COLLOQUIUM ON MATHEMATICAL MUSIC THEORY
H. Fripertinger, L. Reich (Eds.)
Grazer Math. Ber., ISSN 1016–7692
Bericht Nr. 347 (2005), 1-25

Rhythmic canons and Galois theory

Emmanuel Amiot

Abstract

The study of rhythmic canons by mathematicians with musical interest has given rise to unexpected connections to non trivial mathematical problems. The author tried a new approach based on a Galoisian interpretation of the novel results and concepts of Coven and Meyerowitz [4]. Extending this in a second part to finite fields, he concludes with unexpected results.

1 Rhythmic canons, tiling the line, polynomials

1.1 Canons

1.1.1 Basic definition

As an abstraction of the musical notion, a rhythmic canon is a canon debarred of all pitches, intensities and other musical parameters, keeping only rhythm. There are several voices, each playing the same motif, or rhythmic pattern, but beginning at different onsets. A motif (meaning 'rhythmic motif' in the context of this paper) can be modelised by the set A of the onsets of its different notes. For musical ([17]) and mathematical ([13]) reasons, it is desirable to modelise all these onsets by integers, measuring multiples of the unit beat. Usually a musical canon is periodic, and some musicians have added the constraint that on each beat one and only one note is played.

Translates of A (i.e. the different voices) will have the form $b_i + A$; putting all these offsets b_i in one set B, one gets a first possible definition including the periodicity condition (the rhythmic motif A is usually called «inner rhythm», the set of onsets B is called «outer rhythm»):

Definition 1. *A canon with inner rhythm A, outer rhythm B and period n is given by two finite subsets $A, B \subset \mathbb{N}$ and an integer n satisfying*

$$A \oplus B \oplus n\mathbb{Z} = \mathbb{Z}$$

Mathematics Subject Classification 2000: Primary 05E20, Secondary 33C80.
Keywords and phrases: rhythmic canons, tile, line, tiling, Galois, finite fields, cyclotomic, roots of unity.

The symbol $\oplus$ means the sums are direct, i.e. there is one and only one sum whose result is a given number.

It can be understood, musically, that the motif A is repeated in different voices with period n, starting points of each voice being given by B: it suffices to write the preceding equation $(A \oplus n\mathbb{Z}) \oplus B = \mathbb{Z}$.

Of course, in practice, when people are singing 'Frère Jacques' or 'Der Hahn ist todt' there is a beginning and an end, that is to say only a finite part of the whole sum is used. We will ignore these practical details, and concentrate on the mathematical notion and read the preceding equation modulo n, which yields the definition we will effectively consider;

Definition 2. *A canon with inner rhythm A, outer rhythm B and period n is given by two finite subsets $A, B \subset \mathbb{N}$ and an integer n satisfying*

$$A \oplus B = \mathbb{Z}/n\mathbb{Z}$$

meaning that $(A, B) \ni (a, b) \mapsto a + b$ is bijective, onto a complete set of residues modulo n.

*If such an equation is satisfied for a given set A we will say in short that A **tiles**.*

For instance, the motif, or inner rhythm $\{0, 1, 6, 7\}$ makes a rhythmic canon (i.e. tiles) with the outer rhythm $\{0, 2, 4\}$ and period 12. This is clearly equivalent to the problem of tiling the cyclic group $\mathbb{Z}/n\mathbb{Z}$ with translates of A (cf. [13], [4], [11] for instance).

Interesting examples in Midi format may be listened to online ([21], [22]). More on this vocabulary and its history is to be found in [1].

1.1.2 Context

- This definition of rhythmic canons is completely equivalent to the problem of tiling the line, as proposed in [4], [11], [16] and many others. The equivalence with tiling $\mathbb{Z}$ is not obvious but is discussed elsewhere[1], [11]. It is straightforward to see that if $A \oplus B = \mathbb{Z}/n\mathbb{Z}$, then $A \oplus (B + n\mathbb{Z}) = \mathbb{Z}$. The reverse is a theorem by DeBruijn.

- The musical origin of the question of rhythmic canons in the pionneer work of Dan Tudor Vuza is well explained in [3].

- It can be assumed without loss of generality that both sets A, B begin with 0: if A tiles $\mathbb{Z}/n\mathbb{Z}$, meaning $A \oplus B = \mathbb{Z}/n\mathbb{Z}$, so does $A + k$ for any k with the same B. Musically this means shifting the time origin of rhythmic motif A.

- There are several generalisations of the above definition: canons with augmentations ([9]), retrogradations ([20]), multisets ([4]), holes, loops, intervals... Some of these will be mentioned in the present paper as they provided insights and challenging new ideas for mathematical treatment.

- There are alternate definitions, some allowing several notes or even no notes on a single beat. See a detailed introduction in [1], and more references in the bibliography.

- It must be stressed that tiling a cyclic group: $A \oplus B = \mathbb{Z}/n\mathbb{Z}$, and tiling an interval: $A \oplus B = \{0, 1, 2, \dots n-1\}$, are not the same thing. For instance the inner rhythm $A = \{0, 2, 3, 6, 9\}$ tiles with period 10, i.e. tiles $\mathbb{Z}/10\mathbb{Z}$, but does not tile any **interval** of integers (see figure 1). Of course any tiling of an interval provides a tiling of a cyclic group. In the former case, just like in a fuga, in a musical rendering of the canon one first hears successive entries of the motif in different voices, up to a point when t here are no more gaps since on all beats exactly one voice is playing a note; conversely, if the canon is brought to an end, as several voices die out, gaps appear again, as can be seen in the illustration. This musically interesting disorder vanishes when one considers only the mathematical definition stated above

  The first picture shows a canon (with inner rhythm, or motif, $A = \{0, 2, 3, 6, 9\}$, and outer rhythm $B = \{0, 5, 10, 15\}$), first computing $A + B$ in $\mathbb{N}$, then computing $A \oplus \{0, 5\}$ in $\mathbb{Z}/10\mathbb{Z}$: we can see that the reduction modulo 10 corresponds to listening to the canon at a moment when all voices are playing without leaving any gap. As in all figures in this paper, time is represented by the horizontal axis while the different voices, to be read horizontaly, are numbered on the vertical axis. Such a representation is intended to mimick a musical score.

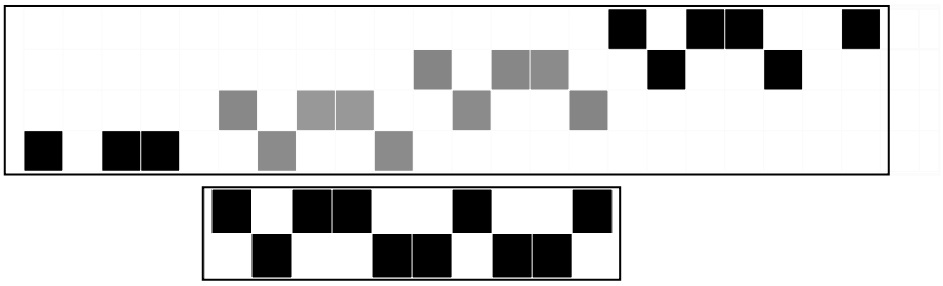

Figure 1: tiling or not tiling an interval

Of course the cyclic nature of these objects (when considering tilings of $\mathbb{Z}/n\mathbb{Z}$ with translates of the set A) might be more properly rendered on a cylindrical (or even toroïdal) representation like the one on figure 2; but for the sake of readability, the linear graphical form has been prefered here.

A musical illustration of these canons may be found in [21] .

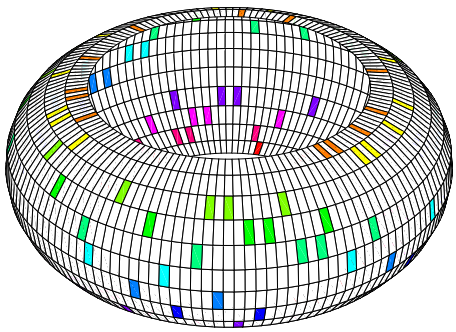

Figure 2: a canon going round

1.2 Polynomial formalisation

A common mathematical tool is exponentiation followed by summation. Here we exponentiate a variable x with the elements of sets A or B, and get a polynomial with coefficients in $\{0, 1\}$, henceforth called a **0-1 polynomial**.

