Polynômes cyclotomiques, canons mosaïques et rythmes k-asymétriques

Édouard Gilbert,
sous la direction de Moreno Andreatta,
Équipe Représentations Musicales, ircam

Juin 2007

Résumé

Nous introduisons les notions de canons mosaïques et de rythmes k-asymétriques et explicitions leur lien avec la notion de pavage des entiers et du cercle (théorème de de Bruijn). Nous fournissons ensuite les outils pour l'étude de tels rythmes au moyen de polynômes : polynômes cyclotomiques, conditions de Coven-Meyerowitz. Nous étudions ensuite la notion d'ensemble spectral, l'appliquons au cas du pavage du cercle et cherchons à l'étudier de manière similaire aux travaux de Amiot pour les conditions de Coven-Meyerowitz. Nous nous intéressons enfin à la structure algébrique d'ensembles de polynôme et à leur utilisation pour la recherche automatique des entrées possibles pour un canon mosaïque.

Remerciements

Je tiens à remercier l'ircam et particulièrement l'équipe « Représentations Musicales » pour m'avoir accueilli en son sein.

Je tiens en particulier à remercier mon encadrant Moreno Andreatta pour la liberté accordée dans mes travaux, pour le temps qu'il m'a consacré et les personnes avec lesquelles il m'a mis en contact, mais également pour les cours dispensés en cours d'année et pendant lesquels j'ai découvert les problèmes posés par l'étude des canons mosaïques. J'adresse également toute ma gratitude à Marc Chemillier pour la découverte des rythmes k-asymétriques.

Je désire également remercier Carlos Agon pour son aide précieuse pour la maîtrise d'OpenMusic et Karim Haddad pour ses conseils d'utilisation du même logiciel et pour la documentation détaillée.

Je me dois de remercier Yun-Kang Ahn pour sa disponibilité, ses conseils et ses relectures, ainsi que Grégoire Carpentier et Antoine Allombert pour m'avoir accueilli dans leur bureau.

Enfin, les conseils et les explications d'Emmanuel Amiot ainsi que les pistes qu'il m'a suggéré et ses réponses (rapides) à mes (nombreuses) questions sur ses travaux m'ont grandement aidé. Je lui suis particulièrement reconnaissant.

Sommaire

Table des symboles

Symboles	Signification
$\mathbf{Z}$	anneau des entiers relatifs
$\mathbf{Z}/n\mathbf{Z}$	anneau des entiers modulo n
$\mathbf{F}_p$	corps des entiers modulo p (premier)
$\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$	corps des nombres rationnels, réels et complexes
$\mathbf{K}$	corps quelconque
$\mathbf{U}$	cercle unité, groupe des complexes de norme 1
$\mathbf{U}_n$	groupe des racines n^{e} de l'unité
ξ	élément de $\mathbf{U}$ ou $\mathbf{U}_n$
A	sous ensemble fini de $\mathbf{Z}$ ou $\mathbf{Z}/n\mathbf{Z}$; le plus souvent vu comme un rythme
B	sous ensemble fini de $\mathbf{Z}$ ou $\mathbf{Z}/n\mathbf{Z}$; le plus souvent vu comme les entrées de différentes voix
$\widetilde{A}$	A transformé par une opération donnée
$\widetilde{B}$	entrées des différentes voix correspondant à $\widetilde{A}$
$\oplus$	somme directe de deux sous-ensembles d'un groupe
X	indéterminée des polynômes
$R[X]$	anneau des polynômes à coefficients dans l'anneau R
$R[X]/(P)$	anneau des polynômes modulo $P \in R[X]$
P, Q	polynômes de $R[X]$ éventuellement modulo un autre polynôme
$\{0,1\}[X]$	polynômes à coefficients dans $\{0,1\}$; vu comme sous-ensemble de l'anneau $\mathbf{Z}[X]$
$\{0,1\}[X]/(P)$	idem pour l'anneau $\mathbf{Z}[X]/(P)$
P_A	polynôme correspondant au rythme A
σ_n	polynôme $1 + X + \cdots + X^{n-1}$
$\mid$	relation d'ordre de division entre polynômes ou entiers
Φ_d	d^{e} polynôme cyclotomique
R_A	ensemble des Φ_d qui divisent P_A
S_A	idem en se limitant à d au puissance de nombre premiers

Symboles	Signification
Z_A	pour un rythme A n-périodique, ensemble des racines de P_A racines n^{e} de l'unité
Λ	spectre d'un rythme, souvent de A
$\widetilde{\Lambda}$	spectre du rythme transformé $\widetilde{A}$
Θ	sous-ensemble de $\mathbf{U}_n$
$\lambda, \widetilde{\lambda}, \theta$	respectivement, élément de $\Lambda, \widetilde{\Lambda}, \Theta$

Introduction

Le canon n'est pas une notion nouvelle en musique. Rappelons-en ici le principe : plusieurs voix jouent une même mélodie, mais tout en étant décalées les unes par rapport aux autres. tout un chacun connaît bien sûr la comptine « Frère Jacques », mais ce principe ou certaines de ses variations se retrouve chez beaucoup de compositeurs, comme Bach, Josquin Desprez.

Nous nous intéressons ici à la notion de canons rythmiques. Autrement dit, nous ne nous intéresserons pas à la mélodie. Nous nous intéresserons particulièrement aux canons mosaïques, dont les différentes voix ne se chevauchent jamais mais recouvrent toutes les pulsations. Nous parlerons également de rythmes k-asymétriques, qui présentes des similarités avec des cas particuliers de canons mosaïques dont les voix rentrent de façon régulière.

La notion de canon mosaïque se ramène en fait au problème mathématique du recouvrement des entiers par décalage d'un sous-ensemble fini. Nous nous intéresserons donc aux outils développés par les scientifiques pour leur étude. Parmi ceux-ci, distinguons les travaux de de Bruijn qui permettent d'assimiler pavage de la ligne (des entiers relatifs) et pavage du cercle (des entiers modulo n).

Les travaux de nombreux mathématiciens, parmi lesquels Hajòs et Sands ainsi que ce de Vuza (qui s'intéressait spécifiquement aux canons mosaïques) ont chacun de leur côté permis d'aboutir au mêmes résultats et à distinguer parmi les canons mosaïques une classe particulière de canons « les plus simples possibles », appelés canon de Vuza.

Coven et Meyerowitz ont, de leur côté, eu pour objectif d'étudier le problème du pavage au moyen de polynômes, et plus particulièrement de polynômes dits cyclotomiques. Ils ont aboutis à l'écriture d'une condition suffisante pour qu'un canon pave. Savoir si cette condition est également nécessaire est encore un problème ouvert. Les travaux d'Amiot ont permis de ramener la résolution de ce problème au cas des canons de Vuza.

D'un tout autre point de vue, la conjecture de Fuglede concerne l'étude de pavage dans un espace de dimension quelconque. Bien que des contre-exemples sont aujourd'hui connus en dimensions 3 ou supérieure, le cas de la dimension 1 est encore non résolu. Cependant, Łaba a démontré certains résultats la liant aux conditions de Coven et Meyerowitz.

Durant notre stage, nous avons cherché à renforcer ces liens en ramenant de manière similaire à Amiot ce problème à l'étude des cas particuliers que

constituent les canons de Vuza. Pour cela, nous avons cherché à changer le point de vue adopté le plus fréquement dans nos lectures et qui tend à étudier le problème Fuglede dans le cadre du pavage de la ligne. Nous avons donc cherché à l'exprimer dans le cadre du pavage du cercle.

Nous avons également étudié la possibilité de calculer à quels instants faire commencer les différentes voix d'un canon en exploitant la structure algébrique de leur représentation sous forme de polynôme.

Chapitre 1

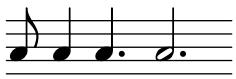
Canons mosaïques et pavage du cercle

Considérons l'ensemble des pulsations possibles, sans limitation de temps. Cet ensemble peut se représenter par l'ensemble **Z** des entiers relatifs, chaque entier représentant une pulsation. Un rythme se définit alors tout naturellement comme suit :

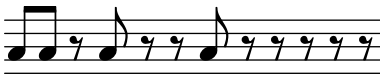
Définition 1. Un *rythme* est un sous-ensemble fini A de **Z**.

A représente alors le rythme formé par les impulsions données sur les temps $a \in A$. Remarquons qu'il est toujours possible de se ramener à un rythme dont le premier élément est 0 en procédant à un changement d'origine ; nous nous placerons toujours dans cette hypothèse par la suite.

Exemple. L'ensemble $\{0, 1, 3, 6\}$ représente le rythme suivant :



La pulsation de base est la croche. Ce rythme est équivalent à



En notant `.` les pulsations sans impulsion et `x` les pulsations avec impulsion, il se note alors (...) `xx.x..x.....` (...). Nous conserverons cette notation par la suite, car elle permet d'aligner les différentes voix aisément.

Définition 2. Soit A et B deux sous-ensembles d'un groupe additif G. On appelle *somme de A et B* et on note $A + B$ l'ensemble

$$\{a + b \mid a \in A \quad b \in B\}.$$

Si, de plus, pour tout $c \in A + B$, il existe un unique $a \in A$ et un unique $b \in B$ tel que $c = a + b$, on dit que la somme est directe et on la note $A \oplus B$.

Si A représente un rythme et que B correspond à l'ensemble des instants où l'on fait commencer ce rythme, $A+B$ est l'ensemble des impulsions du canon généré. Dans ce cas, dire que la somme est directe revient à dire que les différentes occurrences de A débutées aux instants décrits par B ne se chevauchent pas, autrement dit que deux impulsions du canon ne surviennent jamais en même temps.

