MATHÉMATIQUES ET MUSIQUE

À propos des canons rythmiques

Emmanuel Amiot[1]

Cet article fait le point sur une notion riche, issue de préoccupations musicales mais qui s'est avérée féconde en problèmes mathématiques fascinants.

En particulier l'étude des canons rythmiques a permis de découvrir des résultats inédits sur les corps finis et de démontrer de nouveaux cas de la conjecture spectrale. En retour, bien sûr, les outils mathématiques performants utilisés ont donné de nouvelles dimensions à explorer aux compositeurs. La théorie de Galois a donc fait une apparition inattendue dans certains logiciels d'aide à la Composition assistée par ordinateur !

Des illustrations musicales (ou en tout cas, sonores...) de cet article peuvent être trouvées sur le site `http://canonsrythmiques.free.fr/Midi`, sous forme de fichiers MIDI.

Notations

Je note $\mathbb{Z}_n$ le groupe (parfois l'anneau) quotient $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{F}_q$ est le corps à q éléments.

Dans tout anneau, $a \mid b$ signifie que a divise b.

Φ_n désigne le $n^{\text{ème}}$ polynôme cyclotomique dans $\mathbb{Z}[X]$.

Enfin $[\![a, b]\!]$ désigne l'intervalle d'entiers $[a, b] \cap \mathbb{Z}$.

Canons musicaux et canons rythmiques

Canon musical

Le principe du canon musical est probablement bien connu du lecteur ; l'exemple le plus connu des francophones est sans doute « *Frère Jacques* », qui se chante de préférence à quatre, chaque chanteur reprenant exactement la même comptine mais décalée d'une mesure par rapport au chanteur précédent.

Frère Jacques, frère Jacques	Dormez-vous ? dormez-vous ?	Sonnez les matines, sonnez les matines	Ding deng dong, ding, deng dong
	Frère Jacques, frère Jacques	Dormez-vous ? dormez-vous ?	Sonnez les matines, sonnez les matines
		Frère Jacques, frère Jacques	Dormez-vous ? dormez-vous ?
			Frère Jacques, frère Jacques

[1] Pianiste et compositeur.

qui devient, en régime de croisière,

Frère Jacques, frère Jacques	Dormez-vous ? dormez-vous ?	Sonnez les matines, sonnez les matines	Ding deng dong, ding, deng dong
Ding deng dong, ding, deng dong	Frère Jacques, frère Jacques	Dormez-vous ? dormez-vous ?	Sonnez les matines, sonnez les matines
Sonnez les matines, sonnez les matines	Ding deng dong, ding, deng dong	Frère Jacques, frère Jacques	Dormez-vous ? dormez-vous ?
Dormez-vous ? dormez-vous ?	Sonnez les matines, sonnez les matines	Ding deng dong, ding, deng dong	Frère Jacques, frère Jacques

Ce principe de jouer une même mélodie (ou une forme légèrement déformée de la même mélodie) le long de diverses voix est aussi celui de la fugue, dont le plus célèbre spécialiste est J.S. Bach.

C'est tout un art (de la fugue !) que de faire coïncider harmonieusement des notes diverses avec un décalage. J.S. Bach, justement, a par exemple montré sa virtuosité dans les *Variations Goldberg* où il fait des canons décalés dans le temps et dans l'espace des hauteurs, successivement d'un unisson, d'une seconde, d'une tierce, etc.

Pour modéliser de façon constructive les canons, nous allons nous montrer moins ambitieux, en nous concentrant exclusivement sur le domaine rythmique, et plus exigeants, en posant une condition rigoureuse :

sur chaque temps, on doit entendre une seule note.

Sans cette contrainte, on pourrait (on peut !) faire un canon fondé sur n'importe quel motif. Cela n'a pas grand intérêt, sauf peut-être combinatoire.

Le canon rythmique « canonique », si j'ose dire, est donc fondé sur un pattern rythmique discret, qu'on peut imaginer joué par un instrument de percussion (on néglige la question de la durée des notes), pattern qui est répété à l'identique par d'autres voix.

On peut alors modéliser ce pattern très simplifié par une série d'entiers, qui repèrent les moments où une note est jouée. Sans perte de généralité, on peut fixer l'origine des temps à la première note du pattern, qui va donc commencer par le nombre 0. Le principe même du canon signifie que les diverses entrées du motif sont obtenues par des translations, égales aux décalages avec la première entrée : les diverses voix seront $A, A + b_1, A + b_2$...

En mettant dans un même vecteur tous ces décalages, on obtient une première formalisation, provisoire :

Définition 1. — *Soit* $A = \{0, a_1, \dots a_{k-1}\}$ *un sous-ensemble de* $\mathbb{N}$ *;*

A sera le motif (inner rhythm) d'un canon rythmique s'il existe un pattern des voix (outer rhythm) $B = \{0, b_1, \dots b_{\ell-1}\}$ *tel que* $A \times B \ni (a, b) \mapsto a + b$ *est injective.*
A est le motif du canon, B la séquence des entrées (les moments où chaque instrument commence sa partie).

Cette condition s'écrit aussi $A + B = A \oplus B$.

Exemple. — Le motif $A = \{0, 1, 3, 6\}$ donne un canon à quatre voix avec $B = \{0, 4, 8, 12\}$. En effet, $A \oplus B = \{0, 1, 3, 4, 5, 6, 7, 10\}$. Une représentation simplifiée de partition en est donnée figure 1.

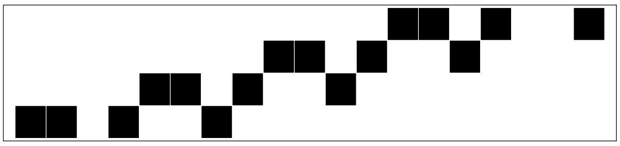

Fig. 1 – Un canon rythmique

Remarque 1. — Chaque note est jouée sur un multiple entier de l'unité de temps ; ceci peut paraître une contrainte artificielle et forte, mais en fait aussi bien Dan Tudor Vuza [20], qui est le pionnier des recherches sur les canons rythmiques, que Lagarias [15] dans un article purement mathématique, ont montré essentiellement que ce cas est le seul possible pour un motif fini.

Un corollaire élémentaire de la définition :

Proposition (Dualité). — *Si $A \oplus B$ est un canon rythmique, il en est de même de $B \oplus A$: on peut échanger les rôles des inner et outer rhythms.*

La commutativité de l'addition permet donc de fabriquer un canon à p voix de q notes en partant d'un canon à q voix de p notes. Avec 4×5 ou 5×4 notes, on obtient par exemple la figure 2.

Un canon et son dual

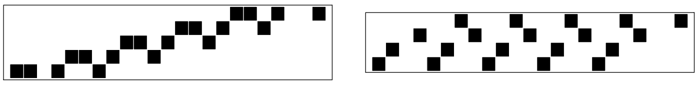

Fig. 2 – Deux canons duaux

Canons périodiques

On remarque, sur l'exemple ci-dessus, qu'il y a des trous dans le canon —- que les musiciens appellent des silences — mais que ces trous se trouveraient naturellement bouchés par d'autres copies du motif. En fait on peut obtenir un canon infini avec une note et une seule par temps, soit avec un nombre infini de voix, soit de façon plus réaliste en prolongeant le motif par périodicité (ici la période 8) comme on le constate sur la figure 3, qui reprend le motif de la figure 1.

Variations sur un canon

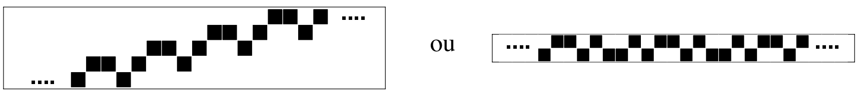

Fig. 3 – Canon prolongé à l'infini

On obtient ainsi un *pavage périodique* de $\mathbb{Z}$ par le motif A. Dorénavant, je parlerai donc indifféremment de pavages (pavages de $\mathbb{Z}$) ou de canons rythmiques. Par passage au quotient, cela revient à dire que l'on a un pavage du groupe cyclique $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. D'où une nouvelle définition, plus restrictive, qui est celle que nous considérerons désormais :

Définition 2. — *On a un canon rythmique de motif* $A = \{a_0, \dots a_{k-1}\}$ *et de période* n *s'il existe* $B \subset \mathbb{N}$ *tel que*

$$A \oplus B = \mathbb{Z}_n.$$

La condition de somme directe ($\oplus$) exprime que sur chaque temps on a exactement une note et une seule.

Exemple. — Le motif $A = \{0, 1, 3, 6\}$ donne un canon de période 8 avec $B = \{0, 4\}$. En effet, $A \oplus B = \{0, 1, 3, 4, 5, 6, 7, 10\} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ si on travaille modulo 8. C'est l'effet obtenu si on reprend périodiquement ce canon (comme *Frère Jacques*).

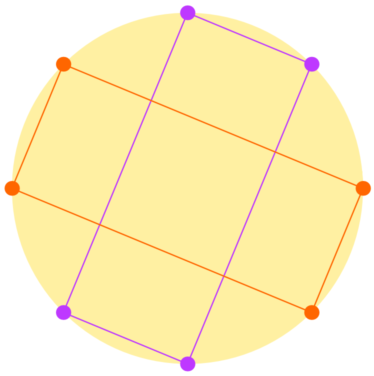

Fig. 4 – La forme d'un motif est définie à une rotation près

Remarque 2. — Comme $\mathbb{Z}_n$ est cyclique, la notion de pavage ou de canon rythmique est indépendante d'un choix d'origine de ce cercle comme on le voit sur les figures 4 et 5. C'est pourquoi en pratique on convient, sans perte de généralité, que A, B commencent par 0. Formellement cela est lié à l'action du groupe $\mathbb{Z}_n$ sur ses parties par translation.

