

THE GAUSSIAN LAW AND LACUNARY SETS OF CHARACTERS

E. DUDLEY and P. HALL

(Received 13 December 1977)

Abstract

Salem and Zygmund (1947, 1948), Baker (1972) and Dudley (1975) have shown that certain lacunary sets P of characters of a compact abelian group have the property that sequences of the form $\{\sum_{k=1}^n a_k \varphi_k\}_{n=1}^{\infty}$ where $\varphi_k \in P$ converge to the normal distribution if suitably normalized. In this paper, a theorem of probability due to McLeish (1974) is applied to clarify and extend the previous results.

Subject classification (Amer. Math. Soc. (MOS) 1970): 42 A 36, 42 A 44, 60 F 05.

1. Introduction

Throughout this paper, unless otherwise stated, the symbol G is used to denote an arbitrary, infinite, compact, abelian group with Haar measure m , normalized so that $m(G) = 1$. The character group of G is denoted by Γ and the unit character is denoted by 1 . For $A \subseteq \Gamma$, we write A^{-1} for the set $A^{-1} = \{\varphi^{-1} : \varphi \in A\}$ and we say that A is *symmetric* if $A = A^{-1}$. A complex-valued function f defined on a symmetric subset A of Γ is said to be *symmetric* if $f(\varphi^{-1}) = \overline{f(\varphi)}$ for all $\varphi \in A$. Note that this implies that $f(\varphi)$ is real if $\varphi = \varphi^{-1}$ or $\varphi^2 = 1$. The cardinality of a set A is denoted by $|A|$ while the symbol Δ is used to denote symmetric difference. The symbols N, Z, R and C are used to denote the usual sets of numbers. All other notation not explained appears in Rudin (1960).

We use the symbol P to denote an infinite subset of Γ and the symbol u to denote a complex-valued function defined on $P \cup P^{-1}$. The symbol \mathcal{S} , possibly with subscripts attached, is used to denote a sequence $\mathcal{S} = \{X(n)\}_{n=1}^{\infty}$ of pair wise-disjoint, finite, nonempty symmetric subsets of Γ . We set

$$P(n) = (P \cup P^{-1}) \cap X(n),$$

$$Q(n) = \bigcup_{k=1}^n P(k),$$

$$S(n) = \sum_{\varphi \in Q(n)} u(\varphi) \varphi,$$

and

$$(1.1) \quad \begin{aligned} B(n) &= \left(\int_G S(n)^2 dm \right)^{\frac{1}{2}} \\ &= \left(\sum_{\varphi \in Q(n)} |u(\varphi)|^2 \right)^{\frac{1}{2}}. \end{aligned}$$

The last calculation is a consequence of the orthogonality relations for characters (that is, $\int_G \varphi \gamma^{-1} dm$ is zero if φ and γ are distinct characters). Note that $P(n)$, $Q(n)$, $S(n)$ and $B(n)$ depend on P , u and \mathcal{S} . However, for simplicity we do not indicate this dependence explicitly except where confusion may arise. We have the following definition.

DEFINITION 1.1. We say that a pair (P, \mathcal{S}) is *compatible* if

- (a) $|Q(n)| \rightarrow \infty$ as $n \rightarrow \infty$,

and

- (b) $\{|P(n)|\}$ is bounded.

We say that a triple (P, u, \mathcal{S}) is *compatible* if

- (c) (P, \mathcal{S}) is compatible,

- (d) $B(n) \rightarrow \infty$ as $n \rightarrow \infty$,

and

- (e) $\lim_{n \rightarrow \infty} B(n)^{-1} \max_{\varphi \in Q(n)} |u(\varphi)| = 0$.

Observe that (P, \mathcal{S}) is compatible if and only if (P, i, \mathcal{S}) is compatible where i is the function mapping each $\varphi \in P \cup P^{-1}$ onto 1. In the central limit theorem, the limiting behaviour of the sequence $\{B(n)^{-1} S(n)\}$ is characterized. Conditions (d) and (e) of the above definition are typical conditions needed for the law to hold while condition (a) is necessary for (d) to hold. The central limit problem is more complicated if we do not have condition (b).

DEFINITION 1.2. A compatible triple (P, u, \mathcal{S}) is said to be *Gaussian* if

$$\lim_{n \rightarrow \infty} B(n)^{-1} S(n) = N(0, 1) \quad \text{in distribution;}$$

that is,

$$\lim_{n \rightarrow \infty} m\{t \in G: B(n)^{-1} S(n)(t) < y\} = (2\pi)^{-\frac{1}{2}} \int_{-\infty}^y \exp(-\frac{1}{2}t^2) dt$$

for all $y \in R$.

The general problem we tackle is to characterize Gaussian triples. In particular, we investigate lacunary properties of the set P which ensure that a wide class of compatible triples (P, u, \mathcal{S}) are Gaussian. In Section 2, we examine invariance properties of compatible triples with respect to the Gaussian property, while in Section 3 we prove our main theorem. We apply our results to the classical case of

the circle group in Section 4, and in Section 5 we consider applications in the general case of an arbitrary compact Abelian group.

2. Invariance properties

In this section, we make the convention that if u_j is a function defined on $P_j \cup P_j^{-1}$ for $j=1$ and 2 , and the u_j 's are the restrictions of a function u defined on $P_1 \cup P_1^{-1} \cup P_2 \cup P_2^{-1}$, then the function u_j is denoted by the symbol u where the domain of the function is clearly understood.

DEFINITION 2.1. Let (P_1, \mathcal{S}_1) and (P_2, \mathcal{S}_2) be compatible pairs. For $j = 1$ or 2 , denote by $P_j(n)$ and $Q_j(n)$, the terms in (1.1) defined with respect to (P_j, \mathcal{S}_j) . For $\{j, k\} = \{1, 2\}$, set

$$a_j(n) = \min \{m \in N : |Q_j(n) \Delta Q_k(m)| = \min \{|Q_j(n) \Delta Q_k(r)| : r \in N\}\}$$

and $A_j = \sup \{|Q_j(n) \Delta Q_k(a_j(n))| : n \in N\}$. We say that (P_1, \mathcal{S}_1) and (P_2, \mathcal{S}_2) are *Gaussian equivalent* if both A_1 and A_2 are finite. (Clearly Gaussian equivalence is an equivalence relation.)