Definition 3. *The polynomial associated with the finite set $A \subset \mathbb{N}$ is*

$$A(x) = \sum_{i \in A} x^i.$$

As usual, exponentiation turns sums into products, that is to say $A + B$ is transformed into the product $A(x) \times B(x)$.

The set $\{0, 1, 2, \ldots n-1\}$ is associated with $1 + x + x^2 + \ldots x^{n-1}$, thus we get the polynomial definition of a rhythmic canon:

Definition 4. *The motif $A \subset \mathbb{N}$ tiles with $B \subset \mathbb{N}$, with period n, if*

$$(T_0) \qquad A(x) \times B(x) \equiv 1 + x + x^2 + \ldots + x^{n-1} \ mod\ x^n - 1$$

is satisfied.

This is equivalent to definition 2.

There are several easy and useful results (see [4], [1], [11]): for instance the cardinality of A is the value of the associated polynomial when $x = 1$, and the period is the product of the cardinalities of A and B :

$$n = A(1) \times B(1).$$

2 Conditions on roots of unity

In condition (T_0) the polynomial $1+x+x^2+\dots x^{n-1}$ appears twice: explicitly, and as a factor of x^n-1, modulo which the equality is taken. It means that it divides the product $A(x)\times B(x)$ (in $\mathbb{Z}[x]$), and by Gauss Lemma, its irreducible factors must divide A or B. These factors are well known:

Definition 5. *The irreducible factors of* $1+x+x^2+\dots x^{n-1}$ *are the cyclotomic polynomials* Φ_d, *with* $d>1$ *and* $d \mid n$ *(d divides n).*

These polynomials are in $\mathbb{Z}[x]$, *are monic, and in* $\mathbb{C}[x]$ *we can factor*

$$\Phi_d(x)=\prod_{\xi}(x-\xi) \qquad \textit{where } \xi \textit{ has exactly the multiplicative order } d.$$

We do not list here all the elementary properties of cyclotomic polynomials. See useful lemmas in [4] or [1].

This simple fact led in 1998 Ethan Coven and Aaron Meyerowitz to substantial progress on the **tiling question**, enabling to answer the question whether a given motif tiles, or not.

2.1 The Coven-Meyerowitz conditions (T_1) and (T_2)

We introduce some notations.

Definition 6. *Let* μ_n *be the group of* n^{th} *roots of unity :* $\mu_n=\{z\in\mathbb{C}, z^n=1\}$.

If $A(x)$ *is a 0-1 polynomial, we define* R_A *to be the set of the roots of unity which are also roots of A.*

Observe that all roots of given order d must lie in the same irreducible factor, namely Φ_d. This a fact from Galois theory, which is the line of thought in the present paper.

We take special notice of roots whose order is a prime power :

Definition 7. *If* $A(x)$ *is a 0-1 polynomial, let* S_A *be the set of roots of unity which are roots of A of order* p^α, *for some prime p and* $\alpha\in\mathbb{N}^*$.

Example: if $A=\{0,1,8,9,17,28\}$ we get $A(x)$ factored as

$$(1+x)(1-x+x^2)(1+x+x^2)(1-x^2+x^4)(1-x^3+x^6)(1+x^3-x^4-x^7+x^8-x^9+x^{11}-x^{12}+x^{13})$$

The procedure `recogListe`, developed in the *Mathematica* notebook **canonCrawler** dedicated to the study of rhythmic canons, identifies the cyclotomic factors $\Phi_2,\Phi_6,\Phi_3,\Phi_{12},\Phi_{18}$ (the last factor is not cyclotomic). So $R_A=\{2,3,6,12,18\}$ while $S_A=\{2,3\}$.

Just as $p-$Sylows are the basic factors of Jordan-Hölder decompositions of abelian finite groups, the elements of S_A play a privileged role in characterizing rhythmic canons.

Theorem 8. *Let*

$(T_1): A(1)=\prod_{p^\alpha\in S_A} p$ *and*

$(T_2):$ *if* $p^\alpha, q^\beta[,\dots]\in S_A$ *then* $p^\alpha\times q^\beta[\times\dots]\in R_A$.

- *If A tiles then (T_1) is true.*
- *If (T_1) is true and (T_2) is true, then A tiles.*
- *If $|A| = A(1)$ has two prime factors and A tiles, then (T_2) is true.*

In the example above, condition (T_1) reads as $2 \times 3 = A(1)$ and (T_2) is $2 \times 3 \in S_A$. Both are true, so A tiles (with $\{0, 3, 15, 18, 21, 33\}$ for instance).

See proofs in [4]. Only the last assertion is really difficult[1], see also [1] for a discussion of musical aspects of the former.

In all known cases of tilings, (T_2) is true. It was also proved to be true in a special case when $|A|$ has three prime factors ([7]). In this paper we will make an even stronger case for the conjecture that (tiling $\Rightarrow (T_2)$) in showing that any counter-example, i.e. a rhythmic canon wherein (T_2) would be false, would have to stand in an already exceptional class of canons.

There is also a connection to the FUGLEDE conjecture (see below and [11]).

2.2 Galoisian Automorphism Proves A Fundamental Lemma

Lemma 9. *If A tiles with B, with period n, then pA tiles with the same B for any p coprime to n.*

This Lemma, deemed «fundamental» in COVEN-MEYEROWITZ [4], was in fact first proved by VUZA [17], going largely unnoticed, then independently by TIJDEMAN [16], then with a nicer proof by [4] and rediscovered by the minimalist composer Tom JOHNSON [private communication]. It is of great interest for music composers, as it enables to tile with the same motif on a different pattern of entries, or the reverse.

An alternate proof will be given in the annex of this paper, putting forward that this Lemma essentially relies on the following fact:

Lemma 10. *The map $\xi \mapsto \xi^p$ inside the unit circle S^1 is an automorphism of the group $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$, when p and n are coprime.*

Indeed, it is the restriction to S^1 of one of the GALOIS automorphisms of the cyclotomic field generated by μ_n.

This means that the order of an element of R_A is unchanged by this transformation, or its reverse. Hence changing A to pA, which changes $A(x)$ into $A(x^p)$, does not change the set R:

Proposition 11. *If p is coprime with the period n of the canon, then $R_A = R_{pA}$.*

The detailed proof is to be found in the annex.

[1] Relying ultimately on a result by SANDS founded on the decomposition as a direct product of the GALOIS group of the cyclotomic field $\mathbb{Q}[e^{2i\pi/(p^\alpha q^\beta)}]$.

2.3 Generating canons

2.3.1 Some generative techniques

Starting from a given rhythmic canon $A \oplus B = \mathbb{Z}/n\mathbb{Z}$, there are several known ways to produce new canons, which are used (and sometimes originated) by music composers. We will see that there is mathematical relevance to these manipulations.

- **Duality**.

  Simple yet effective (especially musically): just exchange A and B.

- **Affine transformation**.

  As in the aforementioned «fundamental Lemma», $pA \oplus B$ is still equal to $\mathbb{Z}/n\mathbb{Z}$ when p is coprime with n. Reducing lists of canons to their orbits under the affine group is a useful way to limit the combinatorial explosion (of course in practice there is already reduction modulo circular permutation, i.e. the action $A \mapsto A + k \bmod n$).

- **Dilatation** (see [6]).

  Each note, and each rest, in the rhythmic motif, is replaced by k copies of itself. In the example below, the original motif is $A = \{0, 2, 7\}$ and it is changed into $\widehat{A} = \{0, 1, 4, 5, 14, 15\}$. Some have formalised this transformation as a kind of tensorial product. I will state it in terms of 0-1 polynomials:

  Definition 12. *The dilatation of the rhythmic canon $A \oplus B = \mathbb{Z}/n\mathbb{Z}$ is the result of turning $A(x)$ into $\widehat{A}(x) = (1 + x + x^2 + \dots x^{k-1}) \times A(x^k)$ and $B(x)$ into $\widetilde{B}(x) = B(x^k)$.*

  It is immediate that $\widehat{A}$ tiles with outer rhythm $kB = \widetilde{B}$ if A tiles with B.