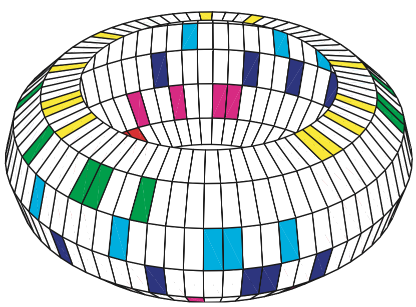

Fig. 5 – Un canon de Vuza, de période 108

Cette condition de périodicité que nous avons apparemment imposée semble très forte. Mais on connait depuis 1950 le théorème suivant :

Théorème 1 (de Bruijn). — *Si A est une partie finie de $\mathbb{N}$ telle qu'il existe $C \subset \mathbb{Z}$ avec $A \oplus C = \mathbb{Z}$, alors il existe un entier n et une partie (finie) B tels que $C = B \oplus n\mathbb{Z}$. Donc le pavage est périodique, et $A \oplus B = \mathbb{Z}_n$.*

La démonstration de ce théorème repose sur l'incontournable principe des tiroirs, je laisse le lecteur intéressé se référer à [2] et à la figure suivante.

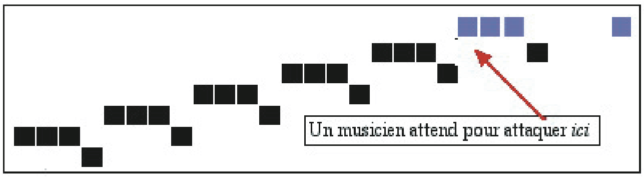

Fig. 6 – Pourquoi tout canon de motif fini est périodique

Mentionnons à ce propos un premier problème ouvert : Si $\ell(A) = \max A - \min A$ est la largeur du motif A, la démonstration de De Bruijn montre que $n \leqslant 2^{\ell(A)}$ majore la période du canon, mais tous les exemples connus vérifient $n \leqslant 2 \times \ell(A)$... Est-ce général ?

Exercice 1. — Donner un motif de largeur ℓ pour lequel la plus petite période possible du canon est effectivement 2ℓ (solution en fin d'article).

En revanche un motif infini peut très bien donner un canon apériodique (par exemple les nombres dont l'écriture binaire n'a que des bits d'ordre impairs), ainsi que des pavages plus « tordus » [2].

Modélisation polynomiale et facteurs cyclotomiques

Pour travailler dans une structure plus riche, on fait comme Sophus Lie passant d'un groupe de Lie à son algèbre : par exponentiation.

Polynôme associé à un motif rythmique

On va enrichir la structure algébrique ambiante, remplaçant les sommes d'ensembles par des produits de polynômes.

Définition 3. — *Soit $A \subset \mathbb{N}$ un sous-ensemble fini non vide. Alors on pose $A(X) = \sum_{k \in A} X^k$.*

Proposition. — *La somme $A + B$ est directe (i.e. $A \times B \ni (a, b) \mapsto a + b$ est injective) ssi*

$$A(X) \times B(X) = (A \oplus B)(X)$$

Sinon on trouverait des coefficients strictement plus grand que 1. Et donc la définition des canons rythmiques est la condition suivante, notée (T_0) :

Théorème 2. — *A est le motif d'un canon rythmique avec « motif des entrées » B et période n ssi*

$$(T_0) \qquad A(X) \times B(X) = 1 + X + X^2 + \dots X^{n-1} \pmod{X^n - 1}.$$

Par exemple $\{0, 1, 3, 6\} \oplus \{0, 8, 12, 20\}$ donne les polynômes

$$(1 + X + X^3 + X^6) \times (1 + X^8 + X^{12} + X^{20})$$

dont le produit est

$$1+X+X^3+X^6+X^8+X^9+X^{11}+X^{12}+X^{13}+X^{14}+X^{15}+X^{18}+X^{20}+X^{21}+X^{23}+X^{26}$$

qui se réduit modulo $X^{16} - 1$ à $1 + X + \dots X^{15}$ — concrètement on applique la règle $X^k \to X^{k \mod n}$.

N.B. : c'est en découvrant cette formalisation appliquée par Andranik Tangian [16] à un problème de Tom Johnson que je me suis enthousiasmé pour la cause des canons rythmiques ; mais ce procédé remonte à Redei dans les années 1950.

Les 'perfect square tilings' de Tom Johnson

Le but de ce paragraphe est de montrer sur un exemple assez simple que l'introduction des polynômes n'est pas qu'une simple commodité d'écriture : si on sort l'artillerie lourde, c'est qu'elle s'impose pour l'étude des canons ! On sait plus de choses dans une algèbre que dans le monoïde $\mathcal{P}(\mathbb{Z}_n)$...

T. Johnson, compositeur minimaliste américain vivant à Paris, s'est posé récemment la question de réaliser une forme très particulière de canon (canon avec augmentations) avec le motif très simple T_1 =(0 1 2) mais avec les contraintes suivantes :

– utilisez des augmentations de ce motif, $T_2 = 2 \times T_1, \dots T_k$ (au sens musical : comprenez des multiples, translatés, comme (5 9 13)= $5 + T_4 = 5+(0\ 4\ 8)=$ $5 + 4 \times T_1$),
– les multiplicandes sont tous distincts,
– et on pave de façon 'compacte', *i.e.* sans faire de réduction modulo *n*.

Ce problème a été exposé dans la rubrique de J.P. Delahaye dans *Pour la science* (novembre 2004) ce qui a donné l'occasion à plusieurs lecteurs, bons programmeurs, de trouver des solutions avec le motif initial (0 1 2 3) — à cette heure la question de l'existence d'un pavage parfait pour un motif de 5 notes est ouverte.

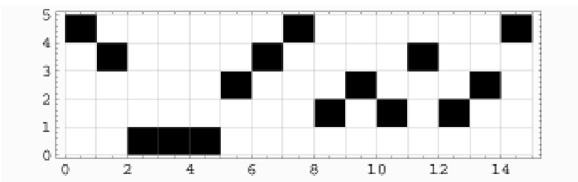

Fig. 7 – Plus petit 'perfect sqare tiling'

Quand Tom s'est ouvert de cette nouvelle question, il nous a présenté la plus petite solution (cf. figure 7, où l'on voit T_1 aux échelles 1,2,4,5,7), et une question troublante : pourquoi était-il impossible de trouver un 'pavage en carré parfait' avec seulement un ou deux des motifs T_3, T_6, T_9 ? Son programme lui donnait soit les trois à la fois (figure suivante), soit aucun.

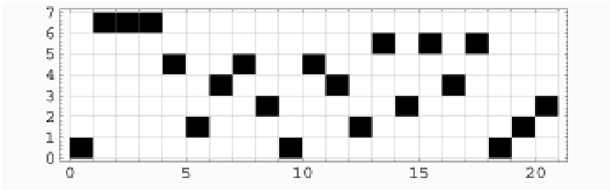

Fig. 8 – Plus petit 'perfect square tiling' avec T_3, T_6, T_9

Cette petite question admet une solution très simple, si l'on exprime le motif de base par le polynôme $\Phi_3(X) = 1 + X + X^2$, ses augmentations sont de la forme $X^k(1 + X^i + X^{2i}) = X^k\Phi_3(X^i)$, et la question de Tom revient à trouver une expression algébrique de la forme

$$\sum_{i\in I} X^{k_i}\Phi_3(X^i) = 1 + X + \ldots = \sum_{j=0}^{3n-1} X^j = \frac{X^{3n}-1}{X-1}.$$

Exercice 2. — Montrer que dans une relation comme la précédente, le nombre d'indices i qui sont multiples de 3 est lui-même un multiple de 3.

Polynômes cyclotomiques

L'intérêt de ce changement d'espace, de $\mathbb{Z}$ à une partie de $\mathbb{Z}[X]$, est que l'on sait plusieurs choses sur les polynômes qui apparaissent dans notre problème (voyez n'importe quel bon livre d'algèbre commutative pour une preuve du théorème suivant).

Théorème 3. — *Les facteurs irréductibles (dans $\mathbb{Q}[X]$ ou $\mathbb{Z}[X]$) de $1 + X + X^2 + \ldots + X^{n-1}$ sont les célèbres polynômes cyclotomiques Φ_d, avec $d \mid n$ (et $d > 1$ ici). Φ_d est le produit (dans $\mathbb{C}[X]$) des $X - \xi$ où ξ décrit l'ensemble des racines de l'unité d'ordre exactement d.*

On peut les calculer par récurrence par la formule $\prod_{d|n} \Phi_d(X) = X^n - 1$ ou par inversion de Möbius $\Phi_n(X) = \prod_{d|n}(X^d - 1)^{\mu(d)}$.

Leurs coefficients sont entiers (relatifs). On a par exemple $\Phi_p(X) = 1 + X + X^2 + \ldots + X^{p-1}$ quand (ssi) p est premier.

On a tout de suite un critère très utile qui résulte du théorème précédent.

Corollaire 1. — *Pour un canon de période n, chaque polynôme cyclotomique $\Phi_d, 1 < d \mid n$, divise $A(X)$ ou $B(X)$.*

Ceci résulte du théorème du Gauss dans l'anneau principal $\mathbb{Q}[X]$, appliqué à la relation (T_0) (cf. Théorème 2). Ce phénomène explique une remarque d'Andreatta, faite sur les canons de Vuza (cf. infra), observant que beaucoup de canons sont « presque » (*i.e.* à peu de termes près, voire exactement) des palindromes. En effet, tous les polynômes cyclotomiques sont autoréciproques, *i.e.* palindromiques, ainsi que leurs produits. Comme ce sont (presque) les seuls facteurs de $A(X), B(X)$ cela explique que ces derniers sont (presque) palindromiques.