DEFINITION 2.2. Given pairs, (P, \mathcal{S}_1) and (P, \mathcal{S}_2) , we say that \mathcal{S}_1 is *P-finer* than \mathcal{S}_2 or \mathcal{S}_2 is *P-coarser* than \mathcal{S}_1 if there exists a nondecreasing sequence $\{n_k\}_{k=1}^\infty$ of positive integers such that $Q_1(n_k) = Q_2(k)$ for all $k \in N$. A sequence \mathcal{S} is said to be a *P-basic* sequence if for each $n \in N$, $P(n)$ is empty or $P(n) = \{\varphi, \varphi^{-1}\}$ for some $\varphi \in \Gamma$.

In the following lemma, some consequences of the previous definitions are given. The proof is easy and is omitted.

LEMMA 2.3

(a) If (P, \mathcal{S}) is compatible, then \mathcal{S} is *P-coarser* than some *P-basic* sequence.

(b) If \mathcal{S}_1 is *P-finer* than \mathcal{S}_2 , then it follows that

(i) a triple (P, u, \mathcal{S}_2) is compatible if and only if (P, u, \mathcal{S}_1) is compatible and $\{|P_2(n)|\}$ is bounded;

and

(ii) if (P, \mathcal{S}_2) is compatible, then (P, \mathcal{S}_2) and (P, \mathcal{S}_1) are *Gaussian equivalent*.

The following is the key theorem in this section.

THEOREM 2.4. Suppose that (P_1, \mathcal{S}_1) and (P_2, \mathcal{S}_2) are *Gaussian equivalent* and that (P_1, u, \mathcal{S}_1) and (P_2, u, \mathcal{S}_2) are compatible. Then if (P_1, u, \mathcal{S}_1) is *Gaussian*, (P_2, u, \mathcal{S}_2) is also *Gaussian*.

PROOF. Let $P_j(n)$, $Q_j(n)$, $S_j(n)$ and $B_j(n)$ be the terms in (1.1) defined with respect to (P_j, u, \mathcal{S}_j) . We use the notation introduced in Definition 2.1. Note that $a_j(n) \rightarrow \infty$ since otherwise there exists m such that $|Q_j(n) \Delta Q_k(m)| < A_j$ for infinitely many n ,

contradicting the fact that $|Q_j(n)| \rightarrow \infty$ (see Definition 1.1(a)). From the definition of $B(n)$, we have

$$|B_2^2(n) - B_1^2(a_2(n))| \leq A_2 \max |u(\varphi)|^2,$$

where the max is taken over all $\varphi \in Q_1(a_2(n)) \Delta Q_2(n)$. We conclude that

$$\begin{aligned} & \min\{|1 - B_2^{-2}(n)B_1^2(a_2(n))|, |1 - B_2^2(n)B_1^{-2}(a_2(n))|\} \\ & \leq A_2 \max\{B_2^{-2}(n) \max\{|u(\varphi)|^2 : \varphi \in Q_2(n)\}, B_1^2(a_2(n)) \max\{|u(\varphi)|^2 : \varphi \in Q_1(a_2(n))\}\}. \end{aligned}$$

The right side of the above inequality tends to 0 as n approaches ∞ by Definition 1.1(e) and it follows that $B_2^{-1}(n) B_1(a_2(n)) \rightarrow 1$. Since (P_1, u, \mathcal{S}_1) is Gaussian, the sequence $\{B_1^{-1}(a_2(n)) S_1(a_2(n))\}$ is tight in the probabilistic sense and it follows that

$$B_1^{-1}(a_2(n)) S_1(a_2(n)) |B_1(a_2(n)) B_2^{-1}(n) - 1| \rightarrow 0$$

in measure. Hence, in order to show that (P_2, u, \mathcal{S}_2) is Gaussian, it suffices to show that

$$|S_1(a_2(n)) - S_2(n)| [B_1(a_2(n))]^{-1} \rightarrow 0$$

in measure. This is an immediate consequence of Definition 1.1(e), the fact that $B_2^{-1}(n) B_1(a_2(n)) \rightarrow 1$ as $n \rightarrow \infty$ and the inequalities

$$\begin{aligned} |S_1(a_2(n)) - S_2(n)| & \leq \sum_{\varphi \in T(n)} |u(\varphi)| \\ & \leq A_2 \max_{\varphi \in T(n)} |u(\varphi)| \end{aligned}$$

where $T(n) = Q_1(a_2(n)) \Delta Q_2(n)$.

3. The main theorem

We begin by defining the key concepts needed.

DEFINITION 3.1. Suppose that (P, \mathcal{S}) is compatible. Let

$$R(n) = \left| \left\{ f \in \prod_{j=1}^{\infty} [P(j) \cup \{1\}] : |\{j : f(j) \neq 1\}| = n, \prod_{j=1}^{\infty} f(j) = 1 \right\} \right|.$$

We say that (P, \mathcal{S}) is *weakly dissociate* if there exists $B > 0$ such that $R(n) \leq B^n$ for all n . In particular, if $R(n) = 0$ for all $n \geq 1$, then we say that (P, \mathcal{S}) is *strongly dissociate*.

DEFINITION 3.2. Suppose that (P, \mathcal{S}) is compatible. For $\varphi \in \Gamma$, let

$$F(\varphi) = \bigcup_{k=1}^{\infty} \{\gamma \in P(k) : \gamma\varphi^{-1} \in P(k)\} = \bigcup_{k=1}^{\infty} \varphi P(k) \cap P(k).$$

We say that (P, \mathcal{S}) is *stable* if there exists $C > 0$ such that

$$|F(\varphi)| \leq C \quad \text{for all } \varphi \in \Gamma - \{1\}.$$

REMARKS 3.3

(a) Clearly, a compatible pair (P, \mathcal{S}) is strongly dissociate if and only if whenever $n_1 < n_2 < \dots < n_k$ and $\{\varphi_j\}_{j=1}^k$ is a sequence such that $\varphi_j \in P(n_j)$, then $\prod_{j=1}^k \varphi_j \neq 1$.

(b) The term *dissociate* as applied to lacunary sets of characters is firmly established in the literature (see López and Ross (1975), 2.5). We generalize and slightly modify López and Ross's definition by saying that a set of characters P is *k-dissociate* if whenever F is a finite subset of P which is asymmetric (that is, $\varphi, \varphi^{-1} \in F$ implies that $\varphi = \varphi^{-1}$) and m is a function from F into $\{-k, -k+1, \dots, 0, 1, \dots, k-1, k\}$, then the implication

$$\prod_{\varphi \in F} \varphi^{m(\varphi)} = 1 \text{ implies that } \varphi^{m(\varphi)} = 1 \text{ for all } \varphi \in F$$

holds. We can readily establish that an infinite subset P of Γ is 1-dissociate if and only if (P, \mathcal{S}) is strongly dissociate for each compatible pair (P, \mathcal{S}) . Similarly, we can easily show that an infinite set P is a Rider set (see López and Ross (1975), 2.13) if and only if (P, \mathcal{S}) is weakly dissociate for each compatible pair (P, \mathcal{S}) .

