ACTA ARITHMETICA
LX.1 (1991)

Generalized Rudin–Shapiro sequences

by

Jean-Paul Allouche (Talence) and Pierre Liardet* (Marseille)

1. Introduction

1.1. The Rudin–Shapiro sequence was introduced independently by these two authors ([21] and [24]) and can be defined by

$$\varepsilon_n = (-1)^{u(n)},$$

where $u(n)$ counts the number of 11's in the binary expansion of the integer n (see [5]). This sequence has the following property:

$$\forall\, N \geq 0, \quad \sup_{\theta\in\mathbb{R}} \Big| \sum_{n<N} \varepsilon_n e^{2i\pi n\theta} \Big| \leq C N^{1/2}, \tag{1}$$

where one can take $C = 2 + 2^{1/2}$ (see [22] for improvements of this value). The order of magnitude of the left hand term in (1), as N goes to infinity, is exactly $N^{1/2}$; indeed, for each sequence (a_n) with values ± 1 one has

$$N^{1/2} = \Big\| \sum_{n<N} a_n e^{2i\pi n(\cdot)} \Big\|_2 \leq \Big\| \sum_{n<N} a_n e^{2i\pi n(\cdot)} \Big\|_\infty,$$

where $\| \ \|_2$ denotes the quadratic norm and $\| \ \|_\infty$ the supremum norm. Note that for almost every sequence (a_n) of ± 1's the supremum norm of the above sum is bounded by $\sqrt{N \operatorname{Log} N}$ (see [23]).

The inequality (1) has been generalized in [2] (see also [3]):

$$\sup_{f\in M_2} \Big| \sum_{n<N} f(n) e^{2i\pi x u(n)} \Big| \leq C' N^{\alpha(x)}, \tag{2}$$

where M_2 is the set of 2-multiplicative sequences with modulus 1. The

* Research partially supported by the D.R.E.T. under contract 901636/A000/DRET/DS/SR

exponent $\alpha(x)$ is explicitly given and satisfies

$$\begin{aligned} &\forall\, x && 1/2 \le \alpha(x) \le 1\,, \\ &\forall\, x \notin \mathbb{Z} && \alpha(x) < 1\,, \\ &\forall\, x \in \mathbb{Z} + 1/2 && \alpha(x) = 1/2\,. \end{aligned}$$

Moreover, the constant C' does not depend on x.

Of related interest see the papers of Rider [20], Brillhart and Carlitz [5], Brillhart and Morton [7], Brillhart, Erdős and Morton [6], Mendès France and Tenenbaum [17], Queffélec [18], and Boyd, Cook and Morton [4].

1.2. In this paper we are going to extend these results to other sequences. One particularly appealing example of generalization consists in counting the number of words of length $d+2$ which begin and end in 1 in the binary expansion of the integer n (the case $d = 0$ gives precisely the Rudin–Shapiro sequence). Extending this idea we will introduce Hadamard matrices: such a matrix (of order q) gives sequences which can be generated by finite automata and which satisfy (2) where M_2 is replaced by the set M_q of q-multiplicative sequences of modulus 1 (for the theory of Hadamard matrices, see for example [25]).

Section 2 is devoted to a general notion of sequences (called chained sequences) in a compact and metrizable group. These sequences satisfy inequalities analogous to (2) where the exponential function is replaced by an irreducible representation of the group. When the group is abelian, the optimal case giving bounds as in (1) implies that the group is necessarily finite. Let us notice (from Lemma 4 below) that bounds as in (1) and (2) depend only on the orbit of the sequence under the shift: for instance every sequence in the closed orbit of the Rudin–Shapiro sequence under the shift on $\{-1,+1\}^{\mathbb{N}}$ satisfies (1) where C is replaced by another suitable constant.

In Section 3 we define generalized Rudin–Shapiro sequences including previous extensions introduced by M. Queffélec ([19]). These sequences still have the Lebesgue measure as spectral measure.

2. Chained sequences

2.1. Notations and definitions. In what follows q is an integer greater than or equal to 2, $\mathcal{A}$ is the alphabet $\{0,1,2,\dots,q-1\}$ with the natural order. The monoid of finite words on $\mathcal{A}$ is denoted by $\mathcal{A}^*$ and is ordered with the lexicographical order, denoted by $\le$. The number of letters in a word w is called the *length* of w and denoted by $|w|$. The empty word Λ is of length 0. Let $\mathcal{A}^r$ be defined by

$$\mathcal{A}^r := \{w \in \mathcal{A}^*; |w| = r\}\,.$$

Let d be a positive integer and $\mathcal{D} := \mathcal{A}^{d+1}$. The set $\mathcal{D}$ can be considered as

an alphabet ordered by the lexicographical order. There exists a canonical one-to-one order-preserving map c from $\mathcal{D}^*$ into $\mathcal{A}^*$ which identifies $\mathcal{D}$ and $\mathcal{A}^{d+1}$.

Expanding an integer in base q allows us to define the maps e_k ("kth digit") from $\mathbb{N}$ to $\mathcal{A}$ by

$$n = \sum_{k\in\mathbb{N}} e_k(n) q^k \,.$$

We denote by $\widetilde{n}$ the word $e_{t(n)}(n)\dots e_0(n)$, with $t(0) = 0$, and for $n \neq 0$, $t(n) = [(\log n)/(\log q)]$ ($[x]$ is the integral part of x). Moreover, to each word $w = w_{r-1}\dots w_0$ in $\mathcal{A}^*$ ($r \geq 1$) we associate the integer

$$\dot{w} = q^{r-1}w_{r-1} + \dots + qw_1 + w_0 \,,$$

and we define $\dot{\Lambda} = 0$.

For every sequence φ with values in a set E, we define $\dot{\varphi} :\ \mathcal{A}^* \to E$ by

$$\dot{\varphi}(w) = \varphi(\dot{w}) \,,$$

and for every map f from $\mathcal{A}^*$ to E we define the sequence $\widetilde{f}$ with values in E by

$$\widetilde{f}(n) = f(\widetilde{n}) \,.$$

Definition 2.1. Let G be a multiplicative group. A map f from $\mathcal{A}^*$ to G is called a *chained map* (over $\mathcal{A}$) if for all letters $a, b \in \mathcal{A}$ and every word w in $\mathcal{A}^*$

(i) $f(0w) = f(w)$,
(ii) $f(abw) = f(ab)f(b)^{-1}f(bw)$.

(The rôle of property (i) is to select chained maps f which derive from a sequence φ by the relation $\dot{\varphi} = f$. If this property is explicitly required we shall speak of *regular* chained map. Otherwise we shall omit this extra condition.)

If G is equal to $\mathbb{C}\setminus\{0\}$ (resp. $\mathbb{R}$), f will be called a *multiplicative chained map* (resp. an *additive chained map*). Note that iterating (ii) gives for all letters $a_1, \dots, a_s$ in $\mathcal{A}$ and every word w in $\mathcal{A}^*$

$$f(a_1\dots a_s w) = (f(a_1a_2)f(a_2)^{-1})\dots(f(a_{s-1}a_s)f(a_s)^{-1})f(a_s w) \,. \tag{3}$$

An easy computation yields

$$f(\alpha\beta\gamma) = f(\alpha\beta)f(\beta)^{-1}f(\beta\gamma) \tag{4}$$

for all nonempty words α, β, γ in $\mathcal{A}^*$.

Finally, if G is abelian one has for every positive integer n

$$\widetilde{f}(n) = f(0)\Big\{\prod_{k\in\mathbb{N}} (f(e_{k+1}(n)))^{-1} f(e_{k+1}(n)e_k(n))\Big\}\,. \tag{5}$$

By (4) the map f which is chained over $\mathcal{A}$ can be lifted through the canonical map c (from $\mathcal{D}^* = (\mathcal{A}^{d+1})^*$ to $\mathcal{A}^*$) to a map defined on $\mathcal{D}^*$ and chained over $\mathcal{D}$.

A sequence φ with values in G is called *chained to base q* (or *chained over $\mathcal{A}$*) if the associated map $\dot{\varphi}$ (from $\mathcal{A}^*$ to G) is chained. Note that $\dot{\varphi}$ is then a regular chained map to base q^{d+1} for every positive integer d.

Example 1. Let φ be a complex sequence such that $\varphi(0) = 1$ and satisfying the functional equation

$$\forall\, k \in \mathbb{N}, \qquad \varphi(n) = \prod_{k\in\mathbb{N}} \varphi(e_k(n))\,.$$

Then φ is said to be *strongly q-multiplicative* (for q-multiplicativity, see [11]). This sequence is multiplicatively chained to base q. Actually, the map $\dot{\varphi}$ is a morphism from the monoid $\mathcal{A}^*$ to the multiplicative group $\mathbb{C}\setminus\{0\}$.

Example 2. Let v be a word in $\mathcal{A}^*$ of length $r+1$ ($r \geq 0$). We denote by 0^r the word consisting of r letters 0 (if $r = 0$ we define $0^0 = \Lambda$). Let $Z_v(w)$ be the number of occurrences of the word v in the word $0^r w$. This number depends only on the integer $n = \dot{w}$ if $v \neq 0^{r+1}$, and we will also denote it by $Z_v(n)$.

Proposition 2.1. *Let v be a word in $\mathcal{A}^*$ such that $|v| = r+1$ and $v \neq 0^{r+1}$. Then the sequence $(Z_v(n))_n$ is additively chained to base q^s for every integer $s \geq \max\{1, r\}$.*

Proof. If $r = 0$ one has, for all words w and w' in $\mathcal{A}^*$, $Z_v(ww') = Z_v(w) + Z_v(w')$, hence the result. Suppose $r \geq 1$. Let $\mathcal{S} = \mathcal{A}^s$ for $s > r$ and let c be the canonical morphism from $\mathcal{S}^*$ to $\mathcal{A}^*$. We have to prove that the map $Z_v \circ c$ from $\mathcal{S}^*$ to $\mathbb{R}$ is additively chained over $\mathcal{S}$.