Nous verrons que la répartition de ces facteurs cyclotomiques entre $A(X)$ et $B(X)$ est cruciale pour permettre l'existence d'un canon rythmique.

Le cas de Φ_p d'indice premier admet une généralisation utile quoique élémentaire (récurrence) :

Lemme 1. — *On a $\Phi_d(1) \neq 1$ ssi d est une puissance d'un nombre premier.*
Si $d = p^\alpha$ on a alors $\Phi_d(1) = p$, car

$$\Phi_{p^\alpha}(X) = 1 + X^{p^{\alpha-1}} + X^{2p^{\alpha-1}} + \ldots + X^{(p-1)p^{\alpha-1}}.$$

Par exemple, $\Phi_9 = 1 + X^3 + X^6$.

Les conditions de Coven-Meyerowitz

Avant 1998, on ne connaissait quasiment aucune condition générale pour déterminer si le motif A était capable d'engendrer un canon rythmique, *i.e.* de paver (à l'exception du cas où $|A|$ était une puissance d'un nombre premier).

Exercice 3. — Sauriez-vous dire par exemple si $(1, 4, 9, 16)$ forme un canon rythmique ?

Des considérations précédentes, les deux mathématiciens Aaron Meyerowitz et Etan Cohen ont déduit (cf. [5]) les critères suivants :

Théorème de Coven-Meyerowitz. — *Soit R_A l'ensemble des $d \in \mathbb{N}$ où Φ_d divise $A(X)$, et S_A le sous-ensemble des puissances de nombres premiers éléments de R_A. On définit alors les conditions*

$$\text{et } \begin{cases} (T_1) : A(1) = \prod\limits_{p^\alpha \in S_A} p, \\ (T_2) : \text{si } p^\alpha, q^\beta, \cdots \in S_A \text{ alors } p^\alpha . q^\beta \cdots \in R_A. \end{cases}$$

Alors
- Thm A1. — *Si A pave, alors (T_1) est vérifiée.*
- Thm A2. — *Si (T_1) et (T_2) sont vérifiées, alors A pave.*
- Thm B. — *Si $|A| = A(1)$ n'a que deux facteurs premiers et si A pave, alors (T_2) est vérifiée.*

Donnons un exemple. — Le motif $A = \{0, 1, 8, 9, 17, 28\}$ a un polynôme associé qui se factorise en

$$\begin{aligned}(1+X)\left(1-X+X^2\right)\left(1+X+X^2\right)\left(1-X^2+X^4\right)\left(1-X^3+X^6\right)\\ \left(1+X^3-X^4-X^7+X^8-X^9+X^{11}-X^{12}+X^{13}\right)\end{aligned}$$

On reconnaît[2] les facteurs cyclotomiques d'indices $2, 3, 6, 12, 18$, plus un outsider qui n'est pas cyclotomique du tout. On a donc $R_A = \{2, 3, 6, 12, 18\}, S_A = \{2, 3\}$; or $2 \times 3 = 6$, ce qui prouve à la fois (T_1) (car $A(1) = 6$) et (T_2) (car $6 \in R_A$). Effectivement, A pave.

[2] j'ai dû implémenter pour cela une procédure qui marie harmonieusement théorie de Galois et mathématiques numériques, utilisant notamment que si toutes les racines d'un polynôme unitaire irréductible à coefficients entiers sont de module 1, alors ce sont des racines de l'unité. La précision du calcul a dû être adaptée au degré du polynôme passé en variable !

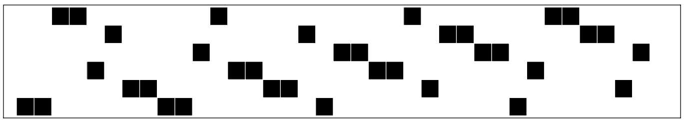

Fig. 9 – Canon vérifiant $(T_1)\&(T_2)$

Seul le troisième de ces résultats (Thm B) est véritablement difficile ; il repose sur un lemme de Sands qui prouve que A ou B est inclus dans $p\mathbb{Z}$ (où p est l'un des deux facteurs premiers), ce qui est faux dans le cas général, et ce en utilisant un résultat on ne peut plus Galoisien :

Lemme 2. — *Si n est premier avec m alors* Φ_n *est encore irréductible dans le corps cyclotomique* $\mathbb{Q}[e^{2i\pi/m}]$.

Qu'on me pardonne de mentionner ce résultat technique : dans une partie ultérieure où l'on travaille dans $\mathbb{F}_q[X]$, les Φ_n cessent généralement d'être irréductibles et le contraste avec la situation en caractéristique 0 méritait, je pense, d'être mentionné.

Cet article serait interminable si toutes les démonstrations y figuraient, mais je vais tout de même reproduire brièvement ici la démonstration du (Thm A1), qui illustre bien l'intérêt d'avoir élargi le contexte de parties de $\mathbb{Z}_n$ à une algèbre de polynômes.

Démonstration. La preuve repose sur le lemme 1. Observons que si $A \oplus B = \mathbb{Z}_n$, on a en termes de polynômes $A(1)B(1) = n$. Mais dans la décomposition en facteurs premiers de $A(1)B(1)$ figurent tous les $\Phi_d(1)$, qui valent 1 ou p (ce dernier cas ssi d est une puissance de p). Le nombre premier p figure un nombre de fois égal au nombre de puissances de p qui divisent n, *i.e.* sa multiplicité dans n.

Donc les facteurs premiers de n apparaissent dans $A(1)B(1)$ sous la forme $\Phi_{p^\alpha}(1)$ et seulement sous cette forme. Les autres facteurs (cyclotomiques ou pas) de $A(X)$ (ou $B(X)$) contribuent seulement pour la valeur 1 quand $X = 1$, puisque tous les facteurs de n sont recensés.

La valeur de $A(1)$ est donc égale au seul produit des facteurs premiers p tels que Φ_{p^α} soit un facteur de $A(X)$: c'est bien la condition (T_1). □

Notons sans insister, pour l'instant, qu'on ignore toujours aujourd'hui si la condition (T_2) est nécessaire dans tous les cas pour paver.

Ces conditions ne sont pas dénuées d'applications pratiques : en septembre, nous avons présenté à Barcelone pour l'ICMC[3] une nouvelle fonctionnalité du logiciel d'aide à la composition *OpenMusic*, développé à l'IRCAM notamment par Carlos Agon et Moreno Andreatta, et qui permet de fabriquer des « canons cyclotomiques », de période donnée, en utilisant les conditions ci-dessus.

3 International Computer Music Conference

Canons et corps finis

Nous allons faire un détour instructif en généralisant de façon naturelle la notion de canon rythmique à celle de canon modulo p. Il s'agit alors d'avoir sur chaque temps un nombre de notes égal à 1 modulo p, condition plus généreuse que « une note et une seule ». On se retrouve naturellement à factoriser des polynômes dans l'anneau $k[X]$, où k est un corps fini. En effet, comme on l'a vu, la condition définissant un canon rythmique est

$$(T_0) \qquad A(X) \times B(X) = 1 + X + X^2 + \ldots + X^{n-1} \mod (X^n - 1).$$

La question se pose alors de considérer les facteurs irréductibles de cette identité polynômiale. Dans le cas de $\mathbb{Z}[X]$ on avait affaire aux polynômes cyclotomiques ; dans l'exposé qui suit la situation est plus compliquée, notamment du fait de la multiplicité > 1 des racines (de l'unité).

Le problème de Johnson

Je résume ici le problème qui m'a poussé à considérer des factorisations dans des corps finis en lieu et place de $\mathbb{Z}[X]$.

Tom Johnson a présenté en 2001 aux *Journées d'Informatique Musicale* [10] le problème suivant de canon par augmentations.

Faire un canon (compact) avec le motif (0 1 4) et (certaines de) ses augmentations $(0, 2, 8)$ (ainsi que $(0, 4, 16)$ etc). Le compositeur et mathématicien A. Tangian, de l'université de Hanovre, rédigea aussitôt [16] un programme en Fortran pour calculer toutes les solutions de taille bornée par un N donné ; il s'avéra que toutes ces solutions avaient une longueur multiple de 15. La plus petite se trouve sur la figure suivante.

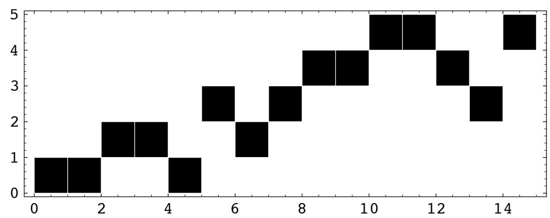

Fig. 10 – Le plus petit pavage avec (0 1 4) et augmentations

Qu'elles soient multiples de 3 n'avait rien de surprenant, mais pourquoi de 15 ?

Si l'on pose $J(X) = 1 + X + X^4$, le problème de Johnson revient à trouver des facteurs 0-1 $A, B \ldots$ tels que

$$A(X)J(X) + B(X)J(X^2) \ldots = 1 + X + X^2 + \ldots X^{n-1}$$

En effet, une augmentation comme $(0, 2, 8)$ a pour polynôme associé $J(X^2) = 1 + X^2 + X^8$.

Dans la plus petite solution, on a $A(X) = 1 + X^2 + X^8 + X^{10}$ et $B(X) = X^5$ pour $n = 15$.

Je me suis demandé s'il y avait moyen de trouver une racine commune de tous ces facteurs. Pour cela il s'est avéré nécessaire de changer de corps. En effet, dans tout corps de caractéristique 2 on a

$$J(X^2) = 1 + X^2 + X^8 = (1 + X + X^4)^2 = \big(J(X)\big)^2$$

par l'automorphisme de Frobenius[4] on a plus généralement

Lemme 3. — *Pour tout polynôme $A(X)$ à coefficients dans $\mathbb{F}_p$, on a $A(X)^p = A(X^p)$.*

De même $J(X^4) = J(X)^4$ et ainsi de suite.