Exemple. Le rythme $A = (\dots)$ `xx.x..x.....` $(\dots) = \{0, 1, 3, 6\}$ combiné avec les entrées $B = (\dots)$ `o.o.o.......` $(\dots) = \{0, 2, 4\}$ ne donne pas un canon. En effet, outre le fait que leur somme n'est évidemment pas $\mathbf{Z}$, des chevauchements (indiqué ci-dessous par des `c`) apparaissent :

$(\dots)$ `....xc.x..x` $(\dots)$
$(\dots)$ `..xc.c..x..` $(\dots)$
$(\dots)$ `xx.c..x....` $(\dots)$

De fait, les nombres 3 et 5 peuvent s'obtenir chacun au moyen de deux sommes différents :

$$\begin{aligned} 3 &= (3 \in A) + (0 \in B) \\ &= (1 \in A) + (2 \in B) \\ 5 &= (3 \in A) + (2 \in B) \\ &= (0 \in A) + (5 \in B). \end{aligned}$$

Définition 3. Soit A un sous-ensemble fini de $\mathbf{Z}$. On dit qu'il pave les entiers par translation ou encore que A est un *canon mosaïque* si et seulement s'il existe $B \subset \mathbf{Z}$ tel que $A \oplus B = \mathbf{Z}$.

D'un point de vue musical cela signifie que des instrumentistes jouant un même rythme en canon joueront sur toutes les pulsations, mais jamais en même temps.

1.1 Propriété fondamentale

Une propriété fondamentale d'un canon rythmique A et de ses entrées B est la suivante :

Théorème 1. *Soit A un sous-ensemble fini de $\mathbf{Z}$ et soit B un sous-ensemble de $\mathbf{Z}$ tels que $A \oplus B = \mathbf{Z}$. Alors il existe $n \in \mathbf{N}^*$ et $\widetilde{B} \subset \mathbf{Z}$ fini tel que $B = \widetilde{B} \oplus \mathbf{Z}/n\mathbf{Z}$. On a alors $\mathbf{Z}/n\mathbf{Z} = A \oplus \widetilde{B}$ et A et $\widetilde{B}$ sont qualifiés de complémentaires.*

Autrement dit, tout canon rythmique est périodique. On dit de n que c'est une période de A ou encore que A est n-périodique. Remarquons que n ne

désigne pas ici la plus petite période que l'on peut découvrir dans A mais qu'il correspond plutôt au $\mathbf{Z}/n\mathbf{Z}$ choisit pour l'étude de A. Une démonstration de cette propriété peut être trouvée dans [5].

Notation. Les exemples que nous emploierons désormais seront des rythmes de $\mathbf{Z}/n\mathbf{Z}$, ils seront notés sous la forme `|: X.x.x. :|` pour expliciter leur circularité. Le `X` indiquera la « première » impulsion du rythme non décalé.

Exemple. Le rythme `|: Xx.x..x..... :|` est un canon mosaïque. Il pave avec les entrées `|: o...o...o :|` ($= \{0, 4, 8\}$) :

```
|: ..x.....Xx.x :|
|: ....Xx.x..x. :|
|: Xx.x..x..... :|.
```

1.2 Rythmes k-asymétriques

Définition 4. Soit A un rythme n-périodique et k un diviseur de n. On dit que A est *k-asymétrique* lorsque

$$\forall a \in A \quad \forall p \in \mathbf{Z}/k\mathbf{Z} \quad a + p \cdot \frac{n}{k} \notin A.$$

Quand $k = 2$, on dit que également qu'il est *impair*.

Un canon n-périodique et k-asymétrique peut être caractérisé par le fait qu'il a pour complémentaire $\left\{p.\frac{n}{k} : p \in \mathbf{Z}/k\mathbf{Z}\right\}$. Il est de plus équivalent au rythme $\frac{n}{k}$-périodique $\left\{0, \cdots, \frac{n}{k} - 1\right\} = A \mod \frac{n}{k}$.

Exemple. `|: Xx.....x..x. :|` est un canon 12-périodique 3-asymétrique. Les entrées `|: o...o...o... :|` donnent en effet :

```
|: ...x..x.Xx.. :|
|: ..x.Xx.....x :|
|: Xx.....x..x. :|.
```

1.3 Transformation de rythmes mosaïques

Certaines opérations sur les rythmes permettent de transformer des canons en autre canons. Au delà de l'intérêt musical qu'elles apportent, elles peuvent avoir une dimension théorique importante, comme nous le verrons plus loin. Nous énumérons ici certains de ses transformations dont la plupart son suggérée dans [3].

Les rythme équivalents de période supérieure à un rythme n-périodique A sont les rythmes $\widetilde{A}$ de période kn-périodique pour un certain $k \in \mathbf{N}^*$ tels que $A = \widetilde{A} \mod n$. S'intéresser à cette transformation permet en outre de négliger dans les autres le modulo dans les autres transformations : si l'on transforme un canon A en $f(A) \mod n$, nous pouvons en fait nous intéresser uniquement à l'étude du rythme $f(A)$. Elle a pour dernier intérêt de correspondre à la transformation à appliquer aux entrées des voix d'une autre opération, la répétition.

Exemple. Considérons le canon 4-périodique $A =$ `|: Xxxx :|`. Alors les canons suivants, de période 12, se ramènent à A modulo 4 :

```
|: Xxxx........ :|
|: Xx....xx.... :|
|: X.xx.....x.. :|
|: Xx.x..x..... :|.
```

L'augmentation d'un rythme A n-périodique est sa transformation par une bijection affine de $\mathbf{Z}/n\mathbf{Z}$, c'est-à-dire le rythme $\widetilde{A}$ défini par

$$\widetilde{A} = a.A + b \mod n$$

où $a, b \in \mathbf{Z}/n\mathbf{Z}$ et *a est inversible dans $\mathbf{Z}/n\mathbf{Z}$* . Cette dernière condition est indispensable pour que la fonction affine soit bijective ; elle est équivalente au fait que a et n soient premiers entre eux. Dans ce cas, lorsque A est un canon, $\widetilde{A}$ en est un également.

Le dual d'un canon mosaïque périodique A qui pave avec les entrées B, c'est-à-dire le canon B muni des entrées A, reste bien sûr périodique de même période.

Exemple. Le canon dual de `|: xx.x..x..... :|`, qui pave avec les entrées `|: o...o...o... :|` est formé du rythme `|: X...x...x... :|` et des entrées `|: oo.o..o..... :|`.

La répétition d'un rythme n-périodique A consiste à faire se suivre un certain nombre de fois A de manière à ce que deux débuts successifs soient séparés par n temps. Autrement dit, le rythme A répété k fois est le rythme kn-périodique

$$\{0, n, 2n \ldots, (k-1)n\} \oplus A$$

Si l'on considère un canon mosaïque n-périodique A qui pave avec les entrées B, alors ses répétitions $\widetilde{A}$ pavent avec le même B, mais considéré comme kn-ériodique. Remarquons qu'on peut également remplacer B par un rythme kn-périodique équivalent à B modulo n.

Exemple. Comme le rythme `|: Xx.x..x..... :|` est un canon mosaïque, le même rythme répété deux fois `|: Xx.x..x.....xx.x..x..... :|` l'est aussi, avec entre autres les entrées `|: o...o...o.............. :|` ou les entrées `|: o...o..............o... :|`, qui se ramènent bien toutes les deux à `|: o...o...o... :|` sur une période 12.

Le multiplexage d'une famille $(A_l)_{(1\leq l\leq k)}$ de canons mosaïques de même période n et qui pavent avec les mêmes entrées B est le rythme kn-périodique $\widetilde{A}$ défini par

$$\widetilde{A} = \bigcup_{l=0}^{k} (l + k.A_l)\,.$$

Il s'agit donc d'entrelacer les différents rythmes. Ce rythme pave avec les entrées kB, c'est-à-dire une version « étirée » de B.

Exemple. Définissons deux rythmes A_1 et A_2 comme suit :

$$A_1 = \texttt{|: Xx.x..x..... :|} \quad \text{et} \quad A_2 = \texttt{|: X.xx.x..... :|}.$$

Ils pavent tous deux avec $B = \texttt{|: o...o...o... :|}$. La multiplication par deux transforme les « `x` » et « `x.` » et les « `.` » en « `..` ». La rythme $\widetilde{A}$ s'écrit alors :

$$\begin{array}{rl} 2.A_1 & \texttt{|: X.x...x.....x..... :|} \\ 1+2.A_2 & \texttt{|: .X...x.x...x..... :|} \\ \widetilde{A} & \texttt{|: Xxx..xxx...xx..... :|}. \end{array}$$

Ce rythme pave bien avec $2.B = \texttt{|: o.......o.......o....... :|}$ comme nous le constatons ci-dessous :

```
|: Xxx..xxx...xx..... :|
|: ........Xxx..xxx...xx... :|
|: ...xx...........Xxx..xxx :|.
```

Le zoom est le cas particulier de multiplexage où tous les A_l sont égaux. « Zoomer » sur un rythme consiste alors à changer toute impulsion (respectivement silence) en un groupe k impulsions (respectivement silences). Autrement dit, à partir de A n-périodique, nous définissons $\widetilde{A}$ kn-périodique par

$$\begin{aligned} \widetilde{A} &= \bigcup_{l=0}^{k} (l + k.A) \\ &= \{0, 1, \cdots k-1\} \oplus k.A. \end{aligned}$$

Comme pour le multiplexage, si B fait paver A, $\widetilde{A}$ pave avec $k\widetilde{B}$.

