Théorème de réorganisation

1 Introduction

J'ai écrit cette preuve à la suite du post de jongle.net suivant :
`http://www.jongle.net/modules.php?name=Forums&file=viewtopic&p=284130`.

C'est une preuve un peu plus « à la matheux » du théorème de réorganisation de siteswaps. Peut-être qu'avec ça on voit un peu mieux ce qui se passe. Pour ma part non, j'ai juste un peu reformulé la preuve traduite par bradypus_tridactyle, et simplifié à peine.

Je commence par des réductions, identifications (histoire de simplifier les notations, ou d'en faire des abus, comme chacun veut).

« Séquence de période n » : élément de $\mathbb{N}^n$ (c'est notre siteswap). Vu qu'on change rien en travaillant modulo n, ben on travaille modulo n, et comme ça va simplifier la tache on va plutôt voir une séquence comme une fonction de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même (on pose $E = \mathcal{F}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$), comme ça on a au lieu de $(a_0, \ldots, a_{n-1})$ la fonction $a : i \mapsto a_i$. On peut alors faire un abus de notation en identifiant $\mathfrak{S}_n$ à un sous ensemble de E. Tout ça bien entendu pour se simplifier la vie (là évidemment ça paraît pas plus simple mais dans la suite oui !).

On dit qu'une séquence a est valide (c'est un siteswap valide) ssi $i \mapsto a(i) + i$ est une permutation de $\mathbb{Z}/n\mathbb{Z}$. C'est à dire que $a + \mathrm{Id} \in \mathfrak{S}_n$. Je retranscrit donc la définition de réorganisable avec ces notations : a est réorganisable ssi il existe une permutation σ telle que la séquence permutée soit valide, c'est à dire que $a \circ \sigma$ est valide, ou enfin $a \circ \sigma + Id \in \mathfrak{S}_n$.

On compose à droite par l'inverse de σ et sachant que $-\mathrm{Id}$ est une permutation de $\mathbb{Z}/n\mathbb{Z}$, on peut tout faire passer à droite, et c'est donc équivalent de dire qu'il existe $\varphi, \psi \in \mathfrak{S}_n$ tels que $a = \psi + \varphi$.

On pose F le sous-ensemble de E constitué des fonctions de somme nulle (qui correspond aux séquences d'entiers de moyenne entière, c'est un sous-module de E). Et le théorème consiste donc à dire que a est dans F (i.e. une séquence d'entiers est de moyenne entière) si et seulement si il existe deux permutations $\varphi, \psi \in \mathfrak{S}_n$ telles que $a = \psi + \varphi$ (i.e. la séquence est réorganisable). On passe en notation ensembliste, et on obtient quelque chose de fort élégant à mon goût !

2 Le théorème

Théoreme 1. *« de réorganisation ».*

$$F = \mathfrak{S}_n + \mathfrak{S}_n.$$

Franchement là on est content, parce que un théorème qui s'énonce comme ça c'est pas tous les jours (surtout quand on fait des maths appliqués un peu sales dans la vie...).

Je retranscris juste la démo traduite par bradypus_tridactyle dans ces termes-là, avec une légère simplification, où on n'utilise que deux cas et demi au lieu de cinq...

Je donne le même lemme qui dit que si on a fait le boulot pour une séquence, il en reste plus trop à faire si on change seulement deux entiers de la séquence sans changer la somme.

Lemme 1. *Soit $\beta \in E$ et $\varphi, \psi \in \mathfrak{S}_n$ tels que :*

$$\forall j \in \mathbb{Z}/n\mathbb{Z}, j \neq x_0, j \neq x_1, \beta(j) = \psi(j) + \varphi(j), \tag{1}$$

$$\beta(x_0) + \beta(x_1) = \psi(x_0) + \psi(x_1) + \varphi(x_0) + \varphi(x_1), \tag{2}$$

où x_0 et x_1 sont deux éléments distincs de $\mathbb{Z}/n\mathbb{Z}$.

Alors on définit par récurrence la suite x_k, pour $k \geqslant 1$, par

$$x_{k+1} = \varphi^{-1}(\beta(x_k) - \psi(x_{k-1})). \tag{3}$$

On pose m le plus grand indice tels que les x_k, pour $k \in [\![0, m]\!]$, soient distincts deux à deux pour et on a le résultat suivant :

Si $x_{m+1} = x_0$, alors $\beta = \psi \circ (x_m\ x_{m-1}\ \ldots\ x_0) + \varphi \circ (x_0\ x_1\ \ldots\ x_m)$.