Donc $J(X)$ doit diviser $1+X+X^2+\ldots+X^{n-1}$ à condition de calculer modulo 2. Or J se décompose dans le corps $\mathbb{F}_{16}$ à 16 elements (résultat élémentaire de Galois : J est irréductible sur $\mathbb{F}_2$ et donc $\mathbb{F}_{16} = \mathbb{F}_{2^{d^\circ J}} \approx \mathbb{F}_2[X]/(J)$), de plus dans ce corps toutes ses racines[5] sont d'ordre (multiplicatif) 15, *i.e.* vérifient $\alpha^n = 1 \iff 15 \mid n$.

Maintenant on a donc, si α est racine de J dans $\mathbb{F}_{16}$, $1 + \alpha + \alpha^2 + \ldots \alpha^{n-1} = J(\alpha) \times (\ldots) = 0$. On en déduit en multipliant par $\alpha - 1$ que $\alpha^n - 1 = 0$, donc $\alpha^n = 1$, ce qui impose bien que $15 \mid n$, cqfd.

« Der verfluchte Ring »

La condition (T_0) a un sens dans tous les anneaux[6] $k[X]$, et même $A[X]$ pour tout anneau A contenant $0, 1$. En effet c'est une identité entre polynômes 0-1, c'est-à-dire entre éléments de l'ensemble $\{0, 1\}[X]$. Je dis bien ensemble : car il n'est fermé ni pour $+$ ni pour $\times$ (par exemple développer $(1 + X^2)^3$ fait intervenir des opérations autres que 0+0 ou 0+1).

Il est bien clair que $\mathbb{Z}[X]$ est beaucoup trop vaste (il y a une écrasante majorité de polynômes NON 0-1), et il est bien difficile de donner des conditions nécessaires et suffisantes sur un polynôme 0-1$\in \mathbb{Z}[X]$ pour déterminer s'il va paver ou non (cela reste un problème ouvert), sinon en exhibant un tel pavage[7].

Il est bien plus tentant de travailler dans $\mathbb{F}_2[X] = \mathbb{Z}_2[X] = \mathbb{Z}/2\mathbb{Z}[X]$ cet anneau ne contient que des polynômes 0-1, et il les contient même tous une fois et une seule.

Malheureusement bien que l'application canonique

$$\mathbb{Z}[X] \to \mathbb{F}_2[X]$$
$$P = \sum a_k X^k \mapsto P \pmod 2 = \sum \overline{a_k} X^k$$

envoie bijectivement $\{0, 1\}[X] \subset \mathbb{Z}[X]$ sur $\mathbb{F}_2[X]$, il n'y a pas de bonne application réciproque vers $\mathbb{Z}[X]$, faute de structure algébrique sur $\{0, 1\}[X]$.

Par exemple on ne peut pas remonter dans $\mathbb{Z}[X]$ l'équation suivante :

$$(1 + X)(1 + X + X^2) = 1 + X^3 \in \mathbb{F}_2[X]$$

[4] Pour p premier, q une puissance de p, $\mathcal{F} : x \mapsto x^p$ est un automorphisme du corps $\mathbb{F}_q$ (et il engendre le groupe de Galois de $\mathbb{F}_q$ sur $\mathbb{F}_p$). L'ensemble de ses points fixes est le sous-corps premier $\mathbb{F}_p$. Cela résulte de l'identité $(x + y)^p = x^p + y^p$ en caractéristique p.

[5] Ceci résulte du théorème de Lagrange : tout élément de $\mathbb{F}_{16}^*$ a un ordre qui divise 15, et du fait que des éléments d'ordre inférieur seraient racines d'autres polynômes (ex. $1 + X + X^2$ pour les éléments d'ordre 3) qui sont premiers avec J.

[6] Sauf peut-être celui des Nibelungen auquel réfère bien sûr le titre de cette section.

[7] Ce serait un problème NP, si l'on en croit [12].

en termes de polynômes $0-1$.

J'ai donc recherché des conditions équivalentes au fait que « (T_0) soit vérifiée dans $\mathbb{Z}[X]$ ». La plus convaincante est :

Théorème 5. — (T_0) *est vraie dans* $\mathbb{Z}[X] \iff$ *elle est vérifiée dans tous les* $\mathbb{F}_p[X]$.

C'est un lointain cousin du théorème chinois, qu'il est bien plus facile [2] de démontrer musicalement que mathématiquement : il signifie que le nombre de notes sur chaque temps est exactement 1, si et seulement si il vaut 1 modulo tous les p premiers (on peut affaiblir les hypothèses d'ailleurs).

Remarque 3. — Il est capital de souligner que l'énoncé ci-dessus est différent de ce qui suit :

« Il existe $B(X) \in \{0,1\}[X] \subset \mathbb{Z}[X]$, n tel que $A(X) \times B(X) \equiv 1+X+\ldots+X^{n-1} \pmod{X^n-1}$ dans $\mathbb{Z}[X]$

$$\iff$$

Pour tout p premier, il existe B_p, n_p tel que $A(X) \times B_p(X) \equiv 1+X+\ldots+X^{n_p-1} \pmod{X^{n_p}-1, p}$ »

Bien sûr, $\Rightarrow$ est vraie. J'ai essayé assez longtemps de prouver la réciproque, conformément à la philosophie de Yoneda ou aux théorèmes (local $\Rightarrow$ global) du genre de ceux de Hasse sur les formes quadratiques. Le résultat fut surprenant...

Canons modulo p : todos locos !

Nous avons posé la question de l'étude locale, i.e modulo p, de la relation (T_0). Quelles conditions a-t-on pour qu'un motif donné pave modulo p ? De façon stupéfiante, il n'y en a aucune ! (cf. [3])

Théorème (Amiot, avril 2004). — *Pour toute partie finie non vide* $A \subset \mathbb{N}$ *(contenant 0), pour tout* p *premier, il existe* $B \subset \mathbb{N}, n \in \mathbb{N}^*$ *tel que*

$$(T_{0,p}) \qquad A(X) \times B(X) \equiv 1 + X + X^2 + \ldots X^{n-1} \pmod{X^n - 1, p}$$

c'est-à-dire qu'on a cette congruence dans $\mathbb{F}_p[X]$.

En termes musicaux, cela signifie que sur chaque temps, le nombre de notes est 1, mais à un multiple de p près.

J'ai d'abord trouvé ce théorème avec le modulo 2, toujours très particulier (dans ce cas on a même un pavage compact, c'est-à-dire que la réduction modulo $X^n - 1$ est superflue).

Ainsi avec le motif (0 1 4), qui ne pave certes pas $\mathbb{Z}$, on a un canon avec des notes isolées ou des accords de trois sons :

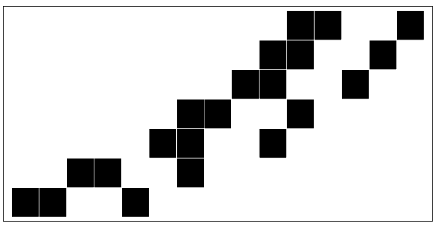

Fig. 11 – Un pavage dans $\mathbb{F}_2$

Exercice 4. — Le lecteur est invité à chercher un tel pavage avec le motif (0,1,3) modulo 2.

L'argument clef est un théorème assez simple, mais frappant, de la théorie de Galois des corps finis :

Théorème 7. — *Dans tout $\mathbb{F}_p[X]$, tout polynôme $A(X)$ non nul en 0 divise $X^n - 1$, pour n assez grand.*

Démonstration. Je ne donne que les grandes lignes (cf. [3]). Toute racine de $A(X) \in \mathbb{F}_p[X]$ est dans un corps $\mathbb{F}_q$, extension de $\mathbb{F}_p$ de degré fini. Or dans ce corps, $\mathbb{F}_q$, tout élément non nul vérifie $X^{q-1} = 1$ (à cause du théorème de Lagrange). Avec quelques points techniques (à cause de la multiplicité des racines), on en déduit un n tel que $A(X) \mid X^n - 1$ (un multiple de tous ces $q - 1$).

Si $A(X)$ représente le motif rythmique, il existe donc n tel que : $A(X) \times (X - 1) \mid X^n - 1$, et donc en posant $C(X) = \dfrac{X^n - 1}{A(X)(X-1)}$, on a bien

$$A(X) \times C(X) = \frac{X^n - 1}{(X - 1)}.$$

Certes, $C(X)$ n'est pas en général un polynôme 0-1 ; mais en caractéristique finie on construit facilement un polynôme 0-1 $B(X)$, qui soit congru à $C(X)$ modulo $X^n - 1$: il suffit de remplacer tout terme αX^k par $(\alpha - 1)X^k + X^{n+k-1}, \alpha > 1$, et d'itérer cette transformation jusqu'à ce qu'il ne reste plus que des coefficients 0 ou 1, ce qui achève la preuve du théorème. □

Ce procédé est constructif : la figure précédente est obtenue par un algorithme qui implémente précisément cette méthode (en optimisant n, en plus).

Des références sur ce sujet trop peu étudié sont [21] et, plus récemment (avec des applications à la cryptographie), [1].

En conclusion, il n'y a PAS de condition locale (modulo p) pour qu'un motif donné A pave : todos locos ! il nous faut donc revenir à $\mathbb{Z}[X]$. Au moins, les facteurs de $\dfrac{X^n - 1}{X - 1} \in \mathbb{Z}[X]$ seront simples... Pour l'amour de l'art, observons en effet que la situation est bien moins claire dans les corps finis :

– $X^n - 1$ peut avoir un discriminant nul (*i.e.* des racines multiples) quand $p \mid n$.

– Des polynômes jadis irréductibles (ex. $\Phi_8 = X^4 + 1$) sont factorisables dans TOUT corps fini.

