Chapitre 3

Ensembles k-libres

Ce chapitre reprend, à peu de choses près et en français, le texte d'un article [4] accepté pour publication dans The Electronic Journal of Combinatorics.

3.1 Introduction

Dans ce chapitre, nous nous intéressons aux ensembles k-libres, que nous pouvons définir dans un monoïde quelconque, même si nous les étudierons ici uniquement dans le cas des entiers naturels et des anneaux $\mathbb{Z}/n\mathbb{Z}$. Tout au long de l'étude, k et n seront des entiers naturels différents de 0. Lorsque nous dirons qu'un ensemble est optimal, cela signifiera qu'il est maximal au sens de la taille (cardinal), à ne pas confondre avec maximal au sens de l'inclusion.

Définition 3.1. Un ensemble A d'un monoïde M est dit k-libre si et seulement si $kx \neq y$ pour tout x, y dans A.

Un ensemble 1-libre étant nécessairement vide, on considèrera maintenant $k \geq 2$. Au-delà de leur propre intérêt, ces ensembles apparaissent naturellement dans l'étude des ensembles k-Sidon ("k-fold Sidon set" en anglais).

Définition 3.2. $A \subset \mathbb{Z}$ est un un ensemble k-Sidon s'il n'admet que les solutions triviales aux équations de la forme $c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 = 0$ où $0 \leqslant |c_i| \leqslant k$, avec les c_i dans $\mathbb{Z}$ et $c_1 + c_2 + c_3 + c_4 = 0$.

Dans cette définition, quitte à réordonner les c_i, on considère que les solutions sont "triviales" dans les cas suivants :

(i) $\{x, x, x, x\}$ est toujours une solution triviale,

(ii) si $c_1 = c_2 = -c_3 = -c_4$, $\{x, y, y, x\}$ est une solution triviale,

(iii) si $c_1 = -c_3$ et $c_2 = -c_4$, $\{x, y, x, y\}$ est une solution triviale.

Ces ensembles ont été introduits par Lazebnik et Verstraëte (voir [3]) dans un travail sur le nombre de Turán généralisé. Remarquons pour commencer qu'un ensemble 1-Sidon est un ensemble de Sidon au sens usuel ($x_1+x_2 = x_3+x_4$ n'admet que les solutions triviales). Si on note $D^*(A) = \{a_1 - a_2, a_1 \neq a_2 \in A\}$, l'ensemble des différences de A privé de 0, un 2-Sidon A est un ensemble de Sidon pour lequel $D^*(A)$ est 2-libre (ou sans double). Plus généralement, si A est un ensemble k-Sidon, $D^*(A)$ est k'-libre, pour tout $1 < k' \leq k$. Bien que cette propriété ne soit pas suffisante en générale pour que A soit un ensemble k-Sidon (pour $k = 3$ par exemple, l'équation $3x_1 = 2x_3 + x_4$ n'admet également que des solutions triviales), c'est en utilisant seulement celle-ci que Cilleruelo et Timons ont prouvé dans [2] que pour tout entier $k \geqslant 1$, un ensemble k-Sidon $A \subset [\![0, n]\!]$ a au plus $(n/k)^{1/2} + O((nk)^{1/4})$ éléments.

On sait seulement que le terme principal $(n/k)^{1/2}$ est optimal pour $k = 1$. En effet, les ensembles de Sidon ont été très largement étudiés (cf. [5]), et on connaît en particulier trois constructions d'ensembles de Sidon maximaux au sens de la taille dans $\mathbb{Z}/n\mathbb{Z}$ pour certains n. Bose et Chowla ont prouvé dans [1] l'existence d'un ensemble de Sidon de cardinal $q + 1$ dans $\mathbb{Z}/\left(q^2 + q + 1\right)\mathbb{Z}$ (ensembles de Singer, voir aussi [7]) et de cardinal q dans $\mathbb{Z}/\left(q^2 - 1\right)\mathbb{Z}$ (ensembles de Bose) où q est une puissance d'un nombre premier. La troisième construction optimale connue a été donnée par Ruzsa dans [6] pour $\mathbb{Z}/\left(p^2 - p\right)\mathbb{Z}$ lorsque p est premier. Pour $k = 2$, si $n = 2^{2^t+1} + 2^t + 1$ avec t un entier positif, on peut extraire (voir [3]) d'un ensemble de Singer un ensemble 2-Sidon dans $\mathbb{Z}/n\mathbb{Z}$ de taille

$$|A| \geqslant \frac{n^{1/2}}{2} - 3.$$

Pour $k \geqslant 3$, on ne sait même pas s'il existe une constante $c_k > 0$ telle que pour tout entier $n \geqslant 1$, il existe un ensemble k-Sidon $A \subset [\![0, n]\!]$ vérifiant $|A| \geqslant c_k n^{1/2}$.

C'est donc en s'intéressant à ces ensembles que nous avons été amenés à étudier les ensembles k-libres. On parlera dans la section 3.2 du cas des entiers naturels, où des résultats étaient déjà connus. Mais pour ces différents problèmes où l'on cherche à optimiser la taille d'un ensemble sous des contraintes arithmétiques, il est important et utile d'étudier le cas des ensembles modulaires $\mathbb{Z}/n\mathbb{Z}$. C'est dans cette optique que l'on va s'intéresser aux ensembles k-libres optimaux dans $\mathbb{Z}/n\mathbb{Z}$, ce dont nous parlerons dans la section 3.3.

3.2 Les ensembles k-libres dans $\mathbb{N}$

Nous appellerons désormais ensemble sans double les ensembles 2-libres. On note

$$r_k(n) = \max\left\{|A|, A \subset [\![1, n]\!], A \text{ ensemble } k\text{-libre}\right\}.$$

Nous verrons à la fin de la section 3.2.1 que rien ne change si on regarde les ensembles k-libres optimaux dans $\mathbb{N}$ tout entier, c'est-à-dire que l'on considère des ensembles infinis cette fois-ci. En effet, les ensembles k-libres optimaux qu'on va construire dans $[\![1, n]\!]$ s'étendent naturellement aux entiers, et la densité maximale obtenue sera donc préservée.

Le premier résultat a été obtenu par Wang en 1989 dans [9] où il a traité le cas des ensembles sans double :

Théorème 3.1 (Wang)**.** *Si n s'écrit $n = a_q 4^q + a_{q-1}4^{q-1} + \cdots + a_1 4 + a_0$ en base 4, alors*

$$r_2(n) = \frac{2n}{3} + \frac{1}{3}\sum_{k=0}^{q} a_k - d$$

où d est le nombre de a_i égaux à 2 ou 3. Cela donne en particulier le résultat asymptotique

$$r_2(n) = \frac{2n}{3} + O(\log_4 n).$$

Wakeham et Wood, dans [8], se sont intéressés à une généralisation des ensembles k-libres, les ensembles $\{a, b\}$-multiplicatifs ($ax \neq by$ pour tous $x, y \in A$), pour lesquels ils ont démontré le résultat suivant :

Théorème 3.2 (Wakeham, Wood)**.** *Soient $b > a \geq 1$ et $g = \mathrm{pgcd}(a, b)$, alors un ensemble $\{a, b\}$-multiplicatif optimal dans $[\![1, n]\!]$ a une densité $\frac{b}{b+g}$.*

Remarque. Le cas des ensembles sans double correspondant à $a = 1$, $b = 2$ et $g = 1$, on retrouve bien le résultat du Théorème 3.1. De plus, le cas des ensembles k-libres est entièrement traité par le théorème précédent ($a = 1$ et $b = k$), et on trouve dans ce cas une densité $\frac{k}{k+1}$ pour un ensemble k-libre optimal. On constate que c'est dans le cas des ensembles sans double ($k = 2$) que les ensembles optimaux sont les moins denses.

Dans la section qui suit, nous allons donner une nouvelle preuve de l'égalité

$$r_k(n) = \frac{k}{k+1}n + O(\log_k^2(n)).$$

Cela va nous permettre d'obtenir une vision adéquate pour traiter ensuite le cas des ensembles modulaires, mais aussi pour donner la taille minimale d'un ensemble k-libre maximal au sens de l'inclusion dans la section 3.2.2.

