ACTA ARITHMETICA
LXVIII.3 (1994)

A characterization of generalized Rudin–Shapiro sequences with values in a locally compact abelian group

by

Jean-Loup Mauclaire (Paris)

1. Introduction. Let G be a locally compact abelian group with a group law denoted additively. Let A be a finite alphabet $\{0,1,2,\ldots,q-1\}$ of q elements naturally ordered, with a fixed integer $q\geq 2$. We denote by A^* the monoid of finite words on A. The number of letters of an element w of A^* is the *length* of the word, and with every word $w=w_0w_1\ldots w_r$ of length $r+1$, we associate the integer $\dot{w}=w_0+qw_1+\ldots+q^rw_r$. Following J.-P. Allouche and P. Liardet (see [1]), we shall say that a map f from A^* to G is a *chained map* if it satisfies the condition that for all letters a and b in A, and any word w in A^*, $f(abw)=f(ab)-f(b)+f(bw)$. Note that, by iteration, for all letters $a_1,a_2,\ldots,a_s$, and every word w in A^*, we have

$$f(a_1a_2\ldots a_sw)=(f(a_1a_2)-f(a_2))+\ldots+(f(a_{s-1}a_s)-f(a_s))+f(a_sw).$$

Now, given a chained map f, if χ is a continuous character of G, we denote by χT the q^2-matrix with entries $a_i^j=\chi(f(ij)-f(j))$, $0\leq j\leq q-1$, $0\leq i\leq q-1$, where a_i^j is the element of the ith line and jth column. By definition, f is said to be a *Rudin–Shapiro map* if for every non-trivial character χ, $(\overline{\chi T})(\chi T)=qI$, or equivalently $(\chi T)(\overline{\chi T})=qI$. Here I denotes the identity matrix and $(\overline{\chi T})$ the adjoint of (χT). With every f we associate a sequence f^* defined by $f^*(\dot{w})=f(w)$. Such a sequence f^* will be called a *generalized Rudin–Shapiro sequence* with values in G if f is a Rudin–Shapiro map.

In [1], motivations are given for the study of these sequences, which generalize in a natural way the classical Rudin–Shapiro sequence. But the authors assume that G is compact and metrizable. In this paper we consider the more general case where G is a locally compact abelian group. One of the interesting results presented in [1] is that if G is a compact metrizable abelian group and if f is a Rudin–Shapiro map, then G must be finite. The proof given in [1] is not quite correct. The purpose of this article is to give a complete proof for the more general case of locally compact abelian groups. Moreover, we give a characterization of the existence of generalized Rudin–Shapiro sequences with values in a locally compact abelian group.

2. The result. We shall give a proof of the following theorem:

THEOREM. *Let G be a locally compact abelian group written additively. A mapping f is a Rudin–Shapiro map from A^* to G if and only if*

(i) *G is a finite group, and its order N divides q,*

(ii) *if $u_{ij}(r) = f(ir) - f(jr)$, $0 \le i, j, r \le q-1$, then for every ϱ in G and every $i \ne j$, the number $N_{ij}(\varrho) = \operatorname{card}\{u_{ij}(r) : 0 \le r \le q-1, u_{ij}(r) = \varrho\}$ is equal to q/N.*

Remark. Property (ii) is equivalent to the fact that the set of the differences $f(ir) - f(jr)$, $0 \le r \le q-1$, $i \ne j$, is the union of q/N copies of G.

3. Proof of the Theorem

I. We assume that f is a Rudin–Shapiro map. Let χ be a non-trivial character of G. Consider χT, the $q \times q$ matrix with entries

$$a_i^j = \chi(f(ij) - f(j)), \quad 0 \le j \le q-1,\ 0 \le i \le q-1.$$

We have $\chi T = (\chi(f(ij)))(\overline{\chi}(f(j)))$, where $(\chi(f(ij)))$ (resp. $(\overline{\chi}(f(j)))$ is the $q \times q$ matrix with entries $\widetilde{a}_i^j = \chi(f(ij))$ (resp. $\widehat{a}_i^j = \overline{\chi}(f(j))$ if $i = j$ and $\widehat{a}_i^j = 0$ otherwise). Now, since f is a Rudin–Shapiro map, we have $(\chi T)(\overline{\chi T}) = qI$, which implies $(\chi(f(ij)))(\overline{\chi(f(ij))}) = qI$ and gives

$$\sum_{r=0}^{q-1} \chi(f(ir) - f(jr)) = \begin{cases} q & \text{if } i = j, \\ 0 & \text{if } i \ne j. \end{cases}$$