Exemple. L'augmentation avec un coefficient 2 de notre exemple habituel `|: Xx.x..x..... :|` est

```
|: Xxxx..xx....xx..... :|.
```

Elle revient à transformer les « `x` » et « `x` » et les « `.` » et « `..` ».

Canons cycliques et groupes de Hajòs

Comme nous l'avons vu ci-dessus, la répétition d'un canon mosaïque est un canon mosaïque. Inversement, certains rythmes peuvent s'écrire (ou ont des complémentaires qui peuvent s'écrire) comme la répétition d'un autre plus simple. Ces rythmes sont qualifiés de *cycliques*.

Définition 5. Soit A un canon mosaïque n-périodique et B des entrées qui font paver A. On dit que A muni des entrées B est *cyclique* si et seulement si A ou B contient une sous-période, c'est-à-dire si et seulement si $A + p = A$ pour un certain $p|n$ ou si B vérifie une relation semblable.

Dire que $A + p = A$ signifie en fait que A est la répétition du rythme de période p $\widetilde{A} = A \cap \{0, 1, \ldots, p-1\}$. Remarquons que si B désigne les entrées correspondant à A, alors les entrées de $\widetilde{A}$ sont $\widetilde{B} = B \mod p$: B est donc un équivalent de $\widetilde{B}$ modulo p.

Un canon qui n'est pas cyclique est appelé canon de Vuza. Pour certaines valeurs particulières de n, tout canon mosaïque de $\mathbf{Z}/n\mathbf{Z}$ est nécessairement cyclique. Ce sont les groupes de Hajòs.

Définition 6. Soit $n \in \mathbf{Z}$. $\mathbf{Z}/n\mathbf{Z}$ est un *groupe de* Hajòs si et seulement si pour toute factorisation $A \oplus B = \mathbf{Z}/n\mathbf{Z}$, il existe $p < n$ tel que $A + p = A$ ou $B + p = B$.

Exemple. Dans notre exemple habituel, les entrées `|: o...o...o... :|` sont évidemment la répétition de `|: o... :|`. Le rythme correspondant est alors `|: Xxxx :|`.

Les travaux de Hajòs, Redei, de Bruijn, Sands et autres ont abouti à une caractérisation des groupes de Hajòs.

Théorème 2. *Les groupes de* Hajòs *sont les* $\mathbf{Z}/n\mathbf{Z}$ *qui s'écrivent, avec* p, q, r, s *des nombres entiers distincts :*

$$n = p^\alpha \qquad n = p^\alpha q \qquad n = p^2q^2 \qquad n = p^2qr \qquad n = pqrs.$$

Exemple. Le premier entier tel que $\mathbf{Z}/n\mathbf{Z}$ n'est pas de Hajòs est $2^3 3^2 = 72$. Un des plus petits canons de Vuza est

$$A = \{0, 3, 6, 12, 23, 27, 36, 42, 47, 48, 51, 71\} \quad B = \{0, 8, 10, 18, 26, 64\}.$$

[2] fait remarquer que, comme la répétition d'un rythme et son passage au dual (2.5) tant pour le rythme que pour ses entrées, tout canon cyclique ne respectant pas cette condition peut se ramener à un canon de Vuza ne la respectant pas non plus. Il suffit donc de montrer que (2.5) est vraie pour tout canon de Vuza pour l'étendre par récurrence à tout canon.

1.4 Représentation polynomiale

À tout ensemble fini $A \subset \mathbf{Z}$, nous pouvons faire correspondre le polynôme $P_A(X) \in \{0,1\}[X]$ défini par

$$P_A(X) = \sum_{a \in A} X^a.$$

Remarquons que la valeur de P_A en 1 est égale au cardinal de A :

$$P_A(1) = \sum_{a \in A} 1 = \#A.$$

Par la suite, la même notation sera utilisée pour désigner le polynôme à coefficients dans $\mathbf{F}_2[X]$ défini par la même formule.

Exemple. Le polynôme correspondant à notre rythme `|: Xx.x..x..... :|` est

$$1 + X + X^3 + X^6.$$

L'intérêt de cette notation et que, si A et B sont en somme directe, alors

$$P_{A \oplus B} = P_A.P_B.$$

Si la somme n'est pas directe, alors $P_A.P_B$ ne sera pas à coefficients dans $\{0,1\}$. Remarquons cependant qu'en prenant en compte la multiplicité des éléments de $A + B$, la relation est toujours vérifiée dans $\mathbf{Z}[X]$. En particulier, si le produit $P_A.P_B \in \{0,1\}[X]$, alors la somme de A et B est nécessairement directe.

1.5 Pavage modulo n

Un des problèmes majeurs de l'écriture polynomiale est que, comme expliqué dans la section 1.4, $\{0,1\}[X]$, n'est pas stable par produit. Autrement dit, composer deux rythmes A et B n'en donne pas nécessairement un troisième car certaines impulsions peuvent se chevaucher. Il est cependant possible de « forcer » le produit de deux polynômes à rester dans $\{0,1\}$ en exploitant sa structure de groupe $\mathbf{Z}/2\mathbf{Z} = \mathbf{F}_2$. Plus généralement, nous pouvons nous intéresser aux polynômes à coefficients dans l'anneau $\mathbf{Z}/p\mathbf{Z}$ pour tout entier p. Nous nous limiterons toutefois aux cas où p est premier. Dans ce cas, $\mathbf{Z}/p\mathbf{Z}$ dispose de la structure du corps fini d'ordre p et est noté $\mathbf{F}_p$.

Il est bien sûr facile de faire correspondre les éléments de $\mathbf{Z}$ et $\mathbf{F}_p$; les éléments de $\{0,1\}$ et $\mathbf{F}_2$ sont même en bijection. Ces opérations se prolongent coefficient par coefficient à $\mathbf{Z}[X]$ et $\mathbf{F}_p[X]$ (respectivement $\{0,1\}$ et $\mathbf{F}_2$). À un rythme, nous pouvons donc très simplement faire correspondre un polynôme à coefficients dans $\mathbf{F}_p$ et à un polynôme à coefficients dans $\mathbf{F}_2$ ou dans $\mathbf{F}_n \cap \{0,1\}$,

nous pouvons faire correspondre un rythme. Nous définissons alors la notion de pavage modulo p.

Définition 7. Soit A un rythme. On dit qu'il pave modulo p s'il existe $n \in \mathbf{N}^*$ et un rythme B tel que

$$AB = \sigma_n \mod X^n - 1$$

dans $\mathbf{F}_p[X]$.

Comme le passage de $\mathbf{Z}/p\mathbf{Z}[X]$ à $\mathbf{Z}$ ne préserve pas les produits, il est intéressant de voir dans quelle mesure le fait de paver dans $\mathbf{Z}$ et de paver modulo p sont corrélés.

Proposition 3. *Soit A, B et C des polynômes à coefficients dans $\{0,1\}$. Les relations suivantes sont vérifiées.*

(i) *$AB = C$ dans $\mathbf{Z}[X]$ si et seulement si $\forall p$ premier $AB = C$ dans $\mathbf{F}_p[X]$.*

(ii) *Si $AB = C$ dans $\mathbf{F}_p[X]$ pour un certain p premier et que $A(1)B(1) = C(1)$ alors $AB = C$ dans $\mathbf{Z}[X]$.*

L'étude de rythme pavant modulo p ne permet donc *a priori* que de déterminer les rythmes qui ne pavent pas. Cependant, le résultat suivant rend cette possibilité caduque.

Théorème 4 (Amiot [2])**.** *Soit A un rythme et p un nombre premier. Alors A pave $\mathbf{Z}$ modulo p.*

Autrement dit, tout rythme pave modulo p quelque soit p. Cependant, à période fixée, le résultat n'est pas vrai en général. Il n'est donc pas inutile de s'intéresser aux rythmes n-périodiques qui pavent modulo p.

Chapitre 2

Polynômes cyclotomiques et canons mosaïques

Nous avons vu qu'un rythme peut s'écrire sous forme polynomiale et que, en fixant un rythme A, le faire commencer aux instants définis par un rythme B revient à calculer $P_A.P_B$. S'intéresser au pavage du cercle $\mathbf{Z}/n\mathbf{Z}$ revient à faire boucler les coefficients du polynômes en considérant que $X^0 = X^n$, c'est-à-dire que en calculant modulo $X^n - 1$. Autrement dit, nous nous intéressons à l'espace $\mathbf{Z}[X]/(X^n - 1)$.

Nous nous intéressons en particulier au polynôme $\sigma_n = 1 + X + X^2 + \cdots + X^{n-1}$. En effet, pour qu'un rythme A pave $\mathbf{Z}/n\mathbf{Z}$ il faut et il suffit qu'il existe un rythme B tel que $A \oplus B = \mathbf{Z}/n\mathbf{Z}$, autrement dit qu'il existe un polynôme P_B de $\{0,1\}[X]$ tel que $P_A.P_B = \sigma_n \mod X^n - 1$. Les polynômes $X^n - 1$ et σ_n sont liés par la simple relation

$$(X - 1).\sigma_n = X^n - 1.$$

Ils possèdent donc essentiellement les mêmes facteurs.

2.1 Polynômes cyclotomiques

Ces facteurs sont les polynômes à coefficients entiers qui ont pour zéros les racines n^{e} de l'unité. Ce sont les *polynômes cyclotomiques*.

Définition 8. On appelle *polynôme cyclotomique d'ordre d* le polynôme Φ_d défini par

$$\Phi_d = \prod_{\substack{d \leq n \\ \gcd(d,n)=1}} \left(X - e^{2i\pi\frac{d}{n}}\right). \tag{2.1}$$

Notation. Pour faciliter la lecture, nous adopterons les notations suivantes :
– **U** désignera l'ensemble des racines de l'unité.