Let α and β be letters in $\mathcal{S}$ and w be a word in $\mathcal{S}^*$. The integer $Z_v(c(\alpha)c(\beta)c(w))$ is equal to the number of occurrences of v in the words $0^s c(\alpha)c(\beta)$ and $0^s c(\beta)c(w)$ minus the number of occurrences of v which:

— either occur at the same places in the words $c(\alpha)c(\beta)$ and $0^s c(\beta)$,

— or occur in $0^s c(\beta)$ but do not occur in $c(\alpha)c(\beta)$.

This last number is precisely $Z_v(c(\beta))$, hence

$$Z_v \circ c(\alpha\beta w) = Z_v \circ c(\alpha\beta) - Z_v \circ c(\beta) + Z_v \circ c(\beta w)\,.$$

In particular, the sequence u discussed in the introduction (which corresponds to $Z_{11}(\cdot)$ with $q = 2$), is additively chained to base 2.

EXAMPLE 3. The following proposition generalizes the previous case:

PROPOSITION 2.2. *Let d be a positive integer and let φ be a periodic sequence with values in G such that the period of φ is q^{d+2}, and $\varphi(0) = 1_G$ (the unity of the group G). Let $x \in G$. Then the sequence*

$$f(n) = x\varphi([n/q^{t(n)}]) \dots \varphi([n/q])\varphi(n) \tag{6}$$

is chained to base q^{d+1}.

P r o o f. For every word w of length r in $\mathcal{A}^*$, say $w = w_{r-1} \dots w_0$, one has by definition (6)

$$\dot{f}(w) = x\dot{\varphi}(w_{r-1})\dot{\varphi}(w_{r-1}w_{r-2}) \dots \dot{\varphi}(w_{r-1} \dots w_0)\,.$$

Note that the value of $\dot{\varphi}(w)$ depends only on the word $w_{d+1} \dots w_0$ (w being replaced by $0^{d+2}w$ if $r \le d+1$). To prove that $\dot{f} \circ c$ is chained (where c is the canonical map from $\mathcal{D}^* = (\mathcal{A}^{d+1})^*$ to $\mathcal{A}^*$) it suffices to check that (ii) (in Definition 1) holds for a and b in $\mathcal{A}^{d+1}$, which is a straightforward computation. ∎

This proposition leads to a particular case of chained sequence:

DEFINITION 2.2. Let $d \in \mathbb{N}$. A sequence f with values in G is called a *d-sequence in base q* if there exists a sequence $\varphi : \mathbb{N} \to G$ such that for every integer n

(a) $\varphi(qn) = 1_G$,

(b) $\varphi(n + q^{d+2}) = \varphi(n)$ (i.e. φ is q^{d+2}-periodic),

and

$$f(n) = f(0)\varphi([n/q^{t(n)}]) \dots \varphi([n/q])\varphi(n)\,. \tag{7}$$

By Proposition 2.2 a d-sequence in base q is chained to base q^{d+1}. Choose x in G and v in $\mathcal{A}^{d+2}$, with $v \neq 0^{d+2}$. The sequence

$$f_v(n) = x^{Z_v(n)} \tag{8}$$

is chained to base q^{d+1} from Proposition 2.1 It is a d-sequence in base q if and only if the last letter of the word v is not 0 (i.e. if $v \notin \mathcal{A}^*0$). The map φ corresponding to f_v by (7) is the characteristic function χ_v of the arithmetic progression $\widetilde{v} + q^{d+2}\mathbb{N}$.

2.2. Chained sequences in an abelian group. Suppose that the group G is abelian. The set of chained sequences over $\mathcal{A}$ with values in G is a commutative group for the usual multiplication:

$$fg(n) = f(n)g(n) \quad \text{for every integer } n\,.$$

The subset of d-sequences in base q is a subgroup, generated by the d-sequences (8). More precisely, if f is a d-sequence in base q, one easily

obtains

$$f(n) = f(0) \prod_{v \in \mathcal{A}^{d+2}} (\varphi(v))^{Z_v(n)}, \quad \text{where } \varphi(v) = f(\dot{v}) f(0)^{-1}.$$

In the general case we have

THEOREM 2.1. *Let G be an abelian group and let $F : \mathcal{A}^* \to G$ be a regular chained map over $\mathcal{A}$. Then*

$$F(\cdot) = F(0) \prod_{b \in \mathcal{A}^2, b \neq 00} (F(b))^{Z_b(\cdot)}. \tag{9}$$

Proof. Let $h : \mathcal{A}^* \to G$ be defined by the right hand side of (9). Using Proposition 2.1 and the commutativity of the group G, one sees that h is chained. By construction $h(w) = F(w)$ for every word w of length at most two. An induction on the length of w and the use of the property (ii) of chained maps then give $h = F$.

2.3. Transition matrices

2.3.1. In what follows the usual hermitian products in the vector spaces $\mathbb{C}^s$ are denoted by $(\cdot|\cdot)$. The corresponding quadratic norms are denoted by $\| \cdot \|$. Every linear operator $A : \mathbb{C}^s \to \mathbb{C}^{s'}$ will be expressed in the canonical bases $\{I_1, \ldots, I_s\}$, $\{I'_1, \ldots, I'_{s'}\}$ unless explicitly stated otherwise. The quadratic norm of A is denoted by $\|A\|$ and defined by

$$\|A\| := \sup_{\|X\|=1} \|AX\|.$$

It is well known that $\|A\|$ is equal to the square root of the largest modulus of the eigenvalues of $\overline{A}A$, where $\overline{A}$ is the adjoint of A (recall that all eigenvalues of $\overline{A}A$ are real).

If A is an endomorphism of $\mathbb{C}^q$ given by a matrix all coefficients of which are of modulus 1, then

$$q^{1/2} \leq \|A\| \leq q.$$

One has $\|A\| = q^{1/2}$ if and only if $\overline{A}A = qI$ (where I is the identity endomorphism), and $\|A\| = q$ if and only if A has rank 1. Let us give a generalization of this result.

Let $E = (\mathrm{End}\, \mathbb{C}^s)^q$ be the space of column vectors X whose q components ${}^iX$ are endomorphisms of $\mathbb{C}^s$. We consider X as an operator from $\mathbb{C}^s$ to $(\mathbb{C}^s)^q$ given by

$$Xx = \begin{bmatrix} {}^1Xx \\ \vdots \\ {}^qXx \end{bmatrix}, \quad x \in \mathbb{C}^s,$$

and we identify $(\mathbb{C}^s)^q$ with $\mathbb{C}^{sq}$ by

$$\begin{bmatrix} {}^1\xi \\ \vdots \\ {}^q\xi \end{bmatrix} = \begin{bmatrix} \bar{I}_1\, {}^1\xi \\ \vdots \\ \bar{I}_s\, {}^1\xi \\ \vdots \\ \bar{I}_1\, {}^q\xi \\ \vdots \\ \bar{I}_s\, {}^q\xi \end{bmatrix}.$$

Hence the norm of $\xi = \begin{bmatrix} {}^1\xi \\ \vdots \\ {}^q\xi \end{bmatrix}$ is given by $\|\xi\|^2 = \|\,{}^1\xi\|^2 + \ldots + \|\,{}^q\xi\|^2$ and for $X \in E$,

$$\|X\| = \sup_{\|x\|=1} (\|\,{}^1Xx\|^2 + \ldots + \|\,{}^qXx\|^2)^{1/2}\,.$$

In terms of matrices, an endomorphism A in E is canonically represented by a matrix

$$\begin{bmatrix} {}^1A_1 & \ldots & {}^1A_q \\ \ldots\ldots\ldots\ldots\ldots & & \\ {}^qA_1 & \ldots & {}^qA_q \end{bmatrix}$$

whose elements (the $({}^iA_j)$) are endomorphisms of $\mathbb{C}^s$. Representing the ${}^iA_j$ in the canonical basis of $\mathbb{C}^s$, the endomorphism A becomes an endomorphism of $(\mathbb{C}^s)^q$ (identified with $\mathbb{C}^{sq}$) and its quadratic norm satisfies

$$\|A\| = \sup\{\|AX\|; X \in E \text{ and } \|X\| = 1\}\,. \tag{10}$$

Indeed, denote by ϱ the supremum on the right hand side of (10) and for ξ in $(\mathbb{C}^s)^q$ (with components ${}^1\xi, \ldots, {}^q\xi$) choose X with components ${}^iX$ in $\operatorname{End}\mathbb{C}^s$ such that

$${}^iXI_j = 0 \quad \text{if } j \neq 1\,,$$
$${}^iXI_1 = {}^i\xi\,.$$

An immediate computation shows that $\|\xi\| = \|X\|$ and $\|A\xi\| = \|AX\|$, hence $\|A\| \leq \varrho$. On the other hand, there exists a vector X_0 in E such that $\|X_0\| = 1$ and $\|AX_0\| = \varrho$. One has

$$\|AX_0\| = \sup_{\|x\|=1} \|AX_0x\|\,,$$

and there also exists a vector ${}^0x$ in $\mathbb{C}^s$ such that $\|\,{}^0x\| = 1$ and $\|AX_0\| = \|AX_0\,{}^0x\|$. Hence, for $\xi = X_0\,{}^0x$ one has $\varrho = \|A\xi\| \leq \|A\|$, which finally gives $\varrho = \|A\|$.

The matrix $\overline{A}$ adjoint to A, seen as an endomorphism of $(\mathbb{C}^s)^q$, is given by its components ${}^i(\overline{A})_j = (\overline{{}^jA_i})$.