Now, we fix i and j, $i \ne j$, and set $u(r) = f(ir) - f(jr)$, $0 \le r \le q-1$. Since G is locally compact, we consider a compact neighbourhood $V(0)$ of the origin. Let F be a continuous non-negative real function with support in $V(0)$ taking the value 1 at 0 and such that its Fourier transform F^* is invertible. The function H defined by

$$H(t) = \sum_{r=0}^{q-1} F(u(r) + t)$$

has a Fourier transform H^* given by

$$H^*(\chi) = \sum_{r=0}^{q-1} \int_G F(u(r) + t)\chi(t)\, dm(t)$$

where m is the normalized Haar measure on G. Therefore

$$H^*(\chi) = \sum_{r=0}^{q-1} \overline{\chi}(u(r)) \int_G F(u(r)+t)\chi(t+u(r))\, dm(t)$$

and so

$$H^*(\chi) = F^*(\chi) \sum_{r=0}^{q-1} \overline{\chi}(u(r)).$$

Hence $H^*(\chi)$ is equal to zero, except if χ is trivial. Denoting by m^* the normalized Haar measure on G^*, the dual group of G, by Fourier inversion we get

$$\int_{G^*} H^*(\chi)\overline{\chi}(t)\, dm^*(\chi) = \int_{G^*} F^*(\chi) \sum_{r=0}^{q-1} \overline{\chi}(u(r))\overline{\chi}(t)\, dm^*(\chi)$$
$$= \sum_{r=0}^{q-1} F(u(r)+t) = H(t).$$

Since H is not identically 0 by construction, we deduce that if 1_{G^*} denotes the trivial character on G, then $m^*(\{1_{G^*}\})$ is not 0 and is finite since a point is compact. But m^* is translation invariant so that $m^*(\{\chi\}) = m^*(\{1_{G^*}\})$ for any character χ of G. Now, any compact neighbourhood V^* of 1_{G^*} has a finite measure and so must be a finite set. Indeed, if $\{\chi_m : 0 \le m \le n\}$ is a set of distinct elements of V^*, we must have

$$\sum_{m=0}^{n} m^*(\{\chi_m\}) = (n+1)m^*(\{1_{G^*}\}) < m^*(V^*),$$

which implies that n is finite. This proves that the topology defined on G^* is discrete. By a classical result of duality theory, we deduce that G is compact. Now, we consider a finite family of compact neighbourhoods $V(r)$ of $u(r)$, $0 \le r \le q-1$, and assume that there exists a continuous non-negative real function F, not identically 0, with compact support $S(F)$ such that $S(F)$ does not intersect any of the $V(r)$. Since G is compact, the space E of finite linear combinations of characters of G is dense in the space of continuous functions on G. Then, for any given $\varepsilon > 0$, there exists an approximation $P_\varepsilon \in E$ such that $\sup_{t\in G} |F(t) - P_\varepsilon(t)| \le \varepsilon$. Note that $|\int_G (F - P_\varepsilon)\, dm| \le \varepsilon$, and recall that $\widehat{P}_\varepsilon(1_{G^*}) = \int_G P_\varepsilon\, dm$, $\widehat{P}_\varepsilon(1_{G^*})$ denoting the Fourier transform of P_ε at 1_{G^*}. But $\sup_{t\in G} |F(t) - P_\varepsilon(t)| \le \varepsilon$ also implies that $|\sum_{r=0}^{q-1} F(u(r)) - P_\varepsilon(u(r))| \le q\varepsilon$ and since $F(u(r)) = 0$ for every r and $\sum_{r=0}^{q-1} \chi(u(r)) = 0$ for every non-trivial character χ of G, we get $|\sum_{r=0}^{q-1} \widehat{P}_\varepsilon(1_{G^*})| \le q\varepsilon$. Therefore $\int_G F = 0$. Since F is continuous, non-negative and not identically 0, this is a contradiction. Hence $S(F)$ intersects at least one of the compact neighbourhoods $V(r)$. This means that the finite set of points $u(r)$, $0 \le r \le q-1$, is dense in G, and so G is finite.

We shall denote by N the number of elements of G.