– $\mathbf{U}_n$ désignera l'ensemble $\{\xi \in \mathbf{U} \mid \xi^n = 1\}$ des racines n^{e} de l'unité.
– ξ_n désignera la racine de $\mathbf{U}_n$ définie par

$$\xi_n e^{2i=\pi \frac{1}{n}}.$$

Remarquons que nous avons alors

$$\mathbf{U}_n = \left\{\xi_n^k \mid 0 \leq k < n\right\}.$$

Comme $X^n - 1 = \prod_{k=1}^{n}(X - e^{2i\pi\frac{k}{n}})$, lui et σ_n se décomposent en produits de polynômes cyclotomiques comme suit :

$$X^n - 1 = \prod_{d|n} \Phi_d \tag{2.2}$$

$$\sigma_n = \prod_{\substack{d|n \\ d\neq 1}} \Phi_d. \tag{2.3}$$

Nous avons donc en particulier, pour tout p premier, $\sigma_p = \Phi_p$.

Les polynômes cyclotomiques partagent des propriétés importantes pour les problèmes qui nous concernent :

Proposition 5. *Les polynômes cyclotomiques sont à coefficients dans* $\mathbf{Z}$*. De plus, tout polynôme cyclotomique est irréductible dans* $\mathbf{Q}[X]$*, a fortiori dans* $\mathbf{Z}[X]$*.*

En particulier, si le polynôme d'un rythme A a pour zéro une racine d'un certain Φ_d, alors il est divisible par ce dernier.

La valeur particulière des polynômes cyclotomiques en 1 joue également sur certains facteurs des canons mosaïques.

Proposition 6. *Les valeurs des polynômes cyclotomiques en 1 sont les suivantes :*

$$\Phi_d(1) = \begin{cases} 0 & \text{si } d = 1 \\ p & \text{si } d = p^\alpha \text{ avec } p \text{ premier} \\ 1 & \text{sinon.} \end{cases}$$

2.2 Facteurs cyclotomiques de canons

Considérons un canon mosaïque $A \oplus B = \mathbf{Z}/n\mathbf{Z}$. Il est naturel de s'intéresser aux facteurs cyclotomiques de P_A et P_B. Il est en particulier intéressant de distinguer certains facteurs parmi ceux-là.

Définition 9. Soit A un rythme et P_A le polynôme de $\{0,1\}[X]$ correspondant. Notons $R_A = \{d \in \mathbf{Z} \mid \phi_d | P_A\}$ et $S_A = \{p^\alpha \in \mathbf{R}_A \mid p \text{ premier}\}$.

Les facteurs cyclotomiques de P_A et P_B sont alors liés par les relations suivantes.

Lemme 7. *Soit A, B et $\widetilde{B}$ trois rythmes tels que $A \oplus B = A \oplus \widetilde{B} = \mathbf{Z}/n\mathbf{Z}$. Alors nous pouvons écrire les relations suivantes :*

(i) $R_A \cup R_B = R_{\mathbf{Z}/n\mathbf{Z}}$;

(ii) $S_A \cup S_B = S_{\mathbf{Z}/n\mathbf{Z}}$;

(iii) $S_A \cap S_B = \emptyset$;

(iv) $S_B = S_{\widetilde{B}}$;

Démonstration. Comme $A \oplus B = \mathbf{Z}/n\mathbf{Z}$, $P_A.P_B = \sigma_n \mod X^n - 1$. Donc $P_A.P_B$ s'écrit $\sigma_n + P.(X^n - 1)$ pour un certain polynôme P. Mais si un polynôme Φ_p divise σ_n, alors il divise $X^n - 1 = \sigma_n(X - 1)$ et donc $\sigma_n + P(X^n - 1) = P_A.P_B$. Inversement, si Φ_p est facteur de $P_A.P_B$, il est nécessairement facteur de $P_A.P_B$. Nous avons bien $R_{A\oplus B} = R_{\mathbf{Z}/n\mathbf{Z}}$. Ceci est également vrai pour $S_{A\oplus B}$ et $S_{\mathbf{Z}/n\mathbf{Z}}$. Remarquons également que $X - 1 \notin R_A$ car sinon $\#A = P_A(1)$ vaudrait 0 et A ne pourrait être que le rythme vide, qui ne pave pas.

(i) Soit Φ_p un facteur cyclotomique de $\sigma_n = P_{A\oplus B} = P_A.P_B$. Comme Φ_p est irréductible, il est soit facteur de P_A, soit facteur de P_B. Il appartient donc à R_A ou R_B.
Réciproquement, tout facteur de P_A ou de P_B est facteur de $P_A.P_B = P_{A\oplus B}$ et donc $R_A \cup R_B \subset R_{A\oplus B} = R_{\mathbf{Z}/n\mathbf{Z}}$.

(ii) Le même raisonnement peut s'appliquer en se limitant aux S.

(iii) Cette propriété se base sur la valeur des divers polynômes au point 1. En effet, notons

$$P_A = Q_A \,.\, \prod_{d \in R_A} \Phi_d \quad \text{et} \quad P_B = Q_B \,.\, \prod_{d \in R_B} \Phi_d.$$

Les Q_A et Q_B contiennent donc les facteurs non cyclotomiques de P_A et P_B ainsi que les facteurs cyclotomiques qui y apparaissent en double. Alors, d'après la propriété 6,

$$P_A(1) = Q_A(1) \,.\, \prod_{q^k \in S_A} q \quad \text{et} \quad P_B(1) = Q_B(1) \,.\, \prod_{q^k \in S_B} q.$$

D'autre part, $\sigma_n = \prod_{d \in R_{\sigma_n}}$ par définition. Donc, au point 1, nous avons

les égalités

$$\begin{aligned}\prod_{q^k\in S_{\sigma_n}} q &= P_A(1).P_B(1)\\ &= \left(\prod_{q^k\in S_A} q\right).\left(\prod_{q^k\in S_B} q\right).Q_A(1).Q_B(1)\\ &= \left(\prod_{q^k\in S_A\cup S_B} q\right).\left(\prod_{q^k\in S_A\cap S_B} q\right).Q_A(1).Q_B(1)\\ &= \left(\prod_{q^k\in S_{\sigma_n}} q\right).\left(\prod_{q^k\in S_A\cap S_B} q\right).Q_A(1).Q_B(1).\end{aligned}$$

Donc $\prod_{q^k\in S_A\cap S_B} q = 1$ et par conséquent, $S_A \cap S_B = \emptyset$. Remarquons par la même occasion que $Q_A(1) = Q_B(1) = 1$, c'est-à-dire que les éventuels facteurs cyclotomiques doubles de P_A ne sont pas dans S_A et que ses facteurs non cyclotomiques valent 1 en au point 1.

(iv) Grâce aux deux propriétés précédentes, il suffit d'écrire

$$\begin{aligned}S_B &= (S_{\sigma_n} \setminus S_A) \cup (S_B \cap S_A)\\ &= S_{\sigma_n} \setminus S_A\\ &= (S_{\sigma_n} \setminus S_A) \cup \left(S_{\widetilde{B}} \cap S_A\right)\\ &= S_{\widetilde{B}}.\end{aligned}$$

□

Remarquons que P_A et P_B peuvent avoir des facteurs communs, y compris cyclotomiques, dès lors que la somme de leurs coefficients vaut 1.

2.3 Conditions de Coven et Meyerowitz

Les conditions de Coven et Meyerowitz [5] expriment une structure dans les facteurs cyclotomiques d'un canon rythmiques. Elle s'écrivent, en conservant les notations employées dans le paragraphe précédent, de la façon suivante :

$$A(1) = \prod_{s\in S_A} \Phi_s(1); \qquad (2.4)$$

$$\forall p_1^{\alpha_1},\ldots,p_m^{\alpha_m} \in S_A \text{ avec les } p_i \text{ distincts deux à deux, } \prod_{k=1}^{m} p_k^{\alpha_k} \in R_A. \qquad (2.5)$$

Théorème 8 (Coven-Meyerowitz [5])**.** *Si* (2.4) *et* (2.5)*, alors A pave. Si A pave, alors* (2.4)*.*

La seconde partie de l'énoncé est en fait inclus dans la démonstration (2.2) du paragraphe précédent.

On ne sait pas encore si, dans le cas général le fait que A pave implique (2.5). Toutefois, le problème est résolu pour certains cas particuliers :

- Si A est un canon k-asymétrique pour un k quelconque, alors (2.5) est nécessaire.
- Si A pave $\mathbf{Z}/n\mathbf{Z}$ avec n qui a moins de deux facteurs premiers.

Chapitre 3

Ensembles spectraux

Dans $\mathbf{R}^n$ et $\mathbf{Z}^n$ (plus généralement, dans tout groupe localement compact), il est possible de définir la notion d'*ensemble spectral*. Un ensemble spectral est un ensemble dont les fonctions de carré intégrable peuvent être décomposées en somme semblables aux transformées de Fourier. Ensemble spectraux et ensemble qui pavent l'espace semblent corrélés dans une certaine mesure. Introduisons donc la notion de pavage par translation dans $\mathbf{R}^n$:

Définition 10. Soit $\Omega \subset \mathbf{R}^n$ un ensemble de mesure non-nulle. On dit qu'il pave R^n par translation s'il existe $T \subset \mathbf{R}^n$ discret tel que, à des ensembles de mesure nulle près, les $t + \Omega$ sont disjoints deux à deux et $T + \Omega = \mathbf{R}$.

Le pavage dans $\mathbf{Z}$ et dans $\mathbf{R}$ sont des notions équivalentes. En fait, le pavage de $\mathbf{Z}$ peut se voir comme un cas particulier de pavage de $\mathbf{R}$ en faisant correspondre le rythme $A \subset \mathbf{Z}$ à l'ensemble $A + [0, 1[$. Définissons alors la notion d'ensemble spectral.