– Le produit des $X - \xi$ où ξ parcourt l'ensemble des racines d'ordre multiplicatif donné dans $\mathbb{F}_q^*$ n'est plus en général un polynôme irréductible dans $\mathbb{F}_p[X]$ (cf. [1]).

Exercice 5. — Trouvez les facteurs irréductibles du produit $\prod(X - \xi)$ quand ξ décrit l'ensemble des huit générateurs du groupe $(\mathbb{F}_{16}^*, \times)$, (les éléments d'ordre 15). Vous pouvez vous référer utilement au paragraphe sur le problème de Johnson.

J'ai découvert incidemment une propriété étrange et mystérieuse, bien que sa preuve ne soit pas très difficile, qui permet de calculer la multiplicité de 1 comme racine de $A(X)$ donné :

Proposition. — *Soit $A(X)$ un polynôme 0-1 qui pave avec période n et soit p un facteur premier de A. Alors*

– la multiplicité de 1 comme racine de A dans $\mathbb{F}_p$, s'exprime en base p comme un nombre dont les chiffres sont exclusivement 0 ou $\overline{p-1}$;

– le nombre des chiffres non nuls dans ce nombre en base p n'est autre que la multiplicité de p comme facteur de $A(1)$ dans $\mathbb{N}$, $A(1)$ étant le nombre de notes du motif A (ceci est quasiment la condition (T_1) de Coven-Meyerowitz).

Curieusement, ce nombre de bits non nuls apparaît pour le calcul de complexité de l'exponentiation rapide, comme dans le difficile théorème de Smale sur l'immersion d'une variété sans singularité dans $\mathbb{R}^n$.

Retour dans $\mathbb{Z}[X]$

Ce bref passage en caractéristique p nous a permis de toucher à d'autres formes de canons. Il en existe autant d'espèces que de compositeurs et je ne puis les énumérer toutes ; mentionnons seulement le résultat remarquable du canadien Jon Wild (2000) : « tout motif de trois notes pave avec son rétrogradé », qui renvoie à une pratique courante à l'âge baroque.

On revient en caractéristique nulle, avec l'intention de pousser l'utilisation des polynômes 0-1 aussi loin que possible. On parviendra au fait remarquable que la conjecture spectrale en dimension 1 repose sur le cas particulier des canons de Vuza, dont l'intérêt dépasse donc de loin les simples applications musicales.

Dans le cas de $\mathbb{Z}[X]$ les facteurs irréductibles de l'identité (T_0) polynomiale sont les polynômes cyclotomiques $\Phi_d, d \mid n$; les conditions trouvées en 1998 par Coven-Meyerowitz sont cruciales pour la suite de cet exposé.

J'ajoute ici un lemme qu'ils jugent capital.

Les automorphismes du groupe $\mathbb{Z}_n$ sont bien connus, ce sont les $x \mapsto \alpha x$ où $\alpha \in \mathbb{Z}_n^*$ est un des éléments inversibles de l'anneau $\mathbb{Z}_n$. Il est donc clair que $A \oplus B = \mathbb{Z}_n \iff \alpha A \oplus \alpha B = \mathbb{Z}_n$. Il est beaucoup moins évident que l'on a

Lemme 4. — *$A \oplus B = \mathbb{Z}_n \iff \alpha A \oplus B = \mathbb{Z}_n$ pour tout α inversible modulo n.*

Coven & Meyerowitz ([5]) donnent une démonstration de ce lemme « capital » dans un anneau de polynômes, apparemment insatisfaits de la démonstration originale (combinatoire) de [17].

Mais en fait sa première preuve est dûe à D.T. Vuza 6 ans auparavant. Il en a senti d'ailleurs la raison profonde, qui est que $\psi_\alpha : z \mapsto z^\alpha$ est un automorphisme du groupe des racines n-ièmes de l'unité, et l'utilise pour une démonstration encore assez compliquée à base de transformée de Fourier et convolution.

Ma version consiste à remarquer que changer A en αA revient à changer $A(X)$ en $A(X^\alpha)$, qui est une bijection sur l'ensemble des polynômes 0-1 considérés modulo $X^n - 1$ (cf. exo), et cela applique (l'inverse de) ψ_α aux racines de $A(X)$, et donc les ensembles des racines n-ièmes de l'unité qui sont racines de $A(X)$ ne sont pas changées, ce qui signifie que les facteurs cyclotomiques de $A(X)$ sont invariants dans cette transformation.

Comme ceux de $B(X)$ n'ont pas bougé, on a encore entre $A(X^\alpha)$ et $B(X)$ tous les facteurs cyclotomiques de $(X^n-1)/(X-1)$, qui doit donc diviser $A(X^\alpha).B(X)$. Un argument de degré permet de conclure (on connaît les $n-1$ racines de $A(X^\alpha).B(X)$ modulo $X^n - 1$).

Exercice 6. — Vérifier que changer $A(X)$ en $A(X^\alpha)$ (modulo $X^n - 1$) conserve sa nature de polynôme 0-1.

Je tiens à souligner que ce procédé est musical[8] : par exemple Tom Johnson l'a redécouvert tout seul, expérimentalement !

Bien sûr cette action de groupe permet une description plus économique des canons : par exemple pour l'ensemble des canons de Vuza de période 72, qui consiste de 3 formes pour A et 6 pour B[9], il ne reste qu'une orbite pour chacun et on peut donc déduire facilement tous les canons de Vuza 72 du couple

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

Les groupes de Hajós, Dan Tudor Vuza, et les canons rythmiques irréductibles

Le mathématicien et musicien roumain Dan Tudor Vuza a passé près de dix ans, de 1980 à 1990, à étudier la question des canons rythmiques en long et en large. En particulier, il s'est intéressé aux canons pour lesquels ni A ni B n'ont de période propre.

Précisons : bien sûr, d'après le théorème de De Bruijn (tout canon de motif fini est périodique), on travaille avec une période globale, n, du canon. Mais il arrive très souvent (presque toujours, en fait) que l'un des termes de la somme directe $A \oplus B = \mathbb{Z}_n$ ait une sous-période. Ainsi pour l'exemple simple de $A = \{0, 1, 4, 5\}$ qui pave avec période 8 : c'est en fait le sous-motif $\{0, 1\}$ répété avec période 4 qui constitue $A = \{0, 1\} \oplus 4$.

Moreno Andreatta s'est aperçu que Vuza avait redécouvert des résultats sur les factorisations des groupes cycliques issus de la conjecture de Hajòs : un groupe cyclique $\mathbb{Z}_n$ est de Hajòs, ou encore est un « bon groupe », si dans toute factorisation $\mathbb{Z}_n = A \oplus B$, on a $A + p = A$ pour un certain $p < n$ (ou la même chose pour B). Vuza a caractérisé tous les groupes de Hajós cycliques en utilisant la théorie de Fourier, suivant une remarque déjà ancienne du grand théoricien Lewin qui remarquait qu'une somme directe de parties revient à un produit de convolution de leurs fonctions caractéristiques.

Cela est décrit en détail dans [4]. Le plus petit « mauvais groupe » est $\mathbb{Z}_{72}$.

On connaît des algorithmes pour fabriquer des canons de Vuza (*i.e.* des factorisations de « mauvais » groupes), mais aucun procédé qui assure de les trouver tous. La formule la plus simple est dûe [11] à Frank Jedrzejewski :

Proposition (2003). — *Si on considère p_1, p_2 premiers et $n_i, i = 1 \dots 3$ tels que $n_1 p_1$ soit premier avec n_2 (et réciproquement) alors en posant $[\![a, b]\!] = \{a, a+1, \dots b\}$ on a pour $n = p_1 p_2 n_1 n_2 n_3$ le canon de Vuza suivant :*

[8] Alban Berg par exemple l'a utilisé pour transformer des séries dodécaphoniques dans son opéra *Lulu*.
[9] À rotation près.

$$A = n_2 n_3 \times (\llbracket 0, p_2 - 1 \rrbracket \oplus p_2 n_1 \times \llbracket 0, p_1 - 1 \rrbracket) \qquad B = n_1 n_3 \times (\llbracket 0, p_1 - 1 \rrbracket \oplus p_1 n_2 \times \llbracket 0, p_2 - 1 \rrbracket)$$

$$S = n_3 (p_2 n_2 \times \llbracket 0, n_1 - 1 \rrbracket \oplus p_1 n_1 \times \llbracket 0, n_2 - 1 \rrbracket) \qquad R = \big(\llbracket 1, n_3 - 1 \rrbracket \oplus B\big) \cup A$$

$$R \oplus S = \mathbb{Z}_n$$

La factorisation de n est générale : si on ne peut ainsi écrire n c'est que $\mathbb{Z}_n$ est un bon groupe ([18]). Une autre façon de l'écrire [18] consiste à énumérer les cardinaux des « bons » groupes :

Théorème (Hajòs, Redei, de Bruijn, Sands,...). — *Les « bons groupes » cycliques sont les $\mathbb{Z}_n$ tels que n s'écrive de l'une des façons suivantes (où p, q, r, s sont des nombres premiers distincts) :*

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

Remarque. — si $\mathbb{Z}_n$ a un sous-groupe qui est « mauvais », alors on montre que $\mathbb{Z}_n$ est aussi « mauvais ».

Ces canons sont d'un grand intérêt pour les compositeurs, car ils introduisent une non-répétitivité dans la régularité (du phénomène globalement périodique), un peu comme la rime en poésie. La notion a beau être relativement récente, une liste d'outils sur les canons de Vuza est présente dans divers logiciels d'aide à la composition, comme *Open Music* développé à l'Ircam, et plusieurs compositeurs contemporains (George Bloch, Fabien Lévy) s'en servent dans leurs œuvres. J'ai par exemple sur mon piano un morceau très simple de G. Bloch qui a servi de musique pour une version française d'un film de Hitchcock. Il nous a expliqué de façon très convaincante pourquoi ces cellules qui se répètent, mais à intervalles imprévisibles, excellent à faire monter la tension du spectateur/auditeur !

