Harmonical structure of digital sequences and applications to s-dimensional uniform distribution mod 1

Pierre LIARDET
(Joint work with Guy Barat)

HARMONICAL STRUCTURE OF DIGITAL SEQUENCES AND APPLICATIONS TO s-DIMENSIONAL UNIFORM DISTRIBUTION MOD 1

I. Objectives and strategy

II. Candidates

III. Dynamical structures

IV. Applications

V. Candidates from Ostrowski α-expansion

I. Objectives and strategy

From numeration systems, build sequences in the s-dimensional box $[0,1[^s$ which are

– uniformly distributed modulo 1,

– with good "discrepancy" occasionally.

Guide line : have in mind the construction of digital sequences given by Niederreiter :

First step, build sets X of N points x_n $(n = 0, \ldots, N-1)$ in $[0,1[^s$ such that the counting function $A_N(J,X) := \#\{0 \leq n < N\,;\ x_n \in J\}$, verifies

$$A_N(J,X) - N.\mathrm{mes}(J) = 0$$

for a good family of boxes J.

This leads to the following definition

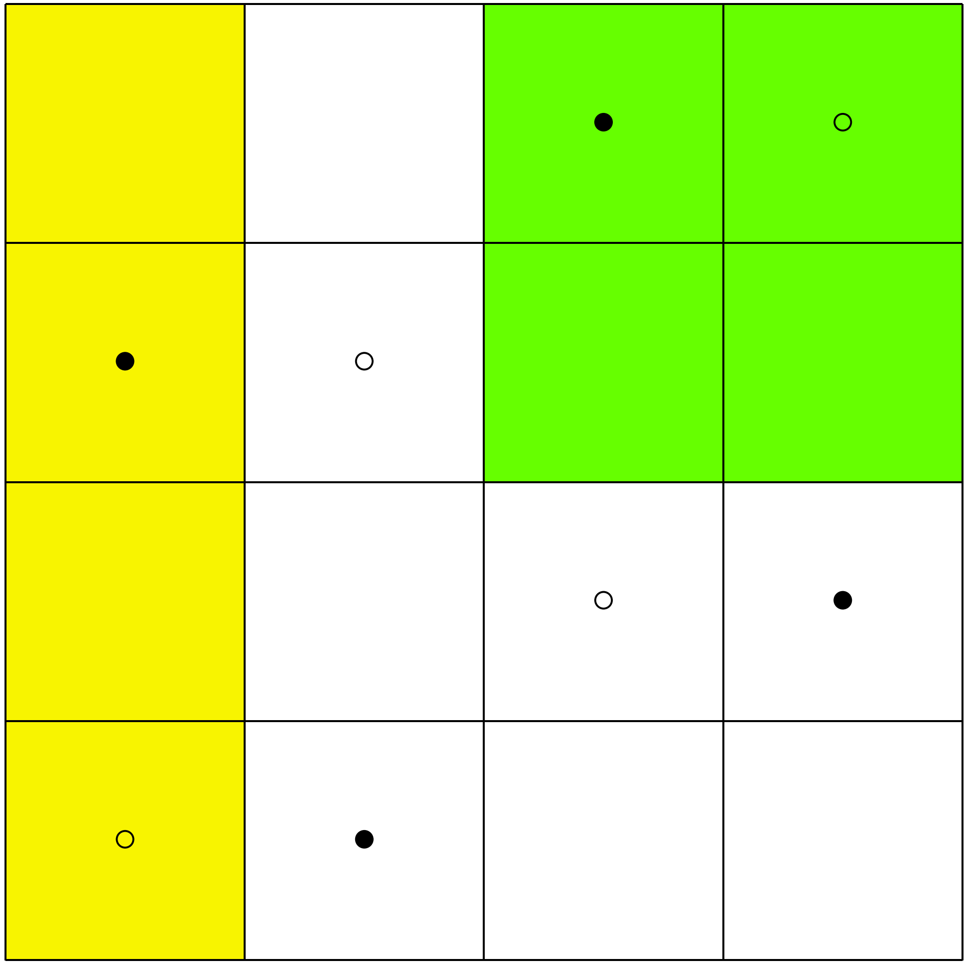
Let t, m be integers with $0 \leq t \leq \mathbf{m}$