En effet, on définit

$$\tilde{R}_k(n) = \min\left\{|A|, A \subset [\![1, n]\!] \text{ ensemble } k\text{-libre maximal au sens de l'inclusion}\right\}.$$

Et nous démontrerons le résultat suivant :

Théorème 3.3.

$$\tilde{R}_k(n) = \frac{k^2}{k^2+k+1}n + O(\log_k^2(n)).$$

3.2.1 Ensembles k-libres optimaux

On définit $\mathcal{O}^k(x) := \{k^j x, j \in \mathbb{N}\}$, ce qu'on appellera l'orbite de x (sous-entendu par la multiplication par k). Afin d'étudier les ensembles k-libres dans $[\![1,n]\!]$, on va partitionner les entiers entre 1 et n comme suit :

$$[\![1,n]\!] = \bigsqcup_{i \not\equiv 0 \pmod{k}} \left(\mathcal{O}^k(i) \bigcap [\![1,n]\!]\right).$$

L'intérêt de cette partition est que les orbites que l'on considère ici sont indépendantes pour notre problème au sens où si x appartient à $\mathcal{O}^k(i)$, kx aussi. Ainsi, on se ramène à voir un ensemble k-libre comme un ensemble qui ne possède pas deux éléments consécutifs au sein de chacune de ces orbites.

Maintenant, pour une orbite donnée $\mathcal{O}^k(i)$, un ensemble k-libre optimal contient $\left\lceil \left|\mathcal{O}^k(i)\right| /2 \right\rceil$ éléments. Pour voir cela, il suffit de considérer la parité du cardinal de l'orbite. En sommant ces quantités sur chacune des orbites, nous allons obtenir $r_k(n)$. Cette méthode nous permet en outre de connaître tous les ensembles optimaux possibles.

Si on note $A_i :=]\!]\frac{n}{k^{i+1}}, \frac{n}{k^i}]\!]$, on a

$$[\![1,n]\!] = \bigcup_{i=0}^{d} A_i$$

où $d = [\log_k(n)]$. De plus,

$$|A_i| = \frac{n}{k^i} - \frac{n}{k^{i+1}} + \alpha(i)$$

avec $|\alpha(i)| \leqslant 1$. Et le nombre de $j \not\equiv 0 \pmod{k}$ dans A_i est

$$\left(1 - \frac{1}{k}\right)\left(\frac{n}{k^i} - \frac{n}{k^{i+1}} + \alpha(i)\right) + \epsilon(i)$$

avec $|\epsilon(i)| \leqslant 1$. Chaque élément de A_i a une orbite de taille $i+1$, ce qui nous permet de calculer $r_k(n)$:

$$\begin{aligned} r_k(n) &= \sum_{i=0}^{d} \left\lceil \frac{i+1}{2} \right\rceil \left(\left(1 - \frac{1}{k}\right)\left(\frac{n}{k^i} - \frac{n}{k^{i+1}} + \alpha(i)\right) + \epsilon(i)\right) \\ &= \sum_{i=0}^{d} \left\lceil \frac{i+1}{2} \right\rceil \left(1 - \frac{1}{k}\right)\left(\frac{n}{k^i} - \frac{n}{k^{i+1}}\right) + O(\log_k^2(n)). \end{aligned}$$

En regroupant par deux les termes pour lesquels la partie entière est la même, afin de faire apparaître un comportement télescopique, on obtient :

$$\begin{aligned} r_k(n) &= \left(1-\frac{1}{k}\right)\sum_{i=0}^{\lfloor \frac{d}{2} \rfloor}(i+1)\left(\frac{n}{k^{2i}}-\frac{n}{k^{2i+1}}+\frac{n}{k^{2i+1}}-\frac{n}{k^{2i+2}}\right) \\ &\quad + \beta(n) + O(\log_k^2(n)) \\ &= \left(1-\frac{1}{k}\right)\sum_{i=0}^{\lfloor \frac{d}{2} \rfloor}(i+1)\left(\frac{n}{k^{2i}}-\frac{n}{k^{2i+2}}\right) + \beta(n) + O(\log_k^2(n)) \end{aligned}$$

avec

$$|\beta(n)| \leqslant \left(1-\frac{1}{k}\right)\left(\frac{d}{2}+1\right)\left(\frac{n}{k^d}-\frac{n}{k^{d+1}}\right) = O(\log_k(n)).$$

Finalement,

$$\begin{aligned} r_k(n) &= \left(1-\frac{1}{k}\right)\sum_{i=0}^{\lfloor \frac{d}{2} \rfloor}\frac{n}{k^{2i}} + O(\log_k^2(n)) \\ &= \frac{k}{k+1}n + O(\log_k^2(n)). \end{aligned}$$

Remarque. Si on note $\mathcal{I}_k$ l'ensemble des entiers i qui ne sont pas des multiples de k, l'ensemble

$$B = \bigcup_{l=0}^{+\infty} k^{2l}\mathcal{I}_k$$

où l'union est disjointe, est un ensemble k-libre dans $\mathbb{N}$. En effet, on a cette fois une partition de $\mathbb{N}\setminus\{0\}$ (0 n'est jamais dans un ensemble k-libre) en orbites infinies

$$\mathbb{N}\setminus\{0\} = \bigcup_{i\not\equiv 0 \pmod{k}} \mathcal{O}^k(i)$$

dans lesquelles on prend un élément sur deux, en commençant par le premier. Il s'agit clairement du prolongement des ensembles qu'on a pu considérer auparavant. B est donc un ensemble k-libre optimal dans $\mathbb{N}$, de densité $k/(k+1)$.

3.2.2 Ensembles k-libres maximaux au sens de l'inclusion

En suivant le même schéma, nous allons calculer la taille minimale d'un ensemble k-libre maximal au sens de l'inclusion. En effet, considérant toujours la partition en orbites

$$[\![1,n]\!] = \bigsqcup_{i\not\equiv 0 \pmod{k}} \left(\mathcal{O}^k(i)\bigcap [\![1,n]\!]\right),$$

pour qu'un ensemble B soit maximal au sens de l'inclusion des ensembles k-libres, cela signifie que sur chacune de ces orbites, B ne contient pas deux éléments consécutifs, il n'existe pas trois éléments consécutifs qui ne soient pas dans B (sinon, on pourrait rajouter par exemple le deuxième de ces trois éléments), l'un des deux premiers éléments de l'orbite est dans B et l'un des deux derniers éléments de l'orbite est dans B. Réciproquement, il est clair que si un ensemble vérifie ces quatre propriétés, il est k-libre, et si on lui ajoute un élément, il ne l'est plus.

Essayer de minimiser la taille d'un tel ensemble nous conduit donc immédiatement au problème combinatoire suivant :

Dans $[\![1, j]\!]$, quelle est la taille minimale d'un ensemble E vérifiant les propriétés suivantes $(\mathcal{P})$

- $1 \in E$ ou $2 \in E$
- $j - 1 \in E$ ou $j \in E$
- $i \in E \Rightarrow (i-1) \notin E$ et $(i+1) \notin E$
- $\forall i \in [\![2, j-1]\!], \{i-1, i, i+1\} \cap E \neq \emptyset$

Notons $h(j)$ la taille minimale d'un ensemble vérifiant $(\mathcal{P})$.

Lemme 3.1.

$$h(j) = \left\lceil \frac{j}{3} \right\rceil$$

Démonstration. Déjà, lorsque $j = 3l$, si on prend $B = \{2, 5, \cdots, 2 + 3(l-1)\}$, B vérifie bien $(\mathcal{P})$ et est de taille $l = j/3$. Etant donné qu'on doit prendre au moins un élément parmi $\{3i+1, 3i+2, 3i+3\}, \forall i \in [\![0, l-1]\!]$, $h(j) \geqslant l$. Finalement, on a bien $h(3l) = l$

Si $j = 3l - 1$, on partitionne de la façon suivante

$$[\![1, 3l-1]\!] = \{1, 2\} \bigcup \left(\bigcup_{i \in [\![1, l-1]\!]} \{3i, 3i+1, 3i+2\} \right)$$

Comme on doit avoir au moins un élément dans chacun de ces ensembles, on a $h(3l-1) \geqslant l$. Or $B = \{2, 5, \cdots, 2 + 3(l-1)\}$ fonctionne à nouveau. Donc $h(3l-1) = l$.