LEMMA 2.1. *Let A be an endomorphism of $E = (\operatorname{End}\mathbb{C}^s)^q$ whose matrix elements ${}^iA_j$ are isometries of $\mathbb{C}^s$. Then*

$$q^{1/2} \le \|A\| \le q\,.$$

Moreover,

(a) $\|A\| = q^{1/2}$ *if and only if* $\overline{A}A = qI$;

(b) $\|A\| = q$ *if and only if there exist isometries* ${}^1S,\dots,{}^qS$, ${}^1U,\dots,{}^sU$ *of* $\mathbb{C}^s$ *and isometries* ${}^iB'_j$ $(1 \le i,j \le q)$ *such that for every i and j*

$$\overline{{}^iS}\;{}^iA_j\;{}^iU = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & {}^iB'_j & \\ 0 & & & \end{bmatrix}.$$

Proof. Using the hypothesis on A and the Schwarz inequality, one has for every ξ in $(\mathbb{C}^s)^q$

$$\begin{aligned}\|A\xi\|^2 &= \sum_{i=1}^{q} \|\,{}^iA_1\;{}^1\xi + \dots + {}^iA_q\;{}^q\xi\|^2 \\ &\le \sum_{i=1}^{q}(\|\,{}^1\xi\|^2 + \dots + \|\,{}^q\xi\|^2) \le \sum_{i=1}^{q}(q\|\xi\|^2) = q^2\|\xi\|^2\,,\end{aligned}$$

hence $\|A\| \le q$. On the other hand, choosing in E the vector Y_i with components $(\overline{{}^iA_k}) = ({}^kA_i)^{-1}$, for $k = 1,\dots,q$, one has $\|Y_i\| = q^{1/2}$ and

$$\|AY_i\| \ge \Big\|\sum_{i=1}^{q} {}^iA_j(\overline{{}^iA_j})\Big\| = q = q^{1/2}\|Y_i\|\,,$$

hence, using (10), $\|A\| \ge q^{1/2}$.

Suppose that $\|A\| = q^{1/2}$ and consider the vector Y_i defined above. We have $\|AY_i\| \le q$, hence $\|AY_i\| = q$. But for every x in $\mathbb{C}^s$ one has

$$\|AY_ix\|^2 = \sum_{k=1}^{q} \|({}^kA_1(\overline{{}^iA_1}) + \dots + {}^kA_q(\overline{{}^iA_q}))x\|^2 \le q^2\|x\|^2\,,$$

where the term corresponding to $k = i$ is $q^2\|x\|^2$, hence all other terms are 0, which gives

$${}^kA_1\,\overline{{}^iA_1} + \dots + {}^kA_q\,\overline{{}^iA_q} = 0 \quad \text{if } k \ne i\,.$$

Thus $A\overline{A} = qI = \overline{A}A$. The other implication in (a) is obvious.

Now suppose that $\|A\| = q$ and let $\xi \in (\mathbb{C}^s)^q$ be such that $\|\xi\| = 1$ and $\|A\xi\| = q$. Then

$$q^2 = \sum_{i=1}^{q} \| {}^iA_1 \, {}^1\xi + \ldots + {}^iA_q \, {}^q\xi\|^2 \,,$$

but

$$\| {}^iA_1 \, {}^1\xi + \ldots + {}^iA_q \, {}^q\xi\|^2 \leq q(\| {}^1\xi\|^2 + \ldots + \| {}^q\xi\|^2) = q \,,$$

hence necessarily

$$q^{1/2} = \| {}^iA_1 \, {}^1\xi + \ldots + {}^iA_q \, {}^q\xi\|^2 \leq \| {}^1\xi\| + \ldots + \| {}^q\xi\| \,.$$

But for ${}^ix \geq 0$ and $({}^1x)^2 + \ldots + ({}^qx)^2 = 1$, the maximum of the sum $({}^1x)^2 + \ldots + ({}^qx)^2$ is obtained when each ${}^ix$ is equal to $q^{-1/2}$, hence for every i

$$\| {}^iA_1 \, {}^1\xi + \ldots + {}^iA_q \, {}^q\xi\| = q^{1/2}$$

and

$$\| {}^iA_1 \, {}^1\xi\| = \ldots = \| {}^iA_q \, {}^q\xi\| = q^{-1/2} \,.$$

The extremal points of the ball $\|x\| \leq 1$ in $\mathbb{C}^s$ are the points of the sphere $\|x\| = 1$, hence there exist ${}^1\eta, \ldots, {}^q\eta$ in $\mathbb{C}^s$ such that

$${}^i\eta = {}^iA_j \, {}^j\xi \quad \text{for } j = 1, \ldots, q \,.$$

Let ${}^jU$ and ${}^iS$ be two isometries such that ${}^j\xi = {}^jUI_1$ and ${}^i\eta = {}^iSI_1$. Then

$$\overline{{}^iS} \, {}^iA_j \, {}^jUI_1 = I_1 \,.$$

The scalar product is preserved, hence $\overline{{}^iS} \, {}^iA_j \, {}^jU$ is represented in the canonical basis by an orthogonal matrix of the kind

$${}^iB_j = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & {}^iB'_j & \\ 0 & & & \end{bmatrix} ,$$

where ${}^iB'_j$ are isometries of $\mathbb{C}^{s-1}$.

Let B be the endomorphism of E defined by the ${}^iB'_j$ and let S and U be defined by

$$S = \begin{bmatrix} {}^1S & & 0 \\ & \ddots & \\ 0 & & {}^qS \end{bmatrix} , \quad U = \begin{bmatrix} {}^1U & & 0 \\ & \ddots & \\ 0 & & {}^qU \end{bmatrix} .$$

S and U are isometries of E and one has

$$\overline{S}AU = B \,.$$

Finally, if the components ${}^iB'_j$ of an endomorphism B of E have the previous form, a straightforward computation gives $\|B\| = q$, which proves the implication $\Leftarrow$ of (b) since $\|\overline{S}AU\| = \|A\|$. ∎

2.3.2. In this part G is a compact metrizable group. We denote by $\mathcal{R}(G)$, or simply $\mathcal{R}$, a complete system of non-trivial irreducible representations π of G. The dimension of π is denoted s_π, its Hilbert space is denoted H_π and the group of isometries of H_π is called $\mathbf{U}_\pi$. Since G is compact and metrizable, the set $\mathcal{R}$ is at most countable and the numbers s_π are finite, thus we will identify H_π and $\mathbb{C}^{s_\pi}$.

Let $F : \mathcal{A}^* \to G$ be a chained map over $\mathcal{A}$ (not necessarily regular), and let T be the $q \times q$ matrix with entries (row i, column j)

$$ {}^iT_j := F(ij)F(j)^{-1} .$$

Definition 2.3. The matrix T (with entries in G) is called the (*forward*) *transition matrix* of F.

Let $\pi \in \mathcal{R}$. Then $\pi \circ F : \mathcal{A}^* \to \mathbf{U}_\pi$ is also a chained map over $\mathcal{A}$, its transition matrix is πT, the entries of πT being the isometries ${}^i(\pi T)_j = \pi({}^iT_j)$. In a general way, to each square matrix T with entries ${}^iT_j$ in G, with indices in the set $\mathcal{A}$ (instead of $\{1, \dots, q\}$ as previously), and to each representation π of G we associate the endomorphism πT of $(\operatorname{End} H_\pi)^q$ defined by its components ${}^i(\pi T)_j = \pi({}^iT_j)$. Lemma 2.1 justifies the following definition:

Definition 2.4. The matrix T with entries in G and indices in $\mathcal{A}$ is a *contracting matrix* (resp. a *Hadamard matrix*) if for every π in $\mathcal{R}$ one has $\|\pi T\| < q$ (resp. $\|\pi T\| = q^{1/2}$).

If T is a Hadamard matrix, the map F is called a *Rudin–Shapiro map*; a sequence φ is called a *generalized Rudin–Shapiro sequence* if the associated map $\dot{\varphi}$ is a Rudin–Shapiro map.

In what follows, we denote by T^* the "normalized form" of the matrix T defined by

$$ {}^i(T^*)_j = {}^0T_0({}^iT_0)^{-1}({}^iT_j)({}^0T_j)^{-1} .$$

Notice that all the entries in the first row and in the first column of T^* are equal to 1_G, the unit element of G. Moreover, for every representation π of G one has

$$ \|\pi T^*\| = \|\pi T\| .$$

Theorem 2.2. *Let T be a matrix with entries in G and indices in $\mathcal{A}$. One has*

(a) *T is a contracting matrix if and only if the entries of T^* span a subgroup of G everywhere dense in G.*

(b) *If G is a commutative group and if T is a Hadamard matrix, then G is finite.*

P r o o f. (a) Suppose that T is not a contracting matrix and let $\pi \in \mathcal{R}$ such that $\|\pi T\| = q$. From the proof of Lemma 2.1, with $A = \pi T^*$ and $s = s_\pi$, there exist vectors ${}^0\xi, \ldots, {}^{q-1}\xi$, ${}^0\eta, \ldots, {}^{q-1}\eta$ in $H_\pi = \mathbb{C}^s$ such that ${}^i\eta = \pi({}^iT_j^*)\,{}^j\xi$. But ${}^iT_0^* = {}^0T_j^* = 1_G$, hence ${}^i\eta = {}^0\xi$ and ${}^0\eta = {}^i\xi$ for all i and j in $\mathcal{A}$. Thus we can choose all isometries ${}^iS$, ${}^jU$ equal to M, say, so that if π' is the representation defined by $\pi'(g) = M^{-1}\pi(g)M$ (π' is equivalent to π), then the first vector I_1 of the canonical basis of $\mathbb{C}^s$ is a fixed point of the isometries $\pi'({}^iT_j^*)$. As π' is a non-trivial representation, the closed subgroup of G spanned by the entries of T^* is different from G.