By our hypothesis, $\sum_{r=0}^{q-1} \chi(u(r)) = 0$ for every non-trivial character χ of G. Now, we write

$$\sum_{r=0}^{q-1} \chi(u(r)) = \sum_{\varrho \in G} \chi(\varrho) N(\varrho) \tag{1}$$

where, as above, $N(\varrho) = \operatorname{card}\{u(r) : 0 \le r \le q-1, u(r) = \varrho\}$. For ϱ in G, the orthogonality relations for characters give

$$N(\varrho) = \frac{1}{N} \sum_{\chi \in G^*} \overline{\chi}(\varrho) \Big(\sum_{\varrho' \in G} \chi(\varrho') N(\varrho') \Big). \tag{2}$$

Using (1), we see that formula (2) can be written

$$N(\varrho) = \frac{1}{N} \sum_{\chi \in G^*} \overline{\chi}(\varrho) \Big(\sum_{r=0}^{q-1} \chi(u(r)) \Big),$$

and since by hypothesis $\sum_{r=0}^{q-1} \chi(u(r))$ is 0 if $\chi \ne 1$ and q if $\chi = 1$, we get $N(\varrho) = q/N$. In particular, N divides q since q/N is an integer.

So, we have shown that

(i) G is a finite group and its order N divides q,

(ii) if we fix i and j, $i \ne j$, and set $u_{ij}(r) = f(ir) - f(jr)$, $0 \le r \le q-1$, then for every ϱ in G,

$$N_{ij}(\varrho) = \operatorname{card}\{u_{ij}(r) : 0 \le r \le q-1,\ u_{ij}(r) = \varrho\} = q/N.$$

II. We prove the converse. To this end, we assume that G is a finite group and its order N divides q. Let f be a chained map satisfying the following property:

For any i and j such that $i \ne j$, the set of the differences $f(ir) - f(jr)$, $0 \le r \le q-1$, is the union of q/N copies of G.

We shall prove that if χ is a non-trivial character of G, then χT, the $q \times q$ matrix with entries $a_i^j = \chi(f(ij) - f(j))$, satisfies $(\chi T)(\overline{\chi T}) = qI$.

We have seen that $\chi T = (\chi(f(ij)))(\overline{\chi}(f(j)))$. Note that $(\chi T)(\overline{\chi T}) = (A_i^j)$ with

$$\begin{aligned} A_i^j &= \sum_{r=0}^{q-1} \chi(f(ir)) \overline{\chi}(r) \overline{\overline{\chi}}(r) \overline{\chi}(f(jr)) = \sum_{r=0}^{q-1} \chi(f(ir)) \overline{\chi}(f(jr)) \\ &= \sum_{r=0}^{q-1} \chi(f(ir) - f(jr)). \end{aligned}$$

By assumption,

$$\sum_{r=0}^{q-1} \chi(f(ir) - f(jr)) = \sum_{\varrho \in G} \frac{q}{N} \chi(\varrho) = \frac{q}{N} \sum_{\varrho \in G} \chi(\varrho).$$

Therefore $A_i^j = q$ if $i = j$ and $A_i^j = 0$ if $i \neq j$. This means that $(\chi T)(\overline{\chi T}) = qI$, i.e., f is a Rudin–Shapiro map. This ends the proof of the Theorem.

EXAMPLES. 1. In the case $q = 2$, $G = \mathbb{Z}/2\mathbb{Z}$, the classical Rudin–Shapiro sequence is obtained by taking $f(ij)$ equal to the coefficient of the ith line and jth column of the 2×2 matrix $\left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$ ([3], [4]).

2. Let q be a prime number. We identify A with the cyclic group of order q. Then, as mentioned in [1] (where the condition on the primality of q has been omitted), the example given by Queffélec in [2] corresponds, in this case, to the A-valued Rudin–Shapiro map f defined on $A \times A$ by $f(a, b) = ab$.

References

[1] J.-P. Allouche and P. Liardet, *Generalized Rudin–Shapiro sequences*, Acta Arith. 60 (1991), 1–27.

[2] M. Queffélec, *Une nouvelle propriété des suites de Rudin–Shapiro*, Ann. Inst. Fourier (Grenoble) 37 (2) (1987), 115–138.

[3] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. 10 (1959), 855–859.

[4] H. S. Shapiro, *Extremal problems for polynomials and power series*, Thesis, M.I.T., 1951.

C.N.R.S., U.R.A. 212
THÉORIES GÉOMÉTRIQUES
UNIVERSITÉ PARIS-VII
TOUR N° 45–55, 5e ÉTAGE
2, PLACE JUSSIEU
75251 PARIS CEDEX 05
FRANCE

Received on 1.3.1993 (2390)