Génération de canons

Poussés par le dynamisme des compositeurs, nous avons étudié nombre de transformations sur les canons rythmiques.

Plusieurs transformations

Le groupe affine

Le Lemme 4 donne l'exemple même d'une transformation non triviale, qui préserve la notion de canon sous l'action d'un groupe. Il s'agit ici du groupe affine $Aff(\mathbb{Z}_n)$. Souvenons-nous en effet que l'on a convenu d'identifier un motif rythmique A à la classe de tous ses translatés $A + m \mod n$. Le lemme 1 rajoute les homothéties (de rapport a inversible) et on a donc affaire aux orbites sous les actions de toutes les bijections $x \mapsto ax + b$ dans $\mathbb{Z}_n$. La figure suivante montre une telle orbite et les canons correspondants : $(0, 1, 4, 5)$ et $(0, 3, 4, 7)$ sont les deux formes du motif modulo 8.

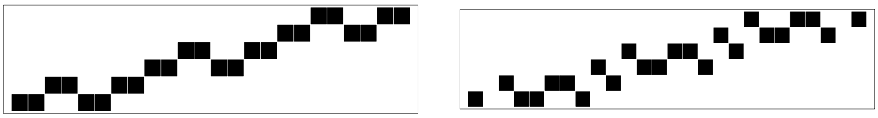

Fig. 12 – Orbite d'un motif sous l'action du groupe affine

Le lemme 4 prouve que les conditions (T_1) et (T_2) de [5] sont préservées par une telle transformation.

Je me suis posé la question de généraliser ce résultat aux autres transformations utilisées par les musiciens. Les voici.

Zoom/augmentation

Cette transformation revient à dilater le temps et à remplacer une note (ou un silence) par k notes (ou silences). Illustration :

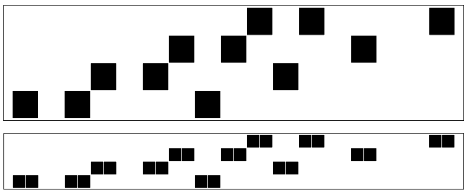

Fig. 13 – Zoom d'un canon rythmique

Du point de vue polynômial, on change $B(X)$ en $B(X^k)$ et $A(X)$ en $A(X^k) \times (1 + X + \ldots + X^{k-1})$. En travaillant par récurrence sur les facteurs premiers de k, j'ai pu montrer dans [3] que cette opération préserve aussi les conditions (T_1) et (T_2) de [5].

L'importance particulière de cette opération vient de ce qu'elle permet de fabriquer de nouveaux « canons de Vuza », à partir d'anciens. On obtient ainsi des canons inédits (non fournis par l'algorithme de Vuza). Cela a été remarqué par divers chercheurs (Carlos Agon, Thomas Noll) et notamment par Harald Fripertinger de l'université de Graz, qui a donné des formules remarquables de dénombrement des canons rythmiques et s'est lancé à la recherche de tous les canons de Vuza de « petite » taille. Une amicale compétition (il a gagné) nous a permis en 2003-2004 de trouver force nouveaux canons de période 108, 120 ou 144. Au colloque de Graz [7] en mai 2004, Harald a fait sensation en montrant que tous les canons de Vuza que nous avions trouvés pour les deux premières périodes, 72 et 108, étaient en vérité les seuls possibles. Pour cela il s'est appuyé à la fois sur des algorithmes habilement conçus par ses soins, des actions de groupes et dénombrements d'orbites à coups d'équation aux classes, et de la combinatoire (théorie de Polya). Incidemment, les canons de Vuza apparaissent comme un matériau exceptionnellement rare (probabilité inférieure au 1 millionième), ce qui a son intérêt pour la suite.

Concaténation

L'opération de concaténation est très simple, elle consiste à répéter un même motif à la queue-leu-leu plusieurs fois :

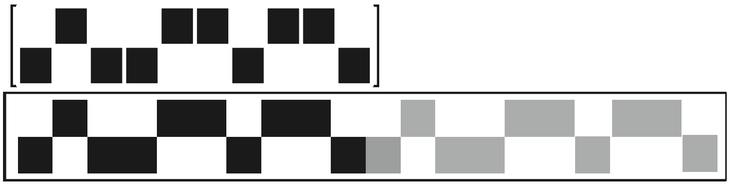

Fig. 14 – Un canon rythmique répété

Je suis redevable à H. Fripertinger pour m'avoir fait comprendre l'importance théorique de cette opération si simple. Elle lui a permis [8] de donner des formules exactes pour dénombrer les canons dans les « bons groupes », puisque par définition même un des facteurs d'une décomposition en somme directe d'un tel groupe est concaténé $\{0,1\} \oplus \{0,2\} \to \{0,1,4,5\} \oplus \{0,2\}$ d'un motif plus court. Ceci permet de proche en proche de trouver tous les canons de période donnée, à condition d'éviter les périodes fatidiques 72, 108, 120, etc.

Cette opération consiste, polynômialement, à multiplier $A(X)$ par ce que j'appelle un métronome :

Définition 4. — *Un métronome est un motif de la forme*

$$A = (0, k, 2k, 3k, \ldots (m-1)k)$$

i.e.

$$A(X) = 1 + X^k + X^{2k} + \ldots + X^{(m-1)k} = \frac{X^{mk}-1}{X^k-1} = \prod_{d|mk \text{ et } d\nmid k} \Phi_d.$$

Il en résulte assez facilement (cf. [3]), travaillant avec m premier sans perte de généralité, le

Théorème 9. — *Si A s'obtient par concaténation de $\tilde{A}$, pavant avec B, alors l'un vérifie (T_2) si et seulement si l'autre vérifie aussi (T_2).*

Entrelacement et équirépartition

Ce procédé n'est pas (encore) connu des musiciens mais je ne doute pas qu'ils en fassent bientôt leurs choux gras. Je l'ai découvert dans un article récent et très général (de Kolountzakis et Matolcsi, [12]) (dans un contexte d'algèbre commutative), mais il s'avère que vu sous un autre angle, c'est un outil essentiel pour le dernier théorème de [5], le plus difficile. Je reformule ensemble ces différents résultats. La démonstration n'en est pas très difficile (le lecteur courageux pourra s'y essayer) :

Théorème 10. — *Soient $A_1, \ldots A_k$ des motifs qui pavent un canon rythmique avec un MÊME B. Alors on obtient un canon rythmique en posant $A = \cup_{i=0\ldots k-1}(i + kA_i)$, qui pave avec kB.*

Réciproquement, un tel canon est caractérisé par le fait que l'« outer rhythm » B est multiple d'une constante $k > 1$: $B \subset k\mathbb{Z}$, ou, de manière équivalente, par le fait que A est équiréparti modulo k : les ensembles

$$\widehat{A}_i = A \cap (i + k\mathbb{Z})$$

ont tous même cardinal, et pavent avec un même $\widehat{B} = B/k$.

On peut ainsi fabriquer de nouveaux canons de Vuza, par exemple en prenant pour les A_i (une partie de) l'orbite d'un motif sous le groupe affine. De façon bien plus remarquable, tous les canons Vuza recensés (ceux obtenus par algorithme et les autres) peuvent être fabriqués par ce procédé à partir de canons plus petits, qu'ils soient de Vuza ou pas.

La figure ci-dessous illustre la genèse d'un canon de période 72. On y reconnaît (cf. la voix supérieure) les deux motifs génériques qui sont dilatés et s'entrelacent pour donner le motif final.

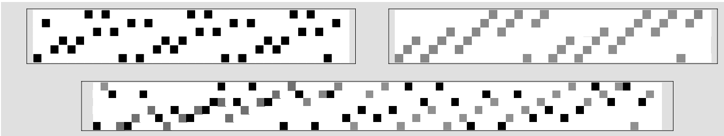

Fig. 15 – Un canon de Vuza 72 *comme entrelacement de deux canons* 36

Réduction des canons rythmiques

Les canons de Vuza sont finalement assez similaires aux nombres premiers, au sens où ils sont《irréductibles》, et engendrent tous les autres canons ; en effet, résulte de leur définition le :

Théorème 11. — *On peut réduire récursivement tout canon par déconcaténation — l'opération inverse de la concaténation — appliquée à l'un des deux termes A ou B, soit à un canon de Vuza, soit au canon trivial ($\{0\} \oplus \{0\}$).*

Nous disposons finalement de diverses transformations, dont plusieurs (zoom, concaténation, entrelacement) changent la période ; toutes ces opérations conservent les conditions $(T_1), (T_2)$ de Coven-Meyerowitz et il est temps de mentionner le lien avec la conjecture spectrale.

La conjecture de Fuglede

La conjecture spectrale

Dans le cas le plus général, la conjecture publiée par Fuglede en 1974 ([13]) est une question qui relie la géométrie et l'analyse harmonique :

Conjecture Spectrale (1974). — *Un domaine K (compact d'intérieur non vide) pave $\mathbb{R}^n$, c'est-à-dire qu'il existe $B \subset \mathbb{R}^n$ tel que*

$$\bigcup_{b\in B} b+K=\mathbb{R}^n \ \textit{et}\ \overbrace{b+K}^{\circ}\cap\overbrace{b'+K}^{\circ}=\varnothing \ \textit{pour}\ b\neq b'$$

si et seulement si K possède une base hilbertienne, i.e. il existe une famille Λ telle que $(x \mapsto e^{2i\pi<\lambda,x>})_{\lambda\in\Lambda}$ est une famille orthonormée qui engendre une partie dense de $\mathcal{L}^2(K)$.