Conversely, suppose that T is contracting and let f be the sequence with values in G defined by

$$f(e_t q^t + \ldots + e_0 q^0) = ({}^{e_t}T^*_{e_{t-1}}) \ldots ({}^{e_1}T^*_{e_0})$$

and

$$f(0) = \ldots = f(q-1) = 1_G\,.$$

The sequence f is chained to base q, and (see Theorem 2.3 below) for every representation π of G

$$\sum_{n<N} \pi(f(n)) = O(N^{(\log \|\pi T\|)/(\log q)})\,.$$

The Weyl criterion (see [13], Chapter 4, Theorem 1.3) implies that f is uniformly distributed in G; this gives the density property.

(b) Suppose that G is an abelian group and that, for each character π of G different from the trivial character π_0, one has $\|\pi T\| = q^{1/2}$. Suppose also that $\pi^n \neq \pi_0$ for every non-zero integer n. The sequence with values in $(\mathbf{U}_\pi)^q$,

$$n \to (\pi^n({}^iT_0^*), \ldots, \pi^n({}^iT_{q-1}^*))\,,$$

admits $(1_\pi, \ldots, 1_\pi)$ as a limit point, but the equality $\|\pi T\| = q^{1/2}$ implies (Lemma 2.1) that

$$\pi^n({}^iT_0^*) + \ldots + \pi^n({}^iT_{q-1}^*) = 0\,,$$

which gives a contradiction for $i \neq 0$. Thus there exists a non-zero integer n such that

$$\pi^n = \pi_0\,.$$

Hence every characted is of finite order; but G is abelian, so every element of G is of finite order. Hence the entries of T^* span a finite subgroup G_0 of G, which is everywhere dense in G (from (a)), therefore $G_0 = G$.

2.4. Summation formulas. Let $\mathbf{U}_s$, be the group of unitary endomorphisms of $\mathbb{C}^s$. For each map $f : \mathcal{A}^* \to \mathbf{U}_s$, define the vector $\mu^{(m)}(f)$ in

$(\mathrm{End}\,\mathbb{C}^s)^q$ by

$$\mu^{(m)}(f) = \begin{bmatrix} {}^0\mu^{(m)}(f) \\ \vdots \\ {}^{q-1}\mu^{(m)}(f) \end{bmatrix} \quad \text{and} \quad {}^j\mu^{(m)}(f) := \sum_{k\in\mathcal{A}^m} f(jk)\,.$$

On the other hand, define the endomorphism τ on the group of sequences $\varphi : \mathbb{N} \to \mathbf{U}_s$ by

$$\tau\varphi(n) = \varphi(qn)\,,$$

and let $[\varphi]_s$ be the matrix

$$[\varphi]_s := \begin{bmatrix} \varphi(0)1_s & & 0 \\ & \ddots & \\ 0 & & \varphi(q-1)1_s \end{bmatrix}$$

where 1_s is the unit element in $\mathbf{U}_s$.

From now on, let $F : \mathcal{A}^* \to \mathbf{U}_s$ be a chained map over $\mathcal{A}$ (not necessarily regular), and let T be the forward transition matrix of F. Let $\varphi : \mathbb{N} \to \mathbf{U}_s$ be a q-multiplicative sequence. Then

$${}^j\mu^{(m+1)}(\varphi\circ F) = \sum_{i\in\mathcal{A}}\sum_{k\in\mathcal{A}^m} \dot\varphi(jik)F(jik) = \tau^{m+1}\varphi(j)\sum_{i\in\mathcal{A}} {}^jT_i\ {}^i\mu^{(m)}(\varphi\circ F),$$

which yields the matrix relation

$$\mu^{(m+1)}(\varphi\circ F) = [\tau^{m+1}\varphi]_s T\mu^{(m)}(\varphi\circ F)\,,$$

and for every non-zero integer m

$$\mu^{(m)}(\varphi\circ F) = ([\tau^m\varphi]_s T)\dots([\tau\varphi]_s T)\mu^{(0)}(\varphi\circ F)\,,$$

where $\mu^{(0)}(\varphi\circ F)$ is defined in $(\mathbf{U}_s)^q$ by its components $\varphi(j)F(j)$.

Taking the quadratic norm we have

$$\|\mu^{(m)}(\varphi\circ F)\| \le q^{1/2}\|T\|^m \tag{11}$$

(if T is a Hadamard matrix, one has $\|\mu^{(m)}(\varphi\circ F)\| = q^{m/2}\|\mu^{(0)}(\varphi\circ F)\|$).

Let N be a non-zero integer and let its base q expansion be

$$N = \sum_{k=0}^{t} e_k(N)q^k \quad \text{with } e_t(N)\neq 0\,.$$

Define s_k in $\mathbb{N}$ and σ_k in $\mathcal{A}^{t-k+1}$ by

$$\begin{aligned} s_k &:= e_t(N)q^t + \dots + e_k(N)q^k, \quad \text{for } 0\le k\le t\,,\\ s_{t+1} &:= 0\,,\\ \sigma_k &:= e_t(N)\dots e_k(N), \quad \text{for } 0\le k\le t\,,\\ \sigma_{t+1} &:= \Lambda\,. \end{aligned}$$

Assuming now that F is regular, we obtain

$$\begin{aligned}\sum_{n<N}\varphi(n)F(\widetilde{n}) &= \sum_{n<e_t(N)q^t}\varphi(n)F(\widetilde{n}) + \sum_{1\le k\le t}\ \sum_{s_k\le n<s_{k-1}}\varphi(n)F(\widetilde{n})\\ &= \sum_{j<e_t(N)} {}^j\mu^{(t)}(\varphi\circ F)\\ &\quad + \sum_{1\le k\le t}\ \sum_{j<e_{k-1}(N)}\ \sum_{i\in\mathcal{A}^{k-1}}\dot\varphi(\sigma_k ji)F(\sigma_k ji)\,.\end{aligned}$$

On the other hand, one has (from (4))

$$F(\sigma_k ji) = F(\sigma_k j)F(j)^{-1}F(ji)\,,$$

and since φ is q-multiplicative,

$$\dot\varphi(\sigma_k ji) = \varphi(s_k)\dot\varphi(ji)\,.$$

Hence

$$\begin{aligned}\sum_{n<N}\varphi(n)F(\widetilde{n}) &= \sum_{j<e_t(N)} {}^j\mu^{(t)}(\varphi\circ F)\\ &\quad + \sum_{1\le k\le t}\ \sum_{j<e_{k-1}(N)}\varphi(s_k)F(\sigma_k j)F(j)^{-1}\,{}^j\mu^{(k-1)}(\varphi\circ F)\\ &= \sum_{0\le k\le t}\ \sum_{j<e_k(N)}\left((\varphi(s_{k+1})F(\sigma_{k+1}j)F(j)^{-1}\right){}^j\mu^{(k)}(\varphi\circ F))\,.\end{aligned}$$

From (11) we then deduce the bound

$$\Big\|\sum_{n<N}\varphi(n)F(\widetilde{n})\Big\| \le q^{1/2}\sum_{r=0}^{\infty}e_r(N)\|T\|^r\,. \tag{12}$$

Note that we have an analogous inequality when F is not regular. Indeed, let $\Sigma(t)$ be defined by

$$\Sigma(t) := \sum_{n<q^t}\varphi(n)F(\widetilde{n})\,.$$

Then the sum $\sum_{n<e_t(N)q^t}\varphi(n)F(\widetilde{n})$ cannot be replaced as above by the sum $\sum_{j<e_t(N)}{}^i\mu^{(t)}(\varphi\circ F)$ but is replaced by

$$\sum_{j<e_t(N)}{}^j\mu^{(t)}(\varphi\circ F) + \Sigma(t-1)\,.$$

One has

$$\Sigma(t) = \Sigma(t-1) + \sum_{j<q}{}^j\mu^{(t-1)}(\varphi\circ F)\,,$$

and (11) gives

$$\|\Sigma(t)\| \le \|\Sigma(t-1)\| + (q-1)q^{1/2}\|T\|^{t-1}\,.$$

Since $\|\Sigma(1)\| \le q \le 2^{1/2}(q-1)q^{1/2}$, we get

$$\|\Sigma(t)\| \le 2^{1/2}(q-1)q^{1/2}\|T\|^t(\|T\|-1)^{-1}\,;$$

but $\|T\| \ge q^{1/2}$, hence

$$\|\Sigma(t)\| \le C_q q^{1/2}\|T\|^t\,,$$

where $C_q = 2^{1/2}(q^{1/2}+1)$. Going back to the previous computation we obtain for the non-regular case

$$\Big\|\sum_{n<N}\varphi(n)F(\widetilde{n})\Big\| \le C_q q^{1/2}\sum_{r=0}^{\infty} e_r(N)\|T\|^r\,. \tag{13}$$

THEOREM 2.3. *Let $\mathbf{U}_s$ be the group of unitary endomorphisms of $\mathbb{C}^s$. Let $F:\ \mathcal{A}^* \to \mathbf{U}_s$ be a regular chained map over $\mathcal{A}$ and let T be its forward transition matrix. Define*

$$\alpha(F) := \alpha(T) := (\log\|T\|)/(\log q)\,,$$
$$c(F) := (q-1)/(q^{\alpha(F)}-1)\,.$$

Then, for every q-multiplicative sequence $\varphi:\ \mathbb{N} \to \mathbf{U}_s$ with modulus 1,

$$\Big\|\sum_{n<N}\varphi(n)F(\widetilde{n})\Big\| \le c(F)q^{1/2}N^{\alpha(F)}\,. \tag{14}$$

P r o o f. Using the bound (12) it is sufficient to prove the following easy lemma:

LEMMA 2.2. *Let α and q be two real numbers with $\alpha \in]0,1]$ and $q>1$. Let $(e_r)_r$ be a sequence of real numbers in $[0,B]$ $(B>0)$. Then*

$$\sum_{r=0}^{k} e_r q^{r\alpha} \le C\Big(\sum_{r=0}^{k} e_r q^r\Big)^{\alpha} \quad \text{for every } k \ge 0\,,$$

where

$$C = C(\alpha,q,B) = \frac{(q-1)^\alpha}{q^\alpha - 1}B^{1-\alpha}\,.$$

Indeed, we may suppose $\alpha \ne 1$ and define two functions H_1 and H_2 by

$$H_1(x,a) = (x+a)^\alpha - x^\alpha\,, \qquad H_2(x) = \frac{(1+x)^\alpha - 1}{x}$$

(a is a fixed positive real number). Both H_1 and H_2 are strictly decreasing on $[0,+\infty[$.