Definition. *A* $(t, \mathbf{m}, s)$*-net (in base* b*) is a set* X *of* $N{=}b^{\mathbf{m}}$ *points in* $[0,1[^s$ *such that* $A_N(J,X) - N.\mathrm{mes}(J) = 0$ *for all*

$$J = \prod_{i=1}^{s} \Big[\frac{a_i}{b^{d_i}}, \frac{a_i+1}{b^{d_i}}\Big[$$

with

- *integers* d_i *and* a_i : $d_i \geq 0,\ \ 0 \leq a_i < b^{d_i}$ $(1 \leq i \leq s,)$ *;*
- $\mathrm{mes}(J) = 1/b^{\mathbf{m}-t}$ *(i.e.,* $\sum_i d_i = \mathbf{m} - t$*).*



Example for $m = 2$ and $t = 0$:

several possibilities,

– one ploted with $\bullet$

– another one plotted with $\circ$

Next step, build sequences...

Definition. *A sequence $X = (x_n)_n$ of points in I^s is a (t,s)-sequence in base b if for all integers $k \geq 0$ and $m > t$ the set of points*

$$\{x_n\,;\ kb^m \leq n < (k+1)b^m\}$$

form a (t,m,s)-net in base b.

H. Niederreiter gave estimates of the star discrepancy ; a simplified bound is

$$ND_N^*(X) \leq C(s,b) \cdot b^t (\log N)^s + \mathcal{O}\left(b^t (\log N)^{s-1}\right)$$

with $C(s,b) = \frac{1}{s!}\frac{b-1}{2\lfloor b/2 \rfloor}\left(\frac{\lfloor b/2 \rfloor}{\log b}\right)^s$ in general, but $C(s,b) = \frac{1}{s} \cdot \left(\frac{b-1}{2\log b}\right)^s$ either $s = 2$ or $b = 2,\ s = 3, 4$.

We do not go inside the general construction of Niederreiter but we set his construction in terms of q-additive sequences and introduce related dynamical systems.

II. Candidates

Sequences wich are behind the classical construction of (t, s)-sequences are b-additive :

Let A be a compact metrizable abelian group (law denoted additively).

Definition. *A sequence $f : \mathbf{N} \to A$ is said to be q-additive if*

$$f(0) = 0_A \quad \textit{and} \quad f(n) = \sum_{j \geq 0} f(e_j(n)q^j)$$

where $n = \sum_{j \geq 0} e_j(n)q^j$ is the usual q-adic expansion of n.

In case $f(e_j q^j) = e_j.f(q^j)$, we say that f is *strongly additive* (or is a weighted sum-of-digits function, following Pillichshammer, UDT 2007).

If A is a subgroup of $\mathbf{U}$, f is said “multiplicative”.

Many possibilities for choosing A to fit our programm.

In this talk we pay attention to the cases where

1) A is a finite,

2) A is the infinite product $G_b = (\mathbf{Z}/b\mathbf{Z})^{\mathbf{N}}$. In that case G_b is metrically identified (as a measured space) to $[0,1[$ using the Mona map $\mu_b : \Omega \to [0,1]$, defined by

$$\mu(a_0, a_1, a_2, \ldots) = \sum_{k=0}^{\infty} \frac{a_k}{b^{k+1}}.$$

Integers $n \geq 0$ are identified with $(e_0(n), e_1(n), e_2(n), \ldots, e_h(n), 0, 0, 0, \ldots)$ and we set

$$\mu(n) = \frac{e_0(n)}{b} + \frac{e_1(n)}{b^2} + \frac{e_2(n)}{b^3} + \cdots + \frac{e_h(n)}{b^{h+1}}.$$

A classical example :

$A = \mathbf{Z}/2\mathbf{Z}$ and $v(n) = \sum_{0 \le k \le h} e_k(n) \bmod 2$ (Thue-Morse sequence).

Construction

Let $\{f_k : \mathbf{N} \to \mathbf{Z}/b\mathbf{Z}\,;\ k \ge 1\}$ be a family of q-additive sequences.

The map $F : \mathbf{N} \to G_b$ defined by

$$F(n) = (f_0(n), f_1(n), f_2(n), \ldots)$$

is a G_b-valued q-additive sequence.

Our aim is :

– produce F from a dynamical system,

– characterize the cases where this system is ergodic,

– determine its spectral type....

