof of Proposition 2.3. — First, we have:

$$\lim_{\substack{P^-(n_r) \to +\infty \\ C_{n_1} \oplus \cdots \oplus C_{n_r} \in \mathcal{E}_{(l_1,\ldots,l_r)}}} \mathsf{k}^*(C_{n_1} \oplus \cdots \oplus C_{n_r}) = \sum_{i=1}^{r} l_i,$$

and since by the Chinese remainder theorem, every $C_{n_1} \oplus \cdots \oplus C_{n_r}$ in $\mathcal{E}_{(l_1,\ldots,l_r)}$ is a direct summand of $C^r_{n_r}$, we obtain using Lemma 6.1 (ii):

$$\begin{aligned} \mathsf{k}(C_{n_1} \oplus \cdots \oplus C_{n_r}) &\leq \mathsf{k}\left(C^r_{n_r}\right) - \mathsf{k}^*\left(C_{\frac{n_r}{n_{r-1}}} \oplus \cdots \oplus C_{\frac{n_r}{n_1}}\right) \\ &= \mathsf{k}\left(C^r_{n_r}\right) - \sum_{i=1}^{r-1} \mathsf{k}^*\left(C_{\frac{n_r}{n_i}}\right). \end{aligned}$$

On the one hand, we have by Lemma 5.2 (ii):

$$\limsup_{\substack{P^-(n_r)\to+\infty\\ \omega(n_r)=l_r}} \mathsf{k}(C_{n_r}^r) \leq \limsup_{\substack{P^-(n_r)\to+\infty\\ \omega(n_r)=l_r}} c_r\big(\alpha(n_r)-\beta(n_r)\big)+r\beta(n_r)=rl_r,$$

on the other hand, since for all $i \in [\![1,r]\!]$, the equality $\gcd(n_i, n_r/n_i) = 1$ implies $\omega(n_r/n_i) = \omega(n_r) - \omega(n_i)$, we also have:

$$\lim_{\substack{P^-(n_r)\to+\infty\\ C_{n_1}\oplus\cdots\oplus C_{n_r}\in\mathcal{E}_{(l_1,\ldots,l_r)}}} \sum_{i=1}^{r-1} \mathsf{k}^*\left(C_{\frac{n_r}{n_i}}\right) = \sum_{i=1}^{r-1}\omega\left(\frac{n_r}{n_i}\right) = \sum_{i=1}^{r}(l_r-l_i).$$

Finally, we obtain:

$$\sum_{i=1}^{r} l_i \leq \liminf_{\substack{P^-(n_r)\to+\infty\\ C_{n_1}\oplus\cdots\oplus C_{n_r}\in\mathcal{E}_{(l_1,\ldots,l_r)}}} \mathsf{k}(C_{n_1}\oplus\cdots\oplus C_{n_r})$$

$$\leq \limsup_{\substack{P^-(n_r)\to+\infty\\ C_{n_1}\oplus\cdots\oplus C_{n_r}\in\mathcal{E}_{(l_1,\ldots,l_r)}}} \mathsf{k}(C_{n_1}\oplus\cdots\oplus C_{n_r}) \leq rl_r - \sum_{i=1}^{r}(l_r-l_i) = \sum_{i=1}^{r} l_i.$$

The corresponding statements for $\mathsf{K}(.)$ and $\mathsf{D}(.)$ are then deduced from Proposition 1.1. □

Since, as mentioned in Section 2, Proposition 2.4 is an immediate corollary of Proposition 2.3 by specifying $n_1 = \cdots = n_r$, we now prove an asymptotical result of an other type.

Proof of Proposition 2.5. — First, we have:

$$\lim_{\omega(n)\to+\infty} \frac{\mathsf{k}^*(C_n^r)}{\omega(n)} = r,$$

Moreover, by Proposition 2.6 applied to C_n^r, we obtain:

$$\frac{\mathsf{k}(C_n^r)}{\omega(n)} \leq c_r\left(\frac{\alpha(n)-\beta(n)}{\omega(n)}\right) + r\frac{\beta(n)}{\omega(n)},$$

which implies, by Lemma 5.2 (i), the following inequalities when $\omega(n)$ tends to infinity:

$$r = \lim_{\omega(n)\to+\infty} \frac{\mathsf{k}^*(C_n^r)}{\omega(n)} \leq \lim_{\omega(n)\to+\infty} \frac{\mathsf{k}(C_n^r)}{\omega(n)} \leq r.$$

The result for $\mathsf{K}(.)$ is then deduced from Proposition 1.1 (i). □

Each of the two previous asymptotical results admits a corollary which may appear more general at first sight. So as to state the first one, we will use the following notation, which recalls the one used for the sets $\mathcal{E}_{(l_1,\ldots,l_r)}$. For every $r, l \in \mathbb{N}^*$, we set:

$$\mathcal{E}_{r,l} = \{G \text{ finite Abelian group} \mid \mathrm{r}(G) = r,\ \omega(\exp(G)) = l\}.$$

With this notation, we obtain the following corollary.

Corollary 7.1. — *For all integers $r, l \in \mathbb{N}^*$ the three following statements hold:*

(*i*)

$$\limsup_{\substack{P^-(\exp(G)) \to +\infty \\ G \in \mathcal{E}_{r,l}}} \mathsf{k}(G) \leq rl,$$

(*ii*)

$$\limsup_{\substack{P^-(\exp(G)) \to +\infty \\ G \in \mathcal{E}_{r,l}}} \mathsf{K}(G) \leq rl,$$

(*iii*)

$$\limsup_{\substack{P^-(\exp(G)) \to +\infty \\ G \in \mathcal{E}_{r,l}}} \frac{\mathsf{D}(G)}{\exp(G)} \leq rl.$$

Proof. — Every G in $\mathcal{E}_{r,l}$ can be injected in the group $H \simeq C^r_{\exp(G)}$. Therefore, using Lemma 6.1, we obtain $\mathsf{k}(G) \leq \mathsf{k}(H)$ and the desired result follows from Proposition 2.4, applied to the group H. The corresponding statements for $\mathsf{K}(.)$ and $\mathsf{D}(.)$ are then deduced from Proposition 1.1. □

Corollary 7.2. — *For all integers $r \in \mathbb{N}^*$, the two following statements hold:*

(*i*)

$$\limsup_{\substack{\omega(\exp(G)) \to +\infty \\ r(G) \leq r}} \frac{\mathsf{k}(G)}{\omega(\exp(G))} \leq r,$$

(*ii*)

$$\limsup_{\substack{\omega(\exp(G)) \to +\infty \\ r(G) \leq r}} \frac{\mathsf{K}(G)}{\omega(\exp(G))} \leq r.$$

Proof. — Every G with rank $r(G) \leq r$ can be injected in the group $H \simeq C^r_{\exp(G)}$. Since we have $\mathsf{k}(G) \leq \mathsf{k}(H)$ by Lemma 6.1, the result follows from Proposition 2.5, applied to the group H. The statement for $\mathsf{K}(.)$ is then deduced from Proposition 1.1 (*i*). □

Acknowledgments

I am grateful to my Ph.D. advisor Alain Plagne for his help during the preparation of this article. I would like also to thank Wolfgang Schmid for his remarks on a preliminary version of this paper.

References

[1] N. Alon and M. Dubiner *A lattice point problem and additive number theory*, Combinatorica **15** (1995), 301-309.

[2] P. Baginski, S. T. Chapman, K. McDonald and L. Pudwell *On cross numbers of minimal zero sequences in certain cyclic groups*, Ars Combin. **70** (2004), 47-60.

[3] S. T. Chapman *On the Davenport constant, the cross number, and their application in factorization theory*, Zero-dimensional commutative rings (Knoxville, TN, 1994), Lecture Notes in Pure and Appl. Math., Dekker, New-York **171** (1995), 167-190.

[4] S. T. Chapman and A. Geroldinger *On cross numbers of minimal zero sequences*, Australas. J. Combin. **14** (1996), 85-92.

[5] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham *Zero-sum problems in finite abelian groups and affine caps*, Q. J. Math. **58** (2007), 159-186.

[6] S. Elledge and G. H. Hurlbert *An application of graph pebbling to zero-sum sequences in abelian groups*, Integers **5** (2005), #A17.

[7] P. van Emde Boas *A combinatorial problem on finite abelian groups II*, Reports ZW-1969-007, Math. Centre, Amsterdam (1969).

[8] W. Gao and A. Geroldinger *Systems of sets of lengths II*, Abh. Math. Sem. Univ. Hamburg **70** (2000), 31-49.

[9] W. Gao and A. Geroldinger *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337-369.

[10] W. Gao, Q. H. Hou, W. A. Schmid and R. Thangadurai *On short zero-sum subsequences II*, Integers **7** (2007), #A21.

[11] A. Geroldinger *On a conjecture of Kleitman and Lemke*, J. Number Theory **44** (1993), 60-65.

[12] A. Geroldinger *The cross number of finite abelian groups*, J. Number Theory **48** (1994), 219-223.

[13] A. Geroldinger and F. Halter-Koch *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics **278**, Chapman & Hall/CRC (2006).

[14] A. Geroldinger and F. Halter-Koch *Non-unique factorizations: a survey*, Multiplicative ideal theory in commutative algebra, Springer, New York (2006), 207-226.

[15] A. Geroldinger and Y. Hamidoune *Zero-sumfree sequences in cyclic groups and some arithmetical application*, J. Théor. Nombres Bordeaux **14** (2002), 221-239.

[16] A. Geroldinger and R. Schneider *The cross number of finite abelian groups II*, European J. Combin. **15** (1994), 399-405.

[17] A. Geroldinger and R. Schneider *The cross number of finite abelian groups III*, Discrete Math. **150** (1996), 123-130.

[18] A. Geroldinger and R. Schneider *On minimal zero sequences with large cross number*, Ars Combin. **46** (1997), 297-303.

[19] U. Krause *A characterization of algebraic number fields with cyclic class group of prime power order*, Math. Z. **186** (1984), 143-148.

[20] U. Krause and C. Zahlten *Arithmetic in Krull monoids and the cross number of divisor class groups*, Mitt. Math. Ges. Hamburg **12** (1991), 681-696.

[21] J. E. Olson *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8-10.

[22] J. E. Olson *A combinatorial problem on finite abelian groups II*, J. Number Theory **1** (1969), 195-199.

[23] A. Plagne and W. A. Schmid *On large half-factorial sets in elementary p-groups: maximal cardinality and structural characterization*, Israel J. Math. **145** (2005), 285-310.

[24] A. Plagne and W. A. Schmid *On the maximal cardinality of half-factorial sets in cyclic groups*, Math. Ann. **333** (2005), 759-785.

[25] M. Radziejewski and W. A. Schmid *Weakly half-factorial sets in finite abelian groups*, Forum Math. **19** (2007), 727-747.

[26] J.B. Rosser *The n-th prime is greater than $n \log n$*, Proc. London Math. Soc. (2) **45** (1939), 21-44.

[27] P. Samuel *Théorie algébrique des nombres*, Hermann (2003).

[28] W. A. Schmid *Differences in sets of lengths of Krull monoids with finite class group*, J. Théor. Nombres Bordeaux **17**(1) (2005), 323-345.

[29] A. Schrijver *Theory of linear and integer programming*, Wiley (1998).

[30] G. Tenenbaum *Introduction à la théorie analytique et probabiliste des nombres*, Cours spécialisés, SMF (1995).

Benjamin Girard, Centre de Mathématiques Laurent Schwartz, UMR 7640 du CNRS, École polytechnique, 91128 Palaiseau cedex, France. • *E-mail :* benjamin.girard@math.polytechnique.fr

INVERSE ZERO-SUM PROBLEMS AND ALGEBRAIC INVARIANTS

by

Benjamin Girard

Abstract. — In this paper, we study the maximal cross number of long zero-sumfree sequences in a finite Abelian group. Regarding this inverse-type problem, we formulate a general conjecture and prove, among other results, that this conjecture holds true for finite cyclic groups, finite Abelian p-groups and for finite Abelian groups with rank two. Also, the results obtained here enable us to improve, via the resolution of a linear integer program, a result of W. Gao and A. Geroldinger concerning the minimal number of elements with maximal order in a long zero-sumfree sequence of a finite Abelian group with rank two.

1. Introduction

Let G be a finite Abelian group, written additively. By $\exp(G)$ we denote the exponent of G. If G is cyclic of order n, it will be denoted by C_n. In the general case, we can decompose G (see for instance [23]) as a direct product of cyclic groups $C_{n_1} \oplus \cdots \oplus C_{n_r}$ where $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$.