One has

$$\Big(\sum_{r=0}^{k} e_r q^r\Big)^\alpha - \Big(\sum_{r=0}^{k-1} e_r q^r\Big)^\alpha = H_1\Big(\sum_{r=0}^{k-1} e_r q^r, e_k q^k\Big) \ge H_1\left(\frac{Bq^k}{q-1}, e_k q^k\right)$$
$$= \left(\frac{B}{q-1}\right)^\alpha q^{k\alpha} \frac{q-1}{B} e_k H_2\left(\frac{q-1}{B} e_k\right)$$
$$\ge \left(\frac{B}{q-1}\right)^\alpha q^{k\alpha} \frac{q-1}{B} e_k H_2(q-1)\,,$$

hence

$$\Big(\sum_{r=0}^{k} e_r q^r\Big)^\alpha - \Big(\sum_{r=0}^{k-1} e_r q^r\Big)^\alpha \ge \frac{1}{C} e_k q^{k\alpha}\,,$$

where C is the constant defined in the lemma (actually the proof holds for $e_k \neq 0$ but the inequality is still valid in the case $e_k = 0$).

Adding these inequalities for $k, k-1, k-2, \dots, 1$, we get

$$\Big(\sum_{r=0}^{k} e_r q^r\Big)^\alpha \ge e_0^\alpha + \frac{1}{C} \sum_{r=1}^{k} e_r q^{r\alpha}\,.$$

This implies the lemma by noticing that

$$e_0^{1-\alpha} \le B^{1-\alpha} \le B^{1-\alpha} \frac{(q-1)^\alpha}{q^\alpha - 1} = C$$

(indeed $(q-1)^\alpha \ge q^\alpha - 1$ by the mean value theorem), which gives $e_0^\alpha \ge (1/C) e_0$.

R e m a r k. The constant in this lemma is optimal (take $e_r = B$ for every r and $k \to +\infty$).

Now, suppose that φ is q^ν-multiplicative ($\nu > 1$), chained, and has modulus 1. As already noticed, the chained map $F : \mathcal{A}^* \to \mathbf{U}_s$ is also chained over $\mathcal{A}^\nu$. Denote by $T(\nu)$ the corresponding forward transition matrix.

Lemma 2.3. $\|T(\nu)\| = q^{\nu-1}\|T\|$.

Indeed, if i and j are in $\mathcal{A}^\nu$, then by definition

$${}^i(T(\nu))_j = F(ij)F(j)^{-1}\,.$$

Let $i = i_1 \dots i_\nu$, $j = j_1 \dots j_\nu$, where i_k and j_k are in $\mathcal{A}$. Using (4) we obtain easily

$${}^i(T(\nu))_j = {}^{i_1}T_{i_2} \dots {}^{i_{\nu-1}}T_{i_\nu}\, {}^{i_\nu}T_{j_1}\,.$$

Let ${}^i(T(\nu))_j = \varrho(i)\, {}^{i_\nu}T_{j_1}$, where $\varrho(i) \in \mathbf{U}_s$. Multiplying on the left the entries of every row i of $T(\nu)$ by $\overline{\varrho(i)}$, we obtain a matrix $T'(\nu)$ such

that $\|T'(\nu)\| = \|T(\nu)\|$. Permute now the columns of $T'(\nu)$ in such a way that the indices $j \in \mathcal{A}^\nu$ are in the reverse lexicographical order "$<$", i.e.

$$j_1 \dots j_\nu \text{ “}<\text{”} j'_1 \dots j'_\nu \;\Leftrightarrow\; j_\nu \dots j_1 < j'_\nu \dots j'_1 .$$

The new matrix $T''(\nu)$ has the same quadratic norm as $T(\nu)$ and has the form

$$T''(\nu) = \begin{bmatrix} T & \dots & T \\ \dots\dots\dots & & \\ T & \dots & T \end{bmatrix} .$$

Write a vector X in $(\mathbb{C}^s)^{q^\nu}$ as a column vector with components ${}^iX$ in $(\mathbb{C}^s)^q$ and notice that

$$\|X\|^2 = \|\,{}^1X\|^2 + \dots + \|\,{}^{q^{\nu-1}}X\|^2 .$$

With these notations,

$$\begin{aligned} \|T(\nu)\|^2 &= \sup_{\|X\|=1} q^{\nu-1} \Big\| \sum_{1\le k\le q^{\nu-1}} T^k X \Big\|^2 \\ &\le q^{\nu-1}\|T\|^2 \sup_{\|X\|=1} \Big(\sum_{1\le k\le q^{\nu-1}} \|\,{}^kX\| \Big)^2 . \end{aligned}$$

This last supremum is classically attained when each $\|\,{}^kX\|$ is equal to $(q^{\nu-1})^{-1/2}$, which implies

$$\|T(\nu)\| \le q^{\nu-1}\|T\| .$$

Choosing ${}^1X$ such that $\|T\,{}^1X\| = \|T\| \cdot \|\,{}^1X\|$ and all the ${}^kX$ equal to ${}^1X$, we deduce that the above inequality is actually an equality.

From Theorem 2.3 we can deduce the following corollary that we write down for sequences:

Corollary 2.1. *Let $f : \mathbb{N} \to \mathbf{U}_s$ be a sequence chained in base q, with transition matrix (that of $\dot f$) equal to T. Then for every non-zero integer ν and for every q^ν-multiplicative sequence $\varphi : \mathbb{N} \to \mathbf{U}_s$ of modulus* 1,

$$\Big\| \sum_{n<N} \varphi(n) f(n) \Big\| \le c_\nu(f) q^{\nu/2} N^{\alpha_\nu(f)} ,$$

where

$$\alpha_\nu(f) = 1 - \nu^{-1}(1 - \alpha(T))$$

and

$$c_\nu(f) = (q^\nu - 1)/(q^{\nu-1+\alpha(T)} - 1) .$$

2.5. Distribution of chained sequences

THEOREM 2.4. *Let G be a compact metrizable group and let $F : \mathcal{A}^* \to G$ be a regular chained map over $\mathcal{A}$ with forward transition matrix T. Suppose that T is contracting. Then the chained sequence*

$$\widetilde{F}(n) := F(\widetilde{n})$$

is well uniformly distributed in G, and has an empty spectrum.

P r o o f. By Theorem 2.3, for every representation $\Pi \in \mathcal{R}$ and every real number θ, one has in End $\mathbb{C}^{s_\Pi}$

$$\lim_{N\to\infty} N^{-1} \sum_{n<N} e^{2i\pi n\theta} \Pi(F(\widetilde{n})) = 0\,.$$

The Peter–Weyl theorem then implies for every $f \in \mathcal{C}(G)$

$$\lim_{N\to\infty} N^{-1} \sum_{n<N} e^{2i\pi n\theta} f(\widetilde{F}(n)) = \int_G f(G) h_G(dg)\,,$$

where h_G is the Haar measure of the group G. Since the sequence $n \mapsto e^{2i\pi n\theta}\widetilde{F}(n)$ is also a chained sequence over $\mathcal{A}$, it only remains to prove that for every $\Pi \in \mathcal{R}$ the sequence of means

$$N^{-1} \sum_{n<N} \Pi(\widetilde{F}(n+k))$$

converges to 0 in End $\mathbb{C}^{s_\Pi}$ uniformly in k (see [13], Chapter 4, Corollary 1.3). We are actually going to prove more:

LEMMA 2.4. *For every q-multiplicative $\varphi : \mathbb{N} \to \mathbf{U}_s$, and for all integers $k \geq 0$ and $N > 0$, one has (using notations of Theorem 2.3)*

$$\Big\| \sum_{n<N} \varphi(n+k) \Pi \widetilde{F}(n+k) \Big\| \leq 1 + c(\Pi F) 2^{3/2-\alpha(\Pi T)} q^{1/2} (1+q^{1/2}) N^{\alpha(\Pi F)}\,.$$

Indeed, for given integers $N > 0$ and $k \geq 0$, define the integer S by $e_S(k) < e_S(k+N)$ and $e_j(k) = e_j(k+N)$ for every $j \geq S+1$. Set

$$u = \sum_{j\leq S} e_j(k) q^j\,, \qquad v = \sum_{j\leq S} e_j(k+N) q^j\,,$$
$$w = (1+e_S(k)) q^S\,, \qquad A = \sum_{j>S} e_j(k) q^j\,.$$

Hence $k = A + u$, $k + N = A + v$.