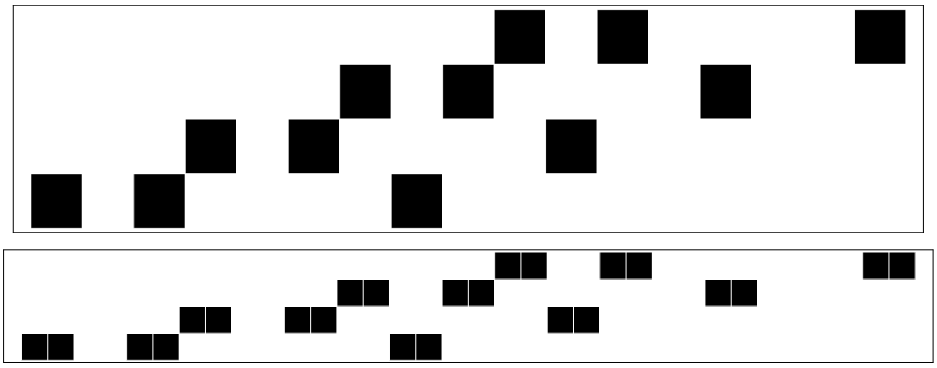

Figure 3: Dilatating a canon

This may be combined with the duality operation.

- **Concatenation**.

  Repeating the motif yields a canon of longer period. See figure 3.

  Definition 13. *The $k-$concatenation of rhythmic canon $A \oplus B = \mathbb{Z}/n\mathbb{Z}$ is the canon*

  $$(A \oplus \{0, n, 2n, \dots (k-1)n) \oplus B = \mathbb{Z}/(kn\mathbb{Z})$$

  I am indebted to Harald Fripertinger for stressing the importance of this seemingly trivial transformation.

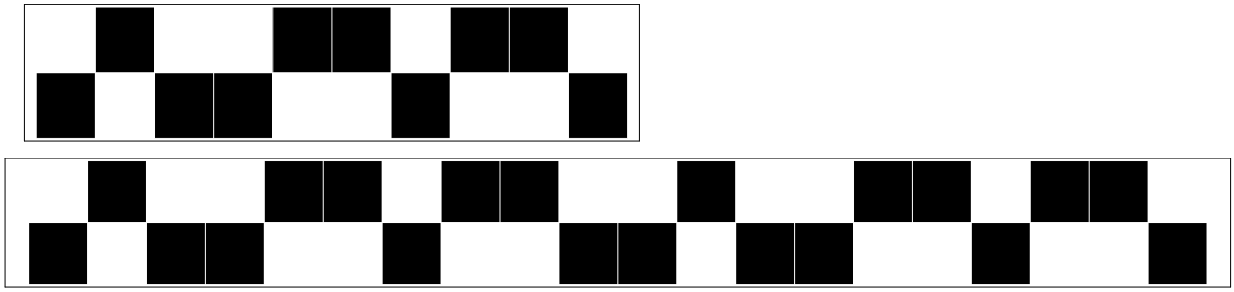

Figure 4: Repeating a canon

- **Complementation**.

  If A tiles, there are several possible 'outer rhythms' B, i.e. solutions of the equation $A \oplus B = \mathbb{Z}/n\mathbb{Z}$. Computers can provide a list of all possible B's though the computing time quickly gets prohibitive for n well over 100.

The last transformations might enter under the general framework of «tensorial products of canons», as proposed by Frank Jedrzejewski [10]. Combining all of these enables to find numerous rhythmic canons, as exposed in seminar MaMuX [2].

2.3.2 What happens to conditions $(T_1), (T_2)$.

Considering the sets R_A, S_A, we prove in the annex the following:

Theorem 14. *All of the above transformations preserve condition (T_1): if a rhythmic motif satisfies (T_1) then any of its transforms by one of the above maps also satisfies (T_1).*

Similarly, all of the above transformations, except perhaps complementation, preserve condition (T_2).

Indeed it looks quite probable that ALL canons can be produced with this set of transformations, from the trivial canon $\{0\} \oplus \{0\} = \{0\}$ (sometimes increasing the period, and then reducing the canon to a smaller one). Such manipulations and generative processes on canons are currently implemented in musical software such as OpenMusic (developed in Ircam, Paris). The only operation which might give an exception to the preservation of (T_2) is complementation: we could not prove that if $A \oplus B = \mathbb{Z}/n\mathbb{Z}$ and A verifies (T_2), then B must verify (T_2) too, though no counter example is known.

2.3.3 About Fuglede's spectral conjecture in dimension 1

Shortly after the paper by Coven-Meyerowitz [4], it was proved by Izabella Laba [11] that conditions $(T_1) + (T_2)$ imply the spectral condition, that is to say one side of the Fuglede's conjecture. Perhaps it is worthwhile to state this conjecture in terms of roots of polynomials, as it stands in [11].

Definition 15. *Let A be a finite subset of $\mathbb{N}$, with smallest element 0, $A(x)$ the associated polynomial and $N = A(1) = \sharp A$.*

A has a spectrum Λ if and only if there exists a set $\Lambda = \{\lambda_0 = 0 < \lambda_1 < \dots \lambda_{N-1} < 1\}$ such that $e^{2i\pi(\lambda_j - \lambda_k)}$ is a root of $A(x)$ for all (j,k) with $j \neq k$.

Fuglede conjecture states that A tiles (i.e. there exists $n \in \mathbb{N}^*, B \subset \mathbb{N}$ and $A \oplus B = \mathbb{Z}/n\mathbb{Z}$) $\iff$ A has a spectrum Λ. It was proved in a number of cases in dimension > 1, and disproved recently in dimension 5, considering some complex Hadamard matrixes, by Terence Tao (see [19]). It is still an open problem in dimension 1.

So by [11], condition (T_2) (along with (T_1)) implies tiling, and also implies the existence of a spectrum (directly related to the $p^\alpha \in S_A$). Moreover, whenever tiling implies (T_2) we have the spectral condition. This is true for instance whenever the number of notes of the motif has at most two prime factors, and so far in all known tilings of the line (i.e. rhythmic canons). Now the question is

Open question *Is (T_2) a necessary condition for tiling in all cases?*

The preceding transformational results allow a drastic reduction of the number of possible exceptions.

Definition 16. *$A \oplus B = \mathbb{Z}/n\mathbb{Z}$ is a cyclic canon if there exists $d \in \mathbb{Z}/n\mathbb{Z}, d \neq 0$, such that $A + d = A$ (or $B + d = B$). An acyclic canon is a canon which is not cyclic.*

This name is simpler than 'Regular Canons of Maximal Category' introduced in [17]. We will prove the following :

Theorem 17. *If a rhythmic canon has a factor not satisfying condition (T_2) then it is collapsible to an acyclic canon, not satisfying condition (T_2).*

By 'collapsible' we mean that such a canon is obtained by concatenation (repetition) of the motif of a smaller canon, and this reduction operation (combined with duality) can be repeated until an acyclic canon is reached. Here is a simple example, with successive reductions; notice the duality operation between the third and fourth versions:

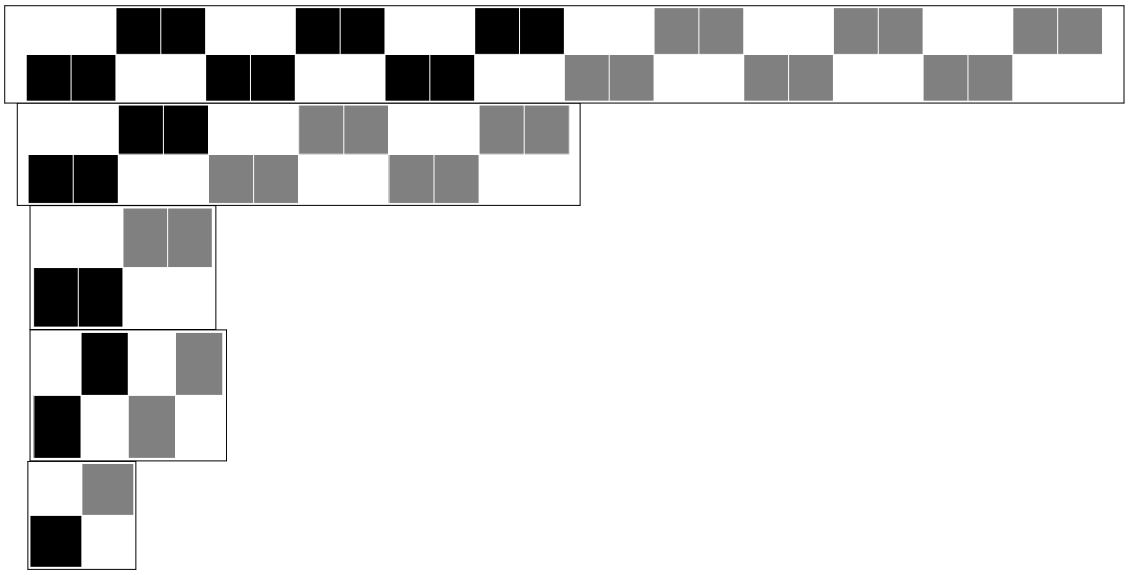

Figure 5: collapsing a canon

Which means that essentially we must look for possible counter examples to condition (T_2) among the acyclic canons.