Sinon on a seulement la possibilité que $x_{m+1} = x_1$ et dans ce cas là on a $\beta = \psi \circ (x_m\ x_{m-1}\ \ldots\ x_0) + \varphi \circ (x_1\ x_2\ \ldots\ x_m)$.

Autrement dit, si $\alpha \in E$ peut être écrit sous la forme $\varphi + \psi \in \mathfrak{S}_n + \mathfrak{S}_n$, que $\beta \in E$ ne diffère de α qu'en deux éléments x_0 et x_1 (c'est l'hypothèse (1)) et que β et α ont la même somme (ce que traduit l'hypothèse (2)), alors $\beta = \widetilde{\varphi} + \widetilde{\psi}$, où on obtient $\widetilde{\varphi}$ et $\widetilde{\psi}$ à partir de φ et ψ en composant à droite par un cycle faisant intervenir les indices x_k.

Démonstration. On suppose que pour $k \in [\![2, l]\!]$, $x_k \notin \{x_0, x_1\}$, et on va montrer que pour $k \in [\![1, l]\!]$ la proposition suivante est vraie.

$$\beta(x_0) + \beta(x_k) = \psi(x_{k-1}) + \psi(x_k) + \varphi(x_0) + \varphi(x_1) \tag{4}$$

C'est vrai pour $k = 1$. Supposons que c'est vrai pour un certain $k \geqslant 1$, avec $k < l$ et montrons qu'elle est vraie pour $k + 1$.

On a $\beta(x_k) = \psi(x_{k-1}) + \varphi(x_{k+1})$ (par la définition de x_{k+1}). Et comme on a supposé que $x_{k+1} \notin \{x_0, x_1\}$, on a par (1) que $\beta(x_{k+1}) = \psi(x_{k+1}) + \varphi(x_{k+1})$. Et donc

$$\begin{aligned}\beta(x_0) + \beta(x_k) &= \beta(x_0) + \psi(x_{k+1}) + \varphi(x_{k+1}) \\ &= \beta(x_0) + \psi(x_{k+1}) + \beta(x_k) - \psi(x_{k-1}) \\ &= \psi(x_{k+1}) + \psi(x_k) + \varphi(x_0) + \varphi(x_1).\end{aligned}$$

Cette propriété est donc vraie pour $k \in [\![1, m]\!]$. Si on suppose que x_{m+1} est différent de x_0 et de x_1, c'est aussi vrai pour $k = m + 1$. Par la définition de m on sait que $x_{m+1} = x_j$ pour un certain $j \in [\![2, m]\!]$. On applique donc l'égalité pour $k = j$ et $k = m+1$ et tous les termes sont les mêmes dans les deux égalités à part ceux pris en $k-1$, donc en faisant la différence de ces deux égalités, on obtient que $\psi(x_{j-1}) = \psi(x_m)$. La fonction ψ étant une permutation, on obtient donc que $x_{j-1} = x_m$, ce qui contredit la définition de m.

On a donc bien $x_{m+1} = x_0$ ou $x_{m+1} = x_1$.

On pose alors $\widetilde{\psi} = \psi \circ (x_m\ x_{m-1}\ \dots\ x_0)$ et $\widetilde{\varphi} = \varphi \circ (x_1\ x_2\ \dots\ x_m)$ si $x_{m+1} = x_1$ (ou alors $\widetilde{\varphi} = \varphi \circ (x_0\ x_1\ \dots\ x_m)$ si $x_{m+1} = x_0$).

Si $j \notin \{x_0, x_1, \dots, x_m\}$ on a $\widetilde{\psi}(j) = \psi(j)$, $\widetilde{\varphi}(j) = \varphi(j)$, et $\beta(j) = \widetilde{\psi}(j) + \widetilde{\varphi}(j)$. Ensuite on a $\widetilde{\psi}(x_k) = \psi(x_{k-1})$ et $\widetilde{\varphi}(x_k) = \varphi(x_{k+1})$ pour $k \in [\![1, m-1]\!]$ donc par (3) on obtient $\beta(j) = \widetilde{\psi}(j) + \widetilde{\varphi}(j)$ pour $j \in \{x_1, x_2, \dots, x_{m-1}\}$.

Il reste à montrer $\beta(j) = \widetilde{\psi}(j) + \widetilde{\varphi}(j)$ pour $j = x_0$ et $j = x_m$.