(c) From a probabilistic viewpoint, weak dissociativity (or stability) ensures that the sequence

$$\left\{ \sum_{\varphi \in P(n)} u(\varphi) \varphi \right\}_{n=1}^{\infty} \text{ (or } \left\{ \left[\sum_{\varphi \in P(n)} u(\varphi) \varphi \right]^2 \right\}_{n=1}^{\infty} \text{),}$$

when suitably normalized, is weakly stochastically dependent. The two conditions together ensure that (P, u, \mathcal{S}) is Gaussian.

We now state the basic probability theorem on which our results depend. The theorem is due to McLeish (1974) but his methods derive from Salem and Zygmund (1947).

THEOREM 3.4. *Let $\{X_{n,j} : j = 1, 2, \dots, k_2\}$ be an array of random variables on a probability triple $(\Omega, \mathcal{F}, \mu)$. For $n \in \mathbb{N}$, $t \in \mathbb{R}$ and $i^2 = -1$, let*

$$T_n = \prod_{j=1}^{k_n} (1 + itX_{n,j})$$

and

$$S_n = \sum_{j=1}^{k_n} X_{n,j}.$$

Suppose that

- (a) $\lim_{n \rightarrow \infty} \int T_n d\mu = 1$;
- (b) the sequence $\{T_n\}$ is uniformly integrable;
- (c) $\lim_{n \rightarrow \infty} \sum_{j=1}^{k_n} X_{n,j}^2 = 1$ in measure; and
- (d) $\lim_{n \rightarrow \infty} \max_{j=1, 2, \dots, k_n} |X_{n,j}| = 0$ in measure.

It then follows that $\lim_{n \rightarrow \infty} S_n = N(0, 1)$ in distribution.

The following generalization of the above theorem is not essential to our key results but is needed in Theorem 5.8 where we compute the limiting distribution of non-Gaussian sequences. The proof follows closely that of McLeish (1974).

THEOREM 3.5. *If in the previous theorem, conditions (b) and (d) hold while, for some random variable X , we have for $t > 0$*

(a') $\lim_{n \rightarrow \infty} \int T_n \exp(-tX) d\mu = \int \exp(-tX) d\mu$, and

(c') $\lim_{n \rightarrow \infty} \sum_{j=1}^{k_n} X_{n,j}^2 = X$ in measure,

then $\lim_{n \rightarrow \infty} S_n = F$ in distribution where the distribution F has characteristic function $\int \exp(-\frac{1}{2}t^2 X) d\mu$.

We apply Theorem 3.4 to obtain sufficient conditions for a compatible triple (P, u, \mathcal{S}) to be Gaussian.

THEOREM 3.6. *Suppose that (P, u, \mathcal{S}) is compatible. For $1 \leq k \leq n$, we set*

$$T(n, k) = B^{-1}(n) (S(k) - S(k - 1))$$

and $T(n): t \rightarrow \prod_{k=1}^n (1 + itT(n, j))$ for $t \in R$.

Suppose that the following are satisfied:

(a) $\lim_{n \rightarrow \infty} \int_G T(n)(t) dm = 1$ for each $t \in R$, and

(b) $\lim_{n \rightarrow \infty} \int_G (\sum_{k=1}^n T^2(n, k))^2 dm = 1$.

Then the triple (P, u, \mathcal{S}) is Gaussian.

The proof of Theorem 3.6 is accomplished via the following lemmas.

LEMMA 3.7. *Suppose that (P, u, \mathcal{S}) is compatible and p is an upper bound for $\{|P(n)|\}$ (see Definition 1.1(b)). Then we have the estimate:*

$$\|T(n)(t)\|_\infty \leq \exp(\frac{1}{2}pt^2)$$

for each $t \in R$.

PROOF. Noting (1.1) and using Hölder's inequality, we have

$$\begin{aligned} \sum_{k=1}^n T^2(n, k) &= B^{-2}(n) \sum_{k=1}^n \left(\sum_{\varphi \in P(k)} u(\varphi) \varphi \right)^2 \\ &\leq pB^{-2}(n) \sum_{k=1}^n \sum_{\varphi \in P(k)} |u(\varphi)|^2 \\ &= p. \end{aligned}$$

Hence we have

$$\begin{aligned} \|T(n)(t)\|_\infty^2 &= \prod_{k=1}^n (1 + t^2 T^2(n, k)) \\ &\leq \exp\left(\sum_{k=1}^n t^2 T^2(n, k)\right) \\ &= \exp(pt^2). \end{aligned}$$

LEMMA 3.8. *Suppose that (P, u, \mathcal{S}) is compatible and r is a positive real number. Then the following are equivalent:*

- (a) $\lim_{n \rightarrow \infty} \sum_{k=1}^n T^2(n, k) = r$ in measure,
- (b) $\lim_{n \rightarrow \infty} \int_G (\sum_{k=1}^n T^2(n, k))^2 dm = 2r - r^2$.

PROOF. As shown in the previous proof, we have

$$\left\| \sum_{k=1}^n T^2(n, k) \right\|_{\infty} \leq p$$

and so the sequence $\sum_{k=1}^n T^2(n, k)$ is uniformly bounded. For such a sequence of random variables and for any $s > 0$, convergence in measure to another variable is equivalent to convergence in L^s . Since $\int_G \sum_{k=1}^n T^2(n, k) dm = 1$, condition (b) of the lemma is equivalent to the condition:

$$\lim_{n \rightarrow \infty} \int_G \left(\sum_{k=1}^n T^2(n, k) - r \right)^2 dm = 0$$

which is simply convergence in L^2 .

LEMMA 3.9. *If (P, u, \mathcal{S}) is compatible, then we have*

$$\lim_{n \rightarrow \infty} \max_{1 \leq k \leq n} \|T(n, k)\|_{\infty} = 0.$$

PROOF. Note that

$$\begin{aligned} \|T(n, k)\|_{\infty} &= \|B^{-1}(n) \sum_{\varphi \in P(k)} u(\varphi) \varphi\|_{\infty} \\ &\leq p B^{-1}(n) \max_{\varphi \in P(k)} |u(\varphi)|. \end{aligned}$$

The lemma now follows from Definition 1.1(e).