Let $f = \varphi \circ \Pi\widetilde{F}$. Then

$$\sum_{n<N} f(k+n) = \sum_{u\leq m<v} f(A+m)$$

and, for $u \le m < v$,

$$f(A+m) = \varphi(A)\Pi\widetilde{F}(Aq^{-S-1})(\Pi\widetilde{F}(e_{S+1}(k)))^{-1}\dot{\varphi}(m)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1}+m)\,.$$

Hence

$$\Big\|\sum_{n<N} f(k+n)\Big\| = \Big\|\sum_{u\le m<v} \varphi(m)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1}+m)\Big\|\,.$$

On the other hand,

$$\sum_{w\le m<v} \varphi(m)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1}+m) = B + \varphi(e_S(k+N)q^S)\cdot C$$

where

$$B = \sum_{1+e_S(k)\le a<e_S(k+N)} \varphi(aq^S) \sum_{m<q^S} \varphi(m)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1}+aq^S+m)$$

and

$$C = \sum_{0\le n<v-e_S(k+N)q^S} \varphi(n)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1}+e_S(k+N)q^S+n)\,.$$

Then

$$B = \sum_{1+e_S(k)\le a<e_S(k+N)} \varphi(aq^S)({}^{e_{S+1}(k)}(\Pi T)_a) \sum_{m<q^S} \varphi(m)\Pi\widetilde{F}(aq^S+m)\,,$$

and

$$C = ({}^{e_{S+1}(k)}(\Pi T)_{e_{S+1}(k+N)}) \sum_{0\le n<v-e_S(k+N)q^S} \varphi(n)\Pi\widetilde{F}(e_S(k+N)q^S+n)\,.$$

Notice that for every chained map F and for every word a in $\mathcal{A}^*$, the map $z \mapsto F(az)$ is also chained over $\mathcal{A}$ and the entries of its transition matrix $T(a)$ are

$${}^i(T(a))_j = [F(ai)F(i)^{-1}]^i T_j [F(aj)F(j)^{-1}]^{-1}\,,$$

hence

$$T(a) = U_a T U_a^{-1}\,,$$

where U_a is the isometry defined by

$$U_a = \begin{bmatrix} {}^aT_0 & & 0 \\ & \ddots & \\ 0 & & {}^aT_{q-1} \end{bmatrix}, \quad \text{where } {}^aT_i = F(ai)F(i)^{-1}\,.$$

Hence $\|T(a)\| = \|T\|$, which implies, using (13),

$$\Big\|\sum_{w\le m<v} \varphi(m)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1}+m)\Big\|$$

$$\le C_q q^{1/2}\Big(\Big(\sum_{j<S} e_j(k+N)\|T\|^j\Big) + (e_S(k+N) - e_S(k) - 1)\|T\|^S\Big)\,.$$

Notice that

$$v - w = \sum_{j<S} e_j(k+N)q^j + (e_S(k+N) - e_S(k) - 1)q^S\,.$$

Since $e_S(k+N) - e_S(k) - 1 \ge 0$, the above equality is exactly the base q expansion of $v - w$. Hence, using Lemma 2.2 with $\alpha = \alpha(T)$, we obtain

$$\Big\|\sum_{w\le m<v} \varphi(m)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1} + m)\Big\| \le C_q q^{1/2}(v-w)^\alpha(q-1)/(q^\alpha - 1)\,.$$

Define, for $0 \le j \le S$,

$$r_j = \sum_{j<i\le S} e_i(k)q^i \qquad (r_S = 0)\,,$$

and let $\{j_1, \dots, j_\sigma\}$ be the set of integers j with $0 \le j \le S$ and $e_j(k) < q-1$ in increasing order. Let $u_0 = u$, and for $1 \le \nu \le \sigma$

$$\begin{aligned} u_\nu &= r_{j_\nu} + (e_{j_\nu}(k) + 1)q^{j_\nu} \\ &= r_{j_{\nu+1}} + (q-1)q^{j_{\nu+1}-1} + \ldots + (q-1)q^{j_\nu+1} + (e_{j_\nu}(k)+1)q^{j_\nu}\,. \end{aligned}$$

One has $u_1 = u_0 + 1$, $u_\sigma = w$, and for $1 \le \nu < \sigma$

$$\begin{aligned} &\sum_{u_\nu\le m<u_{\nu+1}} \varphi(m)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1} + m) \\ &= \sum_{a<q-e_{j_\nu}(k)-1} \varphi(u_\nu) \sum_{m<q^{j_\nu}} \varphi(aq^{j_\nu} + m)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1} + u_\nu + aq^{j_\nu} + m) \\ &= C' \sum_{a<q-e_{j_\nu}(k)-1} \varphi(aq^{j_\nu}) \sum_{m<q^{j_\nu}} \varphi(m)\Pi\widetilde{F}(u_\nu + aq^{j_\nu} + m)\,, \end{aligned}$$

where

$$C' = \varphi(u_\nu)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1} + u_\nu)(\Pi\widetilde{F}(u_\nu))^{-1}\,.$$

Hence, from (11),

$$\Big\|\sum_{u_\nu\le m<u_{\nu+1}} \varphi(m)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1} + m)\Big\| \le q^{1/2}(q - e_{j_\nu}(k) - 1)\|T\|^{j_\nu}\,.$$

Then, from (11) and Lemma 2.2,

$$\begin{aligned} \Big\|\sum_{u\le m<w} \varphi(m)\Pi\widetilde{F}(e_{S+1}(k)q^{S+1} + m)\Big\| &\le 1 + q^{1/2}\sum_{j<S}(q - e_j(k) - 1)\|T\|^j \\ &\le 1 + q^{1/2}(w-u-1)^\alpha(q-1)/(q^\alpha - 1). \end{aligned}$$

Finally,

$$\Big\| \sum_{n<N} f(k+n) \Big\| \le 1 + C_q q^{1/2} [(v-w)^\alpha + (w-u)^\alpha](q-1)/(q^\alpha - 1)$$
$$\le 1 + C_q q^{1/2} 2^{1-\alpha} N^\alpha (q-1)/(q^\alpha - 1)\,.$$

3. Generalized Rudin–Shapiro sequences

3.1. In what follows $q = 2$, $\mathcal{A} = \{0,1\}$, d is a positive integer and $D = 2^{d+1}$.

Definition 3.1. The sequence $u : \mathbb{N} \to \mathbb{N}$ is called a *Rudin–Shapiro sequence of order d on $ab \in \mathcal{A}^2$, $ab \neq 00$*, if

$$u(n) = \sum_{|v|=d} Z_{avb}(n)\,.$$

Theorem 3.1. *Let u be a Rudin–Shapiro sequence of order d on ab, let v be a chained additive sequence in base 2^r, $r \ge d$, and let $\varphi : \mathbb{N} \to \mathbb{C}$ be a 2^k-multiplicative sequence of modulus 1, with $k \ge d+1$. Then, for every $N \ge 1$,*

$$\Big| \sum_{n<N} e^{2i\pi(\alpha u(n)+v(n))} \varphi(n) \Big| \le (1 + D^{1/2}) D^{1/2} N^{\delta(\alpha)}\,,$$

where $\delta(\alpha) = \log(2 + 2|\cos \pi\alpha|)/2\log 2$.

Remarks. 1. The sequence $n \to e^{2i\pi\alpha u(n)}$ is 2-automatic for α rational (see [9] or [8]).

2. For an application of the properties of the sequence $(u(n))_n$ in case $a = b = 1$, see [12].

Proof of the theorem. As the sequence $n \xrightarrow{w} e^{2i\pi(\alpha u(n)+v(n))}$ is multiplicatively chained in base D, it suffices to prove, in view of Theorem 2.3, the following lemma, where T is the transition matrix of w:

Lemma 3.1.

$$\|T\| = \left\| \begin{bmatrix} 1 & 1 \\ 1 & \eta \end{bmatrix} \right\|^{d+1}, \quad \text{where } \eta = e^{2i\pi\alpha}\,,$$
$$\left\| \begin{bmatrix} 1 & 1 \\ 1 & \eta \end{bmatrix} \right\| = (2 + 2|\cos \pi\alpha|)^{1/2}\,.$$

In the proof of Lemma 3.1, the following lemma will be useful (its proof is left to the reader):

Lemma 3.2. *Let E be a Hermitian space, let A and B be two endomorphisms of E, let U be an isometry of E, and η a complex number of*

modulus 1. *Let* C *be the endomorphism of* $E \times E$ *determined by the matrix*

$$\begin{bmatrix} A & B \\ UA & \eta UB \end{bmatrix}.$$

Then $\|C\| \le \max(\|A\|, \|B\|) \cdot \left\| \begin{bmatrix} 1 & 1 \\ 1 & \eta \end{bmatrix} \right\|$, *with equality if* $\|A\| = \|B\|$.

P r o o f o f L e m m a 3.1. Let M and N be in $\mathcal{A}^r$, $r \le d$, and let $A_{M,N}$ be the square submatrix of T with elements $T_{Mj,Nk}$, where $j \in \mathcal{A}^{d+1-r}$ and $k \in \mathcal{A}^{d+1-r}$. Define $\varrho = T_{M0j',N0k'}$, where j' and k' are in $\mathcal{A}^{d-r}$ (if $d = r$ we take $j' = k' = \Lambda$).