It was proved by Hajòs (and others, notably Dan Tudor Vuza [17], theorem 1b) that acyclic canons exist only for very special periods n, the smallest ones being 72,108,120...

Definition 18. *If $\mathbb{Z}/n\mathbb{Z}$ can be expressed as a direct sum of two acyclic subsets, it is called a «bad group». If not, it is a* Hajòs *group.*

It was recently shown that actual acylic canons are very sparse material (see H. Fripertinger's paper in the present proceedings): typically one out of several millions in practice, and this only for very special values of n.

Also we get an extension of [11] where it was stated that when $n = p^\alpha q^\beta$, tiling implies the spectral condition (via (T_2)):

Corollary 19. *If A tiles with period n and $\mathbb{Z}/n\mathbb{Z}$ is a* Hajòs *group, then (T_2) holds, hence A has a spectrum.*

This is the case (see [18]) when $n = p^\alpha, n = p^\alpha q, n = p^2q^2, n = pqr, n = p^2qr, n = pqrs$ (p, q, r, s distinct primes), of which the first three were consequences of theorem **B2** of [4]; the other cases are new as far as we know.

This narrows the possibility of tilings without (T_2) down to really exceptional canons. Unfortunately, we only know algorithms for building *some* acyclic canons (see [3] for instance), no general recipe is known for finding all of them f or a given period. All of these recipes ensure that the resulting canon verifies (T_2).

Remark 20. Among the cases excluded by the above theorem are the special cases of the tilings of $\mathbb{N}$; according to a lemma of Nicholas de Bruijn on 'British Number Systems' [5]), such tilings are collapsible recursively to the most trivial tiling, $\{0\} \oplus \{0\}$ (like in above figure). Hence any such tiling must satisfy (T_2). This was suggested in the end of [4], and Laba mentions on her home page that it has been proved independently.

The theorem above states that a tiling motif A and any concatenation of A must simultaneously satisfy (or infirm) condition (T_2); this leads to an alternate proof of theorem 1.6 in [12], which studies products of 'metronomes' (this tool is defined in the annex). As it is easily shown that if a tiling motif A is spectral then any concatenation of A also is, all this really boils down to this: the difficulty in Fuglede's conjecture lies with Vuza(i.e. acyclic) canons.

Most conjectures on the topic of tiling the line have been proved wrong, will the one above follow suit ? Counter-examples must be tilings with big periods. At the present moment, all aperiodic canons with periods below 120 are known (see Fripertinger's paper in the present proceedings), so all tiles with period below 120, and many others besides, have a spectrum in the sense of definition 15.

2.4 Towards finite fields

The theoretical reason for exploring finite fields in connection with the tiling problem is that the conditions in [4] take for granted that $A(x)$ is a 0-1 polynomial. This is a strong condition, as one sees when trying to construct A from some cyclotomic factors[2] and finite fields will help us take this into account.

But in truth the idea originates in a nice little problem suggested by Tom Johnson [9] whose solution was exposed in Zürich in 2002 [1].

Remark 21. *It is possible to tile an interval with motif $A = \{0, 1, 4\}$ and some of its (binary) augmentations, that is to say with $A, 2A, 4A \ldots$*

The smallest solution, as Johnson found by hand, is

$$(\{0, 1, 4\} \oplus \{0, 2, 8, 10\}) \oplus (\{0, 2, 8\} \oplus \{5\})$$

which tiles an interval of length 15.

[2]Say we compute $\Phi_8 \times \Phi_9 = 1 + x^3 + x^4 + x^6 + x^7 + x^{10}$ or better still (because of (T_2))

$$\Phi_8 \times \Phi_9 \times \Phi_{72} = 1 + x^3 + x^4 + x^6 + x^7 + x^{10} - x^{12} - x^{15} - x^{16} - x^{18} - x^{19} - x^{22} + x^{24} + x^{27} + x^{28} + x^{30} + x^{31} + x^{34}$$

To turn this into a 0-1 polynomial is *not* obvious (multiplication by $1 + x^{12}$ should be avoided as the resulting motif cannot tile because of (T_1); one of the simplest solutions is to multiply by $\left(1 - x^3 + x^6\right) \times \left(1 - x^6 + x^{12}\right)$).

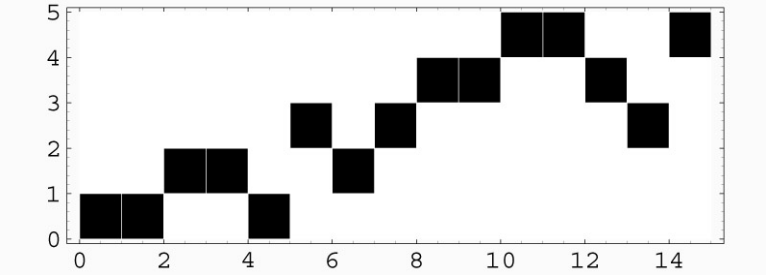

Figure 6: Johnson's shortest solution

Now it happens that all solutions found by computer exhaustive search ([15]) have a length which is a multiple of 15. Johnson asked if this was always true, and why.

Theorem 22. [1] *Any solution of* JOHNSON*'s problem has a length which is a multiple of 15.*

The answer is essentially contained in this result :

Proposition 23. *[Amiot, 2002] The polynomial* $J(x) = 1 + x + x^4$ *divides* $1 + x + x^2 + \dots x^{n-1}$ ***in*** $\mathbb{F}_2[x]$ *if, and only if,* $n \in 15\mathbb{N}$.

The link with the original equation uses the FROBENIUS automorphism $x \mapsto x^2$, which is a GALOIS automorphism of any field of characteristic 2 over its prime field $\mathbb{F}_2$, as

Lemma 24. $J(x^2) = (J(x))^2$ *in* $\mathbb{F}_2[x]$*, and more generally* $J(x^{2^p}) = (J(x))^{2^p}$.

The two last results easily imply theorem 22. Again details can be found in the Annex and in [1].

This kind of result definitely warrants an interest in rhythmic canons in a finite field. First we must make sense of the notion.

3 Rhythmic canons in $\mathbb{F}_p$

3.1 Local to Global Philosophy

3.1.1 Making sense

Observe that all fields share the elements 0 and 1. This means that an equation between 0-1 polynomials **makes sense** in all $\mathbb{K}[X]$, for any field $\mathbb{K}$. We do not mean that it is true in each field : for instance

$$(1 + x^2)^2 \times (1 + x) = 1 + x + x^4 + x^5$$

is true in all fields of characteristic 2, but false in the field with 3 elements, or in the «real world», e.g. $\mathbb{R}[x]$. We just state that such an equation can be **written** in all polynomial

rings $\mathbb{K}[x]$, as a kind of «well-formed expression», and then one may check whether it is true or not.

Next we start from such an equation, true in $\mathbb{R}[x]$ and hence in $\mathbb{Z}[x]$.

We can canonically project it in $\mathbb{F}_p[x]$ by reducing all components modulo p. Thus the equation remains true in all fields, as a field $\mathbb{K}$ includes a prime field which is either $\mathbb{Q}$ or a $\mathbb{F}_p$.