In this paper, any finite sequence $S = (g_1, \ldots, g_\ell)$ of ℓ elements from G will be called a *sequence* of G with *length* $|S| = \ell$. Given a sequence $S = (g_1, \ldots, g_\ell)$ of G, we say that $s \in G$ is a *subsum* of S when it lies in the following set, called the *set of subsums* of S:

$$\Sigma(S) = \left\{ \sum_{i \in I} g_i \mid \emptyset \subsetneq I \subseteq \{1, \ldots, \ell\} \right\}.$$

If 0 is not a subsum of S, we say that S is a *zero-sumfree sequence*. If $\sum_{i=1}^{\ell} g_i = 0$, then S is said to be a *zero-sum sequence*. If moreover one has $\sum_{i \in I} g_i \neq 0$ for all proper subsets $\emptyset \subsetneq I \subsetneq \{1, \ldots, \ell\}$, S is called a *minimal zero-sum sequence*.

In a finite Abelian group G, the order of an element g will be written $\mathrm{ord}(g)$ and for every divisor d of the exponent of G, we denote by G_d the subgroup of G consisting of all the elements of order dividing d:

$$G_d = \{x \in G \mid dx = 0\}.$$

For every divisor d of $\exp(G)$, and every sequence S of G, we denote by α_d the number of elements, counted with multiplicity, contained in S and the order of which is equal to d.

Mathematics Subject Classification (2000): 11R27, 11B75, 11P99, 20D60, 20K01, 05E99, 13F05.

Although the quantity α_d clearly depends on S, we will not emphasize this dependence in the present paper, since there will be no risk of confusion.

Let $\mathcal{P}$ be the set of prime numbers. Given a positive integer $n \in \mathbb{N}^* = \mathbb{N}\backslash\{0\}$, we denote by $\mathcal{D}_n$ the set of its positive divisors and we set $\tau(n) = |\mathcal{D}_n|$. If $n > 1$, we denote by $P^-(n)$ the smallest prime element of $\mathcal{D}_n$, and we put by convention $P^-(1) = 1$. For every prime $p \in \mathcal{P}$, $\nu_p(n)$ will denote the p-adic valuation of n.

Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group. We set:

$$\mathsf{D}^*(G) = \sum_{i=1}^{r}(n_i - 1) + 1 \quad \text{as well as} \quad \mathsf{d}^*(G) = \mathsf{D}^*(G) - 1.$$

By $\mathsf{D}(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G with length $|S| \geq t$ contains a non-empty zero-sum subsequence. The number $\mathsf{D}(G)$ is called the *Davenport constant* of the group G.

By $\mathsf{d}(G)$ we denote the largest integer $t \in \mathbb{N}^*$ such that there exists a zero-sumfree sequence S of G with length $|S| = t$. It can be readily seen that, for every finite Abelian group G, one has $\mathsf{d}(G) = \mathsf{D}(G) - 1$.

If $G \simeq C_{\nu_1} \oplus \cdots \oplus C_{\nu_s}$, with $\nu_i > 1$ for all $i \in [\![1, s]\!]$, is the longest possible decomposition of G into a direct product of cyclic groups, then we set:

$$\mathsf{k}^*(G) = \sum_{i=1}^{s} \frac{\nu_i - 1}{\nu_i}.$$

The *cross number* of a sequence $S = (g_1, \ldots, g_\ell)$, denoted by $\mathsf{k}(S)$, is then defined by:

$$\mathsf{k}(S) = \sum_{i=1}^{\ell} \frac{1}{\operatorname{ord}(g_i)}.$$

The notion of cross number was introduced by U. Krause in [17] (see also [18]). Finally, we define the so-called *little cross number* $\mathsf{k}(G)$ of G:

$$\mathsf{k}(G) = \max\{\mathsf{k}(S) | S \text{ zero-sumfree sequence of } G\}.$$

Given a finite Abelian group G, two elementary constructions (see [11], Proposition 5.1.8) give the following lower bounds:

$$\mathsf{D}^*(G) \leq \mathsf{D}(G) \qquad \text{and} \qquad \mathsf{k}^*(G) \leq \mathsf{k}(G).$$

The invariants $\mathsf{D}(G)$ and $\mathsf{k}(G)$ play a key rôle in the theory of non-unique factorization (see for instance Chapter 9 in [20], the book [11] which presents the different aspects of the theory, and the survey [12] also). They have been extensively studied during last decades and even if numerous results were proved (see Chapter 5 of the book [11], [7] for a survey with many references on the subject, and [14] for recent results on the cross number of finite Abelian groups), their exact values are known for very special types of groups only. In the sequel, we will need some of these values in the case of finite Abelian p-groups and finite Abelian groups with rank two, so we gather them into the following theorem (see [10], [21] and [22]).

Theorem 1.1. — *The two following statements hold.*

(*i*) *Let $p \in \mathcal{P}$, $r \in \mathbb{N}^*$ and $a_1 \leq \cdots \leq a_r$, where $a_i \in \mathbb{N}^*$ for all $i \in [\![1, r]\!]$. Then, for the p-group $G \simeq C_{p^{a_1}} \oplus \cdots \oplus C_{p^{a_r}}$, we have:*

$$\mathsf{D}(G) = \sum_{i=1}^{r} (p^{a_i} - 1) + 1 = \mathsf{D}^*(G) \quad \text{and} \quad \mathsf{k}(G) = \sum_{i=1}^{r} \left(\frac{p^{a_i} - 1}{p^{a_i}} \right) = \mathsf{k}^*(G).$$

(*ii*) *For every $m, n \in \mathbb{N}^*$, we have:*

$$\mathsf{D}(C_m \oplus C_{mn}) = m + mn - 1 = \mathsf{D}^*(C_m \oplus C_{mn}).$$

In particular, we have $\mathsf{D}(C_n) = n$.

The aim of this paper is to study some inverse zero-sum problems of a special type. Instead of trying to characterize explicitly, given a finite Abelian group, the structure of long zero-sumfree sequences (see [5], [3], [9], [25] and [8]), or the structure of zero-sumfree sequences with large cross number (see [13]), we study to what extent a zero-sumfree sequence can be extremal in both directions simultaneously. For instance, what is the maximal cross number of a long zero-sumfree sequence? Regarding this problem, we propose the following general conjecture.

Conjecture 1.2. — *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group. Given a zero-sumfree sequence S of G verifying $|S| \geq \mathsf{d}^*(G)$, one always has the following inequality:*

$$\mathsf{k}(S) \leq \sum_{i=1}^{r} \left(\frac{n_i - 1}{n_i} \right).$$

In particular, one has $\mathsf{k}(S) < r$.

One can notice that Conjecture 1.2 is closely related to the distribution of the orders of elements in a long zero-sumfree sequence. As we will see in this paper, it provides, when it holds, useful informations on this question. In the following proposition, we gather what is currently known, to the best of our knowledge, on the structure of long zero-sumfree sequences in finite Abelian groups with rank two. This result, due to W. Gao and A. Geroldinger, can be found under a slightly different form in [11], Proposition 5.8.4.

Proposition 1.3. — *Let $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbb{N}^*$, be a finite Abelian group with rank two. For every zero-sumfree sequence S of G with length $|S| = \mathsf{d}(G) = m + mn - 2$, the two following statements hold.*

(*i*) *For every element $g \in S$, one has $m \mid \operatorname{ord}(g) \mid mn$.*

(*ii*) *The sequence S contains at least*

$$m + mn - n \left(\frac{2m - 2}{P^-(n)} + 1 \right) - 1 \geq m - 1$$

elements with order mn.

The problem of the exact structure of a long zero-sumfree sequence in groups of the form $G \simeq C_m \oplus C_{mn}$ is also closely related to an important conjecture in additive group theory, which bears upon the so-called Property B. Let $n \geq 2$ be an integer. We say that n has

Property B if every zero-sumfree sequence of $G \simeq C_n \oplus C_n$ with length $|S| = \mathsf{d}(G) = 2n-2$ contains some element repeated at least $n-2$ times.

Property B was introduced and first studied in [4] (see also [11], Section 5.8, [19] and [9]). It is conjectured that every integer $n \geq 2$ has Property B, and recently, it was proved that the set of all integers $n \geq 2$ satisfying this property is closed under multiplication (see [6], Section 8 and [8]). Therefore, it remains to solve this problem for prime values of n. Regarding this, it can be shown that Property B holds for $n = 2, 3, 5, 7$ (see [6], Proposition 4.2), for $n = 11, 13, 17, 19$ (see [1]), and consequently for every integer n being representable as a product of these numbers.

Moreover, W. Schmid proved in [25] that if some integer $m \geq 2$ has Property B, then the zero-sumfree sequences of $G \simeq C_m \oplus C_{mn}$ with length $\mathsf{d}(G) = m + mn - 2$ can be characterized explicitly for all $n \in \mathbb{N}^*$. This result provides a unified way to prove Theorem 3.3 in [5] and Theorem in [3]. It also implies, assuming that Property B holds for every integer $n \geq 2$, that Conjecture 1.2 holds true for every finite Abelian group with rank two.

2. New results and plan of the paper

In this article, we prove that Conjecture 1.2 holds for several types of finite Abelian groups. To begin with, in Section 3, we prove some consequences of this conjecture in the cases where it holds. For instance, Conjecture 1.2, if true, would imply simultaneously two classical and long-standing conjectures related to the Davenport constant of finite Abelian groups of the form C_n^r.

Proposition 2.1. — *Let $n, r \in \mathbb{N}^*$ be such that Conjecture 1.2 holds for the group C_n^r. Then, one has the following equality:*

$$\mathsf{D}(C_n^r) = r(n-1) + 1.$$

Moreover, every zero-sumfree sequence S of C_n^r with length $|S| = \mathsf{d}(C_n^r) = r(n-1)$ consists only of elements with order n.

More generally, Conjecture 1.2, if true, would provide the following general upper bound for the Davenport constant of a finite Abelian group.

Proposition 2.2. — *Suppose that Conjecture 1.2 holds for $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$. Then, one has the following inequality:*

$$\mathsf{D}(G) \leq \sum_{i=1}^{r} \frac{n_r}{n_i}(n_i - 1) + 1 = \mathsf{D}^*(G) + \sum_{i=1}^{r} \left(\frac{n_r}{n_i} - 1\right)(n_i - 1).$$

Then, in Section 3 also, we prove that Conjecture 1.2 holds true for finite cyclic groups and finite Abelian p-groups.

Proposition 2.3. — *Conjecture 1.2 holds for the following groups G.*

(i) G is a finite cyclic group.
(ii) G is a finite Abelian p-group.

In Section 4, we present a general method which was introduced in [14] so as to study the cross number of finite Abelian groups. Then, using this method, we prove in Section 5 two important lemmas, which will be useful in the study of the special case of finite Abelian groups with rank two.

In Section 6, we prove the two main theorems of this paper. The first one states that Conjecture 1.2 holds for every finite Abelian group with rank two. As already mentioned in Section 1, this result supports Property B (see [25]).

Theorem 2.4. — *Let $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbb{N}^*$, be a finite Abelian group with rank two. For every zero-sumfree sequence S of G with length $|S| \geq \mathsf{d}^*(G) = m + mn - 2$, the following inequality holds:*

$$\mathsf{k}(S) \leq \left(\frac{m-1}{m}\right) + \left(\frac{mn-1}{mn}\right).$$

In particular, one always has $\mathsf{k}(S) < 2$.

The second theorem, which is proved in Section 6 as well, is an effective result which states that, in a finite Abelian group with rank two, most of the elements of a long zero-sumfree sequence must have maximal order. This result improves significantly the statement of Proposition 1.3 (ii).

Theorem 2.5. — *Let $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbb{N}^*$, be a finite Abelian group with rank two. For every zero-sumfree sequence S of G with length $|S| = \mathsf{d}(G) = m + mn - 2$, the two following statements hold.*

(i) *If n is a prime power, then S contains at least $mn - 1$ elements with order mn.*
(ii) *If n is not a prime power, then S contains at least*

$$\left\lceil \frac{4}{5}mn + \frac{(n-5)}{5} \right\rceil$$

elements with order mn.