Définition 11. Soit Ω un sous-ensemble d'un groupe commutatif localement compact G et soit $\widehat{G}$ le dual de G au sens de [16], c'est-à-dire l'ensemble des fonctions continues de G dans le cercle unité complexe $\mathbf{U}$. $\Lambda \subseteq \widehat{G}$. On dit que Λ est un spectre de Ω si l'ensemble

$$\{x \in \Omega \mapsto \lambda(x) \mid \lambda \in \Lambda\}$$

des fonctions de Λ restreintes à Ω forme une base orthogonale de $L^2(\Omega)$, l'espace des fonctions de carré intégrable de Ω. Si un tel Λ existe, on dit de Ω qu'il est *spectral*.

Dans le cas des groupes finis, la définition se ramène à la suivante :

Définition 12. Soit A un sous-ensemble fini de $\mathbf{Z}/n\mathbf{Z}$ et soit $N = A(1) = \#A$. Soit $\Lambda = \{0 = \lambda_0 < \lambda_1 < \cdots < \lambda_{N-1} < 1\}$ avec les λ de la forme $\frac{q}{n}$. On dit que Λ est un *spectre* de A si

$$\forall i, j < N \text{ tels que } i \neq j \quad A(e^{2i\pi(\lambda_i - \lambda_j)}) = 0. \tag{3.1}$$

Remarquons que le spectre de A est à proprement parler l'ensemble

$$\left\{x \mapsto e^{2i\pi\lambda} \mid \lambda \in \Lambda\right\}.$$

La seconde notation est toutefois préférée dans l'étude du pavage de $\mathbf{Z}$. Remarquons également que la période du pavage est également nécessaire à la définition. Cette contrainte peut-être mise de côté en ne limitant pas les valeurs des λ.

3.1 Conjecture de Fuglede

Dans le cadre de l'étude de canons rythmiques, l'intérêt des ensembles spectraux est qu'ils sont corrélés aux ensembles qui pavent la ligne. La conjecture de Fuglede, bien qu'elle s'avère fausse dans le cas général (dès la dimension 3, [10, 11]), reste un problème ouvert en dimension 1.

Conjecture 1 (Fuglede)**.** *Soit $\Omega \subset \mathbf{R}^n$ un ensemble de mesure non-nulle. Ω pave R^n si et seulement s'il est spectral.*

Dans certains cas particuliers, elle est avérée. Si A pave avec un ensemble de translations qui a une structure de groupe, c'est-à-dire si A est un canon k-asymétrique, alors il est spectral. Un autre résultat lie les conditions de Coven-Meyerowitz à la condition spectrale.

Théorème 9 (Łaba [14])**.** *Soit A un sous-ensemble fini de $\mathbf{Z}$. Si A vérifie* (2.4) *et* (2.5)*, alors A est spectral.*

3.2 Condition spectrale et transformations

Dans le but de prolonger ce lien entre les conjecture de Fuglede et de Fuglede, nous nous sommes intéressé à la stabilité de la condition spectrale par diverses transformations. Il apparaît qu'elle est préservée par certaines d'entre elles, dont les plus fondamentales.

La première remarque à faire est qu'étant donné un rythme n-périodique A, il suffit de s'intéresser aux zéros de P_A qui sont racines n^{e} de l'unité pour pouvoir étudier ses spectres. Nous utiliserons par la suite une notation particulière pour cette ensemble :

$$Z_A = \{u \in \mathbf{C} \mid u^n = 1, \quad P_A(u) = 0\}.$$

Remarque. Si un rythme A est spectral et si B de même cardinal que A vérifie $Z_A \subset Z_B$, alors tout spectre de A est un spectre de B.

Par la suite, nous noterons $\mathbf{U}_n$ l'ensemble des racines n^{e} de l'unité :

$$\mathbf{U}_n = \{\xi \in \mathbf{C} \mid \xi^n = 1\}.$$

Transformations de base

La première transformation à étudier est le choix d'un autre représentant modulo $X^n - 1$. De cette façon, nous pouvons passer sous silence la difficulté que peut poser le passage au modulo.

Lemme 10. *Soit B un rythme n-périodique, supposé spectral. Alors tout rythme $\widetilde{B}$ dont le polynôme vérifie $P_{\widetilde{B}} = P_B \mod (X^n - 1)$ est spectral.*

Démonstration. Comme $P_{\widetilde{A}} = P_A \mod (X^n - 1)$, il existe un polynôme Q tel que $P_{\widetilde{A}} = P_A + Q \cdot (X^n - 1)$. Or les racines n^{e} sont par définitions toutes zéros de $X^n - 1$ et par conséquent $Z_A = Z_{\widetilde{A}}$. De plus, les cardinaux des rythmes sont préservés :

$$\begin{aligned} \#\widetilde{A} &= P_{\widetilde{A}}(1) \\ &= P_A(1) + 0\ Q(1) \\ &= \#A. \end{aligned}$$

Donc tout spectre de A est également spectre de $\widetilde{A}$. □

Les premières « véritables » transformations concernent alors l'augmentation d'un rythme.

Proposition 11. *Soit A un rythme n-périodique spectral. Le rythme décalé $\widetilde{A} = b + A \mod n$ est également spectral.*

Démonstration. Considérons le polynôme $P_{\widetilde{A}} = X^b P_A \mod X^n - 1$. P_A et $X^b P_A$ ont les mêmes zéros, excepté éventuellement 0 ; donc $Z_A = Z_{X^b P_A}$. Par ailleurs $P_{X^b A}(1) = X^b(1) P_A(1) = P_A(1)$. Il suffit donc d'appliquer la remarque 3.2 et le lemme 10 nous obtenons le résultat attendu. □

Proposition 12. *Soit A un rythme n-périodique spectral. Soit a un entier premier avec n. Alors le rythme multiplié $\widetilde{A} = a.A$ est spectral.*

Démonstration. Le polynôme $P_{\widetilde{A}}$ s'écrit $P_{\widetilde{A}} = P_A(X^a) \mod X^n - 1$. Nous pouvons donc vérifier que $\#\widetilde{A} = P_{\widetilde{A}}(1) = P_A(1) = \#A$. Soit $\{\lambda_k \mid 0 \leq k < \#A\}$ un spectre de A. Comme a es premier avec n, il a un inverse modulo n que nous noterons a^{-1}. Alors $\left\{a^{-1}\lambda_k \mid 0 \leq k < \#A\right\}$ est bien un spectre pour $\widetilde{A}$. En effet, pour tout $i \neq j$,

$$\begin{aligned} P_{\widetilde{A}}\left(e^{2i\pi a^{-1}(\lambda_i - \lambda_j)}\right) &= P_A\left(e^{2i\pi a a^{-1}(\lambda_i - \lambda_j)}\right) \\ &= P_A\left(e^{2i\pi(1+kn)(\lambda_i - \lambda_j)}\right) \\ &= P_A\left(e^{2i\pi(\lambda_i - \lambda_j)}\right). \end{aligned}$$

En effet, $\lambda_i - \lambda_j$ est de la forme $\frac{q}{n}$. Et comme $\{\lambda_i\}$ est un spectre de A, nous avons bien

$$P_{\widetilde{A}}\left(e^{2i\pi a^{-1}(\lambda_i-\lambda_j)}\right) = 0. \qquad \square$$

Stabilité par répétition et dual

Un problème les plus importants que nous avons abordé pendant notre stage est de savoir si, comme pour les canons respectant (2.5), il est possible de ramener tout canon mosaïque à un canon de Vuza tout en préservant la condition spectrale. Comme nous l'avons vu, il suffit pour cela de montrer que la condition spectrale est stable par trois transformations :

- le choix d'un représentant équivalent modulo une période donnée ;
- le passage au dual ;
- la répétition.

Le premier point est en fait une application du lemme 10. Le deuxième est un problème trivial.

Proposition 13. *Soit A un rythme qui pave avec les entrées B, avec A et B spectraux. Alors le rythme dual B avec les entrées A conserve la condition spectrale.*

Reste à démontrer la stabilité de la condition spectrale par répétition.

Proposition 14. *Soit A un canon n-périodique et $\widetilde{A}$ le canon kn-périodique formé de répétitions de A. Si A est spectral, alors $\widetilde{A}$ l'est également.*

Décomposons le polynôme correspondant à $\widetilde{A}$:

$$\begin{aligned} P_{\widetilde{A}} &= P_A\left(1 + X^k + \cdots + X^{k(n-1)}\right) \\ &= P_A\left(\frac{X^{kn}-1}{X^n-1}\right). \end{aligned}$$

Posons $Q = \frac{X^{kn}-1}{X^n-1}$; les zéros de Q sont les éléments de $\mathbf{U}_{kn} \setminus \mathbf{U}_n$. Soit Λ un spectre de A et Θ l'ensemble $\left\{\frac{q}{kn} \mid 0 \leq k\right\}$. Montrons que $\widetilde{\Lambda}$ défini par

$$\widetilde{\Lambda} = \Lambda + \theta$$

est un spectre de $\widetilde{A}$. Commençons par vérifier que son cardinal est bien celui d'un spectre de $\widetilde{A}$ par l'intermédiaire du résultat suivant.

