ILLINOIS JOURNAL OF MATHEMATICS
Volume 23, Number 2, June 1979

A RUDIN-SHAPIRO TYPE THEOREM

BY
T. W. KÖRNER

0. Introduction

Let $P_n(t) = \sum_{r=1}^{n} a_r \exp ik(r)t$ be a trigonometric polynomial with $\sum_{r=1}^{n} |a_r| = 1$. General considerations show that $\sup |P_n(t)| \geq n^{-1/2}$. Direct constructions, of which the most powerful is due to Rudin and Shapiro show that we can find a constant B and polynomials $P_1, P_2, \ldots$ with $\sup |P_n(t)| \leq Bn^{-1/2}$. On the other hand the standard probabilistic constructions only give the existence of polynomials P_n with $\sup |P_n(t)| \leq Bn^{-1/2}(\log n)^{1/2}$ for some.

The natural extension to general locally compact Abelian groups G is to ask what we can say about $\sup_{\chi \in \hat{G}} |\hat{\mu}_n(\chi)|$ if μ is a measure on G with $\|\mu\| = 1$ and supp μ consisting of n points or less. In general we cannot say much, unless G is a finite Abelian group and we have bounds on the number of elements of G. This problem was investigated by Varopoulos and by Kaufman. In the first section we give an exposition of Kaufman's elegant probabilistic method and show that it gives considerably better results than the author claims. Typically, we can show that there exists a constant B such that for each $n \geq 1$ we can find $a_1, a_2, \ldots, a_n \in \mathbf{R}$ with

$$\sum_{r=1}^{n} |a_r| = 1 \quad \text{and} \quad \left| \sum_{r=1}^{n} a_r \omega^r \right| \leq Bn^{-1/2}(\log n)^{1/2}$$

whenever ω is an n-th root of unity.

We give a very detailed description of this method, since in Section 3 we modify it to obtain, again by probabilistic means, improved results in which the $(\log n)^{1/2}$ factor is removed. Thus we can find a constant B such that for each $n \geq 1$ we can find $a_1, a_2, \ldots, a_n \in \mathbf{R}$ with

$$\sum_{r=1}^{n} |a_r| = 1 \quad \text{and} \quad \left| \sum_{r=1}^{n} a_r \omega^r \right| \leq Bn^{-1/2}$$

whenever ω is an n-th root of unity. It is easy to deduce (as we do at the end of Section 2) the result stated in the last but one sentence of the first paragraph.

That this result can indeed be obtained by probabilistic means is perhaps the main point of interest for the general reader, but my purpose in writing

Received September 9, 1977.

this paper was to investigate a more technical but closely related question. How well can the Fourier transform of a function of "relatively small" support imitate the Fourier transform of Haar measure? For finite Abelian groups we obtain Theorem 2.3B which I believe to be new. In the remainder of the paper (Sections 4 and 5) we use this result to obtain, in Theorem 5.1, an improvement (in some cases) of a theorem of Salem.

1. A result of Kaufman

In a short and elegant note [4] which furnishes the inspiration for this paper, Kaufman proved, by probabilistic means, the following result which simplifies and unifies certain earlier work of Varopoulos.

THEOREM 1.1 (Kaufman) *For each $\varepsilon > 0$ there exists an $M(\varepsilon)$ such that any finite Abelian group G of order greater than $M(\varepsilon)$ contains a subset S with the properties:*

(1) $\log |S| \leq \varepsilon \log |G|$;
(2) $|\sum_{s\in S} \chi(s)| < \varepsilon\, |S|$ *for any character* $\chi \neq 1$ *of* G.

(Here $|S| = \text{card}\, S$, the number of elements of S).

However, it is possible to obtain, using ideas already implicit in his construction, a somewhat sharper result.

THEOREM 1.2. (i). *For each $\varepsilon > 0$ there exists an $M(\varepsilon)$ such that any finite Abelian group G of order greater than $M(\varepsilon)$ contains a subset S with the properties:*

(1) $|S| \leq 40\varepsilon^{-2} \log |G|$
(2) $|\sum_{s\in S} \chi(s)| \leq \varepsilon\, |S|$ *for any character* $\chi \neq 1$ *of* G.