It may be observed that for every group $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbb{N}^*$ and $n \geq 2$, there exists a zero-sumfree sequence S of G with length $|S| = \mathsf{d}(G) = m + mn - 2$, and which does not contain strictly more than $mn - 1$ elements with order mn. Indeed, let (e_1, e_2) be a basis of G, with $\text{ord}(e_1) = m$ and $\text{ord}(e_2) = mn$. Then, it suffices to consider the zero-sumfree sequence S consisting of the element e_1 repeated $m - 1$ times and the element e_2 repeated $mn - 1$ times. From this point of view, Theorem 2.5 proves to be "nearly optimal". In [15], the more general problem of the minimal number of elements with maximal order in a zero-sumfree sequence is studied in the special case of finite Abelian p-groups.

Finally, in Section 7, we will present and discuss a general conjecture concerning the maximal possible length of a zero-sumfree sequence with large cross number, which can be seen as a dual version of Conjecture 1.2.

3. Proofs of Propositions 2.1, 2.2 and 2.3

To start with, we prove the two corollaries of Conjecture 1.2 announced in Section 2.

Proof of Proposition 2.1. — Let S be a zero-sumfree sequence of $G \simeq C_n^r$ with maximal length $|S| = \mathsf{d}(G) = \mathsf{D}(G) - 1$. Then, one has the following inequality:

$$\frac{\mathsf{D}(G)-1}{n} = \frac{|S|}{n} \leq \mathsf{k}(S) \leq r\left(\frac{n-1}{n}\right),$$

which implies that $\mathsf{D}(G) \leq r(n-1)+1 = \mathsf{D}^*(G)$, and since $\mathsf{D}^*(G) \leq \mathsf{D}(G)$ always holds, the equality follows. Consequently, one has:

$$\mathsf{k}(S) = r\left(\frac{n-1}{n}\right) = \frac{\mathsf{D}(G)-1}{n} = \frac{|S|}{n},$$

and so, every element g of S verifies $\text{ord}(g) = \exp(G) = n$. □

Proof of Proposition 2.2. — Let S be a zero-sumfree sequence of $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, such that $|S| = \mathsf{d}(G) = \mathsf{D}(G)-1$. Then, one has the following inequality:

$$\frac{\mathsf{D}(G)-1}{n_r} = \frac{|S|}{n_r} \leq \mathsf{k}(S) \leq \sum_{i=1}^{r}\left(\frac{n_i-1}{n_i}\right),$$

which implies the desired result. □

We prove now that Conjecture 1.2 holds true for finite cyclic groups and finite Abelian p-groups.

Proof of Proposition 2.3. — (*i*) Let $n \geq 2$ be an integer and let S be a zero-sumfree sequence of C_n with length $|S| \geq \mathsf{d}^*(C_n) = n-1$. Then, it is well-known (see for instance [11], Theorem 5.1.10 (*i*)) that there exists $g \in C_n$ with $\text{ord}(g) = n$ such that S is of the following form:

$$S = (\underbrace{g, \ldots, g}_{n-1 \text{ times}}).$$

Consequently, we obtain:

$$\mathsf{k}(S) = \frac{n-1}{n},$$

which gives the desired result.

(*ii*) Let $p \in \mathcal{P}$, $r \in \mathbb{N}^*$, and $G \simeq C_{p^{a_1}} \oplus \cdots \oplus C_{p^{a_r}}$, with $a_1 \leq \cdots \leq a_r$ and $a_i \in \mathbb{N}^*$ for all $i \in [\![1, r]\!]$, be a p-group. By Theorem 1.1 (*i*), one has:

$$\mathsf{k}(G) = \sum_{i=1}^{r}\left(\frac{p^{a_i}-1}{p^{a_i}}\right) = \mathsf{k}^*(G).$$

Then, for every zero-sumfree sequence S of G, in particular for those verifying $|S| \geq \mathsf{d}^*(G)$, one indeed has, by the very definition of the little cross number:

$$\mathsf{k}(S) \leq \mathsf{k}(G) = \sum_{i=1}^{r}\left(\frac{p^{a_i}-1}{p^{a_i}}\right),$$

and the proof is complete.

□

4. Outline of a new method

Let G be a finite Abelian group, and let S be a sequence of elements in G. The general method that we will use in this paper (see also [14] and [15] for applications of this method in two other contexts), consists in considering, for every $d', d \in \mathbb{N}$ such that $1 \leq d' \mid d \mid \exp(G)$, the following exact sequence:

$$0 \rightarrow G_{d/d'} \hookrightarrow G_d \overset{\pi_{(d',d)}}{\rightarrow} \frac{G_d}{G_{d/d'}} \rightarrow 0.$$

Now, let U be the subsequence of S consisting of all the elements whose order divides d. If, for some $1 \leq d' \mid d \mid \exp(G)$, it is possible to find sufficiently many disjoint non-empty zero-sum subsequences in $\pi_{(d',d)}(U)$, that is to say sufficiently many disjoint subsequences in U the sum of which are elements of order dividing d/d', then S cannot be a zero-sumfree sequence in G.

So as to make this idea more precise, we proposed in [14] to introduce the following number, which can be seen as an extension of the classical Davenport constant.

Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group and $d', d \in \mathbb{N}$ be two integers such that $1 \leq d' \mid d \mid \exp(G)$. By $\mathsf{D}_{(d',d)}(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G_d with length $|S| \geq t$ contains a subsequence of sum in $G_{d/d'}$.

Using this definition, we can prove the following simple lemma, which is one possible illustration of the idea we presented. This result will be useful in Section 5 and states that given a finite Abelian group G, there exist strong constraints on the way the orders of elements have to be distributed within a zero-sumfree sequence.

Lemma 4.1. — *Let G be a finite Abelian group and $d', d \in \mathbb{N}$ be two integers such that $1 \leq d' \mid d \mid \exp(G)$. Given a sequence S of elements in G, we will write T for the subsequence of S consisting of all the elements whose order divides d/d', and we will write U for the subsequence of S consisting of all the elements whose order divides d (In particular, one has $T \subseteq U$). Then, the following condition implies that S cannot be a zero-sumfree sequence:*

$$|T| + \left\lfloor \frac{|U| - |T|}{\mathsf{D}_{(d',d)}(G)} \right\rfloor \geq \mathsf{D}_{\left(\frac{d}{d'}, \frac{d}{d'}\right)}(G).$$

Proof. — Let us set $\Delta = \mathsf{D}_{\left(\frac{d}{d'}, \frac{d}{d'}\right)}(G)$. When it holds, this inequality implies that there are Δ disjoint subsequences $S_1, \ldots, S_\Delta$ of S, the sum of which are elements of order dividing d/d'. Now, by the very definition of $\mathsf{D}_{\left(\frac{d}{d'}, \frac{d}{d'}\right)}(G)$, S has to contain a non-empty zero-sum subsequence. □

Now, in order to obtain effective inequalities from the symbolic constraints of Lemma 4.1, one can use a result proved in [14], which states that for any finite Abelian group G and every $1 \leq d' \mid d \mid \exp(G)$, the invariant $\mathsf{D}_{(d',d)}(G)$ is linked with the classical Davenport constant of a particular subgroup of G, which can be characterized explicitly. In order to define properly this particular subgroup, we have to introduce the following notation.

For all $i \in [\![1, r]\!]$, we set:

$$A_i = \gcd(d', n_i), \; B_i = \frac{\operatorname{lcm}(d, n_i)}{\operatorname{lcm}(d', n_i)}$$

$$\text{and } \upsilon_i(d', d) = \frac{A_i}{\gcd(A_i, B_i)}.$$

For instance, whenever d divides n_i, we have $\upsilon_i(d', d) = \gcd(d', n_i) = d'$, and in particular $\upsilon_r(d', d) = d'$. We can now state our result on $\mathsf{D}_{(d',d)}(G)$ (see [14], Proposition 3.1).

Proposition 4.2. — *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group and $d', d \in \mathbb{N}$ be such that $1 \leq d' \mid d \mid \exp(G)$. Then, we have the following equality:*

$$\mathsf{D}_{(d',d)}(G) = \mathsf{D}\left(C_{\upsilon_1(d',d)} \oplus \cdots \oplus C_{\upsilon_r(d',d)}\right).$$

5. Two lemmas related to zero-freeness in $G \simeq C_m \oplus C_{mn}$

In this section, we show how the method presented in Section 4 can be used in order to obtain two key lemmas for the proofs of Theorems 2.4 and 2.5. To start with, we prove the following result.

Lemma 5.1. — *Let $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbb{N}^*$, $n \geq 2$, be a finite Abelian group with rank two, and let S be a zero-sumfree sequence of G with length $|S| \geq \mathsf{d}^*(G) = m + mn - 2$. Then, for every $\ell \in \mathcal{D}_n \backslash \{n\}$, one has the following inequality:*

$$\sum_{d \in \mathcal{D}_\ell} \alpha_{md} \leq m - 1.$$

Proof. — Let S be a zero-sumfree sequence of $G \simeq C_m \oplus C_{mn}$ with length $|S| \geq \mathsf{d}^*(G) = m + mn - 2$. Let $\ell \in \mathcal{D}_n \backslash \{n\}$, $d' = n/\ell$ and $d = mn$, which leads to $d/d' = m\ell$. We also set $m' = \gcd(d', m)$. Now, let T and U be the two subsequences of S which are defined in Lemma 4.1. In particular, one has $T \subseteq U = S$, and by Proposition 1.3 (i), we obtain:

$$|T| = \sum_{\bar{d} \in \mathcal{D}_\ell} \alpha_{m\bar{d}}.$$

To start with, we determine the exact value of $\mathsf{D}_{(d',d)}(G)$. One has:

$$\begin{aligned} \upsilon_1(d', d) &= \frac{m'}{\gcd\left(m', \frac{\operatorname{lcm}(d,m)}{\operatorname{lcm}(d',m)}\right)} \\ &= \frac{m'}{\gcd\left(m', \frac{d}{d'}\frac{m'}{m}\right)} \\ &= \frac{m'}{\gcd(m', m'\ell)} \\ &= 1, \end{aligned}$$

and, since $\upsilon_2(d', d) = d'$, one obtains, using Proposition 4.2 and Theorem 1.1 (ii), the following equalities:

$$\begin{aligned}\mathsf{D}_{(d',d)}(G) &= \mathsf{D}\left(C_{\upsilon_1(d',d)} \oplus C_{\upsilon_2(d',d)}\right)\\ &= \mathsf{D}\left(C_{\frac{n}{\ell}}\right)\\ &= \frac{n}{\ell}.\end{aligned}$$

Now, let us suppose that one has $|T| \geq m$. Since $\ell \in \mathcal{D}_n \backslash \{n\}$, we obtain the following inequalities:

$$\begin{aligned}|T| + \frac{|U| - |T|}{\mathsf{D}_{(d',d)}(G)} &\geq |T| + \frac{\ell\,(m + mn - 2 - |T|)}{n}\\ &\geq m + \frac{\ell\,(mn-2)}{n}\\ &= (m + m\ell - 1) - \frac{\ell}{n} + \left(\frac{n-\ell}{n}\right)\\ &> (m + m\ell - 1) - \frac{\ell}{n}\\ &= \mathsf{D}_{\left(\frac{d}{d'},\frac{d}{d'}\right)}(G) - \frac{1}{\mathsf{D}_{(d',d)}(G)},\end{aligned}$$

and, according to Lemma 4.1, S must contain a non-empty zero-sum subsequence, which is a contradiction. Thus, one has $|T| \leq m-1$, which is the desired result. □

Now, let $n \geq 2$ be an integer, and $p_1, \ldots, p_r$ be its distinct prime divisors. Given $m \in \mathbb{N}^*$ and a zero-sumfree sequence S in $G \simeq C_m \oplus C_{mn}$ with length $|S| \geq \mathsf{d}^*(G) = m + mn - 2$, Lemma 5.1 implies that the integers $\alpha_{md} \in \mathbb{N}$, where $d \in \mathcal{D}_n \backslash \{n\}$, have to satisfy the r following linear constraints:

$$\sum_{d \in \mathcal{D}_{n/p_i}} \alpha_{md} \leq m - 1, \text{ for all } i \in [\![1, r]\!].$$

In the next lemma, we solve a linear integer program on the divisor lattice of n, in order to obtain the maximum value of the function

$$(\alpha_{md})_{d \in \mathcal{D}_n \backslash \{n\}} \mapsto \sum_{d \in \mathcal{D}_n \backslash \{n\}} \frac{\alpha_{md}}{d}$$

under the r above constraints (the reader interested by linear programming methods is referred to the book [26], for an exhaustive presentation of the subject).