PROOF OF THEOREM 3.6. We apply Theorem 3.4. Let $\Omega = G$, \mathcal{F} = the Borel σ -field of G , $\mu = m$ (Haar measure) and $X_{n,k} = T(n, k)$ for $k = 1, 2, \dots, n$. Condition (b) of Theorem 3.4 is satisfied by Lemma 3.7, condition (c) of Theorem 3.4 is equivalent to (b) of Lemma 3.8 with $r = 1$, while Lemma 3.9 ensures that condition (d) automatically holds. It follows that if (a) and (b) of Theorem 3.6 hold then $B(n)^{-1} S(n) = \sum_{k=1}^n T(n, k)$ converges to $N(0, 1)$ in distribution, that is, (P, u, \mathcal{S}) is Gaussian.

The principal theorem in this section follows.

THEOREM 3.10. *Suppose that (P, u, \mathcal{S}) is compatible. It follows that*

- (a) *if (P, \mathcal{S}) is weakly dissociate, then condition (a) of Theorem 3.6 is satisfied;*
and
- (b) *if (P, \mathcal{S}) is stable, then condition (b) of Theorem 3.6 is satisfied. Hence if (P, \mathcal{S}) is weakly dissociate and stable, then (P, u, \mathcal{S}) is Gaussian.*

PROOF OF (a). Expanding we obtain

$$\begin{aligned} T(n)(t) &= \prod_{j=1}^n (1 + itT(n, j)) \\ &= \sum_{k=0}^n \sum (it)^k \prod_{j=1}^k u(\varphi_j) \prod_{j=1}^k \varphi_j B(n)^{-k}, \end{aligned}$$

where the inner summation is taken over all subsets $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$ of $Q(n)$ having the property that each set $P(j)$ contains at most one element of $\{\varphi_1, \varphi_2, \dots, \varphi_k\}$. For $R(k)$ as in Definition 3.1. we obtain, using the orthogonality relations,

$$\left| \int_G T(n)(t) dm - 1 \right| \leq \sum_{k=1}^n |t|^k B^{-k}(n) \max_{\varphi \in Q(n)} |u(\varphi)|^k R(k).$$

Let $\alpha_n = B^{-1}(n) \max_{\varphi \in Q(n)} |u(\varphi)|$ and $R = \sup_k R^{1/k}(k)$. Noting that $\alpha_n \rightarrow 0$ as $n \rightarrow \infty$ (see Definition 1.1(e)), we have for all n such that $|t|\alpha_n R < \frac{1}{2}$ the estimate:

$$\begin{aligned} \left| \int_G T(n)(t) dm - 1 \right| &\leq |t|\alpha_n R \sum_{k=0}^{\infty} (|t|\alpha_n R)^k \\ &\leq 2|t|\alpha_n R. \end{aligned}$$

It follows that $\lim_{n \rightarrow \infty} \int_G T(n)(t) dm = 1$ as desired.

PROOF OF (b). Recalling the expression for $F(\psi)$, $\psi \in \Gamma$ given in Definition 3.2, we have

$$\begin{aligned} \sum_{k=1}^n B^2(n) T^2(n, k) &= \sum_{k=1}^n \sum_{\varphi, \gamma \in P(k)} u(\varphi) u(\gamma) \varphi \gamma \\ &= \sum_{k=1}^n \sum_{\psi \in \Gamma} \sum_{\varphi \in F(\psi) \cap P(k)} u(\varphi) u(\psi \gamma^{-1}) \psi \\ &= \sum_{\psi \in \Gamma} \sum_{\varphi \in F(\psi) \cap Q(n)} u(\varphi) u(\psi \varphi^{-1}) \psi \\ &= \sum_{\varphi \in Q(n)} |u(\varphi)|^2 + \sum_{\psi \in \Gamma - \{1\}} \sum_{\varphi \in F(\psi) \cap Q(n)} u(\varphi) u(\psi \varphi^{-1}) \psi. \end{aligned}$$

Since $B^2(n) = \sum_{\varphi \in Q(n)} |u(\varphi)|^2$, we conclude that

$$\int_G \left(\sum_{k=1}^n T^2(n, k) \right)^2 dm = 1 + B^{-4}(n) \sum_{\psi \in \Gamma - \{1\}} \left| \sum_{\varphi \in F(\psi) \cap Q(n)} u(\varphi) u(\psi \varphi^{-1}) \right|^2.$$

We note that if $\varphi \in F(\psi) \cap Q(n)$, then $\psi \varphi^{-1} \in F(\psi) \cap Q(n)$. Using Definition 3.2, Hölder's inequality and the estimate $|u(\varphi) u(\psi \varphi^{-1})| \leq |u(\varphi)|^2 + |u(\psi \varphi^{-1})|^2$, we obtain

$$\begin{aligned} \left| \int_G \left(\sum_{k=1}^n T^2(n, k) \right)^2 dm - 1 \right| &\leq B^{-4}(n) \sum_{\psi \in \Gamma - \{1\}} \left(2 \sum_{\varphi \in F(\psi) \cap Q(n)} |u(\varphi)|^2 \right)^2 \\ &\leq 4 \cdot CB^{-4}(n) \sum_{\psi \in \Gamma - \{1\}} \sum_{\varphi \in F(\psi) \cap Q(n)} |u(\varphi)|^4. \end{aligned}$$

Now if $\varphi \in P(k) \cap F(\psi)$ for some k , then $\varphi \in \psi P(k)$ and hence $\psi \in \varphi P(k)$. It follows that for each $\varphi \in Q(n)$, the term $|u(\varphi)|^4$ appears at most p times in the double summation above where $P = \max |P(k)|$. We deduce that

$$\left| \int_G \left(\sum_{k=1}^n T^2(n, k) \right)^2 dm - 1 \right| \leq 4p \cdot CB^{-4}(n) \sum_{\varphi \in Q(n)} |u(\varphi)|^4$$

$$\leq 4p \cdot CB^{-2}(n) \max_{\varphi \in Q(n)} |u(\varphi)|^2.$$

The convergence of the right side of the above inequality follows from Definition 1.1(e).

4. Applications to the circle group

In this section, we consider the circle group $G = T$ which we represent as the interval $[0, 2\pi)$ with addition modulo 2π . Haar measure is $(2\pi)^{-1}$ times Lebesgue measure while the character group Γ is Z , the additive group of integers, where for each $n \in Z$ we associate the character $e_n: t \rightarrow \exp(\text{int})$. The lacunary sets we consider are defined as follows.