The condition $|G| > M(\varepsilon)$ is troublesome, if we wish ε to depend on $|G|$ itself. In the second section we shall consider the following version of the theorem in which the condition $|G| > M(\varepsilon)$ is omitted at the expense of weakening condition (2).

THEOREM 1.2 (ii). *Let G be a finite Abelian group. Then for every $1 > \varepsilon > 0$ we can find a $\mu \in M^+(G)$ with $\|\mu\| = 1$ such that:*

(1) $|\text{supp}\, \mu| \leq 40\, \varepsilon^{-2} \log |G|$;
(2) $|\hat{\mu}(\chi)| \leq \varepsilon$ *for any character* $\chi \neq 1$ *of* G.

The idea of Kaufman's proof is the following. Let G be an Abelian group of order m and let S be a finite subset of G chosen at random. More precisely, let $S = \{X_1, X_2, \ldots, X_k\}$ where the X_j are independent random variables with uniform distribution on G. We want to estimate

$$\Pr(|\textstyle\sum_{s\in S} \chi(s)| < \lambda)$$

for some particular $1 \neq \chi \in G$.

Observe that χ maps G on to the multiplicative group Γ_r of r-th roots of unity for some $1<r\leq m$. Let ω be a primitive r-th root of unity. Then $\chi^{-1}(1)$ is a subgroup of G with cosets $\chi^{-1}(\omega), \chi^{-1}(\omega^2), \ldots, \chi^{-1}(\omega^{r-1})$. In particular the $\chi(X_j)$ are independent random variables with uniform distribution on Γ_r.

We now diverge very slightly from Kaufmen's proof. Consider $Y_k = \sum_{j=1}^{k} \chi(X_j)$. We can consider Y_k as performing a random walk on the plane $\mathbf{C}$. But for this kind of random walk we know that the probability density of $k^{-1/2}\,|Y_k|$ tends very rapidly and in a very strong sense to that of a normal distribution. This convergence to a density which falls away very rapidly towards infinity enables us to place very good bounds on $\Pr(|\sum_{s\in S}\chi(s)|<\lambda)$ and thus to prove our theorem.

For our purposes it suffices to show that Y_k is sub-Gaussian. The following simple proof goes back to S. Bernstein.

LEMMA 1.3. (i) *Let X be a random variable in* $\mathbf{C}$ *such that* $\Pr(|X|\leq\sigma)=1$ *for some* $\sigma\geq 0$ *and* $\mathscr{E}X^m=0$ *whenever* m *is odd. Then*

$$\mathscr{E}\exp(\lambda \operatorname{Re} X)\leq \exp\sigma^2\lambda^2 \quad \textit{for all } \lambda\geq 0.$$

(ii) *Let* $X_1, X_2, \ldots, X_n$ *be independent random variables in* $\mathbf{C}$ *with* $\Pr(|X_j|\leq\sigma_j)=1$ *for some* $\sigma_j\geq 0$ *and* $\mathscr{E}X^{2n+1}=0$. *Then, writing* $\sigma^2=\sum_{j=1}^{n}\sigma_j^2$, *we have* $\Pr(|\sum_{j=1}^{n} v_j|\geq 4\exp(-\tau^2/6\sigma^2)$ *for all* $\tau\geq 0$.

Proof. (i) We have

$$\begin{aligned}\mathscr{E}\exp\lambda \operatorname{Re} X &= \mathscr{E}\left(1+\lambda \operatorname{Re} X+\frac{\lambda^2(\operatorname{Re} X)^2}{2!}+\cdots\right)\\ &= 1+\frac{\lambda^2\mathscr{E}(\operatorname{Re} X)^2}{2!}+\frac{\lambda^3\mathscr{E}(\operatorname{Re} X)^3}{3!}+\cdots\\ &\leq 1+\frac{\lambda^2\sigma^2}{2!}+\frac{\lambda^3\sigma^3}{3!}+\cdots\\ &\leq 1+\frac{\lambda^2\sigma^2}{1!}+\frac{\lambda^4\sigma^2}{2!}+\cdots\\ &= \exp\lambda^2\sigma^2.\end{aligned}$$