Lemme 15. *$\widetilde{\Lambda}$ est somme directe de Λ et Θ.*

Démonstration. Soit $\lambda_i, \lambda_j \in \Lambda$ et $\theta_i, \theta_j \in \Theta$ tels que

$$\lambda_i + \theta_i = \lambda_j + \theta_j.$$

Nous cherchons à montrer que $\lambda_i = \lambda_j$ et $\theta_i = \theta_j$; résonnons par l'absurde et supposons $\lambda_i \neq \lambda_j$. Quitte à permuter les indices i et j, nous pouvons écrire que $\lambda_i < \lambda_j$ Comme la distance minimale qui sépare deux éléments de Λ est $\frac{1}{n}$, nous pouvons écrire que

$$\lambda_i \leq \lambda_j - \frac{1}{n};$$

de plus, $0 \leq \theta_i < \frac{1}{n}$. En faisant la somme des deux inégalités et en rappelant que $0 \leq \theta_i$, nous aboutissons à la contradiction suivante :

$$\lambda_i + \theta_i < \lambda_j \leq \lambda_j + \theta_j = \lambda_i + \theta_i.$$

Donc $\lambda_i = \lambda_j$ et par conséquent $\theta_i = \theta_j$; la somme $\Lambda + \Theta$ est bien directe. □

Corollaire 16. *$\widetilde{\Lambda}$ a bien le cardinal désiré pour être un spectre de $\widetilde{A}$. Autrement dit*

$$\#\widetilde{\Lambda} = \#\widetilde{A}.$$

Démonstration. Il suffit d'écrire les égalités successives suivantes :

$$\begin{aligned}
\#\widetilde{\Lambda} &= \#\left(\Lambda \oplus \Theta\right) \\
&= \#\left(\Lambda \times \Theta\right) \\
&= \#\Theta \ \#\Lambda \\
&= k \ \#A \\
&= \#\widetilde{A}.
\end{aligned}$$

□

Reste donc à prouver que les éléments de $\widetilde{\Lambda}$ génèrent bien des racines de $P_{\widetilde{A}}$.

Lemme 17. *Soit $\widetilde{\lambda}_i$ et $\widetilde{\lambda}_j$ deux éléments distincts de $\widetilde{\Lambda}$ et soit*

$$\xi = e^{2i\pi\left(\widetilde{\lambda}_i - \widetilde{\lambda}_j\right)}.$$

Alors $P_{\widetilde{A}}(\xi) = 0$.

Démonstration. Posons $\lambda_i, \lambda_j \in \Lambda$ et θ_i, θ_j tels que

$$\begin{aligned}
\widetilde{\lambda}_i &= \lambda_i + \theta_i \text{ et} \\
\widetilde{\lambda}_j &= \lambda_j + \theta_j.
\end{aligned}$$

Distinguons alors les cas suivants :

1°) $\theta_i \neq \theta_j$. Dans ce cas, $\widetilde{\lambda}_i - \widetilde{\lambda}_j$ peut s'écrire sous la forme $\frac{p}{n} + \frac{q}{kn}$ avec q non-multiple de k. Donc u est racine kn^{e} de l'unité, mais n'en est pas racine n^{e} ; c'est donc racine de Q.

2°) $\theta_i = \theta_j$. Dans ce cas, $\widetilde{\lambda}_i - \widetilde{\lambda}_j = \lambda_i - \lambda_j$ et ξ est racine de P_A.

Dans les deux cas, ξ est racine de $P_{\widetilde{A}} = P_A.Q$. □

L'ensemble $\widetilde{\Lambda}$ est donc bien un spectre de $\widetilde{A}$.

Autres transformations

Un cas assez particulier de multiplexage préserve également la condition spectrale.

Proposition 18. *Soit $(A_l)_{0\leq l<k}$ une famille finie de rythmes de même période n et de même cardinal ; supposons qu'il existe un spectre Λ commun à tous les A_l. Posons $\widetilde{A}$ comme étant le multiplexage des (A_l), comme défini dans la section 1.3 Alors le rythme $\widetilde{A}$ est spectral.*

Comme pour la répétition, écrivons le polynôme $P_{\widetilde{A}}$: Le polynôme de $\widetilde{A}$ s'écrit en fonction de ceux de A_l comme suit :

$$P_{\widetilde{A}} = \sum_{l=0}^{k-1} X^l . P_{A_l}(X^k).$$

Définissons alors les ensembles Θ et $\widetilde{\Lambda}$:

$$\Theta = \left\{ \frac{p}{kn} \mid p \in \mathbf{Z}/k\mathbf{Z} \right\} \text{ et}$$
$$\widetilde{\Lambda} = \frac{1}{k}\Lambda + \Theta.$$

Montrons que $\widetilde{\Lambda}$ est bien un spectre de $\widetilde{A}$. Comme précédemment, nous procéderons en deux temps : nous montrerons tout d'abord que le cardinal de $\widetilde{\Lambda}$ est bien celui de $\widetilde{A}$, puis que les éléments de $\widetilde{\Lambda}$ génèrent bien des racines de $P_{\widetilde{A}}$.

Lemme 19. *La somme de $\frac{1}{k}\Lambda$ et Θ est directe et par conséquent $\#\widetilde{\Lambda} = \#\widetilde{A}$.*

Démonstration. Remarquons que tout élément de $\frac{1}{k}\Lambda$ est situé dans l'intervalle $\left[0, \frac{1}{k}\right[$ et que la distance séparant deux éléments de $\left\{ \frac{p}{k} \mid p \in \mathbf{Z}/k\mathbf{Z} \right\}$ vaut au moins $\frac{1}{k}$. Nous pouvons alors appliquer le même raisonnement que pour la démonstration 3.2. Le corollaire 16 s'applique alors de façon semblable. □

Montrons alors que les éléments générés par $\widetilde{\Lambda}$ sont bien des racines de $P_{\widetilde{A}}$.

Lemme 20. *Soit $\widetilde{\lambda}_i$ et $\widetilde{\lambda}_j$ deux éléments distincts de $\widetilde{\Lambda}$ et soit*

$$\xi = e^{2i\pi\left(\widetilde{\lambda}_i - \widetilde{\lambda}_j\right)}.$$

Alors $P_{\widetilde{A}}(\xi) = 0$.

Démonstration. Posons $\lambda_i, \lambda_j \in \Lambda$ et $p_i, p_j \in \mathbf{Z}/k\mathbf{Z}$ tels que

$$\widetilde{\lambda}_i = \frac{1}{k}\lambda_i + \frac{p_i}{k} \text{ et}$$
$$\widetilde{\lambda}_j = \frac{1}{k}\lambda_j + \frac{p_j}{k}.$$

Distinguons alors les cas suivants :

1°) $\lambda_i \neq \lambda_j$. Dans ce cas, nous pouvons écrire

$$\widetilde{\lambda}_i - \widetilde{\lambda}_j = \frac{\lambda_i - \lambda_j}{k} + \frac{p}{k}.$$

Donc, pour tout l, $P_{A_l}\left(\xi^k\right)$ vaut

$$\begin{aligned} P_{A_l}\left(\xi^k\right) &= P_{A_l}\left(e^{2i\pi k\left(\frac{\lambda_i-\lambda_j}{k}+\frac{p}{k}\right)}\right) \\ &= P_{A_l}\left(e^{2i\pi(\lambda_i-\lambda_j+p)}\right) \\ &= P_{A_l}\left(e^{2i\pi(\lambda_i-\lambda_j)}\right) \\ &= 0 \end{aligned}$$

puisque Λ est spectre de A_l. Par conséquent,

$$\begin{aligned} P_{\widetilde{A}}(\xi) &= \sum_{l=0}^{k-1} \xi^l . A_l(\xi)^k) \\ &= \sum_{l=0}^{k-1} \xi^l . 0 \\ &= 0. \end{aligned}$$

2°) $\lambda_i = \lambda_j$. Dans ce cas

$$\widetilde{\lambda}_j - \widetilde{\lambda}_j = \frac{p}{k} \ :$$

ξ est alors une racine k^{e} de l'unité distincte de 1. Donc, pour tout l, $P_{A_l}\left(\xi^k\right)$ vaut

$$P_{A_l}\left(\xi^k\right) = P_{A_l}(1) = \#A_l = \#\Lambda.$$

La valeur de $P_{\widetilde{A}}(\xi)$ est alors

$$\begin{aligned} P_{\widetilde{A}}(\xi) &= \sum_{l=0}^{k-1} \xi^l . P_{A_l}\left(\xi^k\right) \\ &= \sum_{l=0}^{k-1} \xi^l . \#\Lambda \\ &= \#\Lambda . \left(\sum_{l=0}^{k-1} X^l\right)(\xi) \\ &= \#\Lambda . \sigma_k(\xi) \\ &= 0 \end{aligned}$$

car $\xi \in \mathbf{U}_k \setminus \{1\}$.

Nom	Signification
A	Rythme dont on cherche un spectre
$\widehat{\Lambda}$	Spectre proposé jusqu'à présent
Θ	Racines de Z_A qui peuvent éventuellement être ajoutées au spectre
ν	Racine de Z_A considérée pour l'ajout au spectre

TAB. 3.1 – Signification des variables de l'algorithme 3.3

Dans les deux cas, ξ est bien zéro de $P_{\widetilde{A}}$. □

Le zoom d'un rythme A, en tant que multiplexage d'un même rythme, rentre bien sûr dans le cadre de cette proposition.

3.3 Recherche de spectres

Nous nous sommes également intéressés à la recherche de spectres pour un rythme donné. Cette recherche se fait au moyen de l'algorithme 3.3, qui fonctionne par *backtracking*. La recherche se lance par l'appel spectre($\emptyset$, Z_A).