DEFINITION 4.1. Let $P = \{n_k: k \in N\}$ be an infinite subset of N such that $n_{k+1} > n_k$ for each k and let $q = \inf \{n_{k+1} n_k^{-1}: k \in N\}$. We say that P is a q -set. If P is a q -set for $q > 1$, then P is called a *Hadamard set*.

Salem and Zygmund (1947, 1948) proved the following theorem.

THEOREM 4.2. *Let P be a Hadamard set and let $\mathcal{S} = \{-n, n\}_{n=1}^\infty$. If (P, u, \mathcal{S}) is compatible, then it is Gaussian.*

We not only derive this theorem from our results but prove a stronger version. As a preliminary, we formulate:

DEFINITION 4.3. We say that a sequence $\{r_k\}$ of positive integers *increases rapidly* if, for all $n, r_{n+1} > \sum_{k=1}^n r_k$. We say that a sequence $\mathcal{S} = \{X(n)\}_{n=1}^\infty$ (of finite, symmetric, pairwise disjoint subsets of Z) is *dissociate* if there exists a sequence $\{r_k\}_{k=1}^\infty$ of positive integers and an injection $\theta: N \rightarrow N$ such that $\{r_k\}$ increases rapidly and

$$\sum_{k=1}^{\theta(n)-1} r_k < |m| \leq r_{\theta(n)} \quad \text{for all } m \in X(n).$$

The relationship between the concept of dissociativity given above and that which appears in Definition 3.1 is described in the following theorem.

THEOREM 4.4. *If \mathcal{S} is dissociate and (P, \mathcal{S}) is compatible, then (P, \mathcal{S}) is strongly dissociate.*

PROOF. Suppose that \mathcal{S} is defined with respect to a rapidly increasing sequence $\{r_k\}_{k=1}^\infty$. It is readily seen that a sum of the form

$$\sum_{j=1}^m \varepsilon_j n_j \quad \text{where} \quad \sum_{k=1}^{j-1} r_k < n_j \leq r_j, \quad \varepsilon_j \in \{-1, 0, 1\} \quad \text{and} \quad \varepsilon_m = 1$$

is greater than or equal to $n_m - \sum_{k=1}^{m-1} r_k$ and hence is nonzero. It follows that (P, \mathcal{S}) is strongly dissociate.

In considering Hadamard sets, it will prove useful to consider dissociate sequences \mathcal{S} of a certain form. By way of notation, we write $I[n, m]$ where $1 \leq n \leq m$ for the set

$$I[n, m] = \{r \in Z: n \leq |r| \leq m\}.$$

We call $I[n, m]$ an interval, n the lower end point of the interval and m the upper end point.

THEOREM 4.5. Suppose that $\mathcal{S} = \{X(n)\}_{n=1}^\infty$ is a sequence such that each $X(n)$ is contained in an interval I_n and $I_n \cap I_m = \emptyset$ for $n \neq m$. Let $\{\alpha_k\}_{k=1}^\infty$ be the sequence of lower end points of I_n arranged in increasing order and $\{\beta_k\}_{k=1}^\infty$ the corresponding sequence of upper end points. Suppose that

$$\alpha = \inf \alpha_{k+1} \beta_k^{-1} > 1 \quad \text{and} \quad \inf \beta_{k+1} \beta_k^{-1} \geq \alpha(\alpha - 1)^{-1}.$$

Then \mathcal{S} is a dissociate sequence.

(Hereafter such sequences will be described as sequences of type α .)

PROOF. Let $\beta = \alpha(\alpha - 1)^{-1}$. An easy argument shows that $\beta_j \leq \beta^{j-k} \beta_k$ for $j \leq k$ and a further computation shows that $\sum_{j=1}^k \beta_j < \alpha \beta_k \leq \alpha_{k+1} \leq \beta_{k+1}$. It follows that $\{\beta_j\}_{j=1}^\infty$ increases rapidly and hence \mathcal{S} is dissociate.

We need one more concept before the connection between Hadamard sets and dissociate sequences can be described.

DEFINITION 4.6. A segment of a sequence $\{n_k\}_{k=1}^\infty$ is a finite subsequence of the form n_k, n_{k+1}, \dots, n_j for some $1 \leq k \leq j$. For $t \in N$, we say that a rearrangement $\{m_j\}$ of $\{n_k\}$ is t -related to $\{n_k\}$ if each n_k belongs to a sequence of t elements which is a segment of $\{m_j\}$ and of $\{n_j\}$.

COMMENTS 4.7

(a) Except when $t = 1$, the t -relation is not an equivalence relation since transitivity fails to hold.

(b) Every rearrangement of $\{n_k\}$ is 1-related to $\{n_k\}$.

(c) If a rearrangement $\{m_j\}$ is $t + 1$ -related to $\{n_k\}$, then it is also t -related to $\{n_k\}$.

We have the following theorem.

THEOREM 4.8. Let $P = \{n_k: k \in N\}$ be a q -set for $q > 1$ and let t be the smallest positive integer such that $q^{t-1} \geq (q - 1)^{-1}$. Let $\{m_j\}$ be a rearrangement of $\{n_j\}$ which

is t -related to $\{n_j\}$. If \mathcal{S} is any sequence such that $P(j) = \{m_j, -m_j\}$ for all j , then there exists a sequence \mathcal{S}_1 of type α for some $\alpha \geq q$ such that (P, \mathcal{S}) and (P, \mathcal{S}_1) are Gaussian equivalent (see Definition 2.1).

PROOF. For each $j \in N$, let $\gamma(j)$ be the largest integer not exceeding $2t$ such that $m_j, m_{j+1}, \dots, m_{j+\gamma(j)-1}$ is a segment of $\{n_k\}$. We define inductively a sequence $\{r(j)\}_{j=1}^\infty$ as follows. Let $r(1) = 0$. Having defined $r(j)$, we put

$$r(j+1) = \begin{cases} r(j) + t & \text{if } \gamma(r(j)+1) = 2t, \\ r(j) + \gamma(r(j)+1) & \text{if } \gamma(r(j)+1) < 2t. \end{cases}$$

It is clear that $r(j+1) - r(j) < 2t$. We now show that $\gamma(r(j)+1) \geq t$ for all j . Observe that since m_1 belongs to a sequence of length t which is a segment of $\{n_j\}$ and of $\{m_j\}$, we have $\gamma(r(1)+1) \geq t$. It is clear that if $\gamma(r(j)+1) = 2t$, then $\gamma(r(j+1)+1) = \gamma(r(j)+t+1) \geq t$. On the other hand, if $\gamma(r(j)+1) < 2t$, then since $r(j+1) = r(j) + \gamma(r(j)+1)$ it follows that $m_{r(j+1)}$ and $m_{r(j+1)+1}$ are not consecutive elements of the sequence $\{n_k\}$. Since $m_{r(j+1)+1}$ belongs to a sequence of length t which is a segment of $\{n_k\}$ and $\{m_k\}$, we conclude that $\gamma(r(j+1)+1) \geq t$. We have thus shown that $\gamma(r(j)+1) \geq t$ for all t and it follows that $r(j+1) - r(j) \geq t$.