Let us summarize this in the following :

Proposition 25. *If an identity between 0-1 polynomials is true in $\mathbb{Z}[x]$, then it is true in all $\mathbb{F}_p[x]$.*

This is useful for proving that a rhythmic motif *does not* tile: as in JOHNSON's problem, where it was necessary that $J(x) = 1 + x + x^4$ divided $1 + x + \ldots x^{n-1}$ in $\mathbb{F}_2[x]$.

This raises the converse question: knowing that such an identity is true in all, or several, $\mathbb{F}_p[x]$, is it possible to retrieve the same identity in $\mathbb{Z}[x]$? This is a kind of «local to global» philosophy, like HASSE's theory on quadratic forms. It is also reminiscent in the category context of YONEDA's philosophy, which may be relevant to mathemusical analysis as argumented in ([14]).

3.1.2 From finite fields back to $\mathbb{Z}$

The answer to the question above is positive:

Theorem 26. *Let $A(x), B(x), C(x)$ be 0-1 polynomials. Then the equation*

$$A(x) \times B(x) = C(x)$$

holds in $\mathbb{Z}[x]$ if and only if it holds in all $\mathbb{F}_p[x]$.

Remark 27. This theorem can be spelled with «... in $\mathbb{K}[x]$ for all (finite) fields $\mathbb{K}$». Indeed it is enough that (T_0) holds in **several** finite fields.

Also this can be generalized to more complicated equations, with any number of sums (not differences) and products.

This theorem is not difficult, it was stated and proved in [1]. A proof is given in the annex.

3.1.3 An alternate condition

It is possible to relax slightly the hypothesis of the above theorem, just checking the identity in a single finite field and checking also the number of non zero terms in each polynomial:

Proposition 28. *Let $A(x), B(x), C(x)$ be 0-1 polynomials. If $A(x) \times B(x) = C(x)$ holds in $\mathbb{F}_p[x]$ for a given prime p, and it is true in $\mathbb{R}$ for the special value $x = 1$, then it is true in $\mathbb{Z}[x]$.*

The additional condition with $x = 1$ just ensures that there are no cancellations (the sum $A + B$ is direct and $A \oplus B = C$). A detailed proof is left to the reader.

Indeed $x = 1$ may be replaced by any $x = \varepsilon > 0$. This is mentioned here because for integer values of x, like $x = 2$, one gets interesting numbers, like Mersenne numbers (or more generally repunits).

All this suggests a kind of local (in the sense of arithmetics) definition for rhythmic canons:

Definition 29. *We will say that rhythmic motif A* ***tiles modulo*** *p iff (T_0) holds for $A(x)$ (and some 0-1 polynomial $B(x)$) in $\mathbb{F}_p[x]$.*

3.2 The special case of $\mathbb{F}_2$

3.2.1 Is $\mathbb{F}_2[x]$ the set of 0-1 polynomials?

There is an obvious bijection between (the subset $\{0,1\}[x]$ of) 0-1 polynomials and the ring $\mathbb{F}_2[x]$. Unfortunately this map has no structure: it does not always map sums onto sums, or products onto products, as we have seen on the above example. Indeed it only works when there is a canon situation!

To put it in another way, the natural injection

$$\mathbb{F}_2[x] \xrightarrow{i} \{0,1\}[x] \subset \mathbb{Z}[x]$$

is not the reciprocal of the canonical ring projection

$$\mathbb{Z}[x] \xrightarrow{\pi_2} \mathbb{F}_2[x].$$

In a way, the problem of rhythmic canons is the exploration of this deficiency.

3.2.2 A strong result

We study the question of tiling modulo 2:

Theorem 30. *(Galois)*

Any polynomial not vanishing in zero divides $x^n - 1$ in $\mathbb{F}_2[x]$, for some large enough n.

Corollary 31. *Any rhythmic motif tiles modulo 2.*

Let us explain here the gist of Definition 29:

- Musically speaking, it means that any (finite) rhythmic motif generates a generalised kind of canon, whence we allow an **odd** number of notes on every beat. This is a weaker condition than tiling with exactly one note per beat, much weaker indeed as the last theorem shows.

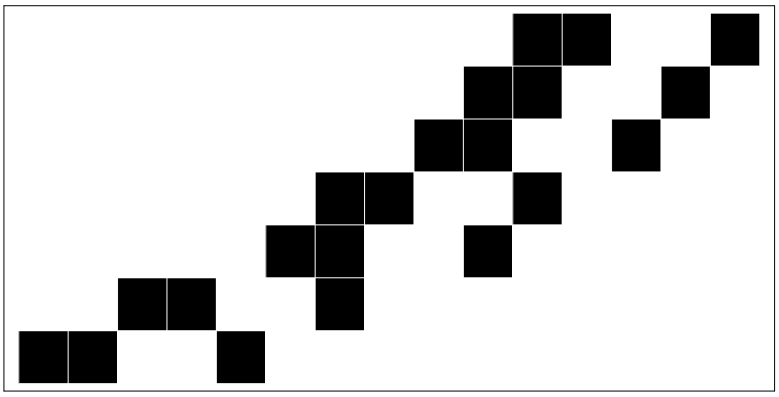

Figure 7: a tiling modulo 2

- Mathematically, it means that if $A = \{0, a_1, \ldots, a_{k-1}\}$ is a set of integers, there exists $B \subset \mathbb{N}, n \in \mathbb{N}$ such that

$$A \times B \ni (a, b) \mapsto a + b \in \{0, 1, 2, \ldots, n-1\}$$

  is onto, and every element in $\{0, 1, 2, \ldots, n-1\}$ has an **odd** number of preimages.

B is defined by the polynomial quotient of $x^n - 1$ by $A(x) \times (x - 1)$ in $\mathbb{F}_2[x]$, for a suitable n provided by Theorem 30. Such a polynomial $B(x)$ will have 0-1 coefficients, as these are the only numbers available in the field $\mathbb{F}_2$! It is possible to actually compute the smallest possible n – this is implemented in the procedure `completeModulo` of the **canonCrawler**.

In the language of *multisets* introduced by [4] it just means that the sum $A + B$ is a multiset with odd weights. Figure 7 is an example of such a tiling modulo 2, with $A = \{0, 1, 4\}$. A does not tile the integers as can be seen directly (or from the fact that condition (T_1) does not hold). This example can be downloaded and heard as a midi file on [21], as all examples in this paper.

Remark 32. Theorem 30 is also true in $\mathbb{F}_p$. But the construction fails for moduli greater than 2, as the quotient $\dfrac{1 + x + \ldots x^{n-1}}{A(x)}$ need not have only 0-1 coefficients.

Indeed, for the same example as above but $p = 3$ we find that

$$\frac{x^{39} - 1}{(x-1)(1 + x + x^4)} = 1 + x^2 + x^5 + 2\,x^6 + 2\,x^7 + 2\,x^8 + x^9 + x^{10} + x^{11} + x^{12} + 2\,x^{13} + x^{14} + 2\,x^{15} + x^{16}$$

$$+ x^{17} + 2\,x^{18} + 2\,x^{22} + 2\,x^{23} + 2\,x^{24} + 2\,x^{25} + 2\,x^{27} + 2\,x^{29} + 2\,x^{30} + x^{32} + x^{33} + x^{34}$$

At that point, it remained to explore the other moduli in order to find sufficiently stringent conditions for a rhythmic motif to tile the line. Let it be enhanced again that when one uses Theorem 26 in order to prove that A tiles, one assumes that the outer

rhythm B is the same, for all moduli p (involved). So even if we proved that a rhythmic motif A tiles in all $\mathbb{F}_p$, it would not be sufficient to ensure that A tiles in the real world. As it happens this makes a great deal of sense, as shown by Theorem 34 below, which greatly surprised the author.

3.3 Tiling in $\mathbb{F}_p$

3.3.1 Strange digits

We mention a strange feature which is connected with condition (T_1). When applying Theorem 30, it often turns out that 1 is a root of $A(x)$ modulo p. Indeed, the multiplicity of 1 may be large.