Then the submatrix

$$\begin{bmatrix} T_{M0j',N0k'} & T_{M0j',N1k'} \\ T_{M1j',N0k'} & T_{M1j',N1k'} \end{bmatrix}$$

has the form

$$\begin{bmatrix} \varrho & \tau_{j'k'}\eta_1'\varrho \\ \tau_{j'}\eta_1\varrho & \tau_{j'}\tau_{j'k'}\eta_0\varrho \end{bmatrix},$$

where, using (3), one has (as usual $e(x)$ denotes $e^{2i\pi x}$)

$$\begin{aligned} \tau_{j'} &= e(\widetilde{v}(M1j'N) - \widetilde{v}(M0j'N)), \\ \tau_{j'k'} &= e(\widetilde{v}(j'N1k') - \widetilde{v}(j'N0k')) \end{aligned}$$

while

$$U_\eta =: \begin{bmatrix} 1 & \eta_1' \\ \eta_1 & \eta_0 \end{bmatrix}$$

is equal to

$$\begin{bmatrix} 1 & \eta \\ 1 & 1 \end{bmatrix} \quad \text{if } ab = 01,$$

$$\begin{bmatrix} 1 & 1 \\ \eta & 1 \end{bmatrix} \quad \text{if } ab = 10,$$

$$\begin{bmatrix} 1 & 1 \\ 1 & \eta \end{bmatrix} \quad \text{if } ab = 11.$$

Hence

$$A_{M,N} = \begin{bmatrix} A_{M0,N0} & A_{M0,N1} \\ \eta_1 U A_{M0,N0} & \eta_0\overline{\eta_1'} U A_{N0,N1} \end{bmatrix},$$

where U is the diagonal matrix with diagonal elements $r_{j'}$ ($j' \in \mathcal{A}^{d-r}$). From Lemma 3.2 one gets

$$\|T\| \le \max\{\|A_{0,0}\|, \|A_{0,1}\|\} \cdot \left\| \begin{bmatrix} 1 & 1 \\ 1 & \eta \end{bmatrix} \right\| \quad \left(\text{as } \|U_\eta\| = \left\| \begin{bmatrix} 1 & 1 \\ 1 & \eta \end{bmatrix} \right\|\right).$$

On the other hand,

$$\|A_{M,N}\| \le \max\{\|A_{M0,N0}\|, \|A_{M0,N1}\|\} \cdot \left\| \begin{bmatrix} 1 & 1 \\ 1 & \eta \end{bmatrix} \right\| ,$$

hence there exist M and N in $\mathcal{A}^{d+1}$ such that

$$\|T\| \le \|A_{M,N}\| \left\| \begin{bmatrix} 1 & 1 \\ 1 & \eta \end{bmatrix} \right\|^{d+1} .$$

But $A_{M,N} = T_{M,N}$ has modulus 1, which gives the bound of Lemma 3.1; equality actually follows from iteration of Lemma 3.2.

3.2. The backward transition matrix. The above results have been partially given in [1] and [16]. The proof in [1] was slightly different. Let us quickly describe it to give a bound for the simplified sum

$$\sum_{n \le m2^N - 1} \exp(2i\pi(\alpha z(n) + V_c(n)))$$

where $m \ge 1$ is a fixed integer, $(z(n))_n$ is the sequence $(u(n))_n$ in case $a = b = 1$, $c = (c_q)_q$ is a sequence of real numbers, and V_c is defined by $V_c(n) = \sum e_q(n) c_q$ if $n = \sum e_q(n) 2^q$ is the binary expansion of n. Define the vector $R(N, c)$ in $\mathbb{C}^2$ by its components $R_u(N, c)$, $1 \le u \le 2^{d+1}$, as follows:

(i) $R_1(N, c) = \sum_{n \le m2^N - 1} \exp(2i\pi(\alpha z(n) + V_c(n)))$;

(ii) if $u \ne 1$, let k be defined by $2^k + 1 \le u \le 2^{k+1}$ (hence $0 \le k \le d$); then

$$R_u(N, c) = \sum_{n \le m2^N - 1} \exp(2i\pi(\alpha z(2^{k+1} n + A(u-1)) + V_c(n))) ,$$

where $A(n)$ is the number obtained by reversing the binary digits of the integer n (if $n = \sum_{j=0}^{r} a_j 2^j$, $a_j = 0$ or 1, $a_r = 1$, then $A(n) = \sum_{j=0}^{r} a_j 2^{r-j} \in 2\mathbb{N} + 1$).

Finally, define the matrix $M(c)$ by $M(c) = (m_{u,v}(c))$, where

(iii) for $1 \le u \le 2^d$,

$$m_{u,v}(c) = \begin{cases} 1 & \text{if } v = 2u - 1, \\ e(c_0) & \text{if } v = 2u , \\ 0 & \text{otherwise;} \end{cases}$$

(iv) for $2^d + 1 \le u \le 2^{d+1}$,

$$m_{u,v}(c) = \begin{cases} 1 & \text{if } v = 2(u - 2^d) - 1, \\ e(c_0 + \alpha) & \text{if } v = 2(u - 2^d) , \\ 0 & \text{otherwise.} \end{cases}$$

M can be considered to some extent as the backward transition matrix associated to the sequence z. We then obtain

$$R(N,c) = M(c)R(N-1,Tc)\,,$$

where Tc is the shifted sequence $(c_{q+1})_q$. Hence

$$R(N,c) = M(c)M(Tc)\dots M(T^{N-1}c)R(0,T^Nc)\,.$$

Evaluating the norms of the matrices $M(T^kc)$ we obtain the same bound as above for the sum $\sum_{n<N}\exp(2i\pi(\alpha z(n)+V_c(n)))$. Moreover, we found an interesting property of the characteristic polynomials of the matrices $M(c)$ which are all multiples of the characteristic polynomial corresponding to the usual Rudin–Shapiro sequence ($d=0$), which is

$$\lambda^2 - (1+e(c_0+\alpha))\lambda + e(c_0)(e(x)-1)\,.$$

More precisely, if λ is one of the two distinct roots of this polynomial, define the vector X in $\mathbb{C}^{2^{d+1}}$ by its components: $X_1=1$, and for $j\neq 1$ and $k\in\mathbb{N}$ such that $2^k+1\le j\le 2^{k+1}$ (hence $0\le k\le d$), put $X_j = \{(\lambda-1)/e(c_0)\}^{1+s(j-2^k-1)}$, where $s(n)$ is the sum of the binary digits of the integer n (hence $s(0)=0$, $s(2n)=s(n)$, $s(2n+1)=1+s(n)$). A straightforward computation then proves that X is an eigenvector of the matrix $M(c)$.

3.3. Spectral properties. We recall that a complex-valued sequence $u:\mathbb{N}\to\mathbb{C}$ has a *correlation* γ_u if for all integers k, the sequence $n\mapsto u(n+k)\overline{u(n)}$ converges in Cesàro means. By definition,

$$\gamma_u(k) := \lim_{N\to\infty}\frac{1}{N}\sum_{n<N} u(n+k)\overline{u(n)}$$

and $\gamma_u(-k)=\overline{\gamma_u(k)}$. Hence γ_u is a positive definite sequence on $\mathbb{Z}$ and by the well-known Bochner–Herglotz representation theorem, there exists a probability measure λ_u on $[0,1[$, called *spectral measure* of u, such that

$$\widetilde{\lambda}_u(k) := \int_0^1 \exp(2\pi ikt)\,\lambda_u(dt) = \gamma_u(k)\,.$$

Moreover (see [19]), the sequence of probabilities

$$\nu_N := \frac{1}{N}\Big|\sum_{n<N} u(n)\exp(2\pi it)\Big|^2\,dt,\qquad N>0\,,$$

weakly converges to λ_u. Let $\mathbf{U}$ be the group of complex numbers of modulus 1 and assume that $u:\mathbb{N}\to\mathbf{U}$ is a generalized multiplicative Rudin–Shapiro sequence to base q, that is to say, its transition matrix T has

quadratic norm $\|T\| = q^{1/2}$. Suppose that $(\nu_N)_N$ weakly converges to a measure ν. Then

$$\frac{1}{N}\Big|\sum_{n<N} u(n)\exp(2\pi it)\Big|^2 \le C$$

for some constant C (Theorem 2.3). Hence for every positive measurable function φ

$$\nu_N(\varphi) \le C\int_0^1 \varphi(t)\,dt\,.$$

Therefore $\nu(\varphi) \le C\int_0^1 \varphi(t)\,dt$, which implies that the measure ν is absolutely continuous with respect to the Lebesgue measure. In fact, the measure ν is known to be the Lebesgue measure in the case of the usual Rudin–Shapiro sequence and its generalization given in [19]. Our definition contains all these sequences and we have the same spectral property, more precisely:

THEOREM 3.2. *Let $u : \mathbb{N} \to \mathbf{U}$ be a generalized multiplicative Rudin–Shapiro sequence. Then u has a correlation function and its spectral measure is the Lebesgue measure.*

Proof. The existence of γ_u is given by the following general lemma:

LEMMA 3.3. *Let G be a group, let $F : \mathcal{A}^* \to G$ be a chained map to base q and let $f : n \mapsto F(\widetilde{n})$ be the associated sequence. For every integer k there exists a family of arithmetic progressions $P_k(m)$, $m = 0, 1, 2\ldots$, with common difference $q^{s_k(m)}$, and a G-valued sequence $m \mapsto g_k(m)$ such that*

(i) *the sequence $\Delta_k f : n \mapsto f^{-1}(n)f(n+k)$ has the constant value $g_k(m)$ on $P_k(m)$;*
(ii) $\sum_{m\ge 0} q^{-s_k(m)} = 1$.