Summarizing, we have a sequence $\{r(j)\}$ of nonnegative integers such that

- (i) $r(1) = 0$;
- (ii) $t \leq r(j+1) - r(j) < 2t$ for each j ;

and

- (iii) $m_{r(j)+1}, m_{r(j)+2}, \dots, m_{r(j+1)}$ is a segment of $\{n_k\}$ for each j .

We define $\mathcal{S}_1 = \{X_1(n)\}_{n=1}^\infty$ by setting $X_1(n) = I[m_{r(n)+1}, m_{r(n+1)}]$ for each n . Since \mathcal{S}_1 is P -coarser than \mathcal{S} (see Definition 2.2), the pairs (P, \mathcal{S}) and (P, \mathcal{S}_1) are Gaussian equivalent by Lemma 2.3(b)(ii). (Clearly (P, \mathcal{S}_1) is compatible.)

We conclude the proof by showing that \mathcal{S}_1 is a dissociate sequence of type α for some $\alpha \geq q$. Let $\{\alpha_j\}$ be the sequence of lower end points of the $X_1(n)$'s arranged in increasing order and let $\{\beta_j\}$ be the corresponding sequence of upper end points. Each $\alpha_j, \beta_j \in P$ and hence

$$\alpha = \inf \alpha_{k+1} \beta_k^{-1} \geq \inf n_{j+1} n_j^{-1} = q.$$

On the other hand, if $\beta_k = n_j$ for some j , then since $r(j+1) - r(j) \geq t$ we have $\{n_{j+1}, n_{j+2}, \dots, n_{j+t}\} \subseteq I[\alpha_{k+1}, \beta_{k+1}]$. Hence we have $\beta_{k+1} \geq n_{j+t}$ and it follows that

$$\begin{aligned} \beta_{k+1} \beta_k^{-1} &\geq n_{j+t} n_j^{-1} \\ &= (n_{j+t} n_{j+t-1}^{-1}) (n_{j+t-1} n_{j+t-2}^{-1}) \dots (n_{j+1} n_j^{-1}) \\ &\geq q^t \\ &> q(q-1)^{-1} \\ &\geq \alpha(\alpha-1)^{-1}. \end{aligned}$$

The theorem is proved.

To complete the preliminary theorems dealing with Hadamard sets, we show that a compatible pair (P, \mathcal{S}) is necessarily stable (see Definition 3.2) if P is a Hadamard set.

THEOREM 4.9. *Let P be a Hadamard set and suppose that (P, \mathcal{S}) is compatible. Then (P, \mathcal{S}) is stable.*

PROOF. Suppose that $P = \{n_k : k \in N\}$ is a q -set and let m be the smallest integer such that $q^m > 2(1 - q^{-1})^{-1}$. Given $n \in N$, we examine the set $D = \{k \in N : n_k + n_j = n \text{ or } n_k - n_j = n \text{ for some } j \leq k\}$. Note that if $n_k + n_j = n$ for some $j \leq k$, then we have

$$(4.1) \quad \frac{1}{2}n \leq n_k \leq n.$$

On the other hand, if $n_k - n_j = n$ for some $j \leq k$, then we have $n \leq n_k$ and $n_k - n_{k-1} \leq n$. Since $n_{k-1} n_k^{-1} \leq q^{-1}$, we have

$$(4.2) \quad n \leq n_k \leq (1 - q^{-1})^{-1} n.$$

Combining (4.1) and (4.2), we conclude that if $k \in D$, then

$$\frac{1}{2}n \leq n_k \leq (1 - q^{-1})^{-1} n.$$

Thus we see that if $k, k + j \in D$, then $n_{k+j} n_k^{-1} \leq 2(1 - q^{-1})^{-1}$. However, since P is a q -set, we have $n_{j+k} n_k^{-1} \geq q^j$ and consequently we have $q^j \leq 2(1 - q^{-1})^{-1}$ which implies that $j < m$. We conclude that D has at most m elements. Noting the definition of $F(n)$ given in Definition 3.2, we have for $n \in N$,

$$F(n) \subseteq \{n_k : n_k + n_j = n \text{ or } n_k - n_j = n \text{ for some } j\} \cup \{-n_k : n_j - n_k = n \text{ for some } j\}.$$

It follows that $|F(n)| \leq 2|D| \leq 2m$. Similarly we have $|F(-n)| \leq 2m$. The pair (P, \mathcal{S}) is therefore stable.

We now state and prove our major theorem in this section.

THEOREM 4.10. *Let $P = \{n_k : k \in N\}$ be a q -set for some $q > 1$ and let t be the least positive integer such that $q^{t-1} \geq (q - 1)^{-1}$. Let (P, u, \mathcal{S}) be a compatible triple such that for each j , $P(j) = \{-m_j, m_j\}$ where $\{m_j, j \in N\}$ is a t -related rearrangement of $\{n_k, k \in N\}$. Then the triple (P, u, \mathcal{S}) is Gaussian.*

PROOF. Theorem 4.8 guarantees the existence of a dissociate sequence \mathcal{S}_1 which is P -coarser than \mathcal{S} and such that (P, \mathcal{S}) and (P, \mathcal{S}_1) are Gaussian equivalent. By Lemma 2.3(b)(i), the triple (P, u, \mathcal{S}) is compatible. Applying Theorem 4.4 and Theorem 4.9, we deduce that (P, \mathcal{S}_1) is strongly dissociate and stable and hence (P, u, \mathcal{S}_1) is Gaussian by Theorem 3.10. Finally, we conclude that (P, u, \mathcal{S}) is Gaussian by Theorem 2.4.

COMMENTS 4.11

(a) Theorem 4.10 is an improvement on the classical result, Theorem 4.2. It asserts that Hadamard sets are ‘Gaussian’ in relation to sequences which are essentially different from the ‘natural’ sequence $\mathcal{S} = \{-n, n\}$. This is not an obvious result since the Hadamard condition is defined in terms of the order property of N which is specified by the sequence \mathcal{S} .

(b) We are unable to find an example of a Hadamard set P and a sequence \mathcal{S} such that (P, u, \mathcal{S}) is compatible but not Gaussian for some function u .