III. Dynamical structures

The following method is quite standard :

– look at F as an element of $\Omega = A^{\mathbf{N}}$,

– introduce the shift map $S : \Omega \to \Omega$ and the orbit closure K_F of F under the action of S,

– Notice that $S(K_F) \subset K_F$ so that we get a topological dynamical system (S, K_F) (in short a *flow*).

It remains to indentify (S, K_F) with a nice system and to put on K_F a suitable S-invariant measure that will give us the expected result!

In fact we have the following general topological result :

Theorem. *Given any compact abelian group A and any A-valued q-additive sequence F, then the flow (S, K_F) is minimal.*

We can say a bit more :

Define $A_n = \overline{\{F(q^n m)\,, m \in \mathbf{N}\}}$ and $A_F = \cap_{n\geq 0} A_n$. The elements of A_F are called *topological essential values* of F.

Theorem. *(i) The set of topological essential values form a subgroup of A ;*

(ii) This group acts on K_F by the diagonal action $(A_u, \Omega) \to \Omega$ defined by

$$\alpha.(\omega_0, \omega_1, \omega_2, \ldots) = (\alpha + \omega_0, \alpha + \omega_1, \alpha + \omega_2, \ldots).$$

Interesting consequences in case A is finite :

1) if $A_F = \{0_A\}$, then there is an integer n_0 such that $A_{n_0} = \{0_A\}$, hence :

$$F \text{ is periodic with period } q^{n_0}\mathbf{N}.$$

2) Otherwise there exists

– a periodic q-additive sequence P with period $q^m\mathbf{N}$,

– a q-additive sequence $G : \mathbf{N} \to A_F$ with $A_G = A_F$

such that

$$F = P + G.$$

For our purpose, the periodic part P plays no role.

More about q-additive sequences F in a finite group A

After changing F if necessary, we may assume that A is also the group of topological essential values A_F.

Theorem. *The flow (S, K_F) is uniquely ergodic, that means there exists only one Borel probability measure ν on K_F such that*

– $\nu \circ S^{-1} = \nu$ *(ν is S-invariant) ;*

– *For any Borel set B in K_F, if $S^{-1}(B) \subset B$ then $\nu(B) = 0$ or 1 (ergodicity).*

Moreover the marginal ν_i of ν along the i-th projection map $\omega \mapsto \omega_i$ is the equiprobability on A.

Skech of the proof. Since A acts along the diagonal on K_F we get K_F homeomorphic to the product $A \times K_{\Delta F}$ with

$$\Delta F(n) = F(n+1) - F(n).$$

The homeomorphism is given by

$$(x_0, x_1, x_2, \ldots) \mapsto (x_0, (x_1 - x_0, x_2 - x_1, x_3 - x_2, \ldots))$$

and the shift action turns to be a skew product on $A \times K_{\Delta F}$, namely

$$T : ((x_0, (x_1 - x_0, x_2 - x_1, \ldots)) \mapsto (x_0 + (x_1 - x_0), (x_2 - x_1, x_3 - x_2, \ldots))$$

Skech of the proof. Since A acts along the diagonal on K_F we get K_F homeomorphic to the product $A \times K_{\Delta F}$ with

$$\Delta F(n) = F(n+1) - F(n).$$

The homeomorphisme is given by

$$(x_0, x_1, x_2, \ldots) \mapsto (x_0, (x_1 - x_0, x_2 - x_1, x_3 - x_2, \ldots))$$

and the shift action turns to be a skew product on $A \times K_{\Delta F}$, namely

$$T : ((x_0, (x_1 - x_0, x_2 - x_1, \ldots)) \mapsto (x_0 + (x_1 - x_0), (x_2 - x_1, x_3 - x_2, \ldots))$$

Now ΔF is constant on the arithmetic progressions $m + q^k\mathbf{N}$ for any $m = 0, \ldots q^m - 2$. It follows easily that $(S, K_{\Delta F})$ has a unique invariant probability measure (and is also a (metrical) factor of the odometer $(x \mapsto x + 1, \mathbf{Z}_q)$).

Finally, it is well known (J. Coquet, T. Kamae, M Mendès France, Bull SMF 1977) that the *spectral measure* of F is **singular continuous**. This leads to

– $n \mapsto F(n)$ is uniformly distributed in A ;

– the sequences $n \mapsto F(n)$ and $n \mapsto S^n(\Delta F)$ are statistically independant.

That ends the proof using previous results (J. Coquet-P. L., J. d'Analyse, 1987).