Fuglede a prouvé sa conjecture dans le cas où B est un réseau ($B \approx \mathbb{Z}^n$). On comprend mieux cette conjecture dans le cas simple où K est par exemple l'hypercube unité : il suffit alors de prendre pour K le réseau $\mathbb{Z}^n$, c'est la théorie de la décomposition en série de Fourier.

Jusqu'à l'été 2003, tous les résultats publiés sont allés dans le sens de la confirmation de cette conjecture. Elle est vraie en particulier pour tous les K assez réguliers (les convexes plans, par exemple). Comme il s'agit d'orthogonalité dans $\mathbb{R}^n$, on a assez vite établi une condition équivalente en terme d'existence d'une matrice de Hadamard douée de propriétés adéquates.

C'est en exhibant des matrices de Hadamard complexes que Terence Tao a finalement prouvé que cette conjecture est fausse en dimension $\geqslant 5$. Depuis on a trouvé des contre-exemples dans les deux sens, dont la dimension est descendue à 3 [12]. Mais cela reste un problème ouvert en dimension 1 malgré une kyrielle de résultats partiels (cf. [13]). Un des plus récents concerne les produits de métronomes, au sens de la définition ci-dessus ([14]). Il est en partie contenu dans le théorème que je démontre ci-dessous.

Notons le lien trivial entre pavages de $\mathbb{R}$ et pavages de $\mathbb{Z}$: si A pave $\mathbb{Z}$ alors $A + [0, 1[$ pave $\mathbb{R}$. La réciproque est moins triviale mais résulte des travaux de Vuza et de façon très différente de Lagarias & Wang [15].

La conjecture spectrale en dimension 1

Izabella Laba, lisant l'article de Coven-Meyerowitz, a rapidement compris qu'on pouvait en tirer une connexion à la conjecture spectrale. Elle publia peu après (2000) [13] le résultat suivant :

Proposition. — $(T_1) + (T_2) \Rightarrow$ *spectral (et spectral* $\Rightarrow (T_1)$*).*

Cela utilise des calculs élémentaires, et le lemme suivant qui caractérise le caractère spectral en dimension 1 (on peut le prendre comme définition) :

Lemme 5. — *A pave* $\mathbb{Z}$ *si et seulement si il existe une famille* $0 = \lambda_0 < \lambda_1 < \dots \lambda_{k-1}, k = |A| = A(1)$ *telle que les* $e^{2i\pi\lambda_j}$ *soient racines de* $A(X)$.

Laba prend tout simplement des λ_j de la forme $i/p^\alpha,\ i = 0 \dots p-1$, pour montrer que si (T_2) est vérifiée alors A est spectral.

Remarque 4. — Il ne faut pas croire que le caractère 0-1 du polynôme $A(X)$ oblige ses racines de module 1 a être d'ordre fini dans S^1. En d'autres termes, théoriquement un spectre peut très bien exister et être irrationnel :

Exercice 7. — Trouver un polynôme 0-1 ayant des racines de module 1 d'ordre infini.

D'après ce résultat de Laba, si un motif rythmique pave mais qu'il n'est pas spectral, il ne peut vérifier (T_2). Mais si l'on en croit le principe de réduction énoncé au théorème 11, cela ne peut se produire que dans un groupe non-Hajós. En effet, tout pavage dans un « bon groupe » se réduit récursivement à des canons plus petits dans des sous-groupes, qui sont donc encore « bons », et donc on peut encore réduire jusqu'à tomber sur le canon trivial à une note, $(0) \oplus (0)$. Qui vérifie la condition (T_2) (!). Par conservation d'icelle dans le procédé de concaténation des canons (voir le théorème 9), on déduit

Théorème (Amiot, juin 2004). — *Si un canon n'est pas spectral, alors il peut se réduire par déconcaténation à un canon de Vuza, lui aussi non spectral. A fortiori, si n a l'une des formes suivantes (p, q, r, s étant des nombres premiers distincts) :*

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

alors tout motif d'un canon rythmique de période n est spectral.

On peut même aller plus loin en prenant au lieu de la période n la taille du motif ($=$ le nombre de notes $= A(1)$). Les trois premiers cas avec deux facteurs premiers résultent du théorème ($B2$) de [5], les deux derniers sont nouveaux à ma connaissance.

Ce résultat s'applique aussi aux pavages d'un intervalle d'entiers, que j'appelle canons compacts (ceux pour lesquels il est inutile de procéder à une réduction modulo n car on a $A \oplus B = [\![0, n-1]\!]$ dans $\mathbb{N}$, par exemple $\{0, 1, 4, 5\} \oplus \{0, 2\} = \{0, 1, 2, 3, 4, 5, 6, 7\}$), car d'après un résultat ancien de De Bruijn ils sont tous déconcaténables.

Corollaire 2. — *En conséquence de l'énumération par Fripertinger des canons de Vuza pour $n = 72, 108$ nous savons que tous les canons de période $\leqslant 108$ (et même jusqu'à 119) sont spectraux (au sens où aussi bien A, le « inner rhythm », que le « outer rhythm » B, sont spectraux).*

Ceci suggère une idée assez intuitive, à savoir que s'il existe un motif A qui pave sans vérifier (T_2), alors A, n doivent être grands. Jusqu'ici, tous les algorithmes qui fabriquent des canons de Vuza assurent que (T_2) est vérifiée, et tous les procédés d'augmentation de taille des canons vus ci-dessus conservent cette propriété : on ne sait donc vraiment pas comment construire un éventuel canon de Vuza qui nie la propriété (T_2), ce qui ne prouve pas qu'il n'en existe pas puisqu'on ne sait pas comment les construire tous...

Réduction par équirépartition

Il ne paraissait pas impossible d'espérer réduire TOUS les canons de Vuza, et donc de démontrer le sens (pave $\Rightarrow$ spectral) de la conjecture de Fuglede.

En effet l'algorithme de Vuza fabrique toujours un second membre multiple de n_3 (cf. la formule de Jedrzejewski). Dans ce cas on a équirépartition de l'inner rhythm modulo n_3 (cf. [5], lemme 2.5). Le groupe affine préserve d'ailleurs cette condition d'équirépartition. Mais elle signifie que l'on peut réduire un tel canon à un canon plus petit, en préservant la condition (T_2). Si donc il s'avérait que TOUT canon de Vuza ait, à l'instar de ceux que l'on sait fabriquer, un facteur équiréparti, la méthode de réduction (utilisant dualité, concaténation, équirépartition selon le cas) permettrait de réduire TOUT canon au canon trivial. Ce qui démontrerait la condition (T_2) pour tout canon, ce dont on pourrait déduire (un sens au moins de) la conjecture de Fuglede.

Le cimetière des conjectures

Mais le champ de bataille des canons rythmiques est jonché des cadavres de nombreuses conjectures... À commencer, historiquement au tout début, par la conjecture de De Bruijn : *si un groupe abélien fini est somme directe de A et B alors l'un des deux est périodique*, tuée dans l'œuf par les canons de Vuza et bien avant cela, par les contre-exemples de Redei, Hajòs, De Bruijn et consorts.

La conjecture de Fuglede a certes tenu 31 ans avant de connaître son premier contre-exemple – mais il est vrai qu'elle aura été prouvée dans nombre de cas particuliers ; au contraire, brèves auront été la vie de celle de Tijdeman 1996 (si ppcm(A)=1 alors il existe un nombre premier tel que $B \subset p\mathbb{Z}$, tuée par Szabó), ou de celle de Lagarias & Wang (si T pave avec les compléments $T_1, \dots T_n$ alors ils sont spectraux et de même spectre) qui fut victime de Kolountzakis & Matolcsi en juin 2004 [12].

On ignore actuellement si la conjecture que Coven et Meyerowitz se sont soigneusement retenus d'énoncer (pave $\Rightarrow$ (T_2)) est prouvable ; elle est logiquement plus forte que le sens (pave $\Rightarrow$ spectral) de celle de Fuglede, d'après Laba. Les résultats en sens inverse sont encore peu nombreux (si A est spectral alors ?...), à part [14] qui utilise des métronomes c'est-à-dire des canons très simples, et il est difficile de se faire une opinion sur cette direction.

Mais je finirai cette hécatombe par l'extermination de ma propre conjecture. En effet, la construction mentionnée par [5] du hongrois Szabó dans [19] réfute au départ une conjecture de Sands, proche de celle de Tijdeman. Mais il s'avère qu'elle donne, incidemment, un canon de Vuza, qui n'est donc par définition pas réductible par dé-concaténation, et par construction pas réductible par équirépartition ! Signalons tout de même que le plus petit contre-exemple donné par cette méthode, que j'ai implémenté avec *Mathematica*™, est de période 30030, ce qui explique qu'il n'ait pas sauté aux yeux. De plus la méthode de construction est particulièrement perfide, même si elle n'est pas sans rappeler certains procédés de construction des canons de Vuza ; j'en donne ici l'idée très simplifiée.

En hommage au théorème de De Bruijn intitulé 'on British Number systems', j'emprunterai une métaphore pécuniaire. On considère un ensemble de pièces et de billets qui permettent de payer exactement n'importe quelle somme ($< n$). On prend pour A la somme des « pièces jaunes », et pour B' les sommes de « gros billets ». De façon encore plus imagée, A contient les unités et B' les dizaines, et $A \oplus B' = [\![0, n-1]\!]$. Dans l'exemple donné plus bas, $B' = \{0, 30, 60, \dots 30k, \dots\}$.