(c) If P is a q -set for some $q \geq 2$, then $t = 1$ in Theorem 4.10 and hence Theorem 4.10 and Comment 4.7(b) combine to show that (P, u, \mathcal{S}) is Gaussian whenever (P, u, \mathcal{S}) is compatible. In the next section, we show that this result is a corollary to a more general result.

5. Applications to an arbitrary compact abelian group

We return to the setting of an arbitrary compact abelian group G and begin with the definition of some lacunary properties.

DEFINITION 5.1. We say that a subset P_1 of a set of characters P is *asymmetric* if $\varphi, \varphi^{-1} \in P_1$ implies that $\varphi = \varphi^{-1}$. Given $P \subseteq \Gamma$, let P_1 be a maximal asymmetric subset of P . For $n \in N$, we let

$$R(n) = |\{\delta: P_1 \rightarrow \{-1, 0, 1\}: \sum_{\delta \in P_1} |\delta(\varphi)| = n, \prod_{\varphi \in P_1} \varphi^{\delta(\varphi)} = 1\}|.$$

(Note that since a maximal asymmetric subset P_1 of P is any subset such that exactly one of φ and φ^{-1} belongs to P_1 for each $\varphi \in P$, the number $R(n)$ is independent of the particular maximal asymmetric subset P_1 chosen.) We say that P is a *Rider set* if $R(n) \leq B^n$ for some $B > 0$ and all n . In particular, we say that P is a *1-dissociate set* if $R(n) = 0$ for all n . (See Remarks 3.3(b).)

REMARKS 5.2. Rider sets were studied firstly by Steckin (1956) and later by Rider (1966) as well as by other authors. They are important in the study of Sidon sets. Sets which are the finite unions of Rider sets are Sidon sets. The converse of this last statement is so far as the authors are aware an open problem. See López and Ross (1975), p. 17 and p. 24 for further details.

The following theorem which is easily proved pinpoints the relevance of Rider sets to the Gaussian property.

THEOREM 5.3. *Let $P \subseteq \Gamma$. The following properties are equivalent:*

- (a) P is a Rider (1-dissociate) set;
- (b) (P, \mathcal{S}) is weakly (strongly) dissociate whenever (P, \mathcal{S}) is compatible; and

(c) (P, \mathcal{S}) is weakly (strongly) dissociate whenever \mathcal{S} is a P -basic sequence and (P, \mathcal{S}) is compatible.

In the following theorem we summarize some well-known results dealing with the relationship between Hadamard sets and dissociate sets.

THEOREM 5.4. *Let $G = T, \Gamma = Z$.*

- (a) *For $q \geq 2$, each q -set is a 1-dissociate set.*
- (b) *Each Hadamard set is the finite union of 1-dissociate sets.*
- (c) *There exists a 1-dissociate subset of Z which is not the finite union of Hadamard sets.*

PROOF

(a) Suppose that $P = \{n_k : k \in N\}$ is a q -set for some $q \geq 2$. For $j \leq k$, we have $n_j \leq q^{j-k} n_k \leq 2^{j-k} n_k$. For $\varepsilon_j \in \{-1, 0, 1\}, j = 1, 2, \dots, k$, we have

$$\begin{aligned} n_{k+1} + \sum_{j=1}^k \varepsilon_j n_j &\geq n_{k+1} - \sum_{j=1}^k n_j \\ &\geq n_{k+1} \left(1 - \sum_{j=1}^k 2^{-(k+1-j)} \right) \\ &> 0. \end{aligned}$$

We conclude that P is 1-dissociate.

(b) For $m \in N$, we write $P = \bigcup_{j=0}^{m-1} P_j$ where $P_j = \{n_{km-j} : k \in N\}$. We readily check that each P_j is an α_j -set for some $\alpha_j \geq q^m$. Choose m such that $q^m \geq 2$.

(c) An example of a 1-dissociate set which is not the finite union of Hadamard sets is the set $\{2^n + 2^{m^2} : n, m \in N \text{ and } (m-1)^2 \leq n < m^2\}$. The example is due to Hewitt and Zuckerman (1959) and is discussed in López and Ross (1975), p. 25.

Theorem 3.10 and Theorem 5.3 combine to show that a compatible triple (P, u, \mathcal{S}) is Gaussian where P is a Rider set if the pair (P, \mathcal{S}) is stable. If (P, \mathcal{S}) is compatible, then \mathcal{S} is P -coarser than a P -basic sequence \mathcal{S}_1 by Lemma 2.3(a). Since (P, \mathcal{S}) and (P, \mathcal{S}_1) are Gaussian equivalent by Lemma 2.3(b)(ii), (P, u, \mathcal{S}) will be Gaussian if (P, u, \mathcal{S}_1) is Gaussian by Theorem 2.4. On the other hand, by reference to Definition 3.2, we note that (P, \mathcal{S}_1) is stable if (P, \mathcal{S}) is stable. It follows that we can restrict our attention to deriving a condition for a compatible pair (P, \mathcal{S}) to be stable given that \mathcal{S} is a P -basic sequence.

For \mathcal{S} a P -basic sequence and $P(n) \neq \emptyset$, we write $P(n) = \{\varphi_n\} \cup \{\varphi_n^{-1}\}$. It will be seen that characters of order two play a special role in our results. We write $\Delta = \{\varphi \in \Gamma : \varphi^2 = 1\}$. For $\gamma \in \Gamma - \{1\}$, we derive

$$F(\gamma) = \{\varphi_k : \varphi_k^2 = \gamma\} \cup \{\varphi_k^{-1} : \varphi_k^{-2} = \gamma\}.$$

It is clear that $F(\gamma)$ is empty unless $\gamma = \varphi^2$ for some $\varphi \in \Gamma$. If $\varphi \in \Gamma$ and $\varphi^2 \neq 1$, we have

$$\begin{aligned} F(\varphi^2) &= \{\varphi_k : \varphi_k^2 = \varphi^2\} \cup \{\varphi_k^{-1} : \varphi_k^{-2} = \varphi^2\} \\ &= \{\varphi_k : \varphi_k \varphi^{-1} \in \Delta\} \cup \{\varphi_k^{-1} : \varphi_k^{-1} \varphi^{-1} \in \Delta\} \\ &= \bigcup_{n=1}^{\infty} P(n) \cap \varphi \Delta. \end{aligned}$$

The above argument yields:

THEOREM 5.5. *Let P be a Rider set and (P, u, \mathcal{S}) a compatible triple. Then (P, u, \mathcal{S}) is Gaussian if there exists $m \in \mathbb{N}$ such that $\bigcup_{n=1}^{\infty} P(n) \cap \varphi \Delta$ has at most m elements for each $\varphi \in \Gamma - \Delta$.*

We have the following slightly more general form of the above theorem.