(ii) Since $X_1, X_2, \ldots$ are independent, we have

$$\begin{aligned}\mathscr{E}\exp\left(\lambda \operatorname{Re}\sum_{j=1}^{n} X_j\right) &= \mathscr{E}\left(\prod_{j=1}^{n}\exp\lambda \operatorname{Re} X_j\right)\\ &= \prod_{j=1}^{n}\mathscr{E}\exp\lambda \operatorname{Re} X_j\\ &\leq \exp\lambda^2\sigma^2.\end{aligned}$$

Thus

$$\Pr\left(\operatorname{Re}\sum_{j=1}^{n} X_j \geq \tau 2^{-1/2}\right) = \Pr\left(\exp\left(\lambda \operatorname{Re}\sum_{j=1}^{n} X_j\right) \geq \exp(\tau 2^{-1/2})\right)$$

$$\leq \mathscr{E}\exp\left(\lambda \operatorname{Re}\sum_{j=1}^{n} X_j\right)\left(\exp(\lambda\tau 2^{-1/2})\right)^{-1}$$

$$\leq \exp(\lambda^2\sigma^2 - \lambda 2^{-1/2}\tau)$$

so, setting $\lambda = 2^{-3/2}\,\tau/\sigma^2$ we have

$$\Pr\left(\operatorname{Re}\sum_{j=1}^{n} X_j \geq \tau 2^{-1/2}\right) \leq \exp(-\tau^2/8\sigma^2).$$

Similarly

$$\Pr\left(\operatorname{Re}\sum_{j=1}^{n} X_j \leq -\tau 2^{-1/2}\right) \leq \exp(-\tau^2/8\sigma^2),$$

$$\Pr\left(\operatorname{Im}\sum_{j=1}^{n} X_j \geq \tau 2^{-1/2}\right) \leq \exp(-\tau^2/8\sigma^2) \quad \text{and} \quad \Pr\left(\operatorname{Im}\sum_{j=1}^{n} X_j \leq -\tau 2^{-1/2}\right) \leq \exp(-\tau^2/8\sigma^2).$$

and the result follows.

Remark. A little thought shows that we can improve the inequalities above to obtain, for example, $\Pr(|\sum_{j=1}^{n} X_j| \geq \tau) \leq 2\exp(-\tau^2/4\sigma^2)$, but we do not need such fine estimates.

We can now complete the proof of Theorem 1.2.

Proof of (ii). Let $X_1, X_2, \ldots, X_n$ be chosen randomly as described in our preliminary discussion. We know that if $1 \neq \chi \in \hat{G}$ then $\Pr(|\chi(X_j)| = 1) = 1$ and $\mathscr{E}\chi(X_j)^m = 0$ whenever m is odd $(1 \leq j \leq n)$. We also know that the $\chi(X_j)$ are independent. Thus by Lemma 1.3,

$$\Pr\left(\left|\sum_{j=1}^{n} \chi(X_j)\right| \geq \varepsilon n\right) \leq 4\exp(-\varepsilon^2 n^2/8n) = 4\exp(-\varepsilon^2 n/8)$$

whenever $\chi \neq 1$ and so

$$\Pr\left(\left|\sum_{j=1}^{n} \chi(X_j)\right| \geq \varepsilon n \text{ for some } 1 \neq \chi \in \hat{G}\right) \leq 4(|\hat{G}| - 1)\exp(-\varepsilon^2 n/8).$$

Since $|G| = |\hat{G}|$ it follows that

$$\Pr\left(\left|\sum_{j=1}^{n} \chi(X_j)\right| \leq \varepsilon n \quad \text{for all} \quad 1 \neq \chi \in \hat{G}\right) \geq 1/2$$

provided only that $n \geq 20\,\varepsilon^{-2}\log|G|$.