On a $\widetilde{\varphi}(x_m) = \varphi(x_{m+1})$ dans les deux cas (selon que $x_{m+1} = x_0$ ou x_1) et également $\widetilde{\psi}(x_m) = \psi(x_{m-1})$. Donc par (3) on obtient bien $\beta(x_m) = \widetilde{\psi}(x_m) + \widetilde{\varphi}(x_m)$.

Dans le cas $x_{m+1} = x_0$, $\varphi(x_0) = \widetilde{\varphi}(x_m)$ et $\varphi(x_1) = \widetilde{\varphi}(x_0)$. Dans le cas $x_{m+1} = x_0$, on a $\varphi(x_0) = \widetilde{\varphi}(x_0)$ et $\varphi(x_1) = \widetilde{\varphi}(x_m)$, l'équation (4) s'écrit donc dans les deux cas

$$\begin{aligned}\beta(x_0) + \beta(x_m) &= \psi(x_{m-1}) + \psi(x_m) + \varphi(x_0) + \varphi(x_1)\\ &= \widetilde{\psi}(x_m) + \widetilde{\psi}(x_0) + \widetilde{\varphi}(x_m) + \widetilde{\varphi}(x_0).\end{aligned}$$

Comme on a déjà $\beta(x_m) = \widetilde{\psi}(x_m) + \widetilde{\varphi}(x_m)$, on a alors $\beta(x_0) = \widetilde{\psi}(x_0) + \widetilde{\varphi}(x_0)$.

□

La démonstration du théorème est alors très rapide.

En effet si $\alpha = \psi + \varphi \in \mathfrak{S}_n + \mathfrak{S}_n$, on a $\sum_{i \in \mathbb{Z}/n\mathbb{Z}} a(i) = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} \psi(i) + \varphi(i) = 0$ (on peut faire la somme « dans $\mathbb{Z}$ » qui vaut $n(n-1)$, mais un simple changement d'indice $j = \psi(i)$ $k = -\varphi(i)$ suffit pour voir que c'est nul).

Donc on a bien $\mathfrak{S}_n + \mathfrak{S}_n \subset F$.

Si $\alpha \in F$ on pose

$$\alpha_k(i) = \begin{cases} \alpha(i) & \text{si } i < k \\ \sum_{j=k}^{n-1} \alpha(j) & \text{si } i = k \\ 0 & \text{si } i > k \end{cases}.$$

Et alors on a que α_k et α_{k+1} ne diffèrent que sur les deux éléments k et $k+1$, et ont la même somme (nulle).

Donc si $\alpha_k = \psi_k + \varphi_k \in \mathfrak{S}_n + \mathfrak{S}_n$, alors $\alpha_{k+1} = \psi_{k+1} + \varphi_{k+1} \in \mathfrak{S}_n + \mathfrak{S}_n$. Comme c'est vrai pour la fonction α_0 (qui est la fonction nulle, égale par exemple à $Id - Id$...), c'est donc vrai pour toutes les fonctions α_k et donc en particulier pour $\alpha_{n-1} = \alpha$. Et on a bien $F \subset \mathfrak{S}_n + \mathfrak{S}_n$.

2.1 Conclusion

Pas grand chose de plus donc en dire si ce n'est que je trouve joli le théorème énoncé de cette manière.

On peut alors se poser le problème de dénombrement soulevé par garnav en ces termes (qui est de calculer le nombre de façons possibles de permuter la séquence de façon à ce qu'elle soit valide).

Dans le cas où toutes les hauteurs sont plus petites que n (ou que deux hauteurs différents données n'ont pas le même reste modulo n) il s'agit donc, pour une séquence donnée α de calculer le cardinal N_α de l'ensemble des couples $(\psi, \varphi) \in (\mathfrak{S}_n)^2$ tels que $\alpha = \psi + \varphi$.

Et là les seul trucs qu'on sait à mon avis, c'est que $N_\alpha \geqslant 1$ pour tout $\alpha \in F$, et que $\sum_{\alpha \in F} N_\alpha = (n!)^2$. Mais c'était pas très dur à voir et ça nous avance pas à grand-chose.

Et d'autant plus qu'il faut ensuite considérer le cas où il y a plusieurs hauteurs qui ont le même reste modulo n, et puis ensuite on voulait aussi quotienter tout ça à permutation près, et ne garder que les « intéressantes »... Enfin à mon avis il y a encore du boulot pour ça...