Lemma 5.2. — *Let $m, n \in \mathbb{N}^*$, with $n \geq 2$, and let $(x_d)_{d \in \mathcal{D}_n \backslash \{n\}}$ be a sequence of positive integers, such that for every prime divisor p of n, one has the following linear constraint:*

$$\sum_{d \in \mathcal{D}_{n/p}} x_d \leq m - 1.$$

Then, one has the following inequality, which is best possible:

$$\sum_{d \in \mathcal{D}_n \backslash \{n\}} \frac{x_d}{d} \leq m - 1.$$

Proof. — Let $n \geq 2$ be an integer, and $p_1, \ldots, p_r$ be its distinct prime divisors. For every $k \in [\![0, m-1]\!]$, let also $\mathcal{S}_k$ be the set of all the sequences of positive integers $x = (x_d)_{d \in \mathcal{D}_n \setminus \{n\}}$ which verify the above linear constraints, and being such that $x_1 = m - k - 1$. Now, we can prove, by induction on $k \in [\![0, m-1]\!]$, that the following statement holds.

$$\text{For every sequence } x \in \mathcal{S}_k, \text{ one has } \sum_{d \in \mathcal{D}_n \setminus \{n\}} \frac{x_d}{d} \leq m - 1.$$

If $k = 0$, then for every $x \in \mathcal{S}_0$, the linear constraints imply that $x_d = 0$ for all $d \in \mathcal{D}_n \setminus \{1, n\}$, which gives the following equality:

$$\sum_{d \in \mathcal{D}_n \setminus \{n\}} \frac{x_d}{d} = m - 1.$$

Assume now that the statement is valid for $k - 1 \geq 0$. Let us define the following map:

$$\begin{array}{rcl} f : \mathcal{D}_n \setminus \{n\} & \rightarrow & \{\mathcal{A} \mid \emptyset \subsetneq \mathcal{A} \subseteq [\![1, r]\!]\} \\ d & \mapsto & \{i \in [\![1, r]\!] \mid d \in \mathcal{D}_{n/p_i}\}. \end{array}$$

Let $x \in \mathcal{S}_k$ and let $\mathcal{L}$ be the set of the elements $d \in \mathcal{D}_n \setminus \{1, n\}$ such that one has $x_d \geq 1$. By definition, and for every $d \in \mathcal{D}_n \setminus \{n\}$, $|f(d)|$ is the number of linear constraints in which the variable x_d appears. Thus, for every prime divisor p of n, $x_{n/p}$ appears in only one linear constraint, and we may assume, without loss of generality, that we have:

$$\sum_{d \in \mathcal{D}_{n/p}} x_d = m - 1.$$

Hence, for every $i \in [\![1, r]\!]$, the set $\mathcal{L} \cap \mathcal{D}_{n/p_i}$ is non-empty, and one obtains:

$$\bigcup_{d \in \mathcal{L}} f(d) = [\![1, r]\!].$$

Let us consider a non-empty subset $\mathcal{L}'$ of $\mathcal{L}$ verifying the following equality:

$$\bigcup_{d \in \mathcal{L}'} f(d) = [\![1, r]\!],$$

and being of minimal cardinality regarding this property. Since $f(d)$ is a non-empty set for every $d \in \mathcal{D}_n \setminus \{n\}$, the following property has to hold:

$$\bigcup_{d \in \mathcal{L}''} f(d) \subsetneq [\![1, r]\!] \text{ for all } \emptyset \subsetneq \mathcal{L}'' \subsetneq \mathcal{L}'.$$

Now, one can notice the two following facts.

Fact 1. For every $d \in \mathcal{L}'$, one has $f(d) \leq r - |\mathcal{L}'| + 1$, and in particular, $|\mathcal{L}'| \leq r$. This fact is a straightforward consequence of the following combinatorial lemma.

Lemma 5.3. — *Let $r \in \mathbb{N}^*$ and $\mathcal{A}_1, \cdots, \mathcal{A}_s$ be s non-empty subsets of $[\![1, r]\!]$ verifying*

$$\bigcup_{i \in [\![1, s]\!]} \mathcal{A}_i = [\![1, r]\!], \text{ and } \bigcup_{i \in I} \mathcal{A}_i \subsetneq [\![1, r]\!] \text{ for every subset } \emptyset \subsetneq I \subsetneq [\![1, s]\!].$$

Then, for all $i \in [\![1, s]\!]$, one has the following inequality:

$$|\mathcal{A}_i| \leq r - s + 1.$$

Proof. — By symmetry, it suffices to prove that one has $|\mathcal{A}_1| \leq r - s + 1$. Assume to the contrary that $|\mathcal{A}_1| \geq r - s + 2$. Since, for all $i \in [\![1, s-1]\!]$, the set $\mathcal{A}_{i+1}$ must contain at least one element from $[\![1, r]\!] \backslash (\mathcal{A}_1 \cup \cdots \cup \mathcal{A}_i)$, one obtains the following inequality:

$$|\mathcal{A}_1 \cup \cdots \cup \mathcal{A}_{i+1}| \geq |\mathcal{A}_1 \cup \cdots \cup \mathcal{A}_i| + 1.$$

Therefore, we deduce by an easy induction argument that one has $|\mathcal{A}_1 \cup \cdots \cup \mathcal{A}_{s-1}| \geq (r - s + 2) + (s - 2) = r$, and so $\mathcal{A}_1 \cup \cdots \cup \mathcal{A}_{s-1} = [\![1, r]\!]$, which is a contradiction. □

Fact 2. For every $d \in \mathcal{D}_n \backslash \{n\}$, one has the following inequalities:

$$\begin{aligned} d &\geq \min f^{-1}(f(d)) \\ &\geq \prod_{i \in [\![1,r]\!] \backslash f(d)} p_i^{\nu_{p_i}(n)} \\ &\geq 2^{r - |f(d)|}. \end{aligned}$$

Now, using Facts 1 and 2, we can prove the desired result, by considering the sequence $y = (y_d)_{d \in \mathcal{D}_n \backslash \{n\}}$ obtained from x in the following way:

$$y_d = \begin{cases} x_1 + 1 \text{ if } d = 1, \\ x_d - 1 \text{ if } d \in \mathcal{L}', \\ x_d \qquad \text{otherwise.} \end{cases}$$

It is readily seen that $y \in \mathcal{S}_{k-1}$. Therefore, Facts 1 and 2 give the following inequalities:

$$\begin{aligned} m - 1 &\geq \sum_{d \in \mathcal{D}_n \backslash \{n\}} \frac{y_d}{d} \\ &= \left(\sum_{d \in \mathcal{D}_n \backslash \{n\}} \frac{x_d}{d} \right) + \left(1 - \sum_{d \in \mathcal{L}'} \frac{1}{d} \right) \\ &\geq \left(\sum_{d \in \mathcal{D}_n \backslash \{n\}} \frac{x_d}{d} \right) + \left(1 - \sum_{d \in \mathcal{L}'} \frac{1}{2^{r - |f(d)|}} \right) \\ &\geq \left(\sum_{d \in \mathcal{D}_n \backslash \{n\}} \frac{x_d}{d} \right) + \left(1 - \sum_{d \in \mathcal{L}'} \frac{1}{2^{|\mathcal{L}'| - 1}} \right) \\ &\geq \left(\sum_{d \in \mathcal{D}_n \backslash \{n\}} \frac{x_d}{d} \right) + \left(1 - \frac{|\mathcal{L}'|}{2^{|\mathcal{L}'| - 1}} \right) \\ &\geq \sum_{d \in \mathcal{D}_n \backslash \{n\}} \frac{x_d}{d}, \end{aligned}$$

which completes the proof. □

6. Proofs of the two main theorems

To start with, we show that every finite Abelian group with rank two satisfies Conjecture 1.2. The following proof of Theorem 2.4 consists in a direct application of Lemmas 5.1 and 5.2.

Proof of Theorem 2.4. — Let $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbb{N}^*$, be a finite Abelian group with rank two, and let S be a zero-sumfree sequence of G with length $|S| \geq \mathsf{d}^*(G) = m + mn - 2$. Since, by Theorem 1.1 (ii), one has $\mathsf{d}(G) = \mathsf{d}^*(G)$, we obtain that $|S| = \mathsf{d}^*(G) = m + mn - 2$.

If $n = 1$, then the desired result follows directly from Proposition 1.3 (i), since every element of S has order m. Now, let us suppose that $n \geq 2$. Using Proposition 1.3 (i), we obtain:

$$\begin{aligned} \mathsf{k}(S) &= \sum_{d \in \mathcal{D}_{mn}} \frac{\alpha_d}{d} \\ &= \sum_{d \in \mathcal{D}_n} \frac{\alpha_{md}}{md}, \end{aligned}$$

and we can distinguish two cases.

Case 1. $\alpha_{mn} \geq mn - 1$. In this case, applying Proposition 1.3 (i), one obtains:

$$\sum_{d \in \mathcal{D}_n \backslash \{n\}} \alpha_{md} = |S| - \alpha_{mn},$$

which implies the following inequalities:

$$\begin{aligned} \mathsf{k}(S) &= \sum_{d \in \mathcal{D}_n \backslash \{n\}} \frac{\alpha_{md}}{md} + \frac{\alpha_{mn}}{mn} \\ &\leq \left(\frac{|S| - \alpha_{mn}}{m}\right) + \frac{\alpha_{mn}}{mn} \\ &\leq \left(\frac{|S| - (mn-1)}{m}\right) + \left(\frac{mn-1}{mn}\right) \\ &= \left(\frac{m-1}{m}\right) + \left(\frac{mn-1}{mn}\right). \end{aligned}$$

Case 2. $\alpha_{mn} \leq mn - 1$. Then, by Lemmas 5.1 and 5.2, we obtain:

$$\begin{aligned} \mathsf{k}(S) &= \sum_{d \in \mathcal{D}_n \backslash \{n\}} \frac{\alpha_{md}}{md} + \frac{\alpha_{mn}}{mn} \\ &\leq \left(\frac{m-1}{m}\right) + \frac{\alpha_{mn}}{mn} \\ &\leq \left(\frac{m-1}{m}\right) + \left(\frac{mn-1}{mn}\right), \end{aligned}$$

which completes the proof. □

Now, we prove Theorem 2.5, which gives a lower bound for the number of elements with maximal order in a long zero-sumfree sequence of a finite Abelian group with rank two.

Proof of Theorem 2.5. — Let $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbb{N}^*$, be a finite Abelian group with rank two, and let S be a zero-sumfree sequence of G with length $|S| = \mathsf{d}(G) = m + mn - 2$.

(i) Let $p \in \mathcal{P}$ and $a \in \mathbb{N}$ be such that $n = p^a$. If $a = 0$, then $G \simeq C_m \oplus C_m$ and, by Proposition 1.3 (i), every element of S has order m. Now, let us suppose that $a \geq 1$, Then, by Lemma 5.1, one has:

$$\begin{aligned} |S| - \alpha_{mn} &= \sum_{d \in \mathcal{D}_{p^{a-1}}} \alpha_{md} \\ &\leq m - 1, \end{aligned}$$

which indeed implies that

$$\begin{aligned} \alpha_{mn} &\geq |S| - (m-1) \\ &= m + mn - 2 - (m-1) \\ &= mn - 1. \end{aligned}$$

(ii) If $\tau(n) \leq 3$, then n has to be a prime power, and the desired result follows by (i). Now, let us suppose that $\mathcal{D}_n = \{d_0 = 1 < d_1 < d_2 < d_3 \dots\}$ contains at least four elements. In particular, one has $n \geq 6$.

By Lemmas 5.1 and 5.2, one has:

$$\sum_{d \in \mathcal{D}_n \setminus \{n\}} \frac{\alpha_{md}}{md} \leq \frac{m-1}{m},$$

that is

$$d_1 \left(\frac{\alpha_{m\frac{n}{d_1}}}{mn} \right) + d_2 \left(\frac{\alpha_{m\frac{n}{d_2}}}{mn} \right) + d_3 \left(\frac{\alpha_{m\frac{n}{d_3}}}{mn} \right) + \sum_{\substack{d \in \mathcal{D}_n \\ d > d_3}} d \left(\frac{\alpha_{m\frac{n}{d}}}{mn} \right) \leq \frac{m-1}{m}. \tag{1}$$

Now, we can distinguish two cases.