Theorem 33. *Let A be a 0-1 polynomial which tiles with period n, and p a prime factor of n. Then*

- *let m be the multiplicity of 1, as a root of $A(x)$ in $\mathbb{F}_p[x]$; then the $p-$adic representation of m contains only digits which are 0's and $p-1$'s.*
- *The number of non zero digits is the multiplicity of p (the $p-$adic valuation) in the integer $A(1) \in \mathbb{N}$, which is the number of notes of the rhythmic motif (this is really another way to express condition (T_1)).*

Let us examine an example with one of the most recently found Vuza canons (see Fripertinger's paper in the present proceedings) :

$$A = \{0, 4, 8, 9, 10, 18, 26, 40, 44, 46, 54, 62, 63, 72, 76, 80, 82, 98\}$$

tiles with period 108. Modulo 3, 1 is a root of $A(x)$ of order 20 (meaning $(x-1)^{20}$ is a factor of $A(x)$ in $\mathbb{F}_3[x]$). But in base 3, 20 reads as 202, whose digits are 0's and 2's, and the number of 2's is the multiplicity of the base, 3, in $A(1) = 18 = 3^2 \times 2$.

3.3.2 The general tiling theorem

It seemed reasonable to expect that some conditions would be required for tiling modulo some prime number p. On the contrary:

Theorem 34. *Any rhythmic motif tiles in $\mathbb{F}_p$, for any prime p.*

This is mainly Theorem 30, with the addition of the following trick that we called « *Unfolding* » *Lemma*:

Lemma 35. *Let $P \in \mathbb{N}[x]$ be polynomial with non negative integer coefficients; then for any integer $n > 1$, P is congruent to a 0-1 polynomial modulo $x^n - 1$:*

$$P(x) \equiv \tilde{P}(x) \in \{0, 1\}[x] \ mod\ (x^n - 1).$$

Theorem and Lemma are proved in the annex.

An example of the lemma : let $P(x) = 1+3x^2+2x^5$ and $n = 5$, then we can «unfold» $3x^2 \mapsto x^2 + 2x^7 \mapsto x^2 + x^7 + x^{12}$. Ultimately,

$$P(x) \equiv 1 + x^2 + x^5 + x^7 + x^{10} + x^{12} \bmod x^5 - 1$$

Figure 8 is an example, tiling modulo 3 with $A = \{0, 1, 3\}$ and period 24.

Contrarily to the case $p = 2$, this is not tiling an interval $\{0, 1 \ldots, n-1\}$, reduction modulo n is mandatory, and the result is not necessarily minimal.

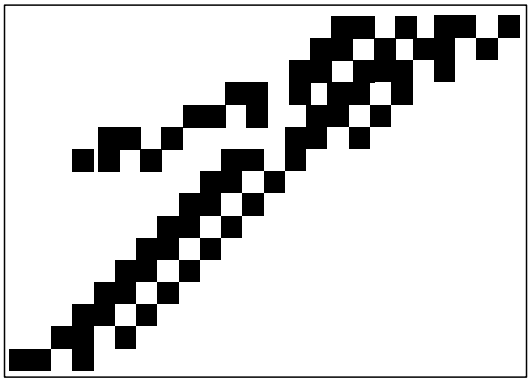

Figure 8: a tiling modulo 3

This opens intriguing possibilities in music; perhaps when several voices compete on the same beat, they might be arranged to play octaves or unisons, or some components of the spectrum of the base note.

It also means that one cannot use finite fields for proving that a given motif tiles, only to prove that it *does not*, as in JOHNSON's problem. The unexpected results found along the way made the adventure worthwhile, though.

4 Annex

4.1 Proof of the Fundamental Lemma 9

1) We recall condition (T_0) : $A(x) \times B(x) \equiv 1 + x + x^2 + \ldots x^{n-1} \bmod x^n - 1$.

2) Let us denote the unit circle in $\mathbb{C}$ by S^1. There is a map $\mathcal{F}_n : \mathbb{Z}[x]/(x^n - 1) \to S^1$ associating to a polynomial $A(x)$ defined modulo $x^n - 1$ the set R_A of the roots of $A(x)$ which are in μ_n, the group of n^{th} roots of unity.

The main point is that the last map is independent of the choice of a representative of $A(x)$ modulo $x^n - 1$. Indeed, $\xi \in \mu_n$ is a root of $A(x) \iff$ it is a root of $A(x) + Q(x)(x^n - 1)$ for any $Q \in \mathbb{Z}[x]$. Also it must be noted that when (T_0) holds, the disjoint union $R_A \cup R_B$ is equal to $\mu_n \setminus \{1\}$.

I stress this map because it enables a better understanding of the stability of tiling under multiplication by some invertible $p \pmod n$: pA corresponds to the polynomial $A(x^p)$, and the map $\xi \mapsto \xi^p$ is an automorphism of the group μ_n, leaving R_A stable.

Indeed it is the restriction of one of the GALOIS automorphisms of the cyclotomic field $\mathbb{Q}[e^{2i\pi/n}]$ (the cyclotomic field, decomposition field of $x^n - 1$, and hence of all the cyclotomic polynomials involved) which is the deeper reason of the following lemma (a more precise version of Lemma 10):

Lemma 36. *If ξ is a root of order $d \mid n$, then so is ξ^p for any p coprime to n.*

Proof. $(\xi^p)^d = (\xi^d)^p = 1$, hence the order of ξ^p is a divisor of d.

Conversely, if $(\xi^p)^e = 1$ then d must divide pe and by GAUSS Lemma (d being a divisor of n, is coprime with p), d divides e. □

This means that $R_{pA} = R_A$, as stated in Proposition 11.

In order to finish the proof of Lemma 9, we still need to show that (T_0) holds for pA, i.e.

$$A(x^p) \times B(x) \equiv 1 + x + x^2 + \dots x^{n-1} \bmod x^n - 1$$

Proof.

1) $A(x^p)$ is still a 0-1 polynomial (mod $x^n - 1$) with exactly $|A| = A(1)$ terms (monomials). This is essentially true because $a \mapsto pa$ is an automorphism of $\mathbb{Z}/n\mathbb{Z}$: $x^{p\alpha}$ and $x^{p\beta}$ must have different residues modulo $x^n - 1$ when $\alpha \neq \beta \bmod n$.

2) The product $A(x^p) \times B(x)$, even taken mod $x^n - 1$, has at least $n - 1$ roots in $\mathbb{C}$, namely $R_A \cup R_B = \mu_n \setminus \{1\}$. This is because $R_{pA} = R_A$.

3) Now this polynomial has degree at most $n - 1$ after reduction mod $x^n - 1$; the constant term is known to be 1, hence it is exactly $1 + x + x^2 + \dots x^{n-1}$, which completes the proof. □

4.2 Generating other canons

In this section we prove Theorem 14 in the different cases enumerated in section **2.3**.

Remark 37. It is not necessary to prove that condition (T_1) is preserved, as all these manipulations deal with effective canons and hence (T_1) is always true by the theorem **B1** in [4] (see Theorem 8). So it will be left as an exercise to the reader.

4.2.1 Affine transform

As we have seen above, the sets R_{pA}, S_{pA} are exactly the same as R_A, S_A: hence (T_2) is true for pA whenever it is true for A.

4.2.2 Dilatation

For convenience let us state again the definition in terms of polynomials :

Definition 38. *The dilatation of canon*

$$A(x) \times B(x) \equiv \frac{x^n - 1}{x - 1} \pmod{x^n - 1}$$

by a factor p is the canon

$$\widehat{A}(x) \times \widetilde{B}(x) \equiv \frac{x^{pn} - 1}{x - 1} \pmod{x^{pn} - 1}$$

where $\widehat{A}(x) = (1 + x + \ldots + x^{p-1}) \times A(x^p)$ and $\widetilde{B}(x) = B(x^p)$.

It suffices to list the sets of roots of unity of $\widehat{A}(x), \widetilde{B}(x)$. It is enough to prove that (T_2) is preserved in the case when p is a prime number. Let us consider a cyclotomic factor Φ_d of either $A(x)$ or $B(x)$.

Lemma 39. *If p is coprime with d, then $\Phi_d(x^p) = \Phi_d(x) \times \Phi_{pd}(x)$.*
If p divides d then $\Phi_d(x^p) = \Phi_{pd}(x)$.