L'idée hongroise consiste alors à perturber B' en une nouvelle partie B, en modifiant certains éléments, choisis exprès irrégulièrement, par l'ajout d'un élément variable de A, tout cela variant circulairement ; ceci ne modifie pas le fait que $A \oplus B = \mathbb{Z}_n$ mais cela rend B plus irrégulier. Avec certaines conditions techniques (cf. [19]) on montre que B (ainsi que, plus trivialement, A) engendre $\mathbb{Z}_n$ et en conséquence, qu'il n'est pas contenu dans un sous-groupe strict $k\,\mathbb{Z}_n$: donc pas de réduction possible par équirépartition. De plus, la méthode employée assure qu'on a affaire à deux facteurs A, B apériodiques, et donc à un canon de Vuza... Le plus petit que j'ai pu construire de cette façon est de période 900 :

$$A = (0, 36, 72, 100, 108, 136, 144, 172, 200, 208, 225, 236, 244, 261, 272, 297, 308,\\ 325, 333, 344, 361, 369, 397, 425, 433, 461, 469, 497, 533, 569)$$

$$B = (0, 30, 60, 90, 156, 210, 240, 250, 270, 330, 336, 360, 390, 405, 420, 510,\\ 516, 540, 550, 570, 600, 690, 696, 720, 780, 810, 850, 855, 870, 876).$$

Coda

Stretta

Nous pouvons nous croire arrivés bien loin de *Frère Jacques* et de son petit canon à quatre voix. Mais les contre-exemples obtenus par des arguments sophistiqués à ces conjectures mathématiques pointues permettent de mettre en évidence des objets musicaux doués de propriétés intéressantes, qui vont certainement faire leur apparition dans des partitions prochaines : cela a déjà été le cas par le passé, particulièrement avec les canons de Vuza mais aussi dans bien des domaines – il n'est pas nouveau que des idées mathématiques servent, consciemment ou non, l'inspiration de musiciens.

En retour, et de façon bien plus novatrice, on peut espérer que les suggestions des compositeurs continuent, comme elles ont commencé de le faire, à éclairer la recherche mathématique de leurs idées spécifiques. L'étonnante fécondité de cette irruption de la musique dans les mathématiques s'explique à mon avis par la fringale des mathématiciens pour les concepts nouveaux, qui ont toujours servi spectaculairement l'avancement de notre science : bien des outils mathématiques aujourd'hui banals sont issus de la physique, bien sûr, mais aussi de la biologie, de l'économie, etc. Prophétisons que le temps est venu de reformer et d'élargir le *Quadrivium* antique, la musique reprenant avec les autres son statut de pilier de la connaissance.

Solutions des exercices

Exercice 1. Canon de période $2 \times \ell(A)$

Il suffit de prendre $A = (0, n-1)$ qui pave avec $B = (0, 1, \dots, n-1)$ mais pas moins.

Exercice 2. Perfect square tilings

Partant de : $\sum_{i\in I} X^{k_i}\Phi_3(X^i) = 1 + X + \dots = \sum_{j=0}^{3n-1} X^j = \dfrac{X^{3n}-1}{X-1}$, on pose $X = j = e^{2i\pi/3}$: les indices i multiples de 3 sont caractérisés par le fait que $\Phi_3(j^i) = \Phi_3(1) = 3 \neq 0$. Pour tout autre indice on aura $\Phi_3(j^i) = 0$ – c'est la relation classique $1 + j + j^2 = 0$. Il reste donc une somme des $j^{k_i}, i \in 3\mathbb{N}$ qui doit valoir 0. Or la plus courte somme valant 0 est encore $1 + j + j^2 = 0$, ce qui impose qu'il y ait 0 ou 3 (ou 6, ou 9...) multiples de trois parmi les indices i. Cela explique pourquoi T_3 n'apparaît pas sans T_6 et T_9.

Exercice 3. $(1, 4, 9, 16)$ pave-t-il ?

Non. On a bien deux facteurs cyclotomiques, d'indices 2 et 10, mais la condition (T_1) n'est pas vérifiée, sans parler de (T_2).

$$X^{16} + X^9 + X^4 + X = X \times (1+X) \times (1 - X + X^2 - X^3 + X^4) \times (1 + X^3 - X^5 + X10)$$

(il faut un logiciel de calcul formel si on veut factoriser sans efforts ; en revanche on liste facilement les polynômes cyclotomiques du style $\Phi_{p^\alpha} = 1 + X^{p^{\alpha-1}} + X^{2p^{\alpha-1}} + \dots$ et on teste s'ils sont diviseurs).

Exercice 4. Pavage modulo 2

La plus petite solution pour paver modulo 2 avec $A = (0,1,3)$ est $B = (0,2,3)$. En effet $A + B = \{0,1,2,3,3,3,4,5,6\}$.

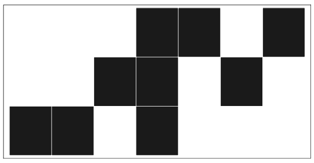

Fig. 16 – pavage modulo 2 *avec* $(0,1,3)$

Exercice 5. Éléments d'ordre 15 dans le corps à 16 éléments

Dans la discussion du problème de Johnson, on a vu que le polynôme (irréductible sur $\mathbb{F}_2[X]$) $J(X) = 1 + X + X^4$ a 4 racines d'ordre 15 dans $\mathbb{F}_{16}$. Leurs inverses sont aussi d'ordre 15, elles sont racines du polynôme réciproque $1 + X^3 + X^4$. On a alors $\Phi(15) = 8$ éléments d'ordre 15, on n'en trouvera pas plus (Φ désignant la fonction d'Euler).

Exercice 6. Transformation affine

Si α est premier avec n, alors l'application $k \mapsto \alpha k \mod n$ est une bijection. Donc A et αA sont en correspondance bijective, et leurs polynômes associés sont bien 0-1.

Exercice 7. Nombres algébriques de module 1 non racines de l'unité

Ma plus petite solution est $A(X) = 1 + X + X^3 + X^5 + X^6$, dont les quatre racines non réelles peuvent être exprimées par radicaux (poser $Y = X + 1/X$) et sont de module 1, mais ce ne sont pas des racines de l'unité (sinon $A(X)$ aurait un facteur cyclotomique).

Références

[1] Al Fakir, S., *Algèbre et théorie des nombres*, T2, Ellipses 2004.

[2] Amiot, E., *Why Rhythmic Canons are Interesting*, in : E. Lluis-Puebla, G. Mazzola et T. Noll (eds.), *Perspectives of Mathematical and Computer-Aided Music Theory, EpOs*, 190–209, Universität Osnabrück, 2004.

[3] Amiot, E., *Rhythmic canons and Galois theory*, Grazer Math. Ber., 347 (2005), 1–25.

[4] Andreatta, M., *On group-theoretical methods applied to music : some compositional and implementational aspects*, in : E. Lluis-Puebla, G. Mazzola et T. Noll (eds.), *Perspectives of Mathematical and Computer-Aided Music Theory, EpOs*, 122–162, Universität Osnabrück, 2004.

[5] Coven, E., and Meyerowitz, A. *Tiling the integers with one finite set*, in : *J. Alg.*, 212 :161-174, 1999.

[6] DeBruijn, N.G., *On Number Systems*, Nieuw. Arch. Wisk. (3) 4, 1956, 15–17.

[7] Fripertinger, H. *Remarks on Rhythmical Canons*, Grazer Math. Ber., 347 (2005), 55–68.

[8] Fripertinger, H. *Tiling problems in music theory*, in : E. Lluis-Puebla, G. Mazzola et T. Noll (eds.), *Perspectives of Mathematical and Computer-Aided Music Theory, EpOs*, 149–164, Universität Osnabrück, 2004.

[9] Hajós, G., *Sur les factorisations des groupes abéliens*, in : *Casopsis Pest. Mat. Fys.*,74 :157-162,1954.

[10] Johnson, T., *Tiling The Line*, proceedings of J.I.M., Royan, 2001.

[11] Jedrzejewski, F., *A simple way to compute Vuza canons*, MaMuX seminar, January 2004, http ://www.ircam.fr/equipes/repmus/mamux/.

[12] Kolountzakis, M. & Matolcsi, M., *Complex Hadamard Matrices and the spectral set conjecture* , http ://arxiv.org/abs/math.CA/0411512.

[13] Laba, I., *The spectral set conjecture and multiplicative properties of roots of polynomials*, J. London Math. Soc. 65 (2002), 661-671.

[14] Laba, I., and Konyagin, S., *Spectra of certain types of polynomials and tiling of integers with translates of finite sets*, J. Num. Th. 103 (2003), n° 2, 267-280.

[15] Lagarias, J., and Wang, Y. *Tiling the line with translates of one tile*, in : *Inv. Math.*, 124 :341-365, 1996.

[16] Tangian, A., *The Sieve of Eratosthene for Diophantine Equations in Integer Polynomials and Johnson's problem*, disc. paper N° 309 Fern Universität Hagen.

[17] Tijdeman, R., *Decomposition of the Integers as a direct sum of two subsets*, in : *Séminaire de théorie des nombres de Paris*, 3D, p.261-276, Cambridge U.P, 1995.

[18] Sands, A.D., *The Factorization of abelian groups*, Quart. J. Math. Oxford, 10(2) :45–54.

[19] Szabó, S., A type of factorization of finite abelian groups, Discrete Math. 54 (1985), 121–124.

[20] Vuza, D.T., *Supplementary Sets and Regular Complementary Unending Canons*, in four parts in : *Canons. Persp. of New Music*, nos 29(2) pp.22-49 ; 30(1), pp. 184-207 ; 30(2), pp. 102-125 ; 31(1), pp. 270-305, 1991-1992.

[21] Warusfel, *Structures Algébriques finies*, Classiques Hachette, 1971.

[22] Wild, J., *Tessellating the chromatic*, Perspectives of New Music, 2002.

[23] *Midi files for the illustrations in this paper*, as part of my website dedicated to rhythmic canons, at http ://canonsrythmiques.free.fr/midiFiles/, 2004.