Si $j = 3l - 2$, on partitionne de la façon suivante

$$[\![1, 3l-2]\!] = \{1, 2\} \bigcup \left(\bigcup_{i \in [\![1, l-2]\!]} \{3i, 3i+1, 3i+2\} \right) \bigcup \{3l-3, 3l-2\}$$

Comme on doit avoir au moins un élément dans chacun de ces ensembles, on a $h(3l-2) \geqslant l$; Or $B = \{1, 4, \cdots, 1 + 3(l-1)\}$ fonctionne. Donc $h(3l-2) = l$.

□

Nous pouvons désormais prouver le Théorème 3.3 en effectuant des calculs similaires à ceux utilisés pour $r_k(n)$.

Démonstration. Avec $d = [\log_k(n)]$, on aboutit comme précédemment à :

$$\begin{aligned}\tilde{R_k}(n) &= \sum_{i=0}^{d} \left\lceil \frac{i+1}{3} \right\rceil \left(\left(1 - \frac{1}{k}\right) \left(\frac{n}{k^i} - \frac{n}{k^{i+1}} + \alpha(i) \right) + \epsilon(i) \right) \\ &= \sum_{i=0}^{d} \left\lceil \frac{i+1}{3} \right\rceil \left(1 - \frac{1}{k}\right) \left(\frac{n}{k^i} - \frac{n}{k^{i+1}} \right) + O(\log_k^2(n)).\end{aligned}$$

Et en regroupant cette fois-ci les termes par trois, on obtient :

$$\begin{aligned}\tilde{R_k}(n) &= \left(1 - \frac{1}{k}\right) \sum_{i=0}^{\lfloor \frac{d}{3} \rfloor} (i+1) \left(\frac{n}{k^{3i}} - \frac{n}{k^{3i+1}} + \frac{n}{k^{3i+1}} - \frac{n}{k^{3i+2}} + \frac{n}{k^{3i+2}} - \frac{n}{k^{3i+3}} \right) \\ &\quad + \beta(n) + O(\log_k^2(n)) \\ &= \left(1 - \frac{1}{k}\right) \sum_{i=0}^{\lfloor \frac{d}{3} \rfloor} (i+1) \left(\frac{n}{k^{3i}} - \frac{n}{k^{3i+3}} \right) + \beta(n) + O(\log_k^2(n))\end{aligned}$$

avec

$$|\beta(n)| \leqslant \left(1 - \frac{1}{k}\right) \times 2 \left(\frac{d}{3} + 1 \right) \left(\frac{n}{k^{d-1}} - \frac{n}{k^{d+1}} \right) = O(\log_k(n)).$$

Finalement,

$$\begin{aligned}\tilde{R_k}(n) &= \left(1 - \frac{1}{k}\right) \sum_{i=0}^{\lfloor \frac{d}{3} \rfloor} \frac{n}{k^{3i}} + O(\log_k^2(n)) \\ &= \frac{k^2}{k^2 + k + 1} n + O(\log_k^2(n)).\end{aligned}$$

□

3.3 Les ensembles k-libres modulaires

Dans cette partie, nous étudions les ensembles k-libres dans $\mathbb{Z}/n\mathbb{Z}$. Remarquons tout d'abord que cela englobe le cas des ensembles $\{a, b\}$-multiplicatifs dans $\mathbb{Z}/n\mathbb{Z}$ lorsque $\text{pgcd}(a, n) = 1$, puisqu'il s'agit alors d'un ensemble ba^{-1}-libre.

On définit

$$R_k(n) = \max \{ |A|, A \text{ est un ensemble } k\text{-libre dans } \mathbb{Z}/n\mathbb{Z} \}$$

et nous allons voir comment obtenir cette quantité récursivement en n (Théorèmes 3.4, 3.5, 3.6 et 3.7). En outre, comme dans le cas des entiers naturels, les preuves seront constructives.

L'étude de ces ensembles avec la contrainte modulaire dépend fortement des propriétés arithmétiques entre n et k, c'est pourquoi nous présenterons les résultats en quatre théorèmes. Nous commencerons par traiter le cas où k et n sont premiers entre eux, ce qu'on peut d'ailleurs considérer comme le cas le plus important. En effet, comme le précise Cilleruelo et Timmons dans [2], quand on définit un ensemble k-Sidon dans $\mathbb{Z}/n\mathbb{Z}$, on doit ajouter la condition "n est premier avec tous les entiers entre 1 et k". Sinon, on pourrait avoir $c_i(a_1 - a_2) = 0$ avec $a_1 \neq a_2$ pour $|c_i| \leqslant k$, ce qui donnerait une solution non triviale à $c_i(x_1 - x_2) + x_3 - x_4 = 0$ par exemple.

Avant d'énoncer les premiers résultats, introduisons quelques notations. Pour des entiers k et d premiers entre eux, on note $\ell_k(d)$ l'ordre multiplicatif de k dans $(\mathbb{Z}/d\mathbb{Z})^*$. On désignera par I la fonction indicatrice des nombres impairs et par φ la fonction indicatrice d'Euler. On est désormais en mesure de donner le premier théorème.

Théorème 3.4. *Si* $\mathrm{pgcd}(n, k) = 1$,

$$R_k(n) = \frac{n-1}{2} - \sum_{d|n, d\neq 1} \frac{\varphi(d) I(\ell_k(d))}{2\ell_k(d)}.$$

Remarque. En ce qui concerne la borne supérieure pour la taille d'un ensemble 2-Sidon, ce sont les "petits" $R_2(n)$ qui nous intéressent. Dans le cas où $n = 2^m - 1$ est un nombre premier de Mersenne, ce qui implique m premier, alors $\ell_2(n) = m$, et

$$R_2(n) = \frac{n-1}{2} - \frac{n-1}{2\log_2(n+1)}.$$

Ainsi, pour un ensemble 2-Sidon A dans $\mathbb{Z}/n\mathbb{Z}$, comme $D^*(A)$ est un ensemble 2-libre, on a

$$2\binom{|A|}{2} \leq R_2(n),$$

ce qui donne

$$|A| \leqslant \sqrt{\frac{n-1}{2} - \frac{n-1}{2\log_2(n+1)} + \frac{1}{4}} + \frac{1}{2}.$$

En outre, on prouvera dans la section 3.3.1.2 qu'à k fixé, le terme d'erreur est un $o(n)$. Ainsi, $R_k(n) = (n-1)/2 - o(n)$.

Lorsque k divise n, le problème est plus facile et on a les deux résultats suivants :

Théorème 3.5. *Si m n'est pas divisible par k, alors*

$$R_k(km) = (k-1)m.$$

Si k^2 divise n, on obtient une formule récursive :

Théorème 3.6. *Considérons les entiers k, m, et n. On a alors :*

$$R_k(k^2 m) = R_k(m) + \left(k^2 - k\right) m.$$

Remarquons que les trois théorèmes précédents permettent de calculer précisément $R_k(n)$ lorsque k est premier. De plus, rappelons que la densité maximale d'un ensemble k-libre dans $[\![1, n]\!]$ est $k/(k+1)$. Dans le cas modulaire, en appliquant le Théorème 3.6, on obtient

$$R_k(k^{2m}) = \frac{k}{k+1}\left(k^{2m} - 1\right)$$

ce qui conduit à la proposition suivante.

Proposition 3.1. *Soit k un entier, $k \geqslant 1$, on a*

$$\limsup_n \frac{R_k(n)}{n} = \frac{k}{k+1}.$$

Maintenant, pour illustrer les deux théorèmes précédents, appliquons les à un exemple, et calculons $R_{15}(826875)$:

$$\begin{aligned} R_{15}(826875) &= R_{3.5}(3^3.5^4.7^2) \\ &= R_{3.5}(3.5^2.7^2) + (15^2 - 15).3.5^2.7^2 \\ &= (15-1)5.7^2 + (15^2 - 15).3.5^2.7^2 \\ &= 775180. \end{aligned}$$

Nous reviendrons sur cet exemple dans la section 3.3.2.3.