Now there must exist a particular instance of an event with non-zero probability, so, in particular, we can find $x(1), x(2), \ldots, x(n) \in G$ with $|\sum_{j=1}^{n} \chi(x(j))| \leq \varepsilon n$. Setting $\mu = n^{-1} \sum_{j=1}^{n} \delta_{x(j)}$ we obtain a measure satisfying the conclusions of Theorem 1.2(ii).

Proof of (i). Again we take $X_1, X_2, \ldots, X_n$ as in the preliminary discussion. Then

$$\begin{aligned}
&\Pr(X_1, X_2, \ldots, X_n \text{ distinct})\\
&\quad = \prod_{j=1}^{n} \Pr(X_j \neq X_i \text{ for } 1 \leq i \leq j-1 \text{ given that } X_1, X_2, \ldots, X_{j-1} \text{ are distinct})\\
&\quad = \prod_{j=1}^{n} (1-(j-1)/|G|)\\
&\quad \geq \prod_{j=1}^{n} \exp(-2(j-1)/|G|)\\
&\quad = \exp\left(-\sum_{j=1}^{n} 2(j-1)/|G|\right)\\
&\quad = \exp(-n(n-1)/|G|)\\
&\quad \geq 3/4
\end{aligned}$$

provided only that $n^2 \leq |G|/10$.

Now suppose that $|G| \geq M(\varepsilon) = 10^4 \exp \varepsilon^{-2}$. Then

$$(|G|/10)^{1/2} \geq 40\varepsilon^{-2} \log |G|$$

and we can find an integer n with $40\,\varepsilon^{-2} \log |G| \geq n \geq 20\varepsilon^{-2} \log |G|$. For this particular n we know by the estimate of the previous paragraph and the estimate

$$\Pr\left(\left|\sum_{j=1}^{n} \chi(X_j)\right| \leq \varepsilon n \quad \text{for all} \quad 1 \neq \chi \in \hat{G}\right) \geq 1/2$$

obtained in the proof of (ii) that

$$\Pr\left(X_1, X_2, \ldots, X_n \text{ distinct and } \left|\sum_{j=1}^{n} \chi(X_j)\right| \leq \varepsilon n \text{ for all } 1 \neq \chi \in \hat{G}\right) \geq 1/4.$$

Since there must exist a particular instance of an event with non zero probability, it follows that we can find distinct $x(1), x(2), \ldots, x(n) \in G$ with $|\sum_{j=1}^{n} \chi(x(j))| \leq \varepsilon n$. Setting $S = \{x(j): 1 \leq J \leq n\}$ we obtain a set satisfying the conclusions of Theorem 1.2(i).

2. A Rudin Shapiro type theorem

If we take $G = \Gamma_n$ where Γ_n is the multiplicative group of n-*th* roots of unity, we may rewrite Theorem 1.2(ii) in the following form.

LEMMA 2.1. *Let $n \geq 1$, $1 > \varepsilon > 0$ be given. Then we can find a $\mu \in M^+(\Gamma_n)$ with $\|\mu\| = 1$ such that*

(1) $|\text{supp}\, \mu| \leq 40\varepsilon^{-2}$

(2) $|\hat{\mu}(\chi)| \leq \varepsilon(\log n)^{1/2}$ for all $1 \neq \chi \in \hat{G}$.

In spite of the simplicity of its derivation, this is a very good estimate. Under a slightly different guise, it forms the basis for Salem's method for the construction of thin sets by probabilistic means [3, Chapter IX] and for certain of Kahane's methods. So far as I know, all such probabilistic methods give results with a factor corresponding to $(\log n)^{1/2}$ in condition (2) of Lemma 2.1.

However, the following famous result discovered by Shapiro and rediscovered independently by Rudin, shows that, at least in the special case when ε is of the order of $n^{-1/2}$ and so $|\text{supp}\, \mu|$ is comparable with n, Lemma 2.1 does not give all the information possible.