Case 1. $d_3 = 4$. Then $d_1 = 2$, $d_2 = 3$ and (1) implies:

$$2 \left(\frac{\alpha_{m\frac{n}{2}}}{mn} \right) + 3 \left(\frac{\alpha_{m\frac{n}{3}}}{mn} \right) + 4 \left(\frac{\alpha_{m\frac{n}{4}}}{mn} \right) + 5 \left(\sum_{\substack{d \in \mathcal{D}_n \\ d > d_3}} \frac{\alpha_{m\frac{n}{d}}}{mn} \right) \leq \frac{m-1}{m}. \tag{2}$$

But since

$$\sum_{\substack{d \in \mathcal{D}_n \\ d > d_3}} \alpha_{m\frac{n}{d}} = |S| - \alpha_{mn} - \alpha_{m\frac{n}{2}} - \alpha_{m\frac{n}{3}} - \alpha_{m\frac{n}{4}},$$

relation (2) implies:

$$5 \left(\frac{m + mn - 2 - \alpha_{mn}}{mn} \right) - 3 \left(\frac{\alpha_{m\frac{n}{2}}}{mn} \right) - 2 \left(\frac{\alpha_{m\frac{n}{3}}}{mn} \right) - \left(\frac{\alpha_{m\frac{n}{4}}}{mn} \right) \leq \frac{m-1}{m},$$

that is

$$5 \left(\frac{m + mn - 2 - \alpha_{mn}}{mn} \right) - \left(\frac{\alpha_{m\frac{n}{2}} + \alpha_{m\frac{n}{4}}}{mn} \right) - 2 \left(\frac{\alpha_{m\frac{n}{2}} + \alpha_{m\frac{n}{3}}}{mn} \right) \leq \frac{m-1}{m},$$

Now using the fact that, by Lemma 5.1, one has:

$$\alpha_{m\frac{n}{2}} + \alpha_{m\frac{n}{4}} \leq m-1 \quad \text{as well as} \quad \alpha_{m\frac{n}{3}} \leq m-1,$$

we obtain

$$5\left(\frac{m+mn-2-\alpha_{mn}}{mn}\right) - \left(\frac{m-1}{mn}\right) - 2\left(\frac{2\,(m-1)}{mn}\right) \leq \frac{m-1}{m},$$

which is equivalent to

$$5\left(\frac{mn-1-\alpha_{mn}}{mn}\right) \leq \frac{m-1}{m},$$

that is

$$5(mn-1) - n(m-1) \leq 5\alpha_{mn},$$

and thus

$$\frac{4}{5}mn + \frac{(n-5)}{5} \leq \alpha_{mn},$$

which is the desired result.

Case 2. $d_3 \geq 5$. Then (1) implies:

$$d_1\left(\frac{\alpha_{m\frac{n}{d_1}}}{mn}\right) + d_2\left(\frac{\alpha_{m\frac{n}{d_2}}}{mn}\right) + 5\left(\sum_{\substack{d\in\mathcal{D}_n \\ d\geq d_3}} \frac{\alpha_{m\frac{n}{d}}}{mn}\right) \leq \frac{m-1}{m}. \tag{3}$$

But since

$$\sum_{\substack{d\in\mathcal{D}_n \\ d\geq d_3}} \alpha_{m\frac{n}{d}} = |S| - \alpha_{mn} - \alpha_{m\frac{n}{d_1}} - \alpha_{m\frac{n}{d_2}},$$

relation (3) implies:

$$5\left(\frac{m+mn-2-\alpha_{mn}}{mn}\right) + (d_1-5)\left(\frac{\alpha_{m\frac{n}{2}}}{mn}\right) + (d_2-5)\left(\frac{\alpha_{m\frac{n}{d_2}}}{mn}\right) \leq \frac{m-1}{m}.$$

Therefore, since $d_1 \geq 2$ and $d_2 \geq 3$, we have

$$5\left(\frac{m+mn-2-\alpha_{mn}}{mn}\right) - 3\left(\frac{m-1}{mn}\right) - 2\left(\frac{m-1}{mn}\right) \leq \frac{m-1}{m},$$

that is

$$5\left(\frac{mn-1-\alpha_{mn}}{mn}\right) \leq \frac{m-1}{m},$$

which leads to

$$\frac{4}{5}mn + \frac{(n-5)}{5} \leq \alpha_{mn},$$

and the proof is complete.

□

7. A concluding remark

Given a finite Abelian group G, the investigation of the maximal possible length of a zero-sumfree sequence S of G with large cross number may also be of interest. Concerning this question, we propose the following general conjecture, which can be seen as a dual version of Conjecture 1.2.

Conjecture 7.1. — *Let G be a finite Abelian group and $G \simeq C_{\nu_1} \oplus \cdots \oplus C_{\nu_s}$, with $\nu_i > 1$ for all $i \in [\![1, s]\!]$, be its longest possible decomposition into a direct product of cyclic groups. Given a zero-sumfree sequence S of G verifying $\mathsf{k}(S) \geq \mathsf{k}^*(G)$, one always has the following inequality:*

$$|S| \leq \sum_{i=1}^{s}(\nu_i - 1).$$

It can easily be seen, by Theorem 1.1 (i), that Conjecture 7.1 holds true for finite Abelian p-groups. Even in the case of finite cyclic groups which are not p-groups, this problem is still wide open. Yet, in this special case, the following result supports the idea that a zero-sumfree sequence with large cross number has to be a "short" sequence.

Theorem 7.2. — *Let $n \in \mathbb{N}^*$ be such that n is not a prime power, and let S be a zero-sumfree sequence of C_n verifying $\mathsf{k}(S) \geq \mathsf{k}^*(C_n)$. Then, one has the following inequality:*

$$|S| \leq \left\lfloor \frac{n}{2} \right\rfloor.$$

Proof. — So as to prove this result, we will use the notion of *index* of a sequence in a finite cyclic group, which was introduced implicitly in [16], Conjecture p.344, and more explicitly in [2]. Let $g \in C_n$ with $\text{ord}(g) = n$, and let $S = (g_1, \ldots, g_\ell) = (n_1 g, \ldots, n_\ell g)$, where $n_1, \ldots, n_\ell \in [\![0, n-1]\!]$, be a sequence of C_n. We define:

$$\|S\|_g = \sum_{i=1}^{\ell} \frac{n_i}{n}.$$

Since, for every $i \in [\![1, \ell]\!]$, we have

$$\frac{\gcd(n_i, n)}{n} = \frac{1}{\text{ord}(g_i)},$$

one can notice that $\|S\|_g \geq \mathsf{k}(S)$ for all $g \in C_n$ with $\text{ord}(g) = n$. Then, the index of S, denoted by $\text{index}(S)$, is defined in the following fashion:

$$\text{index}(S) = \min_{\substack{g \in C_n \\ \text{ord}(g) = n}} \|S\|_g.$$

Now, if n is not a prime power and S is a zero-sumfree sequence of C_n such that $\mathsf{k}(S) \geq \mathsf{k}^*(C_n)$, one obtains, by the very definition of the index, the following inequalities:

$$\begin{aligned} \text{index}(S) &\geq \mathsf{k}(S) \\ &\geq \mathsf{k}^*(C_n) \\ &> 1. \end{aligned}$$

Therefore, using a result of Savchev and Chen (see Theorem 9 in [24]), one must have the following inequality:

$$|S| \leq \left\lfloor \frac{n}{2} \right\rfloor,$$

which completes the proof. □

In particular, Theorem 7.2 implies that Conjecture 7.1 holds true for all the cyclic groups of the form C_{2p^a}, where $p \in \mathcal{P}$ and $a \in \mathbb{N}$.

Acknowledgments

I am grateful to my Ph.D. advisor Alain Plagne for his help during the preparation of this paper. I would like also to thank Alfred Geroldinger and Wolfgang Schmid for useful remarks on a preliminary version of this work.

References

[1] G. Bhowmik, I. Halupczok and J.C. Schlage-Puchta *The structure of maximal zero-sum free sequences II*, submitted.

[2] S. T. Chapman, M. Freeze and W.W. Smith *Minimal zero sequences and the strong Davenport constant*, Discrete Math. **203** (1999), 271-277.

[3] F. Chen and S. Savchev *Minimal zero-sum sequences of maximum length in the group* $C_3 \oplus C_{3k}$, Integers **7** (2007), #A42.

[4] W. Gao and A. Geroldinger *On long minimal zero sequences in finite abelian groups*, Period. Math. Hung. **38**(3) (1999), 179-211.

[5] W. Gao and A. Geroldinger *On the order of elements in long minimal zero-sum sequences*, Period. Math. Hung. **44**(1) (2002), 63-73.

[6] W. Gao and A. Geroldinger *On zero-sum sequences in* $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, Integers **3** (2003), #A8.

[7] W. Gao and A. Geroldinger *Zero-sum problems in finite abelian groups : a survey*, Expo. Math. **24** (2006), 337-369.

[8] W. Gao, A. Geroldinger and D. Grynkiewicz *Inverse zero-sum problems III*, submitted.

[9] W. Gao, A. Geroldinger and W. Schmid *Inverse zero-sum problems*, Acta Arith. **128** (2007), 245-279.

[10] A. Geroldinger *The cross number of finite abelian groups*, J. Number Theory **48** (1994), 219-223.

[11] A. Geroldinger and F. Halter-Koch *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics **278**, Chapman & Hall/CRC (2006).

[12] A. Geroldinger and F. Halter-Koch *Non-unique factorizations : a survey*, Multiplicative ideal theory in commutative algebra, Springer, New York (2006), 207-226.

[13] A. Geroldinger and R. Schneider *On minimal zero sequences with large cross number*, Ars Combin. **46** (1997), 297-303.

[14] B. Girard *A new upper bound for the cross number of finite Abelian groups*, Israel J. Math., to appear.

[15] B. Girard *Inverse zero-sum problems in finite Abelian p-groups*, submitted.

[16] D. Kleitman and P. Lemke *An addition theorem on the integers modulo n*, J. Number Theory **31** (1989), 335-345.

[17] U. Krause *A characterization of algebraic number fields with cyclic class group of prime power order*, Math. Z. **186** (1984), 143-148.

[18] U. Krause and C. Zahlten *Arithmetic in Krull monoids and the cross number of divisor class groups*, Mitt. Math. Ges. Hamburg **12** (1991), 681-696.

[19] G. Lettl and W. Schmid *Minimal zero-sum sequences in $C_n \oplus C_n$*, Eur. J. Comb. **28** (2007), 742-753.

[20] W. Narkiewicz *Elementary and analytic theory of algebraic numbers*, 3rd edition, Springer (2004).

[21] J. E. Olson *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8-10.

[22] J. E. Olson *A combinatorial problem on finite abelian groups II*, J. Number Theory **1** (1969), 195-199.

[23] P. Samuel *Théorie algébrique des nombres*, Hermann (2003).

[24] S. Savchev and F. Chen *Long zero-free sequences in finite cyclic groups*, Discrete Math. **307** (2007), 2671-2679.

[25] W. Schmid *Inverse zero-sum problems II*, submitted.

[26] A. Schrijver *Theory of linear and integer programming*, Wiley (1998).

Benjamin Girard, Centre de Mathématiques Laurent Schwartz, UMR 7640 du CNRS, École polytechnique, 91128 Palaiseau cedex, France. • *E-mail :* `benjamin.girard@math.polytechnique.fr`

INVERSE ZERO-SUM PROBLEMS IN FINITE ABELIAN p-GROUPS

by

Benjamin Girard

Abstract. — In this paper, we study the number of elements with maximal order contained in a zero-sumfree sequence of a finite Abelian p-group. For this purpose, in the general context of finite Abelian groups, we introduce a new number, for which lower and upper bounds are proved in the special case of finite Abelian p-groups. Among other consequences, the method that we use here enables us to show that, if $\exp(G)$ denotes the exponent of the Abelian p-group G which is considered, then a zero-sumfree sequence S with maximal possible length in G must contain at least $\exp(G) - 1$ elements with maximal order, which improves a previous result of W. Gao and A. Geroldinger.

1. Introduction

Let $\mathcal{P}$ be the set of prime numbers and let G be a finite Abelian group, written additively. By $\exp(G)$ we denote the exponent of G. If G is cyclic of order n, it will be denoted by C_n. In the general case, we can decompose G (see for instance [13]) as a direct product of cyclic groups $C_{n_1} \oplus \cdots \oplus C_{n_r}$ where $1 < n_1 \mid \dots \mid n_r \in \mathbb{N}$, so that every element g of G can be written $g = [a_1, \dots, a_r]$ (this notation will be used freely in this paper), with $a_i \in C_{n_i}$ for all $i \in [\![1, r]\!] = \{1, \dots, r\}$.