Nous cherchons à évaluer la complexité $T(k)$ de la fonction spectre en fonction de la longueur k de Θ. L'opération la plus complexe de chaque itération, hors appel récursif, est l'intersection d'ensemble qui nécessite le parcours de Θ et de $\nu.Z_A$. En faisant un simple calcul de phase, nous constatons qu'il est possible de se limiter à parcourir les k premiers éléments de $\nu.Z_A$ car les suivants ne peuvent appartenir à Θ. Le temps nécessaire à cette opération est donc, en supposant un mise en œuvre naïve de l'intersection de k^2. $T(k)$ vérifie alors l'inégalité récursive suivante

$$T(k) \leq C.n + 2.T(k-1).$$

pour une certain constante C. La complexité de spectre est donc en $O(2^n)$, comme on pouvait s'y attendre.

Algorithme 1 Recherche de spectre d'un rythme A par backtracking.

spectre($\widehat{\Lambda}$, Θ) :
si $\#\widehat{\Lambda} = \#A$ **alors**
  retourner $\widehat{\Lambda}$ {on a trouvé un spectre}
sinon si $\#\widehat{\Lambda} + \#\Theta < \#A$ **alors**
  retourner $\perp$ {la recherche ne peut plus aboutir}
sinon
  résultat $\leftarrow \perp$
  $\nu \leftarrow$ le plus petit élément de Θ
  $\Theta \leftarrow \Theta \setminus \{\nu\}$
  résultat $\leftarrow$ spectre($\widehat{\Lambda} \cup \{\nu\}$, $\Theta \cap (\nu + Z_A)$)
  si résultat $= \perp$ **alors**
    {si la première recherche n'a pas abouti}
    resultat $\leftarrow$ spectre($\widehat{\Lambda}$, Θ)
  fin si
  retourner résultat
fin si

Chapitre 4

Recherche de complémentaires par décomposition

Comme nous l'avons observé section 4.1, les anneaux $\mathbf{K}[X]/(P)$ se décomposent en produit d'anneaux plus simples. Nous nous intéressons ici à la possibilité d'utiliser ces décomposition dans le cadre de la recherche de complémentaire d'un rythme à période donnée. En d'autres termes, étant donné un polynôme $P_A \in \{0,1\}[X]/(X^n-1)$, nous cherchons à déterminer un $P_B \in \{0,1\}[X]/(X^n-1)$ tel que $P_A.P_B = \sigma_n$ en exploitant par la décomposition de $\mathbf{K}[X]/(X^n-1)$, avec $\mathbf{K} = \mathbf{Q}$ ou $\mathbf{K} = \mathbf{F}_2$.

4.1 Décomposition de $\mathbf{K}[X]/(X^n-1)$

Soit $\mathbf{K}$ un corps et P un polynôme de $\mathbf{K}[X]$. Soit $(P_i)_{1\leq i\leq q}$ ses facteurs irréductibles distincts et $(\gamma_i)_{1\leq i\leq q}$ leurs multiplicités respectives. Alors, d'après le théorème chinois, les anneaux $\mathbf{K}[X]/(P)$ et

$$\prod_{i=1}^{q} \mathbf{K}[X]/(P_i^{\gamma_i})$$

sont isomorphes. Plus précisément, à un ensemble polynômes $Q \in \mathbf{K}[X]/(P)$ correspondent les polynômes $(Q_i = Q \mod P_i^{\gamma_i}) \in \prod P_i^{\gamma_i}$. La reconstruction se fait en utilisant les restes chinois. De plus, si P est un polynôme irréductible, alors $\mathbf{K}[X]/(P)$ est un corps.

Pour faciliter l'étude et notamment la recherche de complémentaire dans $\mathbf{Q}[X]/(X^n-1)$ (dont $\mathbf{Z}[X]/(X^n-1)$ est sous-ensemble) et $\mathbf{F}_2[X]/(X^n-1)$, nous nous intéressons donc à la décomposition de ces ensembles en de tels produits.

Le morphisme de $\mathbf{K}[X]/(P)$ dans $\prod_{i=1}^{q} \mathbf{K}[X]/(P_i^{\gamma_i})$ associe à $Q \mod P$ le q-uplet :

$$\begin{pmatrix} Q & \mod P_1^{\gamma_1} \\ & \vdots \\ Q & \mod P_q^{\gamma_q} \end{pmatrix}.$$

Comme $P_i^{\gamma_i}$ est un facteur de P, $P = 0 \mod P_i^{\gamma_i}$ et tout représentant de la classe $Q \mod P$ appartient bien à la même classe modulo $P_i^{\gamma_i}$: cette définition à bien un sens.

Pour calculer le morphisme inverse, fixons un i tel que $1 \leq i \leq q$ et posons

$$\widehat{P}_i = \frac{P}{P_i^{\gamma_i}}.$$

P_i et $\widehat{P}_i$ sont alors premiers entre eux et, d'après l'égalité de Bézout, il existe U_i et $V_i \in K[X]$ tels que

$$U_i.P_i + V_i.\widehat{P}_i = 1.$$

Ces coefficients peuvent s'obtenir grâce à l'algorithme d'Euclide étendu. En posant $E_i = V_i.\widehat{P}_i$, nous obtenons alors un polynôme tel que

$$\begin{aligned} E_i &= 1 \mod P_i \\ E_i &= 0 \mod P_j \text{ lorsque } i \neq j. \end{aligned}$$

Pour un q-uplet quelconque $(Q_i \mod P_i)_{1 \leq i \leq q}$, il suffit alors de calculer la somme

$$\sum_{i=1}^{q} Q_i.E_i.$$

4.2 Décomposition dans $\mathbf{Z}[X]/(X^n - 1)$

Comme $X^n - 1 = \prod_{d|n} \Phi_d$ et que les Φ_d sont irréductibles, $\mathbf{Z}[X]/(X^n - 1)$ se décompose en

$$\mathbf{Q}[X]/(X^n - 1) \equiv \prod_{d|n} \mathbf{Q}[X]/(\Phi_d). \tag{4.1}$$

Comme Φ_d est irréductible, il est premier avec tout polynôme de degré inférieur. Par conséquent, tout $P \in \mathbf{Q}[X]/(\Phi_d)$ non nul vérifie la relation de Bézout :

$$U.Q + V.\Phi_d = 1$$

et a donc un inverse U modulo Φ_d. Chacun des $Q[X]/(\Phi_d)$ est donc un corps.

Comme $P \mod (\Phi_1 = X - 1) = P(1)$, $\sigma_n = \prod_{\substack{d|n \\ d \neq 1}} \Phi_d$ se décompose en

$$\begin{pmatrix} \sigma_n(1) = n \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Soit alors A un rythme, et $(A_d)_{d|n}$ sa décomposition, le terme A_d correspondant au polynôme cyclotomique Φ_d. Remarquons que $A_1 = A(1) = \#A$; pour que A est une chance de paver, il faut donc que A_1 divise n. Un rythme B qui fait paver A s'écrit alors $(B_d)_{d|n}$ qui vérifient les conditions suivantes :

$$B_1 = n(A_1)^{-1} = \frac{n}{\#A} \tag{4.2}$$

$$A_d \neq 0 \Rightarrow B_d = 0. \tag{4.3}$$

Remarquons que la condition (4.3) n'est vraie que parce que Φ_d est irréductible et que par conséquent tout $A_d \neq 0$ est inversible. La seule condition sur les B_d est que le résultat final doit être un élément de $\mathbf{Z}$ et même de $\{0,1\}$. Cependant, si cela nous permet de nous limiter aux B_d à coefficients dans $\mathbf{Z}$, se limiter aux coefficients $\{0,1\}$ est exclus. La difficulté est donc de trouver des $B_d \in \mathbf{Z}[X]/(\Phi_d)$ qui donne un $B \in \{0,1\}[X]/(X^n-1)$.

4.3 Décomposition dans $\mathbf{F}_2[X]/(X^n+1)$

Comme il nous est impossible de nous limiter aux polynômes à coefficients $\{0,1\}$ dans le cas précédent, nous pouvons nous demander si se limiter aux polynômes à coefficients dans $\mathbf{F}_2$ est intéressant. La première difficulté vient du fait que les polynômes irréductibles de $\mathbf{Z}[X]/(n)$e le sont plus nécessairement dans $\mathbf{F}_2[X]/(.)$ En effet, le produit n'est pas préservé en passant de $\mathbf{Z}[X]$ à $\mathbf{F}_p[X]$.

Plus précisément, si un polynôme est irréductible modulo p, il est irréductible dans $\mathbf{Z}$, mais pas l'inverse. Certains polynômes cyclotomiques peuvent notamment se décomposer une fois projetés sur $\mathbf{F}_2[X]$. Par exemple, $\Phi_7 = \sigma_7$ est irréductible dans $\mathbf{Z}[X]$, mais, dans $\mathbf{F}_2[X]$

$$(1+X+X^3)(1+X^2+X^3) = 1+X+X^2+3X^3+X^4+X^5+X^6 = \sigma_7,$$

puisque $3 = 1$ dans $\mathbf{F}_2$. Ceci est lié aux structures des anneaux $\mathbf{Z}[X]/(X^n-1)$ et $\mathbf{F}_p[X]/(X^n-1)$ qui sont par conséquent fort différentes.

Il en résulte que les γ_i ne sont plus nécessairement tous égaux à 1. Cependant ils sont tous égaux d'après le résultat suivant, suggéré par Emmanuel Amiot lors de nos échanges.