Pour le cas général, nous ne pouvons obtenir une formule satisfaisante, mais nous donnerons un algorithme dans la section 2.4 qui permet de calculer $R_k(n)$.

Théorème 3.7. *Il existe un algorithme qui donne la taille maximale d'un ensemble k-libre dans $\mathbb{Z}/n\mathbb{Z}$ et une méthode pour en construire un en $O((\log(n))^2)$ opérations.*

Cet algorithme et la complexité associée présupposent que l'on connaisse les factorisations en nombre premiers de k et n, qui sont malheureusement difficiles à obtenir en général. Cependant, nous verrons dans la section 3.3.2.3 comment appliquer cet algorithme pour calculer R_k et obtenir une formule explicite pour de nouvelles catégories de k et n. Ce sera l'objet du Théorème 3.8.

3.3.1 Les trois premiers théorèmes

3.3.1.1 Lemmes préparatoires

Introduisons tout d'abord quelques notations utiles pour la suite. Rappelons qu'on note $\mathcal{O}^k(x) := \{k^j x, j \in \mathbb{N}\}$ l'orbite de x (pour la multiplication par k), $\ell_k(d)$ l'ordre multiplicatif de k dans $(\mathbb{Z}/d\mathbb{Z})^*$ et $k \cdot A := \{ka, a \in A\}$, à ne pas confondre avec kA. On définit de plus, pour m diviseur de n, A_m un sous-ensemble de $\mathbb{Z}/n\mathbb{Z}$ par

$$A_m = \{x, \operatorname{pgcd}(x,n) = m\} = \left\{x = mu, \operatorname{pgcd}\left(u, \frac{n}{m}\right) = 1\right\}$$

dont le cardinal vérifie $|A_m| = \varphi(n/m)$.

La partition de $\mathbb{Z}/n\mathbb{Z}$ en l'union des A_m, indexée par les diviseurs de n, nous sera très utile pour l'étude des ensembles k-libres. Il est donc naturel de se demander comment celle-ci se comporte vis-à-vis de la multiplication par k. Le premier lemme permet de décrire $k \cdot A_m$.

Lemme 3.2. *Si la décomposition en facteurs premiers de n s'écrit*

$$n = \prod_{i=1}^{r} p_i^{n_i} \prod_{i=r+1}^{s} p_i^{n_i} \text{ et } k = u \prod_{i=1}^{r} p_i^{k_i}$$

où $\operatorname{pgcd}(u, p_i) = 1, \forall i \in [\![1, s]\!]$, *alors, tout m diviseur de n s'écrit sous la forme*

$$m = \prod_{i=1}^{r} p_i^{m_i} \prod_{i=r+1}^{s} p_i^{m_i}$$

avec $m_i \leqslant n_i, \forall i \in [\![1, s]\!]$, *et nous avons*

$$k \cdot A_m = A_{m'} \text{ où } m' = m \prod_{i=1}^{r} p_i^{\min(k_i, n_i - m_i)}.$$

Démonstration. Soit $x \in A_m$, alors $x = mv$ avec $\operatorname{pgcd}(v, n/m) = 1$. Ainsi, on a

$$\begin{aligned}
\operatorname{pgcd}(kx, n) &= m \operatorname{pgcd}(kv, \frac{n}{m}) \\
&= m \operatorname{pgcd}(k, \frac{n}{m}) \\
&= m \operatorname{pgcd}(\operatorname{pgcd}(k, n), \frac{n}{m}) \\
&= m \operatorname{pgcd}(\prod_{i=1}^{r} p_i^{k_i}, \prod_{i=1}^{r} p_i^{n_i - m_i} \prod_{i=r+1}^{s} p_i^{n_i - m_i}).
\end{aligned}$$

On obtient ainsi $k \cdot A_m \subset A_{m'}$.

Réciproquement, on sait maintenant qu'il existe $y \in A_{m'}$ tel que $y = kx$ et $x \in A_m$ (puisque $A_m \neq \emptyset$). Mais pour tout z dans $A_{m'}$, il existe w vérifiant $\text{pgcd}(w, n) = 1$ et $z = wy$. Il est clair que xw appartient à A_m et $z = kxw$, ce qui conclut la preuve. □

Maintenant, nous déterminons dans le lemme suivant la taille de l'orbite d'un élément dans un cas qui nous intéressera par la suite.

Lemme 3.3. *Soient m un diviseur de n, et k un entier tel que* $\text{pgcd}(k, n/m) = 1$ *et $x \in A_m$. Alors*

$$\left|\mathcal{O}^k(x)\right| = \ell_k\left(\frac{n}{m}\right).$$

Démonstration. Comme $x \in A_m$, si on note $< x >$ le sous-groupe engendré par x, on a

$$< x > \cong \mathbb{Z}/\left(\frac{n}{m}\right)\mathbb{Z}.$$

Mais puisque k est inversible dans ce sous-groupe

$$\mathcal{O}^k(x) \cong \mathcal{O}^k(1) =< k > \subset \mathbb{Z}/\left(\frac{n}{m}\right)\mathbb{Z}$$

et la taille de $< k >$ dans ce sous-groupe est exactement $\ell_k(n/m)$.

□

3.3.1.2 Preuves des Théorèmes 3.4, 3.5 et 3.6

Commençons par le Théorème 3.4, le cas $\text{pgcd}(n, k) = 1$.

Démonstration. Rappelons que I désigne la fonction indicatrice des nombres impairs.

Considérons la partition

$$(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\} = \bigsqcup_{m|n, m<n} A_m.$$

Dans le cas où n est premier, cette partition est triviale.

D'après le Lemme 3.2, $\mathcal{O}^k(x) \subset A_m$, pour tout x dans A_m, puisque les k_i sont nuls dans ce cas précis. De plus, par le Lemme 3.3, si $x \in A_m$, on a

$$\left|\mathcal{O}^k(x)\right| = \ell_k\left(\frac{n}{m}\right).$$

Ainsi, on peut partitionner A_m en $\varphi(n/m)/\ell_k(n/m)$ orbites distinctes de longueur $\ell_k(n/m)$. Et ces orbites sont naturellement indépendantes du point de vue de la multiplication par k. Maintenant, au sein de chacune de ces orbites, pour obtenir

un ensemble k-libre optimal, nous devons prendre le plus d'éléments possibles sans qu'il y ait d'éléments consécutifs. Le raisonnement est similaire à ce qu'on a vu dans le cas des entiers naturels, mais ici, les orbites sont cycliques, c'est pourquoi lorsque la longueur l d'une orbite est paire, on peut prendre jusqu'à $l/2$ éléments, tandis que lorsque l est impaire, il y en a au plus $(l-1)/2$. Cela nous conduit à la formule

$$\begin{aligned} R_k(n) &= \sum_{d|n, d\neq 1} \frac{\varphi(d)}{\ell_k(d)} \left(\frac{\ell_k(d) - I(\ell_k(d))}{2} \right) \\ &= \frac{n-1}{2} - \sum_{d|n, d\neq 1} \frac{\varphi(d) I(\ell_k(d))}{2\ell_k(d)}. \end{aligned}$$

□

Analysons maintenant le terme d'erreur. À k fixé, on a l'asymptotique

$$R_k(n) = (n-1)/2 - o(n).$$

En effet, pour tout $\varepsilon > 0$, il existe d_0 tel que $\log_k d_0 \geqslant 1/\varepsilon$ et il existe n vérifiant $d_0^2/6 \leqslant \varepsilon n/2$. Ainsi,

$$\begin{aligned} \sum_{d|n, d\neq 1} \frac{\varphi(d) I(\ell_k(d))}{2\ell_k(d)} &= \sum_{d|n, d\neq 1, d\leqslant d_0} \frac{\varphi(d) I(\ell_k(d))}{2\ell_k(d)} + \sum_{d|n, d\neq 1, d> d_0} \frac{\varphi(d) I(\ell_k(d))}{2\ell_k(d)} \\ &\leqslant \sum_{d|n, d\neq 1, d\leqslant d_0} \frac{\varphi(d)}{6} + \sum_{d|n, d\neq 1, d> d_0} \frac{\varphi(d)}{2 log_k d} \\ &\leqslant \frac{d_0^2}{6} + \frac{\varepsilon n}{2} \\ &\leqslant \varepsilon n. \end{aligned}$$

Considérons maintenant le cas $n = k^2 m$, pour lequel on va utiliser la partition suivante de $\mathbb{Z}/n\mathbb{Z}$:

Lemme 3.4. *Pour $n = k^2 m$, on a*

$$\mathbb{Z}/n\mathbb{Z} = \left(k^2\mathbb{Z}/n\mathbb{Z}\right) \bigsqcup \left(\bigcup_{h\not\equiv 0 \pmod{k}} \{h, kh\} \right)$$

où la première union est disjointe.