In this paper, any finite sequence $S = (g_1, \dots, g_\ell)$ of ℓ elements from G, where repetitions are allowed and the ordering of the elements within S is disregarded, will be called a *sequence* of G with *length* $|S| = \ell$. For convenience, we will sometimes use the following notation, which is a shorter way to write a sequence S when some of its elements appear several times. For every $g \in G$, we denote by $\mathsf{v}_g(S)$ the multiplicity of g in S, so that:

$$S = \prod_{g \in G} g^{\mathsf{v}_g(S)}, \text{ where } \mathsf{v}_g(S) \in \mathbb{N} \text{ for all } g \in G.$$

Given a sequence $S = (g_1, \dots, g_\ell)$ of G, we say that $s \in G$ is a *subsum* of S when it lies in the following set, called the *set of subsums* of S:

$$\Sigma(S) = \left\{ \sum_{i \in I} g_i \mid \emptyset \subsetneq I \subseteq \{1, \dots, \ell\} \right\}.$$

Mathematics Subject Classification (2000): 11R27, 11B75, 11P99, 20D60, 20K01, 05E99, 13F05.

If 0 is not a subsum of S, we say that S is a *zero-sumfree sequence*. If $\sum_{i=1}^{\ell} g_i = 0$, then S is said to be a *zero-sum sequence*. If moreover one has $\sum_{i\in I} g_i \neq 0$ for all proper subsets $\emptyset \subsetneq I \subsetneq \{1,\ldots,\ell\}$, S is called a *minimal zero-sum sequence*.

In a finite Abelian group G, the order of an element g will be written $\text{ord}_G(g)$ and for every divisor d of the exponent of G, we denote by G_d the subgroup of G consisting of all the elements of order dividing d:

$$G_d = \{x \in G \mid dx = 0\}.$$

For every sequence S of elements in G, we denote by S_d the subsequence of S consisting of all the elements of order d which are contained in S.

Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group. We set:

$$\mathsf{D}^*(G) = \sum_{i=1}^{r}(n_i - 1) + 1 \quad \text{as well as} \quad \mathsf{d}^*(G) = \mathsf{D}^*(G) - 1.$$

By $\mathsf{D}(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G with length $|S| \geq t$ contains a non-empty zero-sum subsequence. The number $\mathsf{D}(G)$ is called the *Davenport constant* of the group G.

By $\mathsf{d}(G)$ we denote the largest integer $t \in \mathbb{N}^*$ such that there exists a zero-sumfree sequence S of G with length $|S| = t$. It can be readily seen that, for every finite Abelian group G, one has $\mathsf{d}(G) = \mathsf{D}(G) - 1$.

If $G \simeq C_{\nu_1} \oplus \cdots \oplus C_{\nu_s}$, with $\nu_i > 1$ for all $i \in [\![1, s]\!]$, is the longest possible decomposition of G into a direct product of cyclic groups, then we set:

$$\mathsf{k}^*(G) = \sum_{i=1}^{s} \frac{\nu_i - 1}{\nu_i}.$$

The *cross number* of a sequence $S = (g_1, \ldots, g_\ell)$, denoted by $\mathsf{k}(S)$, is then defined by:

$$\mathsf{k}(S) = \sum_{i=1}^{\ell} \frac{1}{\text{ord}_G(g_i)}.$$

The notion of cross number was introduced by U. Krause in [9] (see also [10]). Finally, we define the so-called *little cross number* $\mathsf{k}(G)$ of G:

$$\mathsf{k}(G) = \max\{\mathsf{k}(S) | S \text{ zero-sumfree sequence of } G\}.$$

Given a finite Abelian group G, two elementary constructions (see [5], Proposition 5.1.8) give the following lower bounds:

$$\mathsf{D}^*(G) \leq \mathsf{D}(G) \qquad \text{and} \qquad \mathsf{k}^*(G) \leq \mathsf{k}(G).$$

The invariants $\mathsf{D}(G)$ and $\mathsf{k}(G)$ play a key rôle in the theory of non-unique factorization (see for instance Chapter 9 in [11], the book [5] which presents the different aspects of the theory, and the survey [6] also). They have been extensively studied during last decades and even if numerous results were proved (see Chapter 5 of the book [5], [3] for a survey with many references on the subject, and [7] for recent results on the cross number of finite Abelian groups), their exact values are known for very special types of groups only.

In the sequel, we will need some of these values in the case of finite Abelian p-groups, so we gather them into the following theorem (see [12] and [4]).

Theorem 1.1. — *Let $p \in \mathcal{P}$, $r \in \mathbb{N}^*$ and $1 \leq a_1 \leq \cdots \leq a_r$, where $a_i \in \mathbb{N}$ for all $i \in [\![1, r]\!]$. Then, for the p-group $G \simeq C_{p^{a_1}} \oplus \cdots \oplus C_{p^{a_r}}$, the two following statements hold.*

(*i*)

$$\mathsf{D}(G) = \sum_{i=1}^{r} (p^{a_i} - 1) + 1 = \mathsf{D}^*(G).$$

(*ii*)

$$\mathsf{k}(G) = \sum_{i=1}^{r} \left(\frac{p^{a_i} - 1}{p^{a_i}} \right) = \mathsf{k}^*(G).$$

In [12], J. Olson actually proved a more general result than Theorem 1.1 (*i*), which will be useful in this article. So as to state this theorem, we need to introduce the following notation. For every element $g \in G$, the *height* of g, denoted by $\alpha(g)$, is defined in the following fashion:

$$\alpha(g) = \max\{p^n \mid \exists h \in G \text{ with } g = p^n h\}.$$

We can now state Olson's result.

Theorem 1.2. — *Let G be a finite Abelian p-group and $S = (g_1, \ldots, g_\ell)$ be a sequence of G such that one has:*

$$\sum_{i=1}^{\ell} \alpha(g_i) \geq \mathsf{D}^*(G).$$

Then, S cannot be a zero-sumfree sequence.

2. Four inverse-type problems in zero-sum theory

Let G be a finite Abelian group. What can be said about the exact structure of a long zero-sumfree sequence in G? The answer to this question, which would be useful in order to tackle problems in non-unique factorization theory, seems very difficult to obtain in general, and proves to highly rely on the structure of the group itself. Indeed, several results (see for instance [1]) show that one cannot hope to find a simple and exact structural characterization which would describe long zero-sumfree sequences in general. Nevertheless, one could try to find, instead of a complete characterization, some general properties which have to be satisfied by all the long zero-sumfree sequences, whatever the group is. In [8], the author adressed two general conjectures concerning this type of inverse problems.

The first one bears upon the distribution of orders within a long zero-sumfree sequence of a finite Abelian group G, and is the following.

Conjecture 2.1. — *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group. Given a zero-sumfree sequence S of G verifying $|S| \geq \mathsf{d}^*(G)$, one always has the following inequality:*

$$\mathsf{k}(S) \leq \sum_{i=1}^{r} \left(\frac{n_i - 1}{n_i}\right).$$

The following theorem gathers what is currently known concerning this conjecture (see Proposition 2.3 and Theorem 2.4 in [8]).

Theorem 2.2. — *Conjecture 2.1 holds for the following groups G.*

(*i*) *G is a finite cyclic group.*
(*ii*) *G is a finite Abelian group with rank two.*
(*iii*) *G is a finite Abelian p-group.*

The reader interested in this type of problems is also referred to Section 7 in [8], where the following dual version of Conjecture 2.1, on the maximal possible length of a zero-sumfree sequence with large cross number, is discussed.

Conjecture 2.3. — *Let G be a finite Abelian group and $G \simeq C_{\nu_1} \oplus \cdots \oplus C_{\nu_s}$, with $\nu_i > 1$ for all $i \in [\![1, s]\!]$, be its longest possible decomposition into a direct product of cyclic groups. Given a zero-sumfree sequence S of G verifying $\mathsf{k}(S) \geq \mathsf{k}^*(G)$, one always has the following inequality:*

$$|S| \leq \sum_{i=1}^{s} (\nu_i - 1).$$

For instance, it can easily be seen, by Theorem 1.1 (*i*), that Conjecture 2.3 holds true for finite Abelian p-groups. It would be interesting to prove this conjecture even in the special case of finite cyclic groups.

In this article, we study two other inverse zero-sum problems. The first one deals with the minimal number of elements with maximal order in a long zero-sumfree sequence of a finite Abelian group. This question was raised and investigated by W. Gao and A. Geroldinger (see Section 6 in [1]), and more recently, studied by the author in the case of finite Abelian groups with rank two (see Theorem 2.5 in [8]). In the present paper, we consider the more general problem of the minimal number of elements with maximal order contained in any zero-sumfree sequence of a finite Abelian group, and obtain new results in the context of finite Abelian p-groups.

In order to study this kind of inverse zero-sum problems, we propose to introduce the following number. Given a finite Abelian group G and an integer $\delta \in [\![0, \mathsf{d}(G) - 1]\!]$, we denote by $\Gamma_\delta(G)$ the minimal number of elements with maximal order contained in a zero-sumfree sequence S with length $|S| \geq \mathsf{d}(G) - \delta$.

In Section 3, we present a general method which was introduced in [7] for the study of the cross number of finite Abelian groups. Then, using this method, we prove in Section 4 the following theorem, which gives a lower bound for $\Gamma_\delta(G)$ in the special case of finite Abelian p-groups, and improves significantly a result of W. Gao and A. Geroldinger (see Corollary 5.1.13 in [5]).

Theorem 2.4. — *Let* $G \simeq C_{p^{a_1}} \oplus \cdots \oplus C_{p^{a_r}}$*, where* $p \in \mathcal{P}$*,* $r \in \mathbb{N}^*$ *and* $1 \leq a_1 \leq \cdots \leq a_r$*, with* $a_i \in \mathbb{N}$ *for all* $i \in [\![1, r]\!]$*. Let also* $\delta \in [\![0, \mathsf{d}^*(G)-1]\!]$ *and* $j_0 = \min\{i \in [\![1, r]\!] \mid a_i = a_r\}$*. Then, one has:*

$$\Gamma_\delta(G) \geq (p^{a_r} - 1) + (r - j_0)(p-1)p^{a_r-1} - \delta - \left\lfloor \frac{\delta}{(r - j_0 + 1)(p-1)} \right\rfloor.$$

Consequently, by specifying $\delta = 0$ in Theorem 2.4, we obtain the following result.

Corollary 2.5. — *Every zero-sumfree sequence* S *with maximal possible length in a finite Abelian* p*-group* G *must contain at least* $\exp(G) - 1$ *elements with maximal order.*

In Section 4 as well, we obtain a general upper bound for $\Gamma_\delta(G)$ in the case of finite Abelian p-groups (see Proposition 4.1), which, combined with the lower bound of Theorem 2.4, implies the following result.

Proposition 2.6. — *Let* $p \in \mathcal{P}$*,* $r \in \mathbb{N}^*$ *and* $1 \leq a_1 \leq \cdots \leq a_{r-1} < a_r$*, where* $a_i \in \mathbb{N}$ *for all* $i \in [\![1, r]\!]$*. Then, for* $G \simeq C_{p^{a_1}} \oplus \cdots \oplus C_{p^{a_r}}$ *and* $\delta \in [\![0, \mathsf{d}^*(G) - 1]\!]$*, we have:*

$$\Gamma_\delta(G) = \max\left(0, (p^{a_r} - 1) - \delta - \left\lfloor \frac{\delta}{p-1} \right\rfloor\right).$$

In Section 5, we study the following general conjecture, which bears upon the greatest common divisor of the orders of the elements in a long zero-sumfree sequence of a finite Abelian group.

Conjecture 2.7. — *Let* $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$*, with* $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$*, be a finite Abelian group. Given a zero-sumfree sequence* S *of* G *verifying* $|S| \geq \mathsf{d}^*(G)$*, one has for all* $g \in S$*:*

$$n_1 \mid \operatorname{ord}_G(g).$$

Conjecture 2.7 is known to be true in the trivial case of finite cyclic groups, and also for finite Abelian groups with rank two (see Proposition 6.3.1 in [1]). We shall prove in Section 5 that it holds for finite Abelian p-groups too, which is statement (*iii*) of the following theorem.

Theorem 2.8. — *Conjecture 2.7 holds for the following groups* G*.*

(*i*) *G is a finite cyclic group.*
(*ii*) *G is a finite Abelian group with rank two.*
(*iii*) *G is a finite Abelian p-group.*

Finally, in Section 6, we propose and discuss a general conjecture concerning the behaviour of $\Gamma_\delta(G)$, when G is a finite Abelian p-group.