THEOREM 5.6. *Let P be a Rider set and suppose that there exists $m \in \mathbb{N}$ such that $|P \cap \varphi \Delta| \leq m$ for all $\varphi \in \Gamma - \Delta$. Then each compatible triple (P, u, \mathcal{S}) is Gaussian.*

As a corollary we deduce:

COROLLARY 5.7. *If G is connected and P a Rider set, then each compatible triple (P, u, \mathcal{S}) is Gaussian.*

We suspect that the converse to Theorem 5.6 is true. Such a converse states that if P is a Rider set such that $\{|P \cap \varphi \Delta| : \varphi \in \Gamma - \Delta\}$ is unbounded, then some compatible triple (P, u, \mathcal{S}) is not Gaussian. The following is a partial converse.

THEOREM 5.8. *Let P be a Rider set and suppose that $P \cap \varphi \Delta$ is infinite for some $\varphi \in \Gamma - \Delta$. Then some compatible triple (P, u, \mathcal{S}) is not Gaussian.*

PROOF. Note that at most one element of the form φ^k for $k \in \mathbb{N}$ can belong to Δ . Using the fact that $\varphi^{-1} P \cap \Delta$ is infinite and an easy induction argument, we construct a sequence $\{\gamma_j\}_{j=1}^{\infty}$ of elements of $\varphi^{-1} P \cap \Delta$ such that for each k and each choice of $\varepsilon_j = 0$ or 1 we have that

$$\varphi^n \prod_{j=1}^k \gamma_j^{\varepsilon_j} = 1 \quad \text{implies that } \varepsilon_1 = \varepsilon_2 = \dots \varepsilon_k = 0 \quad \text{and} \quad \varphi^n = 1.$$

Let u be the function mapping each element in $P \cup P^{-1}$ onto 1 and let $\mathcal{S} = \{\{\varphi \gamma_j, \varphi^{-1} \gamma_j\}\}_{j=1}^{\infty}$. We apply Theorem 3.5 for $\Omega = G$, \mathcal{F} = the Borel σ -algebra of G , $\mu = m$ (Haar measure) and where for $j = 1, 2, \dots, n$,

$$\begin{aligned} X_{n,j} &= T(n, j) \\ &= B^{-1}(n) (S(j) - S(j-1)) \\ &= (2n)^{-\frac{1}{2}} \gamma_j (\varphi + \varphi^{-1}). \end{aligned}$$

We note that

$$\sum_{j=1}^n X_{n,j}^2 = \frac{1}{2}(\varphi + \varphi^{-1})^2 = X$$

in the notation of Theorem 3.5.

Observe that by choice of the sequence $\{\gamma_{jj}\}$, we can write

$$\begin{aligned} T_n &= \prod_{j=1}^n (1 + itX_{n,j}) \\ &= 1 + R, \end{aligned}$$

where R is a linear combination of characters distinct from φ^n for $n \in \mathbb{Z}$. Hence we have, in particular,

$$\int_G T_n X^k dm = \int X^k dm \quad \text{for all } k \in \mathbb{N}.$$

Since $\exp(-tX)$ is the uniform limit of its power series, we deduce that

$$\int_G T_n \exp(-tX) dm = \int_G \exp(-tX) dm.$$

Condition (a') of Theorem 3.5 is satisfied and hence (P, u, \mathcal{S}) is not Gaussian.

COMMENTS 5.9

(a) Theorem 5.6 is a significant improvement on Theorem 3.1 of Dudley (1975). As an example, consider $G = \prod_{j=1}^{\infty} G_j$ where each G_j is the multiplicative group $\{1, -1, i, -i\}$. Let φ_j be the character mapping an element of G onto its j th component. The set $P = \{\varphi_j \varphi_{j+1}^2, \varphi_j : j \in \mathbb{N}\}$ does not have property (R_2) (see Definition 2.1 of Dudley (1975)) since $(\varphi_j \varphi_{j+1}^2)^2 \varphi_j^{-2} = 1$. However, P is a 1-dissociate set and $|P \cap \varphi \Delta| \leq 2$ for all $\varphi \in \Gamma - \Delta$.

(b) Theorem 5.4(a) and Corollary 5.7 combine to show that if $P \subseteq \mathbb{Z}$ is a q -set for some $q \geq 2$, then each compatible triple (P, u, \mathcal{S}) is Gaussian. (See Comments 4.11(c).)

References

R. C. Baker (1972), 'On Wiener's theorem on Fourier Stieltjes coefficients and the Gaussian law', *Proc. London Math. Soc.* (3) **25**, 525–542.
 E. Dudley (1975), 'The Gaussian law and the law of the iterated logarithm for lacunary sets of characters', *Trans. Amer. Math. Soc.* **214**, 187–214.
 E. Hewitt and H. S. Zuckerman (1959), 'Some theorems on lacunary Fourier series with extensions to compact groups', *Trans. Amer. Math. Soc.* **93**, 1–19.
 J. M. López and K. A. Ross (1975), *Sidon sets* (Lecture notes in pure and applied mathematics 13, Marcel Dekker, New York).

- D. L. McLeish (1974), 'Dependent central limit theorems and invariance principles', *Ann. Prob.* (4) **2**, 620–628.
- D. G. Rider (1966), 'Gap series on groups and spheres', *Canad. J. Math.* **18**, 389–398.
- W. Rudin (1960), *Fourier analysis on groups* (Interscience tracts in pure and applied mathematics 12, Interscience Publishers, New York).
- R. Salem and A. Zygmund (1947), 'On lacunary trigonometric series I', *Proc. Nat. Acad. Sci. U.S.A.* **33**, 333–338.
- R. Salem and A. Zygmund (1948), 'On lacunary trigonometric series II', *Proc. Nat. Acad. Sci. U.S.A.* **34**, 54–62.
- S. B. Steckin (1956), 'On absolute convergence of Fourier series', *Izv. Akad. Nauk SSSR Ser. Mat.* **20**, 385–412 (in Russian).

Department of Mathematics
University of Melbourne
Parkville, Victoria 3052
Australia

Author's current address:
28 Burdekin Street
Duffy, A.C.T. 2611
Australia

Department of Statistics
University of Melbourne
Parkville, Victoria 3052
Australia

Author's current address:
Department of Statistics, S.G.S.
Australian National University
P.O. Box 4, Canberra
A.C.T. 2600, Australia