Démonstration. En effet, si $x \not\equiv 0 \pmod{k^2}$ et $x \equiv 0 \pmod{k}$, alors $x = kh$ avec $h \not\equiv 0 \pmod{k}$. Ainsi, nous retrouvons bien tous les éléments dans cette union. De plus, si on a $h \not\equiv 0 \pmod{k}$, alors $kh \not\equiv 0 \pmod{k^2}$, ce qui montre que cette union est bien disjointe. □

Voyons maintenant en quoi c'est une bonne répartition des éléments pour notre problème, à travers la preuve du Théorème 3.6 :

Démonstration. Remarquons deux choses :
- $k^2\mathbb{Z}/n\mathbb{Z}$ est stable pour la multiplication par k.
- Si $h \not\equiv 0 \pmod{k}$, on ne peut pas écrire $h = ku$ dans $k^2\mathbb{Z}/n\mathbb{Z}$.

Soit alors A un ensemble k-libre dans $\mathbb{Z}/n\mathbb{Z}$. Premièrement, pour chaque $h \not\equiv 0 \pmod{k}$, au plus un élément de $\{h, kh\}$ est dans A. En outre, par la première remarque, $A \cap k^2\mathbb{Z}/n\mathbb{Z}$ est aussi un ensemble k-libre, ce qu'on peut voir comme un ensemble k-libre dans $\mathbb{Z}/m\mathbb{Z}$. Cela conduit à

$$R_k(k^2m) \leqslant R_k(m) + |\{h \not\equiv 0 \pmod{k}\}| = R_k(m) + \left(k^2 - k\right) m.$$

Construisons désormais un ensemble k-libre optimal. D'après la deuxième remarque, on peut prendre tout $h \not\equiv 0 \pmod{k}$ dans A, et on sait alors que $kh \notin k^2\mathbb{Z}/n\mathbb{Z}$, alors on peut prendre $R_k(m)$ éléments de $k^2\mathbb{Z}/n\mathbb{Z}$ dans A. Ainsi, on a

$$R_k(k^2m) = R_k(m) + \left(k^2 - k\right) m$$

ce qui conclut la preuve.

□

Finalement, venons-en au cas $n = km$ avec $m \not\equiv 0 \pmod{k}$. Dans ce cas, on a :

Lemme 3.5. *Si $n = km$ avec $m \not\equiv 0 \pmod{k}$,*

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{h \not\equiv 0 \pmod{k}} \{h, kh\}.$$

Démonstration. Si $x \equiv 0 \pmod{k}$, il existe u tel que $x = ku$. Si $u \not\equiv 0 \pmod{k}$, x est de la forme souhaitée. Sinon, $u \equiv 0 \pmod{k}$, alors il existe v, $u = kv$ et nous avons $x = x + n = x + km = k^2v + km$. Mais $m \not\equiv 0 \pmod{k}$ par hypothèse, alors on peut écrire $m = lk + a$ avec $a \not\equiv 0 \pmod{k}$, ce qui donne

$$x + km = k(kv + lk + a).$$

Comme $h = kv + lk + a \not\equiv 0 \pmod{k}$, on est parvenu à écrire $x = x + km = kh$ avec $h \not\equiv 0 \pmod{k}$, ce qui conclut le lemme. □

On peut maintenant facilement prouver le Théorème 3.5.

Démonstration. Si A est un ensemble k-libre, pour chaque $h \not\equiv 0 \pmod{k}$, au plus un élément de $\{h, kh\}$ est dans A, et donc $|A| \leqslant (k-1)m$. Si $h \not\equiv 0 \pmod{k}$, on ne peut pas écrire $h = ku$ dans $\mathbb{Z}/n\mathbb{Z}$ étant donné que $n = km$. Ainsi $\{h \not\equiv 0 \pmod{k}\}$ est un ensemble k-libre et on a bien

$$R_k(km) = (k-1)m.$$

□

3.3.2 Dans le cas général

La situation dans le cas général est nettement plus complexe. En effet, contrairement à ce qui se passe dans le cadre du Théorème 3.4, l'orbite d'un élement n'est pas nécessairement incluse dans un A_m. Il va falloir gérer le fait qu'on passe d'un A_m à un autre en multipliant les éléments par k. Pour cela, notre stratégie sera de créer un graphe qui aura pour sommets les diviseurs de n et qui seront reliés si $k \cdot A_m = A_{m'}$ lorsque $m \neq m'$. Il nous faudra cependant traiter à part les m tels que $k \cdot A_m = A_m$. Il s'agira en fait des racines de notre graphe (une fois qu'on l'aura interprété comme une forêt). Une fois cela fait, on aura envie de prendre certains A_m sans qu'aucun ne soit relié, et de façon à maximiser le cardinal de notre ensemble k-libre. C'est pourquoi nous allons avoir besoin d'un résultat sur les arbres enracinés dont les sommets sont pondérés. C'est l'objet de la section suivante.

3.3.2.1 Un algorithme sur les arbres enracinés

Soit T un arbre enraciné dont l'ensemble des noeuds est $V = \{v_i\}_{i \in I}$ où I est un ensemble fini et E est l'ensemble des arêtes. On associe une valeur $\alpha_i \geqslant 0$ à chaque noeud v_i et on note l_i son niveau (autrement appelé hauteur ou profondeur). Rappelons que le niveau d'un noeud est égal au nombre de noeuds à partir de la racine (en comptant la racine) pour aller jusqu'au noeud. On peut le définir de manière équivalente comme étant 1+ le nombre minimal d'arêtes entre le noeud et la racine. Supposons que T a la propriété suivante :

$$\text{Si } v_i \text{ est le parent de } v_j, \text{ alors } \alpha_i < \alpha_j. \tag{3.1}$$

En d'autres mots, α croît strictement sur chaque branche. On remarque que cette condition implique que si v_i n'est pas la racine de T, $\alpha_i > 0$. Nous recherchons un sous-ensemble A de I satisfaisant :

$$\forall (i,j) \in A^2, (v_i, v_j) \notin E \text{ et } \alpha_i \neq 0 \tag{3.2}$$

qui maximise la quantité

$$\Lambda_A = \sum_{i \in A} \alpha_i.$$

Notons l la profondeur maximum de T et construisons un ensemble B de la façon suivante :
Initialisation : $B = \{v_i | l_i = l\}$.
Ensuite, pour k allant de 1 à $l-1$: pour tout i tel que $l_i = l - k$, on ajoute v_i à B si et seulement $\alpha_i \neq 0$ et v_i n'a pas d'enfant dans B.

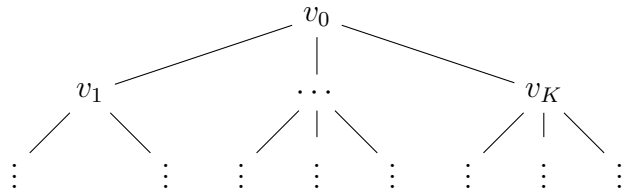
Il est clair que B satisfait (3.2). En fait, on va voir que B est l'ensemble recherché.