Proposition 21. *Soit $n \in \mathbf{N}^*$, p impair et k tels que $n = p.2^k$. Soit $(P^i)_{i\in I}$ les facteurs irréductibles de X^n+1 dans $\mathbf{F}_2$ et soit $(\gamma_i)_{i\in I}$ leurs multiplicités respectives. Alors*

$$\forall i \in I \quad \gamma_i = 2^k.$$

Démonstration. Remarquons tout d'abord que pour tout P et Q dans $\mathbf{F}_2[X]$, $(P+Q)^2 = P^2+2P.Q+Q^2 = P^2+Q^2$. Par récurrence, nous pouvons en déduire que $\forall P \in \mathbf{F}_2[X] \quad P^2 = P(X^2)$. Donc $X^n+1 = (X^p+1)^{2^k}$; X^n+1a donc

exactement les mêmes facteurs que X^p+1 avec une multiplicité multipliée par 2^k. Pour montrer le résultat, il suffit alors de montrer que la multiplicité des facteurs de X^p+1 pour tout p impair est 1. Si un facteur de X^p+1 a une multiplicité supérieure à 2, alors il est également facteur de $(X^p+1)' = p.X^{p-1} = X^{p-1}$. Or la seule racine de X^{p-1} est 0, qui n'est pas racine de X^n+1. Tous les γ_i sont donc égaux à 1. □

Cette fois, la multiplicité commune γ ne vaut pas 1, les $\mathbf{F}_2[X]/(P_i^\alpha)$ ne sont pas des corps. 0 est donc décomposable (en $P_i^{\gamma-1}.P_i$, par exemple) et les conditions sont plus compliquées. La décomposition de $\sigma_n = \frac{X^n+1}{X+1}$ est, en choisissant $P_1 = X+1$,

$$\begin{pmatrix} (X+1)^{\gamma-1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Considérons alors un polynôme P_A et notons sa décomposition

$$\begin{pmatrix} P_{A_1} = P_1^{\alpha_1}.P_{\widehat{A}_1} \\ \vdots \\ P_{A_q} = P_q^{\alpha_q}.P_{\widehat{A}_q} \end{pmatrix}$$

avec les $(P_{\widetilde{A}_i})$ respectivement non-multiples des (P_i). Nous cherchons un B se décomposant de façon similaire en

$$\begin{pmatrix} P_{B_1} = P_1^{\beta_1}.P_{\widehat{B}_1} \\ \vdots \\ P_{B_q} = P_q^{\beta_q}.P_{\widehat{B}_q} \end{pmatrix}$$

tel que $P_A.P_B = \sigma_n \mod X^n+1$, donc tel que

$$\begin{aligned} P_{A_1}.P_{B_1} &= (X+1)^{\gamma-1} \\ \forall i \neq 1 \quad P_{A_i}.P_{B_i} &= 0. \end{aligned}$$

Pour qu'il existe un tel P_B, il suffit que $P_{A_1} \neq 0$. Les (P_{B_i}) doivent alors vérifier les conditions suivantes.

$$\beta_1 = \gamma - \alpha_1 - 1 \tag{4.4}$$

$$P_{\widehat{B}_1} = P_{\widehat{A}_1}^{-1} \tag{4.5}$$

$$\beta_i \geq \gamma - \alpha_i. \tag{4.6}$$

Autrement dit, P_B se décompose en

$$\begin{pmatrix} P_1^{\gamma-\alpha_1-1}.P_{\widehat{A}_1}^{-1} \\ P_2^{\gamma-\alpha_2}.P\widehat{B}_2 \\ \vdots \\ P_q^{\gamma-\alpha_q}.P\widehat{B}_q \end{pmatrix}$$

avec $P_{\widehat{B}_i} \in \mathbf{F}_2[X]/(P_i^{\alpha_i})$.

Cette-fois, nous sommes sûr que le polynôme obtenu sera à coefficients dans $\{0,1\}$ et pavera modulo 2, mais il faut encore vérifier que le produit pave dans $\mathbf{Z}$. Pour cela, il faut et suffit de vérifier que $A(1)B(1) = n$, c'est-à-dire s'intéresser au nombre de coefficients de B. Il faut donc tester

$$\#\left(\prod_{i=2}^{q} \mathbf{F}_2[X]/(P_i^{\alpha_i})\right) = \prod_{i=2}^{q} \#\left(\mathbf{F}_2[X]/(P_i^{\alpha_i})\right) = \prod_{i=2}^{q} 2^{\alpha_i \deg P_i}. = 2^{\sum_{i=2}^{q} \alpha_i \deg P_i}$$

Ce nombre augmente avec les α_i, qui exprime les libertés que laisse A dans la recherche d'un complémentaire. Il est à mettre en vis-à-vis du nombre de polynômes à tester en prenant juste en compte la contrainte de cardinal. Dans ce cas, il faut examiner tous les polynômes à coefficients dans $\{0,1\}$ de degré inférieur à n, et dont $\frac{n}{\#A}$ coefficients valent 1. Ces polynômes sont au nombre de

$$\binom{n}{\frac{n}{\#A}}$$

Il n'est donc pas intéressant d'utiliser cette démarche pour les cas peu contraints.

Conclusion et perspectives

Nous avons lors de ce stage exploré les liens qui unissaient les canons de Vuza. Pour cela, nous avons fait le parallèle avec les résultats d'Amiot concernant les conditions de Coven et Meyerowitz. Cela nous renforce dans notre idée que les deux sont plus fortement corrélés que nous ne le savons pour le moment.

La conjecture de Fuglede, bien que nous sachions qu'elle est fausse à partir de la dimension 3, est encore un problème ouvert pour le pavage de la ligne. En nous intéressant à son rapport avec le pavage du cercle, nous espérons avoir apporté notre petit pierre à l'édifice qu'est la recherche sur le sujet.

Comme nous l'avons constaté dans la section 3.2, le multiplexage de rythmes qui pavent avec les mêmes entrées préserve la condition spectrale. Nous pouvons alors nous demander si le spectre d'un canon et de ses complémentaires sont liés, comme l'avaient conjecturé (à tort) Lagarias et Wang dans le cas des dimensions quelconques. Nous avons commencé à nous intéresser à ce problème en munissant les ensembles $\mathbf{K}[X]/(X^n-1)$ de structures en treillis. Le but de la démarche est de définir un éventuel « plus petit complémentaire » d'un canon n-périodique donné.

Les algorithmes que nous avons mis-en-œuvre au sein d'OpenMusic seront, nous l'espérons, utiles à l'un ou l'autre musicien. Si la recherche de rythmes complémentaires à un canon donné semble être difficile à résoudre (certains indices poussent à croire qu'il s'agit d'un problème NP-complets, [11]), les méthodes que nous proposons peuvent demeurer intéressantes par rapport à celle disponible actuellement dans OpenMusic et basées sur des techniques de résolution de contraintes. En effet, elles permettent d'exploiter la structure algébriques de canons et donc de limiter l'espace de recherche. Cependant, les deux ont leurs inconvénients : décomposer un polynôme de $\mathbf{Z}[X]/(X^n-1)$ nous forcé à chercher des polynômes à coefficients entiers quelconque alors que le décomposer dans $\mathbf{F}_2[X]/(X^n-1)$ ne nous assure que d'obtenir un canon qui pave modulo 2. Il serait intéressant de chercher à combiner les deux, en étudiant par exemple les rapports entre les polynômes cyclotomiques et les polynômes irréductibles de $\mathbf{F}_2[X]/(X^n-1)$.

Bibliographie

[1] E. Amiot. À propos des canons rythmiques. *Gazette des mathématiciens*, 106, Octobre 2005.

[2] E. Amiot. Rhythmic canons and galois theory. In H. Fripertinger and L. Reich, editors, *Proceedings of the colloquium on MaMuTh*, volume 347, pages 1–25, Graz, Austria, 2005. Colloquium on Mathematical Music Theory, Grazer Mathematische Berichte.

[3] E. Amiot. Gammes bien réparties et transformée de fourier discrète, April 2006.

[4] E. Amiot, M. Andreatta, and C. Agon. Tiling the (musical) line with polynomials : Some theoretical and implementational aspects. In *ICMC 2005*, pages 227–230, Barcelona, Espagne, September 2005.

[5] E. M. Coven and A. Meyerowitz. Tiling the integers with translates of one finite set. *Journal of Algebra*, 212(1) :161–174, February 1999.

[6] N. G. de Bruijn. On number systems. *Nieuw Archief voor Wiskunde*, 3(4) :15–17, 1956.

[7] M. Demazure. *Cours d'algèbre*. Nouvelle bibliothèque mathématique. Cassini, 1997.

[8] R. W. Hall and P. Klinsberg. Asymmetric rhythms and tiling canons. *American Mathematical Monthly*, 113(10) :887–896, 2006.

[9] F. Jedrzejewski. *Mathematical theory of music*. collection Musique/sciences. Ircam/Delatour Paris, 2006.

[10] M. N. Kolountzakis and M. Matolsci. Tiles with no spectra. To appear in Forum Math., June 2004.

[11] M. N. Kolountzakis and M. Matolsci. Complex Hadamard matrices and the spectral set conjecture. *Collectanea Mathematica*, Extra :281–291, 2006.

[12] S. Konyagin and I. Łaba. Spectra of certain types of polynomials and tiling of integers with translates of finite sets. *Journal of Number Theory*, 103 :267—280, September 2004.

[13] I. Łaba. The spectral set conjecture and multiplicative properties of roots of polynomials. *Journal of the London Mathematical Society*, 65(3) :661–671, 2002.

[14] I. Łaba. Tiling problems and spectral sets, February 2002.

[15] A. Poli and P. Guillot. *Algèbre et protection de l'information.* Hermes Science Publications, 2005.

[16] W. Rudin. *Fourier analysis on groups.* Wiley Interscience, 1962.

[17] R. Tijdeman. Decomposition of the integers as a direct sum of two subsets. In S. David, editor, *Number Theory*, London Mathematical Society Lecture Note Series, pages 261–276. Cambridge University Press, 1995.