3. Outline of the method

Let G be a finite Abelian group, and let S be a sequence of elements in G. The general method that we will use in this paper (see also [7] and [8] for applications of this method in two other contexts), consists in considering, for every $d', d \in \mathbb{N}$ such that $1 \leq d' \mid d \mid \exp(G)$, the following exact sequence:

$$0 \rightarrow G_{d/d'} \hookrightarrow G_d \overset{\pi_{(d',d)}}{\rightarrow} \frac{G_d}{G_{d/d'}} \rightarrow 0.$$

Now, let U be the subsequence of S consisting of all the elements whose order divides d. If, for some $1 \leq d' \mid d \mid \exp(G)$, it is possible to find sufficiently many disjoint non-empty zero-sum subsequences in $\pi_{(d',d)}(U)$, that is to say sufficiently many disjoint subsequences in U the sum of which are elements of order dividing d/d', then S cannot be a zero-sumfree sequence in G.

So as to make this idea more precise, we proposed in [7] to introduce the following number, which can be seen as an extension of the classical Davenport constant.

Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group and $d', d \in \mathbb{N}$ be two integers such that $1 \leq d' \mid d \mid \exp(G)$. By $\mathsf{D}_{(d',d)}(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G_d with length $|S| \geq t$ contains a subsequence of sum in $G_{d/d'}$.

Using this definition, we can prove the following simple lemma, which is one possible illustration of the idea we presented. This result will be useful in Section 4 and states that given a finite Abelian group G, there exist strong constraints on the way the orders of elements have to be distributed within a zero-sumfree sequence.

Lemma 3.1. — *Let G be a finite Abelian group and $d', d \in \mathbb{N}$ be two integers such that $1 \leq d' \mid d \mid \exp(G)$. Given a sequence S of elements in G, we will write T for the subsequence of S consisting of all the elements whose order divides d/d', and we will write U for the subsequence of S consisting of all the elements whose order divides d (In particular, one has $T \subseteq U$). Then, the following condition implies that S cannot be a zero-sumfree sequence:*

$$|T| + \left\lfloor \frac{|U| - |T|}{\mathsf{D}_{(d',d)}(G)} \right\rfloor \geq \mathsf{D}_{\left(\frac{d}{d'}, \frac{d}{d'}\right)}(G).$$

Proof. — Let us set $\Delta = \mathsf{D}_{\left(\frac{d}{d'}, \frac{d}{d'}\right)}(G)$. When it holds, this inequality implies that there are Δ disjoint subsequences $S_1, \ldots, S_\Delta$ of S, the sum of which are elements of order dividing d/d'. Now, by the very definition of $\mathsf{D}_{\left(\frac{d}{d'}, \frac{d}{d'}\right)}(G)$, S has to contain a non-empty zero-sum subsequence. □

Now, in order to obtain effective inequalities from the symbolic constraints of Lemma 3.1, one can use a result proved in [7], which states that for any finite Abelian group G and every $1 \leq d' \mid d \mid \exp(G)$, the invariant $\mathsf{D}_{(d',d)}(G)$ is linked with the classical Davenport constant of a particular subgroup of G, which can be characterized explicitly. In order to define properly this particular subgroup, we have to introduce the following notation.

For all $i \in [\![1, r]\!]$, we set:

$$A_i = \gcd(d', n_i), \ B_i = \frac{\mathrm{lcm}(d, n_i)}{\mathrm{lcm}(d', n_i)}$$

$$\text{and } \upsilon_i(d', d) = \frac{A_i}{\gcd(A_i, B_i)}.$$

For instance, whenever d divides n_i, we have $\upsilon_i(d', d) = \gcd(d', n_i) = d'$, and in particular $\upsilon_r(d', d) = d'$. We can now state our result on $\mathsf{D}_{(d',d)}(G)$ (see [7], Proposition 3.1).

Proposition 3.2. — *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group and $d', d \in \mathbb{N}$ be such that $1 \leq d' \mid d \mid \exp(G)$. Then, we have the following equality:*

$$\mathsf{D}_{(d',d)}(G) = \mathsf{D}\left(C_{\upsilon_1(d',d)} \oplus \cdots \oplus C_{\upsilon_r(d',d)}\right).$$

4. On the quantity $\Gamma_\delta(G)$ for finite Abelian p-groups

In this section, we will show how the method presented in Section 3 can be used in order to study the minimal number of elements with maximal order contained in a zero-sumfree sequence of a finite Abelian p-group. First, we prove Theorem 2.4, which, given a finite Abelian p-group G and an integer $\delta \in [\![0, \mathsf{d}^*(G) - 1]\!]$, gives a lower bound for the number $\Gamma_\delta(G)$.

Proof of Theorem 2.4. — Let S be a zero-sumfree sequence of $G \simeq C_{p^{a_1}} \oplus \cdots \oplus C_{p^{a_r}}$. We set $d' = p$ and $d = p^{a_r}$, which leads to $d/d' = p^{a_r - 1}$. Let also T and U be the two subsequences of S which are defined in Lemma 3.1. In particular, one has $T \subseteq U = S$.

To start with, we determine the exact value of $\mathsf{D}_{(d',d)}(G)$. One has, for every $i \in [\![1, r]\!]$:

$$\begin{aligned} \upsilon_i(d', d) &= \frac{p}{\gcd\left(p, \frac{p^{a_r}}{p^{a_i}}\right)} \\ &= \begin{cases} 1 \text{ if } i < j_0, \\ p \text{ if } i \geq j_0. \end{cases} \end{aligned}$$

Therefore, using Proposition 3.2 and Theorem 1.1 (i), we obtain:

$$\begin{aligned} \mathsf{D}_{(d',d)}(G) &= \mathsf{D}\left(C_{\upsilon_1(d',d)} \oplus \cdots \oplus C_{\upsilon_r(d',d)}\right) \\ &= \mathsf{D}(C_p^{r-j_0+1}) \\ &= (r - j_0 + 1)(p - 1) + 1. \end{aligned}$$

Now, let us set, for all $i \in [\![1, r]\!]$:

$$\beta_i = \begin{cases} a_i \text{ if } i < j_0, \\ a_r - 1 \text{ if } i \geq j_0. \end{cases}$$

If we had the following inequality:

$$|T| > \sum_{i=1}^{r-1} (p^{\beta_i} - 1) + \frac{\delta}{(r - j_0 + 1)(p - 1)},$$

then it would imply that:

$$\begin{aligned}
|T| + \frac{|U|-|T|}{\mathsf{D}_{(d',d)}(G)} &\geq |T| + \frac{\displaystyle\sum_{i=1}^{r}(p^{a_i}-1) - \delta - |T|}{(r-j_0+1)(p-1)+1} \\
&> \sum_{i=1}^{r-1}(p^{\beta_i}-1) + \frac{\displaystyle\sum_{i=1}^{r}(p^{a_i}-1) - \sum_{i=1}^{r-1}(p^{\beta_i}-1)}{(r-j_0+1)(p-1)+1} \\
&= \sum_{i=1}^{r-1}(p^{\beta_i}-1) + \frac{(p^{a_r}-1) + (r-j_0)(p^{a_r}-p^{a_r-1})}{(r-j_0+1)(p-1)+1} \\
&= \sum_{i=1}^{r-1}(p^{\beta_i}-1) + \frac{((r-j_0+1)(p-1)+1)\, p^{a_r-1} - 1}{(r-j_0+1)(p-1)+1} \\
&= \sum_{i=1}^{r}(p^{\beta_i}-1) + 1 - \frac{1}{(r-j_0+1)(p-1)+1} \\
&= \mathsf{D}_{\left(\frac{d}{d'},\frac{d}{d'}\right)}(G) - \frac{1}{\mathsf{D}_{(d',d)}(G)},
\end{aligned}$$

and, according to Lemma 3.1, S would contain a non-empty zero-sum subsequence, which is a contradiction. Thus, one obtains:

$$|T| \leq \sum_{i=1}^{r-1}(p^{\beta_i}-1) + \left\lfloor \frac{\delta}{(r-j_0+1)\,(p-1)} \right\rfloor,$$

which gives the following lower bound for the number of elements with maximal order contained in S:

$$\begin{aligned}
|S_{p^{a_r}}| &= |S| - |T| \\
&\geq \sum_{i=1}^{r}(p^{a_i}-1) - \delta - \sum_{i=1}^{r-1}(p^{\beta_i}-1) - \left\lfloor \frac{\delta}{(r-j_0+1)\,(p-1)} \right\rfloor \\
&= (r-j_0+1)\,(p^{a_r}-1) - (r-j_0)\left(p^{a_r-1}-1\right) - \delta - \left\lfloor \frac{\delta}{(r-j_0+1)\,(p-1)} \right\rfloor \\
&= (p^{a_r}-1) + (r-j_0)(p-1)p^{a_r-1} - \delta - \left\lfloor \frac{\delta}{(r-j_0+1)\,(p-1)} \right\rfloor,
\end{aligned}$$

and the proof is complete. □

Given a finite Abelian p-group G and an integer $\delta \in [\![0, \mathsf{d}^*(G)-1]\!]$, we can also obtain, using some explicit constructions, an upper bound for the number $\Gamma_\delta(G)$.

Proposition 4.1. — *Let $G \simeq C_{p^{a_1}} \oplus \cdots \oplus C_{p^{a_r}}$, where $p \in \mathcal{P}$, $r \in \mathbb{N}^*$ and $a_1 \leq \cdots \leq a_r$, with $a_i \in \mathbb{N}^*$ for all $i \in [\![1,r]\!]$. Let $\delta \in [\![0, \mathsf{d}^*(G)-1]\!]$ and $j_0 = \min\{i \in [\![1,r]\!] \mid a_i = a_r\}$. Then, one has:*

$$\Gamma_\delta(G) \leq \max\left(0, (r-j_0+1)\,(p^{a_r}-1) - \delta - f(\delta)\right),$$

where

$$f(\delta)=\min\left(\left\lfloor \frac{\delta}{p-1}\right\rfloor, (r-j_0+1)\left(p^{a_r-1}-1\right)\right).$$

Proof. — Let $(e_1,\dots,e_r)$ be a basis of G, with $\mathrm{ord}(e_i)=p^{a_i}$ for every $i\in [\![1,r]\!]$. One can distinguish the three following cases.

Case 1. If $0\leq \delta<(r-j_0+1)(p-1)\left(p^{a_r-1}-1\right)$, then let us write:
$\delta=\delta_1(p-1)\left(p^{a_r-1}-1\right)+\delta_2,$ with $\delta_1\in [\![0,(r-j_0)]\!]$ and $\delta_2\in [\![0,(p-1)\left(p^{a_r-1}-1\right)-1]\!]$.
Thus, the sequence

$$S=\left(\prod_{i=1}^{r-\delta_1-1} e_i^{p^{a_i}-1}\right)\left(\prod_{i=r-\delta_1}^{r-1}(e_i)^{p-1}(pe_i)^{p^{a_i-1}-1}\right)(e_r)^{p^{a_r}-1-\delta_2-\left\lfloor\frac{\delta_2}{p-1}\right\rfloor}(pe_r)^{\left\lfloor\frac{\delta_2}{p-1}\right\rfloor}$$

is a zero-sumfree sequence of G. On the one hand, since $\delta_1\leq(r-j_0)$, one obtains:

$$\begin{aligned}
|S| &= \sum_{i=1}^{r-\delta_1-1}(p^{a_i}-1)+\sum_{i=r-\delta_1}^{r-1}\left[(p-1)+\left(p^{a_r-1}-1\right)\right]+(p^{a_r}-1)-\delta_2-\left\lfloor\frac{\delta_2}{p-1}\right\rfloor+\left\lfloor\frac{\delta_2}{p-1}\right\rfloor\\
&= \sum_{i=1}^{r}(p^{a_i}-1)+\sum_{i=r-\delta_1}^{r-1}\left[(p-1)+\left(p^{a_r-1}-1\right)-(p^{a_r}-1)\right]-\delta_2\\
&= \sum_{i=1}^{r}(p^{a_i}-1)-\delta_1(p-1)\left(p^{a_r-1}-1\right)-\delta_2\\
&= \mathsf{d}^*(G)-\delta.
\end{aligned}$$

On the other hand, S contains the following number of elements with maximal order p^{a_r}:

$$\begin{aligned}
|S_{p^{a_r}}| &= \sum_{i=j_0}^{r-\delta_1-1}(p^{a_r}-1)+\sum_{i=r-\delta_1}^{r-1}(p-1)+(p^{a_r}-1)-\delta_2-\left\lfloor\frac{\delta_2}{p-1}\right\rfloor\\
&= (r-\delta_1-j_0+1)(p^{a_r}-1)+\delta_1(p-1)-\delta_2-\left\lfloor\frac{\delta_2}{p-1}\right\rfloor\\
&= (r-j_0+1)(p^{a_r}-1)-\delta-\delta_1\left(p^{a_r-1}-1\right)-\left\lfloor\frac{\delta_2}{p-1}\right\rfloor\\
&= (r-j_0+1)(p^{a_r}-1)-\delta-\left\lfloor\frac{\delta}{p-1}\right\rfloor,
\end{aligned}$$

and we are done.