Lemme 3.6. *B est l'unique sous-ensemble de I maximisant Λ_A parmi les ensembles A satisfaisant (3.2).*

Démonstration. Procédons par récurrence sur la taille de I. Si $|I| = 1$, il n'y a rien à faire.

Soit n un entier et supposons que le lemme est vrai pour k plus petit que n. Supposons $|I| = n + 1$. Soient B l'ensemble provenant de l'algorithme expliqué ci-dessus, appliqué à T, et C un sous-ensemble de I maximisant Λ_A parmi les ensembles A satisfaisant (3.2). On veut montrer que $B = C$.

Notons v_0 la racine de T, et v_i, pour $i \in [\![1, K]\!]$, les enfants de v_0. On définit également, pour tout i dans $[\![1, K]\!]$, T_i le sous-arbre (enraciné) de T qui a pour racine v_i, $B_i = B \cap T_i$ et $C_i = C \cap T_i$. On pourra éventuellement mieux visualiser ces ensembles en s'appuyant sur le schéma ci-dessous, où T_1 est par exemple le sous-arbre (à gauche) issu de v_1.



Ce qui est intéressant dans cet algorithme, c'est que si on l'applique à T_i, on obtient l'ensemble B_i. Cela vient du fait que l'algorithme a pour point de départ les éléments de profondeur maximale dans l'arbre. Ainsi, d'après l'hypothèse de récurrence, on a pour tout i, $\Lambda_{C_i} \leqslant \Lambda_{B_i}$ avec égalité si et seulement si $B_i = C_i$.

Si $v_0 \in B$ et $v_0 \in C$, on a

$$\Lambda_C - \alpha_0 = \sum_{i=1}^{K} \Lambda_{C_i} \leqslant \sum_{i=1}^{K} \Lambda_{B_i} = \Lambda_B - \alpha_0.$$

Ainsi, par définition de C, il s'agit d'une égalité, et on a finalement $B = C$.

Si $v_0 \notin B$ et $v_0 \notin C$, on a

$$\Lambda_C = \sum_{i=1}^{K} \Lambda_{C_i} \leqslant \sum_{i=1}^{K} \Lambda_{B_i} = \Lambda_B$$

ce qui assure $B = C$ pour la même raison.

Si $v_0 \in B$ et $v_0 \notin C$, comme $\alpha_0 > 0$ (autrement, v_0 n'est pas dans B d'après l'algorithme), on a

$$\Lambda_C = \sum_{i=1}^{K} \Lambda_{C_i} \leqslant \sum_{i=1}^{K} \Lambda_{B_i} = \Lambda_B - \alpha_0 < \Lambda_B$$

ce qui conduit à une contradiction.

Si $v_0 \notin B$ et $v_0 \in C$, $\alpha_0 > 0$ (comme C satisfait (3.2)) et cela signifie qu'il existe i_0 dans $[\![1, K]\!]$ tel que $v_{i_0} \in B$. Considérons alors la branche issue de v_0 qui contient v_{i_0}. Si $K > 1$, elle contient strictement moins de $n+1$ noeuds et on peut alors appliquer l'hypothèse de récurrence pour obtenir $\Lambda_{C_{i_0}} + \alpha_0 < \Lambda_{B_{i_0}}$. Ainsi,

$$\Lambda_C = \sum_{i \neq i_0} \Lambda_{C_i} + \Lambda_{C_{i_0}} + \alpha_0 < \sum_{i \neq i_0} \Lambda_{B_i} + \Lambda_{B_{i_0}} = \Lambda_B$$

et on a une contradiction. Si $K = 1$, notons v_1 l'unique enfant de v_0. On a $v_1 \in B$ et $v_1 \notin C$. En considérant maintenant n'importe quel sous-arbre enraciné en les enfants de v_1, on a (avec des notations évidentes) :

$$\Lambda_C = \sum \Lambda_{C'_i} + \alpha_0 < \sum \Lambda_{B'_i} + \alpha_1 = \Lambda_B$$

puisque $\alpha_1 > \alpha_0$. Cela fournit à nouveau une contradiction.

Finalement, dans chacun de ces cas, on obtient $B = C$. Le lemme est alors prouvé.

□

Nous allons maintenant voir comment on se ramène à un arbre de ce type pour notre problème.

3.3.2.2 L'algorithmique du cas général

L'objectif est de définir une forêt (une union disjointe d'arbres enracinés) satisfaisant (3.1) et telle que l'algorithme du paragraphe précédent conduise à un ensemble k-libre optimal.

Définissons le graphe $G = (V, E)$ par l'ensemble de ses sommets $V = \{m\}_{m|n}$ et de ses arêtes E :

$$(m, m') \in E \text{ si et seulement si } m < m' \text{ et } k \cdot A_m = A_{m'}. \tag{3.3}$$

Essayons de bien comprendre ce graphe avant d'assigner des valeurs aux différents sommets qui nous permettront de résoudre le problème. On écrit

$$n = \prod_{i=1}^{r} p_i^{n_i} \prod_{i=r+1}^{s} p_i^{n_i} \text{ et } k = u \prod_{i=1}^{r} p_i^{k_i}$$

avec $\text{pgcd}(u, p_i) = 1, \forall i \in [\![1, s]\!]$ et $k_i > 0$ pour tout i. Notons $\mathcal{M}$ l'ensemble des diviseurs de n de la forme

$$m = \prod_{i=1}^{s} p_i^{m_i}$$

avec $m_i \leqslant n_i, \forall i \in [\![1, s]\!]$, et tel qu'il existe $i_0 \leqslant r$ vérifiant $m_{i_0} < \min(k_{i_0}, n_{i_0})$. La proposition suivante donne la structure de G.

Proposition 3.2. *G est une union disjointe d'arbres enracinés. En outre :*

(i) Une composante connexe de G est entièrement déterminée par le choix de $\{d_i\}_{i=r+1}^{s}$ avec $d_i \leqslant n_i$.

(ii) Les feuilles sont exactement les éléments de $\mathcal{M}$.

(iii) La racine de l'arbre défini par $\{d_i\}_{i=r+1}^{s}$ est

$$m = \prod_{i=1}^{r} p_i^{n_i} \prod_{i=r+1}^{s} p_i^{d_i}.$$

(iv) La profondeur de m est $j_m + 1$ où

$$j_m = \min \{j | jk_i \geqslant n_i - m_i, \forall i \in [\![1, r]\!]\}.$$

Démonstration. On définit

$$k^j * m = m \prod_{i=1}^{r} p_i^{\min(jk_i, n_i - m_i)}.$$

D'après le Lemme 3.2, $A_{k*m} = k \cdot A_m$, donc si (m, m') est une arête, on a $m_i = m'_i$ pour tout i dans $[\![r+1, s]\!]$. Ainsi, s'il existe un chemin entre deux sommets, ils ont les mêmes $\{d_i\}_{i=r+1}^{s}$. La réciproque, pour le premier point, sera démontrée à la fin de cette preuve.

Dans le lemme suivant, on montre qu'un sommet est ou bien dans $\mathcal{M}$ ou bien est un ancêtre d'un élément de $\mathcal{M}$.

Lemme 3.7. *Soit $m' = \prod_{i=1}^{s} p_i^{m'_i}$ un diviseur de n qui n'est pas dans $\mathcal{M}$, alors il existe $t > 0$ et m dans $\mathcal{M}$ tel que $m' = k^t * m$.*

Démonstration. Soit t defini par

$$t = \min\left\{j | \exists i_0 \leqslant r, m'_{i_0} - jk_{i_0} < \min(k_{i_0}, n_{i_0})\right\}$$

et introduisons $\alpha_i = \max(0, m'_i - tk_i)$ et

$$m = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{i=r+1}^{s} p_i^{m'_i}$$

qui appartient à $\mathcal{M}$ par définition de t. Remarquons que $t > 0$ puisque $m' \notin \mathcal{M}$. On a alors

$$\begin{aligned} k^t * m &= m \prod_{i=1}^{r} p_i^{\min(tk_i, n_i - m_i)} \\ &= \prod_{i=1}^{r} p_i^{\alpha_i + \min(tk_i, n_i - \alpha_i)} \prod_{i=r+1}^{s} p_i^{m'_i}. \end{aligned}$$

Nous devons étudier trois cas :

- $\alpha_i = 0$ et $k_i < n_i$: $m'_i \geqslant k_i$ car $m' \notin M$, alors $m'_i = tk_i$ par définition de t et on obtient dans ce cas $\alpha_i + \min(tk_i, n_i - \alpha_i) = m'_i$.
- $\alpha_i = 0$ et $n_i \leqslant k_i$: $m'_i = n_i$ car $m' \notin M$ et on a $\alpha_i + \min(tk_i, n_i - \alpha_i) = n_i = m'_i$.
- Sinon, $n_i - \alpha_i = n_i - m'_i + tk_i \geqslant tk_i$, donc $\alpha_i + \min(tk_i, n_i - \alpha_i) = m'_i$.