Moreover, if $G = \mathbf{U}$ then f has a correlation given by

$$\gamma_f(k) = \sum_{m=0}^{\infty} g_k(m)q^{-s_k(m)}\,.$$

In fact, it is enough to prove the lemma for $k = 1$. Let $0 \le a < q-1$, $b \in \mathcal{A}$, $j \ge 0$ and define

$$R_j(a,b) := \{n \in \mathbb{N};\ n \equiv \alpha_j \ (\mathrm{mod}\ q^{j+2}) \text{ and } n \ne \alpha_j \text{ if } b = 0\}\,,$$

where $\alpha_j := (\sum_{\ell<j}(q-1)q^\ell)+aq^j+bq^{j+1}$. Then for any integer n in $R_j(a,b)$ one has $n+1 \equiv ((a+1)+bq)q^j \mod q^{j+1}$ so that $\Delta_1 f$ is constant on $R_j(a,b)$, equal to $F(b(a+1)0^j)F^{-1}(\widetilde{\alpha}_j)$. Clearly the set of arithmetic progressions $R_j(a,b)$ form the required family. Notice that if F is regular then we can add α_j to $R_j(a,0)$ and then we get a partition of $\mathbb{N}$. Now assume that f

is complex-valued of modulus 1; then by (ii) the series $\sum_{m=0}^{\infty} g_k(m) q^{-s_k(m)}$ converges and its sum is equal to $\gamma_f(k)$. ∎

Going back to the generalized Rudin–Shapiro sequence u, let F be the chained map over $\mathcal{A}$ corresponding to u, let T be the transition matrix of F and for each letter a let F_a be the map defined on $\mathcal{A}^*$ by $F_a(w) := F(aw)$. We know that F_a is chained over $\mathcal{A}$ (but not regular for $a \neq 0$) with Hadamard transition matrix. Hence the sequence $u^{(a)}$ corresponding to F_a has a correlation, say $\gamma^{(a)}$. Let γ be the correlation of u. We claim that $\gamma = (1/q) \sum_{a \in \mathcal{A}} \gamma^{(a)}$. In fact, for any integer $k > 0$ and for $L > 0$ such that $k < q^{L-1}$ one has

$$\frac{1}{q^L} \sum_{n < q^L} u(n+k)\overline{u(n)} = \frac{1}{q^{L-1}} \sum_{a \in \mathcal{A}} \frac{1}{q} \sum_{n < q^{L-1}} u(aq^{L-1}+n+k)\overline{u(aq^{L-1}+n)}\,. \tag{15}$$

But $u^{(a)}(n+k) = u(aq^{L-1}+n+k)$ if $n + k < q^{L-1}$ so that

$$\Big| \sum_{n < q^{L-1}} u(aq^{L-1}+n+k)\overline{u(aq^{L-1}+n)} - \sum_{n < q^{L-1}} u^{(a)}(n+k)\overline{u^{(a)}(n)} \Big| \leq k\,.$$

Taking the limit in (15) we get the desired formula. Let $\lambda^{(a)}$ be the spectral measure of $u^{(a)}$. We have just proved that $\lambda_u = (1/q) \sum_{a<q} \lambda^{(a)}$ and with the above notations,

$$\begin{aligned} \nu_{q^L} &= \frac{1}{q^L} \Big| \sum_{a \in \mathcal{A}} \Big(\sum_{n < q^{L-1}} u^{(a)}(n) \exp(2\pi i n t) \Big) \exp(2\pi i q^{L-1} a t) \Big|^2 dt \\ &= \frac{1}{q} \sum_{a<q} \frac{1}{q^{L-1}} |u^{(a)}(n) \exp(2\pi i n t)|^2\, dt + W_L(t)\, dt\,, \end{aligned}$$

where W_L is a trigonometric polynomial such that

$$\lim_{L \to \infty} \int_0^1 W_L(t) \exp(2\pi i k t)\, dt = 0$$

for all integers k. Moreover, by (11) (which is an equality since T is a Hadamard matrix) we have

$$\nu_{q^L} = (1 + W_L(t))\, dt\,.$$

This implies that $(\nu_{q^L})_L$ converges weakly to the Lebesgue measure and finishes the proof. ∎

R e m a r k s. 1. Theorem 3.2 can be extended to any G-valued chained sequence with Hadamard transition matrix (with G finite and abelian). Let $\mathcal{A}$ be endowed with an abelian group law (where 0 is the neutral element), let

$\widehat{\mathcal{A}}$ be its dual group and let $a \mapsto \chi_a$ be an isomorphism from $\mathcal{A}$ to $\widehat{\mathcal{A}}$. Then $T := (\chi_a(b))_{ab\in\mathcal{A}^2}$ is a Hadamard matrix and gives rise to many examples of generalized Rudin–Shapiro sequences.

2. Recall that the Kronecker product $A \otimes B$ of matrices $A := (a_{ij})_{ij\in\mathcal{A}^2}$, $B := (a_{kl})_{kl\in\mathcal{B}^2}$ is defined by

$$A \otimes B := (a_{ij}B)_{ij} .$$

Set $A^{(1)} := A$, $A^{(n+1)} = A \otimes A^{(n)}$ for $n \geq 1$. The transition matrix corresponding to the Rudin–Shapiro sequence of order d on 11 (Definition 3.1) is given by

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^{(d+1)} .$$

The proof is left to the reader. Notice this matrix is obtained from the above example with $\mathcal{A}$ identified with the group $(\mathbb{Z}/2\mathbb{Z})^{d+1}$.

3. Let $\mathcal{A}$ be the cyclic group of order q identified by $a \mapsto \zeta^a$ ($\zeta = \exp(2\pi i/q)$) to the corresponding cyclic subgroup of $\mathbf{U}$. Then the example given by M. Queffélec in [18] is the one obtained as in Remark 1 through the isomorphism $\zeta^a \mapsto \chi_a$, $\chi_a(\zeta^b) := \zeta^{ab}$ $(a, b = 0, 1, \ldots, q-1)$.

4. In a forthcoming paper we shall study the flows associated to chained sequences, proving that they are (except for degenerate cases) strictly ergodic and can be obtained as group extensions of a q-adic rotation; we shall also give the spectral study of these flows (in this direction, see also [10, 14, 18, 19]).

The authors thank Michel Mendès France for many helpful discussions, and the referee for suggesting to sharpen Lemma 3.2 and its consequences. The present version of this lemma is inspired by personal communications of Gérald Tenenbaum and of Michel Balazard (see also [2], [17] and J.-P. Allouche, M. Mendès France and G. Tenenbaum, *Entropy: an inequality*, Tokyo J. Math. 11 (1988), 323–328).

References

[1] J.-P. Allouche, *Les suites de Rudin–Shapiro généralisées: des suites déterministes de "dimension" maximale*, in: Colloque "Fractals", C.I.R.M., Marseille 1986.

[2] J.-P. Allouche and M. Mendès France, *On an extremal property of the Rudin–Shapiro sequence*, Mathematika 32 (1985), 33–38.

[3] —, —, *Suite de Rudin–Shapiro et modèle d'Ising*, Bull. Soc. Math. France 113 (1985), 275–283.

[4] D. W. Boyd, J. Cook and P. Morton, *On sequences of ±1's defined by binary patterns*, Dissertationes Math. 283 (1989).

[5] J. Brillhart and L. Carlitz, *Note on the Shapiro polynomials*, Proc. Amer. Math. Soc. 25 (1970), 114–118.

[6] J. Brillhart, P. Erdős and P. Morton, *On sums of Rudin–Shapiro coefficients II*, Pacific J. Math. 107 (1978), 39–69.
[7] J. Brillhart und P. Morton, *Über Summen von Rudin–Shapiroschen Koeffizienten*, Illinois J. Math. 22 (1978), 126–148.
[8] G. Christol, T. Kamae, M. Mendès France et G. Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France 108 (1980), 401–419.
[9] A. Cobham, *Uniform tag-sequences*, Math. Systems Theory 6 (1972), 164–192.
[10] J. Coquet and P. Liardet, *A metric study involving independent sequences*, J. Analyse Math. 49 (1987), 15–53.
[11] A. O. Gelfond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. 13 (1968), 259–265.
[12] J.-P. Kahane, *Hélices et quasi-hélices*, in: Math. Anal. Applic., Part B, Adv. in Math. Suppl. Stud. 7B, 1981, 417–433.
[13] L. Kuipers and H. Niederreiter, *Uniform Distributions of Sequences*, John Wiley & Sons, New York 1974.
[14] M. Lemańczyk, *Toeplitz $\mathbf{Z}_2$-extensions*, Ann. Inst. H. Poincaré 24 (1) (1988), 1–43.
[15] P. Liardet, *Propriétés harmoniques de la numération, d'après Jean Coquet*, in: Colloque S.M.F.-C.N.R.S. "Jean Coquet", Publications Mathématiques d'Orsay 88–02, Orsay 1988, 1–35.
[16] —, *Automata and generalized Rudin–Shapiro sequences*, Arbeitsbericht, Math. Institut der Universität Salzburg, 1990.
[17] M. Mendès France et G. Tenenbaum, *Dimension des courbes planes, papiers pliés et suite de Rudin–Shapiro*, Bull. Soc. Math. France 109 (1981), 207–215.
[18] M. Queffélec, *Une nouvelle propriété des suites de Rudin–Shapiro*, Ann. Inst. Fourier (Grenoble) 37 (2) (1987), 115–138.
[19] —, *Substitution Dynamical Systems—Spectral Analysis*, Lecture Notes in Math. 1294, Springer, 1987.
[20] D. Rider, *Transformations of Fourier coefficients*, Pacific J. Math. 19 (1966), 347–355.
[21] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. 10 (1959), 855–859.
[22] B. Saffari, *Une fonction extrémale liée à la suite de Rudin–Shapiro*, C. R. Acad. Sci. Paris 303 (1986), 97–100.
[23] A. Salem and A. Zygmund, *Some properties of trigonometric series whose terms have random signs*, Acta Math. 91 (1954), 245–301.
[24] H. S. Shapiro, *Extremal problems for polynomials and power series*, Thesis, M.I.T., 1951.
[25] A. P. Street, J. S. Wallis and W. D. Wallis, *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*, Lecture Notes in Math. 292, Springer, 1972.

CNRS URA 226
UNIVERSITÉ BORDEAUX I
MATHÉMATIQUES ET INFORMATIQUE
351, COURS DE LA LIBÉRATION
F-33405 TALENCE CEDEX, FRANCE

UNIVERSITÉ DE PROVENCE
URA 225, CASE 96
3, PLACE VICTOR-HUGO
F-13331 MARSEILLE CEDEX 3, FRANCE

Received on 3.11.1989
and in revised form on 30.11.1990 (1984)