Case $A = G_b$.

The statistical study of F relies on sequences $\chi \circ F$ where χ is any non trivial character of G_b.

Notice that $\chi(G_b)$ is a sub-group of the group of b-th roots of the unity.

Let Φ be the group of $\mathbf{Z}/b\mathbf{Z}$-valued q-additive sequences, periodic with period $q^m\mathbf{N}$ for some $m \geq 0$.

Applying the above results, we obtain the following theorem which extends a theorem of G. Larcher and H. Niederreiter :

Theorem. *Let* $\{f_0, f_1, \ldots\}$ *be a family of* q*-additive sequences,* $F = (f_0, f_1, \ldots)$ *the corresponding* G_b*-valued* q*-additive sequence. Then the sequence* F *is uniformly distributed in* G_q *if and only if for all* $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{m-1}) \in (\mathbf{Z}/q\mathbf{Z})^m$ *one has*

$$(\varepsilon_0 f_0 + \cdots + \varepsilon_{m-1} f_{m-1} \in \Phi) \;\Rightarrow\; (\varepsilon_0 = \varepsilon_1 = \cdots = \varepsilon_{m-1} = 0).$$

More dynamics, more results

To study the sum-of-digits functions for two coprime bases p, q, Kamae introduced a skew produit over the p-odometer $(x \mapsto x+1, \mathbf{Z}_p)$ and the q-odometer $(x \mapsto x+1, \mathbf{Z}_p)$.

That is a very fruitful idea used on various occasions by several authors.

Let us present the classical construction, starting with :

"Cocycle" associated to a q-additive sequence $v : \mathbf{N} \to A$

Here A is a locally compact metrizable abelian group.

Let τ denote the ***q-odometer*** : $(\tau, \mathbf{Z}_q, \mu_q)$,

$$\boxed{\tau(x) = x+1.}$$

The discrete derivative

$$\boxed{\Delta v(n) = v(n+1) - v(n)}$$

plays a fundamental role.

Using the fact that Δv has a constant value $c_k(m)$ on arithmetic progressions $P_k(m) = m + 2^{k+1}\mathbf{N}$, $0 \leq m < q^{k+1} - 1$, we may extend Δv to an A-valued map on $\mathbf{Z}_q$ called **Δ-cocycle** and defined by

$$\Delta v(x) = \begin{cases} c_k(m) & \text{if } x \in [e_0(m), \ldots, e_k(m)] \text{ (cylinder set)}, \\ 0_A & \text{if } x = (q-1, q-1, q-1, \ldots) \ (= -1). \end{cases}$$

$\rightarrow$ $\Delta v(\cdot)$ is continuous except possibly at $x = (q-1, q-1, q-1, \ldots)$.

Skew product $\tau_v : \mathbf{Z}_q \times A \to \mathbf{Z}_q \times A$

By definition :

$$\boxed{\tau_v(x, a) = (\tau x, a + \Delta v(x))}$$

Let λ_A be the Haar measure on A.

Easy fact : *τ_v preserves the product measure $\mu_q \otimes \lambda_A$.*

Essential values of K. Schmidt

An element $a \in A$ is said to be a ***metrical essential value*** of $\varphi : \mathbf{Z}_q \to A$ (for τ) if for any neighborhood V of a and any Borel set B in $\mathbf{Z}_q$ such that $\mu_q(A) > 0$, one has

$$\boxed{\mu_q(\bigcup_{n\in\mathbf{Z}} \Big(B \cap \tau^{-n} B \cap \{x \in \mathbf{Z}_q \,;\ \varphi_n(x) \in V\})\Big) > 0,}$$

where

$$\varphi_n(x) = \begin{cases} \varphi(x) + \cdots + \varphi(\tau^{n-1}(x)) & \text{if } n > 0\,; \\ 0_A & \text{if } n = 0\,; \\ -\varphi(\tau^n x) - \varphi(\tau^{n+1} x) - \ldots - \varphi(\tau^{-1} x) & \text{if } n < 0. \end{cases}$$

→ The set $E(\varphi)$ of essential values of φ is a **closed subgroup** of A.