Case 2. If $(r-j_0+1)(p-1)\left(p^{a_r-1}-1\right)\leq\delta<(r-j_0+1)(p-1)p^{a_r-1}$, then let us write:

$$\delta'=\delta-(r-j_0+1)(p-1)\left(p^{a_r-1}-1\right),$$

and

$$\delta'=\delta'_1(p-1)+\delta'_2,\ \text{ with } \delta'_1\in[\![0,(r-j_0)]\!] \text{ and } \delta'_2\in[\![0,p-2]\!].$$

Thus, the sequence

$$S=\left(\prod_{i=1}^{j_0-1}e_i^{p^{a_i}-1}\right)\left(\prod_{i=j_0}^{r-\delta'_1-1}(e_i)^{p-1}(pe_i)^{p^{a_r-1}-1}\right)\left(\prod_{i=r-\delta'_1}^{r-1}(pe_i)^{p^{a_r-1}-1}\right)(e_r)^{p-1-\delta'_2}(pe_r)^{p^{a_r-1}-1}$$

is a zero-sumfree sequence of G. On the one hand, since $\delta'_1 \leq (r - j_0)$, one obtains:

$$\begin{aligned} |S| &= \sum_{i=1}^{j_0-1} (p^{a_i} - 1) + (r - \delta'_1 - j_0)(p-1) + (r - j_0 + 1)\left(p^{a_r - 1} - 1\right) + (p-1) - \delta'_2 \\ &= \sum_{i=1}^{j_0-1} (p^{a_i} - 1) + (r - j_0 + 1)(p-1) + (r - j_0 + 1)\left(p^{a_r - 1} - 1\right) - \delta' \\ &= \sum_{i=1}^{j_0-1} (p^{a_i} - 1) + (r - j_0 + 1)\left[(p-1) + \left(p^{a_r-1} - 1\right) + (p-1)\left(p^{a_r-1} - 1\right)\right] - \delta \\ &= \sum_{i=1}^{j_0-1} (p^{a_i} - 1) + (r - j_0 + 1)(p^{a_r} - 1) - \delta \\ &= \mathsf{d}^*(G) - \delta. \end{aligned}$$

On the other hand, S contains the following number of elements with maximal order p^{a_r}:

$$\begin{aligned} |S_{p^{a_r}}| &= (r - \delta'_1 - j_0)(p-1) + (p-1) - \delta'_2 \\ &= (r - \delta'_1 - j_0)(p-1) + (p-1) - \delta'_2 \\ &= (r - j_0 + 1)(p-1) - \delta' \\ &= (r - j_0 + 1)(p^{a_r} - 1) - \delta - (r - j_0 + 1)\left(p^{a_r-1} - 1\right), \end{aligned}$$

and we are done.

Case 3. If $(r - j_0 + 1)(p-1)p^{a_r-1} \leq \delta \leq \mathsf{d}^*(G) - 1$, then we have:

$$\begin{aligned} (r - j_0 + 1)(p^{a_r} - 1) - \delta - f(\delta) &\leq (r - j_0 + 1)\left[(p^{a_r} - 1) - (p-1)p^{a_r-1} - \left(p^{a_r-1} - 1\right)\right] \\ &\leq 0, \end{aligned}$$

as well as

$$\begin{aligned} \mathsf{d}^*(G) - \delta &\leq \sum_{i=1}^{r} (p^{a_i} - 1) - (r - j_0 + 1)(p-1)p^{a_r-1} \\ &= \sum_{i=1}^{j_0-1} (p^{a_i} - 1) + (r - j_0 + 1)\left[(p^{a_r} - 1) - (p-1)p^{a_r-1}\right] \\ &= \sum_{i=1}^{j_0-1} (p^{a_i} - 1) + (r - j_0 + 1)\left(p^{a_r-1} - 1\right). \end{aligned}$$

Now, let us consider the zero-sumfree sequence

$$S = \left(\prod_{i=1}^{j_0-1} e_i^{p^{a_i}-1}\right)\left(\prod_{i=j_0}^{r} (pe_i)^{p^{a_r-1}-1}\right),$$

which does not contain any element with maximal order. Thus, choosing any subsequence of S with length $\mathsf{d}^*(G) - \delta$, we obtain that $\Gamma_\delta(G) = 0$, which is the desired result. □

It is now easy, using Theorem 2.4 and Proposition 4.1, to derive Proposition 2.6, which gives, in the case where $j_0 = r$, the exact value of the number $\Gamma_\delta(G)$ for every integer $\delta \in [\![0, \mathsf{d}^*(G) - 1]\!]$.

Proof of Proposition 2.6. — Since $j_0 = r$, one obtains the following lower bound:

$$\Gamma_\delta(G) \geq (p^{a_r} - 1) - \delta - \left\lfloor \frac{\delta}{p-1} \right\rfloor.$$

Consequently, one can distinguish three cases.

Case 1. If $0 \leq \delta < (p-1)\,(p^{a_r-1} - 1)$, then the upper bound given by Proposition 4.1 implies that:

$$\Gamma_\delta(G) = (p^{a_r} - 1) - \delta - \left\lfloor \frac{\delta}{p-1} \right\rfloor.$$

Case 2. If $(p-1)\,(p^{a_r-1} - 1) \leq \delta < (p-1)p^{a_r-1}$, then the upper bound of Proposition 4.1 implies that:

$$\Gamma_\delta(G) \leq (p^{a_r} - 1) - \delta - \left(p^{a_r-1} - 1\right).$$

Now, since

$$\left(p^{a_r-1} - 1\right) = \left\lfloor \frac{\delta}{p-1} \right\rfloor,$$

one obtains the desired equality:

$$\Gamma_\delta(G) = (p^{a_r} - 1) - \delta - \left\lfloor \frac{\delta}{p-1} \right\rfloor.$$

Case 3. If $(p-1)p^{a_r-1} \leq \delta \leq \mathsf{d}^*(G) - 1$, then Proposition 4.1 implies that $\Gamma_\delta(G) = 0$, and the proof is complete. □

5. Proof of Theorem 5.2

To start with, we prove the following lemma, which can be seen as a little more general version of Proposition 4.3 in [2].

Lemma 5.1. — *Let G be a finite Abelian p-group and $S = (g_1, \ldots, g_\ell)$ be a zero-sumfree sequence of G with length $|S| \geq \mathsf{d}^*(G) - p + 2$. Then, every element of S has height* 1.

Proof. — Suppose that there exists an element in S, say g_1, verifying $\alpha(g_1) > 1$. Then $\alpha(g_1) \geq p$, and setting $T = S \backslash g_1$, we deduce that:

$$\begin{aligned} \sum_{i=1}^{\ell} \alpha(g_i) &\geq p + |T| \\ &\geq p + (\mathsf{d}^*(G) - p + 1) \\ &= \mathsf{d}^*(G) + 1 \\ &= \mathsf{D}^*(G). \end{aligned}$$

Thus, by Theorem 1.2, S cannot be a zero-sumfree sequence, which is a contradiction. □

We can now prove Theorem 2.8 (*iii*), as a simple corollary of the following stronger theorem.

Theorem 5.2. — *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian p-group. Given a zero-sumfree sequence S of G verifying $|S| \geq \mathsf{d}^*(G) - p + 2$, one has for all $g \in S$:*

$$n_1 \mid \operatorname{ord}_G(g).$$

Proof. — The sequence S, with $|S| \geq \mathsf{d}^*(G) - p + 2$, is a zero-sumfree sequence. Thus, by Lemma 5.1, every element of S has height 1. Let $g = [a_1, \ldots, a_r]$ be an element of S. The equality $\alpha(g) = 1$ implies that there exists $i_0 \in [\![1, r]\!]$ such that p does not divide a_{i_0}. Therefore, one has $\operatorname{ord}_{C_{n_{i_0}}}(a_{i_0}) = n_{i_0}$, and we obtain:

$$\begin{aligned} \operatorname{ord}_G(g) &= \max_{i \in [\![1,r]\!]} \operatorname{ord}_{C_{n_i}}(a_i) \\ &\geq \operatorname{ord}_{C_{n_{i_0}}}(a_{i_0}) \\ &= n_{i_0} \\ &\geq n_1, \end{aligned}$$

which completes the proof. □

6. A concluding remark

Let G be a finite Abelian p-group with rank $r \geq 1$. It would be interesting to find the exact value of $\Gamma_\delta(G)$ for every integer $\delta \in [\![0, \mathsf{d}^*(G) - 1]\!]$. Regarding this problem, we propose the following conjecture, supported by Theorem 2.4, and which states that the upper bound given by Proposition 4.1 is actually the right value for $\Gamma_\delta(G)$.

Conjecture 6.1. — *Let $G \simeq C_{p^{a_1}} \oplus \cdots \oplus C_{p^{a_r}}$, where $p \in \mathcal{P}$, $r \in \mathbb{N}^*$ and $a_1 \leq \cdots \leq a_r$, with $a_i \in \mathbb{N}^*$ for all $i \in [\![1, r]\!]$. Let $\delta \in [\![0, \mathsf{d}^*(G) - 1]\!]$ and $j_0 = \min\{i \in [\![1, r]\!] \mid a_i = a_r\}$. Then, one has:*

$$\Gamma_\delta(G) = \max\left(0, (r - j_0 + 1)\left(p^{a_r} - 1\right) - \delta - f(\delta)\right),$$

where

$$f(\delta) = \min\left(\left\lfloor \frac{\delta}{p-1} \right\rfloor, (r - j_0 + 1)\left(p^{a_r - 1} - 1\right)\right).$$

By our Proposition 2.6, this conjecture holds true in the case where $j_0 = r$. One can also notice that in the special case where $j_0 = 1$, Theorem 5.2 implies that Conjecture 6.1 holds for every $\delta \in [\![0, p - 2]\!]$.

Acknowledgments

I am grateful to my Ph.D. advisor Alain Plagne for his help during the preparation of this paper. I would like also to thank Alfred Geroldinger and Wolfgang Schmid for useful comments on a preliminary version of this article, as well as the Centre de Recerca Matemàtica in Barcelona, where this work was begun.

References

[1] W. Gao and A. Geroldinger *On long minimal zero sequences in finite abelian groups*, Period. Math. Hung. **38**(3) (1999), 179-211.

[2] W. Gao and A. Geroldinger *On the order of elements in long minimal zero-sum sequences*, Period. Math. Hung. **44**(1) (2002), 63-73.

[3] W. Gao and A. Geroldinger *Zero-sum problems in finite abelian groups : a survey*, Expo. Math. **24** (2006), 337-369.

[4] A. Geroldinger *The cross number of finite abelian groups*, J. Number Theory **48** (1994), 219-223.

[5] A. Geroldinger and F. Halter-Koch *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics **278**, Chapman & Hall/CRC (2006).

[6] A. Geroldinger and F. Halter-Koch *Non-unique factorizations : a survey*, Multiplicative ideal theory in commutative algebra, Springer, New York (2006), 207-226.

[7] B. Girard *A new upper bound for the cross number of finite Abelian groups*, Israel J. Math., to appear.

[8] B. Girard *Inverse zero-sum problems and algebraic invariants*, Acta Arith., to appear.

[9] U. Krause *A characterization of algebraic number fields with cyclic class group of prime power order*, Math. Z. **186** (1984), 143-148.

[10] U. Krause and C. Zahlten *Arithmetic in Krull monoids and the cross number of divisor class groups*, Mitt. Math. Ges. Hamburg **12** (1991), 681-696.

[11] W. Narkiewicz *Elementary and analytic theory of algebraic numbers*, 3rd edition, Springer (2004).

[12] J. E. Olson *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8-10.

[13] P. Samuel *Théorie algébrique des nombres*, Hermann (2003).

Benjamin Girard, Centre de Mathématiques Laurent Schwartz, UMR 7640 du CNRS, École polytechnique, 91128 Palaiseau cedex, France. • *E-mail :* `benjamin.girard@math.polytechnique.fr`