THEOREM 2.2 (Rudin Shapiro). (A) *We can find a $\mu \in M(\Gamma_n)$ with $|\mu(\{x\})| = n^{-1}$ for all $x \in \Gamma_n$ (and so $\|\mu\| = 1$) such that*

$$|\hat{\mu}(\chi)| \leq \frac{2n^{-1/2}}{\sqrt{2}-1} \quad \textit{for all} \quad \chi \in \hat{\Gamma}_n.$$

(B) *We can find a $\mu \in M^+(\Gamma_n)$ with $\|\mu\| = 1$, $\mu(\{x\}) = \mu(\{y\})$ for all $x, y \in \text{supp}\, \mu$ such that*

(i) $$|\text{supp}\, \mu| \leq n/2,$$

(ii) $$|\hat{\mu}(\chi)| \leq \frac{2n^{-1/2}}{\sqrt{2}-1} \quad \textit{for all} \quad 1 \neq \chi \in \Gamma_n.$$

Proof. The 2 versions of the result are very close. Let $\sigma = n^{-1} \sum_{j=1}^{n} \delta_{\omega(j)}$ where $\omega(j) = \exp 2\pi ij/n$ (i.e. let σ be Haar measure normalised to have mass 1). Then, if μ satisfies the conditions of version (A), at least one of $\mu + \sigma$ and $\mu - \sigma$ will satisfy (B).

A proof of version (A) can be found, for example in [2, p. 34].

In the next section we shall prove by probabilistic means a result which, while not as strong as that of Rudin and Shapiro, is considerably more flexible in its application.

THEOREM 2.3. (A) *Let G be a finite Abelian group with n elements. Then for every $A \geq 2$ we can find a $\mu \in M(G)$ with $\|\mu\| = 1$ such that*

(i) $|\text{supp}\, \mu| \leq n/A$

(ii) $|\hat{\mu}(\chi)| \leq 4 \cdot 10^4 (\log A)^{1/2} (n/A)^{-1/2}$ *for all* $\chi \in \hat{G}$.

(B) *Let G be a finite Abelian group with n elements. Then for every $A \geq 2$ and $1 \geq \eta > 0$ we can find a $\mu \in M(G)$ with $\|\mu\| = 1$ such that*

(i) $|\text{supp}\, \mu| \leq n/A$,

(ii) $|\hat{\mu}(\chi)| \leq 10^4(\log (A\eta^{-1}))^{1/2}(n/A)^{-1/2}$ *for all* $1 \neq \chi \in \hat{G}$,

(iii) $|\hat{\mu}(0) - 1| < \eta$.

Remark 1. If μ satisfies the conditions of (B), then

$$\|\mu-\mu*\delta_x\|^{-1}(\mu-\mu*\delta_x)$$

will satisfy the conditions of (A) for some $x\in G$. A simpler version of our proof of (B) will also give (A).

Remark 2. The claim of greater flexibility is based not on the substitution of G for Γ_n but on the replacement of the condition $|\text{supp}\,\mu|\le n/2$ by $|\text{supp}\,\mu|\le n/A$. The result would, however, only become really powerful if we could remove the factor $(\log A)^{1/2}$ in (ii).

We can use Theorem 2.3 to obtain a result on trigonometric polynomials which, while much weaker than the best known result of Rudin and Shapiro, is the strongest that I know which is obtained by probabilistic means.

THEOREM 2.4. *There is a constant A such that for every $n\ge 1$ we can find $a_1, a_2, \ldots, a_n\in\mathbf{C}$ with $\sum_{r=1}^n |a_1|=1$ and $|\sum_{r=1}^n a_r \exp irt|\le An^{-1/2}$ for all $t\in\mathbf{R}$.*

Since we shall not need the result later, and the deduction is rather easy, we only sketch the proof. First note that, applying Theorem 2.3(A) to the multiplicative group of n-*th* roots of unity, we have the following result.

LEMMA 2.5. *There is a constant A_1 such that for every $n\ge 1$ we can find a measure $\mu\in M(\mathbf{T})$ with n supp $\mu=\{0\}$, $\|\mu\|=1$ and $|\hat\mu(r)|\le A_1 n^{-1/2}$ for all $r\in\mathbf{Z}$.*

Moreover by translation we see that we may add the following condition.