The following two results, due to K. Schmidt, are fundamental :

Theorem (K. S.). *φ is a coboundary (i.e. there exists $g : \mathbf{Z}_q \to A$ such that $\varphi = g \circ \tau - g$) if and only if $E(\varphi) = \{0_A\}$.*

Theorem (K. S.). *$(\tau_v, \mathbf{Z}_q \times A, \mu_q \otimes \lambda_A)$ is ergodic if and only if $E(\Delta v) = A$.*

The following two results, due to K. Schmidt, are fundamental :

Theorem (K. S.). *φ is a coboundary (i.e. there exists $g : \mathbf{Z}_2 \to A$ such that $\varphi = g \circ \tau - g$) if and only if $E(\varphi) = \{0_A\}$.*

Theorem (K. S.). *$(\tau_v, \mathbf{Z}_q \times A, \mu_q \otimes \lambda_A)$ is ergodic if and only if $E(\Delta v) = A$.*

Application to uniform distribution :

We have

Theorem. *Assume that A is compact. If $(\tau_v, \mathbf{Z}_q \times A, \mu_q \otimes \lambda_A)$ is ergodic then it is uniquely ergodic.*

That follows from the fact that Δv is continuous except at the point $(q-1)^\infty$, and we can prove a little bit more :

Theorem. *Assume that A is compact. If $(\tau_v, \mathbf{Z}_q \times A, \mu_q \otimes \lambda_A)$ is ergodic then for any point (x, a) the sequence $n \mapsto (\tau_v)^n(x, a)$ is well distributed.*

Metrical and topological essential values

Theorem *For a given q-additive sequence, the group of metrical essential values of the cocycle Δu is a subgroup of the group of topological essential values.*

In case u takes a finite set of values, the situation is fine :

Theorem. *Assume that A is finite, then for any A-valued q-additive sequence u the group of topological values is equal to the group of metrical essential values :*

$$A_u = E(\Delta u).$$

After adding a coboundary to u (the opposite of the periodic part of u), we get

– a q-additive sequence which takes its values in the group A_u

– the corresponding skew product is ergodic,

– the ergodic measure is unique, given by the product measure.

IV. Applications

1) Going back to the s-dimensional unit box $[0,1[^s$:

Use the fact the $G_b = G_b^s$ (with suitable identification), the map

$$(q_1,\dots,g_s) \mapsto (\mu(g_1),\dots,\mu(g_s))$$

carries F to a sequence $U := (u_1,\dots,u_s)$ in $[0,1[^s$ which is uniformly distributed mod 1 (and in fact well distributed), if F is uniformly distributed in G_b.

2) Let $q_1,\dots,q_h$ be paiwisely coprime integers ≥ 2 and let $U^{(1)},\dots,U^{(h)}$ be sequences produced as above, with bases $q_1,\dots,q_h$ respectively.

Theorem. *If each sequences $U^{(j)}$ are uniformly distributed mod 1 in $[0,1[^{s_j}$ then the sequence $(U^{(1)},\dots,U^{(h)})$ is uniformly well distributed mod 1 in* $[0,1[^{s_1}\times\cdots\times[0,1[^{s_h}$.

V. Candidates from Ostrowski α-expansion

We consider the Ostrowki numeration from a given irrational number α having its continued fraction expansion with bounded partial quotients.

Let q_n be the sequence of denominators of convergents of α (starting with $q_0 = 1 < q_1 < \ldots$).

Any integers n has a unique expansion

$$n = e_0(n)q_0 + e_1(n)q_1 + \ldots + e_k(n)q_k$$

satisfying

$$\forall j\ ,\ e_0(n)q_0 + e_1(n)q_1 + \ldots + e_j(n)q_j < q_{j+1}.$$

We define α-additive sequences $u : \mathbf{N} \to A$ similarly to the q-additive case :

$$u(0) = 0_A \quad \text{and} \quad u(n) = \sum_{j \geq 0} u(e_j(n)q_j).$$

The dynamical study of α-additive sequence is more technical but the results are rather similar. See G. Barat, P. L., Annals Univ. Sci. Budapest, 2004.

For finite valued sequences. one has :

(1) Topological essential values and metrical essential values form the **same group**.

(2) The α-additive sequence u can decomposed in a sum $u = p + v$ where p can be extend by continuity to the α-ostrowski odometer and v take its values in A_u.

If Δv is not constant, then (S, K_v) is an ergodic skew product above the α-Ostrowski odometer.

(3) Theses results can be used to build sequences in the s-dimensional unit box which are

– uniformly well distributed modulo one ;

– similar to (t, s)-sequences ;

– with good discrepancy.