This classical Lemma is used in [4], it is easy to prove by considering the order of a root of $\Phi_d(x^p)$ or by using the generating formula

$$\Phi(n) = \prod_{d|n} (x^d - 1)^{\mu(d)} \qquad \text{where } \mu \text{ is the MÖBIUS function.}$$

Hence when proceeding to the dilatation of canon $A \oplus B$, the cyclotomic factor Φ_d is replaced by Φ_{pd} when p divides d; on the other hand, when p and d are coprime, the factor Φ_d remains and Φ_{pd} is added to the list of cyclotomic factors. In the case of $\widehat{A}(x)$ we also have to include the new factor Φ_p (see the definition of $\widehat{A}(x)$). To sum it up:

Corollary 40. *$R_{\widetilde{B}} = (p \times R_B) \cup (R_B \setminus p\mathbb{N})$ and $R_{\widehat{A}} = \{p\} \cup (p \times R_A) \cup (R_A \setminus p\mathbb{N})$.*

Now it is easy to check that condition (T_2) is true for $\widetilde{B}$ (resp. $\widehat{A}$) if and only if it is true for B (resp. A): if q is a prime, we have

$$q^\alpha \in S_{\widehat{B}} \iff \begin{cases} q^\alpha \in S_B & (q \neq p) \\ q^{\alpha-1} \in S_B & (q = p) \end{cases}.$$

Hence the products $(p^\gamma)q^\alpha r^\beta \ldots$ occur in $S_{\widetilde{B}}$ if and only if the products $(p^{\gamma-1})q^\alpha r^\beta \ldots$ already are in S_B.

The case of $\widehat{A}$ is similar, with special consideration for the lone factor $p^1 = p \in S_{\widehat{A}}$. This completes the proof of the dilatation-part of Theorem 14. □

4.2.3 Repetition (concatenation)

• First we prove that concatenating with itself a rhythmic motif that tiles a canon, yields a new rhythmic motif that tiles also:
Proof. Assume $A \oplus B = \mathbb{Z}/n\mathbb{Z}$ and let $1 < k \in \mathbb{N}$. It is not difficult to prove the claim reasoning on integers, or better still on a commutative diagramm with the canonical projections $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \mathbb{Z} \to \mathbb{Z}/(kn)\mathbb{Z}$. For consistency with what follows we will give a slightly less elegant proof with polynomials instead. So we start from condition (T_0):

$$A(x) \times B(x) \equiv \frac{x^n-1}{x-1} \bmod x^n-1 \iff A(x) \times B(x) = \frac{x^n-1}{x-1} + Q(x) \times (x^n-1).$$

Choose the representative A minimal ($A \subset \{0, 1 \dots n-1\}$) and define A repeated k times by $A' = A \oplus \{0, n, 2n, \dots, (k-1)n\}$. Then

$$A'(x) = A(x) \times (1 + x^n + x^{2n} + \dots x^{(k-1)n}) = A(x)\frac{x^{kn}-1}{x^n-1}.$$

Now from equation (T_0) we get

$$A'(x) \times B(x) = \Big(\frac{x^n-1}{x-1} + Q(x) \times (x^n-1)\Big)\frac{x^{kn}-1}{x^n-1} = \frac{x^{kn}-1}{x-1} + Q(x) \times (x^{kn}-1).$$

which is what we claimed. □

• Now we prove that the concatenation operation preserves condition (T_2).

Proof. We begin with the polynomial $M_{n,k} = 1 + x^n + x^{2n} + \dots x^{(k-1)n} = \dfrac{x^{kn}-1}{x^n-1}$, very important for musicians, as it is the modelisation of any metronomical rhythm. It has been shown recently that products of two such metronomes tile $\iff$ (T_1) and (T_2) are satisfied [12], which is a corollary of the current Theorem.

Algebraically though, $M_{n,k}$ is a just a product of cyclotomic polynomials:

Lemma 41. *$M_{n,k}$ is the product of cyclotomic factors Φ_d with d dividing kn, but not n.*

This lemma easily results from the definition of $M_{n,k}$ as a quotient and the decomposition of $x^n - 1$ in a product of cyclotomic polynomials.

We infer that $A'(x)$ has as new roots of unity those of such orders d:

$$R_{A'} \setminus R_A = \{\text{the roots of order } d, \text{ with } d \text{ dividing } kn, \text{ but not } n\}.$$

It is enough to prove that (T_2) is preserved when $k = p$ is a prime (by iterating the process one gets the more general case, dividing the period into several steps instead of a single one). Summarizing:

Lemma 42. *$R_{A'}$ contains R_A. If $n = p^{v_p(n)}.m$, m coprime with p, then the only additional elements have the following form: $p^{v_p(n)+1}q^\beta \dots \mid pn$*

We investigate the relationship between $R_{A'}$ and $S_{A'}$ in order to check if (T_2) is still true; there are two cases to discuss:

- If $p^\alpha \in S_A$ then $p^{\alpha+1}$ will stand in $S_{A'}$ only when $\alpha = v_p(n)$ i.e. p^α is a factor of n of maximal exponent, as we have just seen. We check in that case for new factors $p^{\alpha+1}q^\beta\dots$ in $R_{A'}$, and indeed they are here, as $p^\alpha q^\beta\dots$ divides n, hence $p^{\alpha+1}q^\beta\dots$ divides pn but does not divide n, by the maximality of α which means that $p^{\alpha+1}q^\beta\dots \in R_{A'}$ (cf. Lemma 42).
- Consider another element $q^\beta \in S_A, q \neq p$. Then in addition to factors $q^\beta r^\gamma\dots$ which are (by condition (T_2), assumed for A) already in R_A and hence in $R_{A'}$, we must consider eventual $q^\beta p^\alpha r^\gamma\dots$ for $p^\alpha, r^\gamma\dots \in S_{A'}$. But this is the case only if $\alpha - 1 = v_p(n)$, i.e. $p^{\alpha-1}$ is the greatest power of p dividing n (Lemma 42 again). Then $p^{\alpha-1}, r^\gamma\dots \in S_A$ and hence by Lemma 42 again

$$q^\beta p^{\alpha-1} r^\gamma\dots \in R_A \iff q^\beta p^\alpha r^\gamma\dots \in R_{A'}$$

which ends the proof that condition (T_2) is preserved by concatenation ; it works in the same way for the reverse operation of 'collapsing'. □

• Next we consider a cyclic canon, that is to say $A + d = A \bmod n$, and prove that A is collapsible, meaning this is reducible to a smaller canon $A' \oplus B = \mathbb{Z}/m\mathbb{Z}$.

Proof. We can assume that d is a divisor of n (else replace d by $m = \gcd(d, n)$, as

$$n\mathbb{Z} - d\mathbb{Z} = \{an - bd \mid a, b \in \mathbb{Z}\} = \gcd(n, d)\mathbb{Z} = m\mathbb{Z}$$

and thus $A = A + (un + vd) = A + m$ is $m-$cyclic). Let $p = n/d$ (we could assume that it is a prime factor of n, but is not necessary). Again, the proof is possible within number sets:

$$\mathbb{Z} = A \oplus B \oplus n\mathbb{Z} = B \oplus (A \oplus n\mathbb{Z}) = B \oplus (A' \oplus m\mathbb{Z}) = A' \oplus B \oplus m\mathbb{Z},$$

but computation with polynomials is an instructive alternative. So we start from

$$A(x) \times x^{n/p} = A(x) \times x^d \equiv A(x) \bmod x^n - 1 \quad \text{i.e.} \quad A(x) \times x^d = A(x) + Q(x) \times (x^n - 1).$$

We infer

$$A(x) = Q(x) \times \frac{x^n - 1}{x^d - 1} = Q(x) \times (1 + x^d + \dots x^{(p-1)d}).$$

We choose $A'(x) = Q(x) = A(x) \times \dfrac{x^d - 1}{x^n - 1}$: we have condition (T_0) with period d, as

$$A'(x) \times B(x) = \frac{x^d - 1}{x^n - 1} \times A(x) \times B(x) = \frac{x^d - 1}{x^n - 1} \times \Big(\frac{x^n - 1}{x - 1} + Q'(x) \times (x^n - 1)\Big) \equiv \frac{x^d - 1}{x - 1} \bmod x^d - 1.$$

It only remains to prove that $A'(x)$ is 0-1. Remember that A' is defined by

$$A(x) \times x^d = A(x) + A'(x) \times (x^n - 1)$$

with $d < n$ and $A(x)$ a 0-1 polynomial of degree $< n$.