On obtient $k^t * m = m'$, ce qui était attendu. □

Réciproquement, si $m \in M$ et $t > 0$, $k^t * m \notin M$, donc les éléments de $\mathcal{M}$ n'ont pas d'enfant. De plus, si on regarde

$$m = \prod_{i=1}^{r} p_i^{n_i} \prod_{i=r+1}^{s} p_i^{d_i}$$

il est clair que $k * m = m$, donc m n'a pas de parent, et il s'agit bien d'un racine. Finalement, pour montrer le dernier point et la réciproque du premier point, si m' a les mêmes $\{d_i\}_{i=r+1}^{s}$, on a $k^{j_m} * m' = m$ et $k^{j_m - 1} * m' \neq m$ par définition de j_m.

On a bien obtenu les quatre conclusions de la proposition.

□

Voyons maintenant quelles valeurs donner aux sommets (ou noeuds). On a construit ce graphe de telle sorte qu'un noeud différent de la racine est envoyé sur son parent via la multiplication par k (si on identifie le noeud m à l'ensemble A_m). Il nous faut alors regarder ce qu'il se passe pour les racines du graphe, c'est-à-dire les m satisfaisant $k \cdot A_m = A_m$. Le lemme suivant donne la taille maximale d'un ensemble k-libre inclus dans A_m où m est une racine du graphe.

Lemme 3.8. *Si m est une racine du graphe G (ce qui est équivalent à dire* $\mathrm{pgcd}(k, n/m) = 1$*), la taille maximale d'un ensemble k-libre inclus dans A_m est*

$$R_k(A_m) = \frac{\varphi(n/m)}{\ell_k(n/m)} \left(\frac{\ell_k(n/m) - I(\ell_k(n/m))}{2} \right).$$

Démonstration. On a un isomorphisme :

$$A_m \cong A'_1 = \left\{ x \in \mathbb{Z}/(n/m)\mathbb{Z}, \mathrm{pgcd}(x, \frac{n}{m}) = 1 \right\}.$$

Comme on est dans le cas $\mathrm{pgcd}(k, n/m) = 1$, si on procède comme dans la preuve du Théorème 3.4, on a alors immédiatement le résultat.

□

Ainsi, on va assigner les valeurs aux noeuds m comme suit :

$$\alpha_m = \begin{cases} R_k(A_m) \text{ si } m \text{ est une racine} \\ \varphi\left(\dfrac{n}{m}\right) \text{ sinon.} \end{cases}$$

Remarquons que G vérifie la propriété (3.1), que nous rappelons ici :

$$\text{Si } v_i \text{ est le parent de } v_j, \text{ alors } \alpha_i < \alpha_j.$$

En appliquant l'algorithme de la section 3.3.2.1, un obtient un ensemble de noeuds de G, que l'on va noter B. Afin de construire un ensemble k-libre, on va prendre l'union des A_m pour m dans B qui n'est pas une racine de G, et pour les racines m qui sont dans B on ajoute K_m un ensemble k-libre optimal inclus dans A_m. Plus précisément, on définit

$$\overline{B} := \left(\bigsqcup_{\substack{m \in B \\ \mathrm{pgcd}(k,n/m) \neq 1}} A_m \right) \bigsqcup \left(\bigsqcup_{\substack{m \in B \\ \mathrm{pgcd}(k,n/m) = 1}} K_m \right)$$

qui est clairement un ensemble k-libre car B vérifie (3.2) et par définition de K_m.

Voyons maintenant pourquoi cet ensemble est celui que l'on recherche.

Proposition 3.3. *$\overline{B}$ est un ensemble k-libre optimal dans $\mathbb{Z}/n\mathbb{Z}$ et a un cardinal*

$$\sum_{\substack{m \in B \\ \mathrm{pgcd}(k,n/m) \neq 1}} \varphi\left(\frac{n}{m}\right) + \sum_{\substack{m \in B \\ \mathrm{pgcd}(k,n/m) = 1}} R_k(A_m).$$

Démonstration. Supposons que C est un ensemble k-libre optimal de $\mathbb{Z}/n\mathbb{Z}$ vérifiant $|C| > \left|\overline{B}\right|$. Soient alors x un élément de $C\backslash\overline{B}$ que l'on prend de profondeur t maximale parmi de tels éléments, m le diviseur de n tel que $x \in A_m$ et T_i la composante connexe de G (ou l'arbre enraciné) contenant m.

Premier cas : $t = 1$ et $m \notin B$. Ainsi, m est une racine qui n'est pas dans B, ce qui signifie qu'il existe m' un enfant de m dans B (autrement $\alpha_m = R_k(A_m) = 0$ et C ne serait pas un ensemble k-libre). Or, l'ensemble $k^{-1}(x) = \{y \in A_{m'} | y = kx\}$ n'a aucun élément dans C mais a un cardinal

$$\left|k^{-1}(x)\right| = \frac{\varphi(n/m')}{\varphi(n/m)} > 1.$$

Ainsi, en remplaçant, dans C, $\{x\}$ par $k^{-1}(x)$, on obtient toujours un ensemble k-libre. En effet, comme t est la profondeur maximale d'un élément de $C\backslash\overline{B}$, aucun élément de C n'est dans un A_{m_0} avec m_0 un enfant de m' (puisque m' est dans B). L'ensemble k-libre que l'on obtient ainsi est de taille strictement plus grande que C, ce qui fournit une contradiction.

Deuxième cas : $t > 1$. Par construction de $\overline{B}$, m n'appartient pas à B et on peut procéder exactement comme dans le cas précédent.

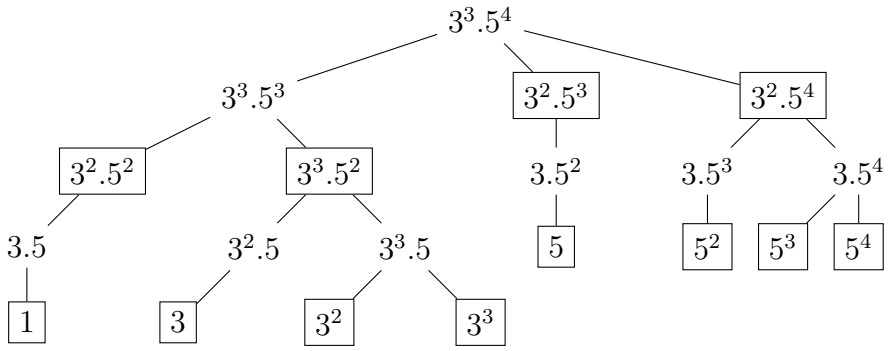
Ces deux cas menant à une contradiction, tout élément x de $C\backslash\overline{B}$ satisfait $t = 1$ et m appartient à B. Ainsi, m est une racine et on peut remplacer $C \cap A_m$ par K_m pour toutes les racines, ce qui nous donne $|C| \leqslant \left|\overline{B}\right|$. Le calcul de la taille de $\overline{B}$ est pour sa part immédiat.

□

Ainsi, pour obtenir $R_k(n)$, dans le cas où les factorisations en nombres premiers de k et n sont connues, on doit construire G ($O(\log(n))$ opérations), lui appliquer l'algorithme ($O(\log(n))$ opérations), calculer α_m pour les m dans B ($O((\log(n))^2)$ opérations puisque nous connaissons la factorisation de m) et finalement ajouter ces différentes contributions.