Assume A' is not 0-1: let ux^k be the greatest degree monomial of A' with coefficient $u \neq 1$. Now we compute the coefficient of x^{n+k} in $A(x) \times x^d$ which is u, as $d^\circ A < n$. But $A(x) \times x^d$ is a 0-1 polynomial: contradiction.

The proof is now complete. □

As stated in the main text, this process $A \mapsto A'$ of collapsing can be iterated as long as the canon is not acyclic, and hence until we get an acyclic canon (maybe interchanging A, B sometimes), or the trivial canon $\{0\} \oplus \{0\}$ in the case of a fully collapsible canon.

4.3 Proof of «Local to Global» Theorem 26

Proof. We consider the case of equation $A(x) \times B(x) = C(x)$ for instance. An equality between polynomials in $\mathbb{Z}[x]$ holds iff it is true for a great number of values of x. Here we assume it is true that $A(a)B(a) \equiv C(a) \bmod p$ for all a, p. Hence for all $a \in \mathbb{Z}, A(a)B(a) = C(a)$ in $\mathbb{Z}$ (Chinese Remainder Theorem), hence $A(x) \times B(x) = C(x)$ in $\mathbb{Z}[x]$. □

A musician would not need the CRT for a proof: he would notice that if the number of notes on a given beat of a canon is $\equiv 1 \bmod p$ for all p, then it must be exactly 1.

4.4 Tiling modulo p

4.4.1 Proof of Theorem 30

Proof. Though we first use it for $p = 2$, it is true for any prime p. Consider an irreducible [in $\mathbb{Z}[x]$] factor $A(x)$ of $P(x)$. It is completely decomposed in an extension, namely $\mathbb{F}_q = \mathbb{F}_p[X]/(A(X))$. This field is finite and of characteristic p, as indeed $q = p^{d^\circ A}$. Since by Lagrange theorem all (non zero) elements of this field satisfy $a^{q-1} = 1$ and A has only simple roots (a finite field is perfect) we have $A(x) \mid x^q - 1$ [this stands in $\mathbb{F}_p[x]$].

This enables to decompose all factors of $P(x)$. But there is the question of multiple roots. Say $A(x) \mid x^n - 1$; we get

$$A(x)^k \mid (x^n - 1)^k \mid (x^n - 1)^{p^\alpha}$$

for $p^\alpha > k$. But we recognize a power of the Frobenius automorphism (extended to $\mathbb{F}_p[x]$), and

$$(x^n - 1)^{p^\alpha} = x^{n.p^\alpha} - 1 = x^m - 1 \qquad \text{in } \mathbb{F}_\mathrm{p}[\mathrm{x}].$$

The LCM of such $x^m - 1$ for all irreducible factors of a given polynomial divides some $x^N - 1$, and we have found an exponent N with $P(x) \mid x^N - 1$. □ This proof is constructive. An improvement of the algorithm checks whether (T_0) is verified for divisors of N till the smallest solution is reached.

4.4.2 Proof of corollary (every motif tiles a canon modulo 2)

Now let $p = 2$: all polynomials are 0-1 polynomials.

Let A be an inner rhythm. We want (T_0) mod 2, i.e. we want $A(x)$ to divide $\dfrac{x^N-1}{x-1}$, we just have to set $P(x) = A(x) \times (x-1)$ in the above computation. This proves that any $A(x)$ (non vanishing in 0) divides some $1 + x + x^2 + \ldots x^{n-1}$ for some n. The quotient is a 0-1 polynomial, having no choice, and this proves that any rhythmic motif tiles modulo 2.

4.4.3 Strange digits

Proof. We begin with a lemma used in [4].

Lemma 43. $\Phi_k(1) = \begin{cases} p & \text{if } k \text{ is a power of } p \\ 1 & \text{else.} \end{cases}$

This lemma is well known and easy to prove from most definitions of cyclotomic polynomials.

Hence 1 is a root of $A(x)$ modulo p, i.e. $p \mid A(1)$, iff $A(x)$ admits a factor $\Phi_{p^\alpha}, p^\alpha \mid n$ (in the proof of condition (T1) in [4] it is made clear that the value of any (eventual)(monic) non-cyclotomic factors in 0 is ± 1, because when counting the total multiplicity of a prime factor p in $A(1) \times B(1) = n$, which is the total multiplicity of root 1 in $\dfrac{x^n-1}{x-1}$ modulo p, it accounts exactly for all Φ_{p^α} where $p^\alpha \mid n$).

The multiplicity of 1 in

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

is computed from the following identity, which is a consequence of Frobenius automorphism (modulo p)

$$\Phi_{p^\alpha}(x) = (1 + x + x^2 + \ldots x^{p-1})^{p^{\alpha-1}} = \Big(\frac{x^p-1}{x-1}\Big)^{p^{\alpha-1}} = \Big(\frac{(x-1)^p}{x-1}\Big)^{p^{\alpha-1}} \in \mathbb{F}_p[x].$$

Hence this multiplicity is $p^{\alpha-1}(p-1)$, and this happens for several different α's (whenever $p^\alpha \in R_A$).

The sum of these multiplicities expressed in base p is $\sum_{p^\alpha \in R_A} (p-1)p^{\alpha-1}$: it has digit $p-1$ only at positions α and 0's elsewhere, which proves the first point.

Now the number of digits $p-1$ is also the number of factors Φ_{p^α} in $A(x)$, and this is the multiplicity of p in $|A| = A(1)$ by condition (T_1). □

This theorem is devoid of any interest when $p = 2$, as all binary numbers are obviously written with 0 and 1 only.

4.4.4 Applications to tiling modulo p

Theorem 30 is true modulo any prime p without modification. So there exists, for all A, a polynomial $B(x) = \dfrac{x^n-1}{A(x)(x-1)} \in \mathbb{F}_p[x]$, unfortunately its coefficients are usually different from 0,1.

As we only need a 0-1 member of the class of $B(x)$ mod $x^n - 1$, it is sufficient to prove the Unfolding Lemma.

But this relies on iterating a simple transformation (hence the idea of 'unfolding'): write $B(x)$ as a polynomial with coefficients in $\mathbb{N}$, then apply

```
If a>1, a*x^m -> (a-1)x^m + x^(n+m)
```

This transformation does not change $B(x)$ mod $x^n - 1$, as it adds a multiple of $x^n - 1$, but it decreases all coefficients greater than 1. So after a finite number of iterations (at most the sum $B(1)$ of all coefficients of B) we get a 0-1 polynomial, congruent to $B(x)$ mod $x^n - 1$. □

Acknowledgements. I am much indebted to Harald Fripertinger for invitation to speak in Graz and publish the present paper, but also for many productive discussions on the topic of rhythmic canons, some memorable. The comments of an anonymous reviewer were extremely thorough and helpful; he deserves much credit for enhancing the readability of the final text.

My beloved wife managed to unravel a number of misspellings at the last moment. My gratitude for her rereading is all the greater as she knows nothing of mathematics.

References

[1] 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.

[2] Amiot, E., *Some new canons*, in seminar MaMuX, january 2004, online at http://canonsrythmiques.free.fr/someNewCanons.pdf.

[3] 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.

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

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

[6] 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.

[7] Granville, A.; Laba, I.; and Wang, Y., *On finite sets that tile the integers*, in Math-Archive or http://www.math.gatech.edu/ wang/preprints.html.

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

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

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

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

[12] 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), no. 2, 267-280.

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

[14] Mazzola, G., *The Topos of Music*, Birkhäuser, Basel, 2003.

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

[16] 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.

[17] 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.

[18] Sands, A.D., *The Factorization of abelian groups*, Quart. J. Math. Oxford, 10(2):4554.

[19] Tao, T., *Fuglede's conjecture is false in 5 and higher dimensions*, http://arxiv.org/abs/math.CO/0306134.

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

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

[22] *Midi files of Vuza canons*, complete compendium for $n = 72$ and $n = 108$, http://www.mathe2.uni-bayreuth.de/frib/canons/canon.html, 2004.

Emmanuel Amiot
1 rue du Centre
F – 66570 St Nazaire, France
e-mail: *manu.amiot@free.fr*
website *http://canonsrythmiques.free.fr/menuEnglish.htm*