3.3.2.3 Illustrations de l'algorithme

Commençons par illustrer cette méthode sur l'exemple que nous avons déjà considéré au début de la partie 3.3, $n = 3^3.5^4.7^2 = 826875$ et $k = 3.5 = 15$. Dans ce cas, nous obtenons une forêt à trois arbres, de racines $3^3.5^4$, $3^3.5^4.7$ a $3^3.5^4.7^2$. On représente le premier ci-dessous. Pour obtenir le deuxième, on doit multiplier chaque noeud par 7, et pour le troisième, par 7^2. En appliquant l'algorithme, on obtient un ensemble de noeuds que l'on a encadré :



Pour obtenir la taille d'un ensemble 15-libre optimal dans $\mathbb{Z}/826875\mathbb{Z}$, nous devons alors sommer les $\varphi(n/m)$ pour les m choisis par l'algorithme dans chaque arbre. Et nous retrouvons le résultat $R_{15}(826875) = 775180$ que nous avions précédemment déduit des Théorèmes 3.5 et 3.6.

Cette façon de calculer $R_k(n)$ ne donne pas une formule générale, c'est pourquoi nous étudions dans le théorème suivant trois nouveaux cas particuliers.

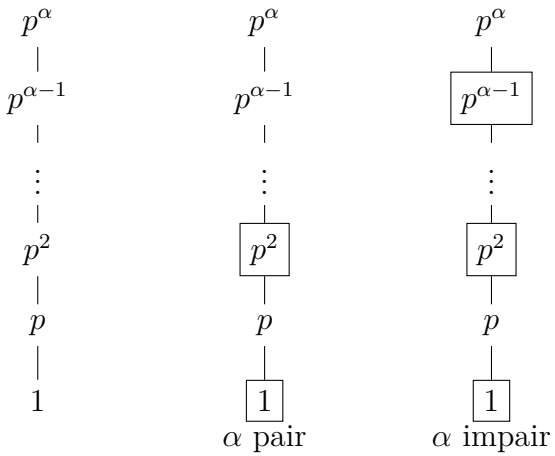
Théorème 3.8. *Soient p et q des nombres premiers, α, β et u des entiers.*

1. *Si* $\mathrm{pgcd}(u,p) = 1$,
$$R_{up}(p^\alpha) = \sum_{i=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \varphi(p^{\alpha-2i}).$$

2. *Si* $\mathrm{pgcd}(u,p) = 1$,
$$R_{up^2}(p^\alpha) = \sum_{i=0}^{\lfloor \frac{\alpha-1}{4} \rfloor} \left(\varphi(p^{\alpha-4i}) + \varphi(p^{\alpha-4i-1})\right).$$

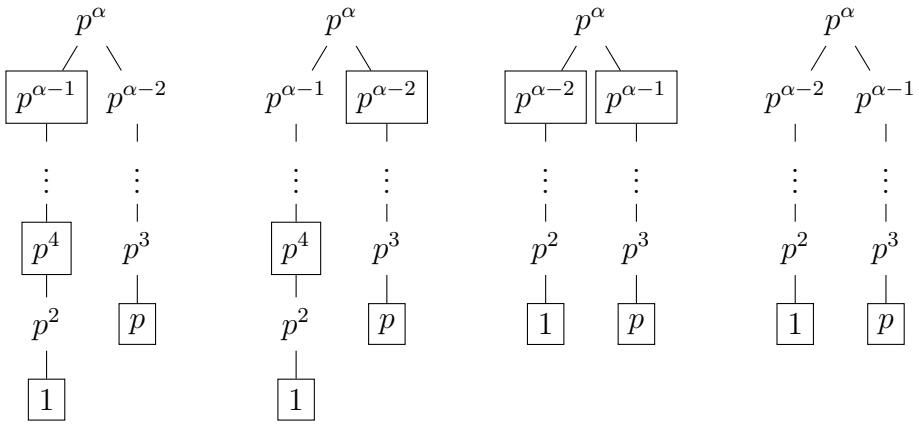
3. *Si* $\mathrm{pgcd}(u,p) = \mathrm{pgcd}(u,q) = 1$,
$$R_{up}(p^\alpha q^\beta) = \sum_{j=0}^{\beta} \sum_{i=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \varphi(p^{\alpha-2i} q^{\beta-j})$$
$$R_{up^2}(p^\alpha q^\beta) = \sum_{j=0}^{\beta} \sum_{i=0}^{\lfloor \frac{\alpha-1}{4} \rfloor} \left(\varphi(p^{\alpha-4i} q^{\beta-j}) + \varphi(p^{\alpha-4i-1} q^{\beta-j})\right).$$

Démonstration. 1. Le premier graphe qui suit est celui qu'on obtient dans ce cas particulier ($n = p^\alpha$, $k = up$ avec $\mathrm{pgcd}(u,p) = 1$), et où on a là aussi encadré l'ensemble des noeuds issus de l'algorithme. Le deuxième graphe correspond à α pair et le troisième à α impair :



Comme $A_{p^\alpha} = \{0\}$, $R_{up}(p^\alpha) = 0$, c'est pourquoi p^α n'est jamais considéré par l'algorithme. En appliquant la Proposition 3.3, on obtient le résultat.

2. On donne ci-dessous le graphe issu de l'algorithme ($n = p^\alpha$, $k = up^2$ avec $\text{pgcd}(u, p) = 1$), qui dépend de la valeur de α modulo 4 (on utilise aussi $R_{up^2}(p^\alpha) = 0$) :



Et on calcule $R_k(n)$ à nouveau grâce à la Proposition 3.3.

3. Si $k = up$ et $n = p^\alpha q^\beta$ où $\text{pgcd}(u, p) = gcd(u, q) = 1$, on obtient une forêt de $\beta + 1$ arbres $(T_j)_{j=0\cdots\beta}$ où T_j est représenté ci-dessous :

$$
\begin{array}{c}
p^\alpha q^j \\
| \\
p^{\alpha-1} q^j \\
| \\
\vdots \\
| \\
p^2 q^j \\
| \\
p q^j \\
| \\
q^j
\end{array}
$$

On obtient alors la taille d'un ensemble k-libre optimal sur T_j (sous-entendu inclus dans l'union des A_m, où m parcourt les noeuds de T_j) :

$$\sum_{i=0}^{\lfloor \frac{\alpha-1}{2} \rfloor} \varphi(p^{\alpha-2i} q^{\beta-j}).$$

Le résultat provient ensuite de l'addition des contributions de chaque T_j.
Pour $k = up^2$, il s'agit d'une conséquence du deuxième cas.

□

De la même manière, on pourrait évidemment aller plus loin et étudier les cas $k = up^3$ ou $n = p^\alpha q^\beta r^\gamma$ par exemple, mais cela donnerait des formules de moins en moins agréables.

Bibliographie

[1] R. C. Bose, S. Chowla, *Theorems in the additive theory of numbers* , Commentarii Mathematici Helvetici, 37, 141-147, 1962/1963.

[2] J. Cilleruelo and C. Timmons, *k-fold Sidon sets*, Electronic Journal of Combinatorics, 4, 2014, 9pp.

[3] F. Lazebnik, J. Verstraëte, *On hypergraphs of girth five*, Electronic Journal of Combinatorics, 10, 2003, #R25, 9pp.

[4] V. Lambert, *On modular k-free sets*, Electronic Journal of Combinatorics, 22, 2015, 18pp.

[5] K. O'Bryant, *A complete annotated bibliography of work related to Sidon sequences*, Electronic Journal of Combinatorics, DS 11, 2004, 39pp.

[6] I. Ruzsa, *Solving a linear equation in a set of integers I*, Acta Arithmetica, 65, 259-282, 1993.

[7] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Transactions of the American Mathematical Society 43, 377-385, 1938.

[8] D. Wakeham and D.R.Wood, *On Multiplicative Sidon Sets*, Integers 13, Paper No. A26, 2013.

[9] E.T.H. Wang, *On Double-Free Sets of Integers*, Ars Combinatoria, 28, 97-100, 1989.