LEMMA 2.5′. *In Lemma 2.5 we may demand $|\mu|(-\pi/4,\pi/4)\ge 4^{-1}$.*

Now choose f twice differentiable with $f(t)=1$ for $t\in[-\pi/4,\pi/4]$ and $f(t)=0$ for $t\notin[-\pi/2,\pi/2]$, and set $B=\sum_{r=-\infty}^{\infty}|\hat f(r)|$. If μ is as in Lemma 2.5′, then $\|\mu f\|\ge 4^{-1}$, supp $\mu\subseteq[-\pi/2,\pi/2]$ and $|\widehat{\mu f}(r)|\le BA_1$ for all $r\in\mathbf{Z}$. Thus we have the next lemma.

LEMMA 2.6. *There is a constant A_2 such that for every $n\ge 1$ we can find a measure $\mu\in M(\mathbf{T})$ with n supp $\mu=\{0\}$, supp $\mu\subseteq[-\pi/2,\pi/2]$, $\|\mu\|=1$ and $|\hat\mu(r)|\le A_2 n^{-1/2}$ for all $r\in\mathbf{Z}$.*

Now if $\lambda\in\mathbf{R}$ then we can find $b_i\in\mathbf{C}$ with $\sum_{k=-\infty}^{\infty}|b_k|\le 100$ and

$$\exp i\lambda t=\sum_{k=-\infty}^{\infty} b_k \exp ikt \quad \text{for all} \quad |t|\le\pi/2$$

(see e.g. [2, p. 96]). Thus "unrolling $\mathbf{T}$" we may deduce from Lemma 2.6 the following result for $\mathbf{R}$.

LEMMA 2.6′. *There is a constant A_3 such that for every $n\ge 1$ we can find a measure $\mu\in M(\mathbf{R})$ with*

$$\text{supp}\,\mu\subseteq\{2\pi u/n\colon u\in\mathbf{Z}\}\cap[-\pi/2,\pi/2],\ \|\mu\|=1$$

and

$$\hat\mu(\lambda)|\le A_3 n^{-1/2} \quad \textit{for all} \quad \lambda\in\mathbf{R}.$$

In other words,

LEMMA 2.6″. *There is a constant A_3 such that for every $n \geq 1$ we can find $a_u \in \mathbf{C}[1 < n/4]$ with $\sum_{u=-n/4}^{n/4} |a_u| = 1$ and $|\sum_{u=-n/4}^{n/4} a_u \exp iu\lambda| \leq A_3 n^{-1/2}$ for all $\lambda \in \mathbf{R}$.*

Since Lemma 2.6″ is, essentially, Theorem 2.4, we are done.

For the reasons given in Remark 1 and also because measures satisfying condition (iii) of Theorem 2.3(B) are much easier to handle in the construction of new measures by limit constructions (see for instance our Section 5), we shall give the proof of Theorem 2.3(B) rather than (A).

Our proof will run as follows. We shall find a measure $\mu_1 \in M(G)$ which satisfies (i) and (iii) with something to spare, and satisfies (ii) for most $\chi \in \hat{G}$. We then find a μ_2 of small mass but with support the whole of G such that $\mu_1 + \mu_2$ satisfies (ii) and (iii) with something to spare. We now replace μ_2 by a measure μ_2' of small support and much the same mass, so that $\mu_1 + \mu_2'$ satisfies (i) and (iii), but $\hat{\mu}_2'(\chi)$ still so resembles $\hat{\mu}_2(\chi)$ for most $\chi \in \hat{G}$ that $\mu_1 + \mu_2'$ fails to satisfy (ii) for many fewer $\chi \in G$ than $\mu_1 + \mu_2$ did. By successive approximations of this kind we can obtain a measure of the type required.

3. Proof of the theorem

Throughout this section G will be a finite Abelian group with n elements. We shall use the term a random measure in $M(G)$ in the usual loose manner, but if the reader looks closely, she will see that we have actually a function from a finite sample space to $M(G)$, so that no problems should be caused by our inexactness.

We begin with yet another version of the results in Section 1.

LEMMA 3.1. *For every $m \geq 1$ there exists a random measure $\mu \in M^+(G)$ with $\|\mu\| = 1$ such that*

(i) $|\text{supp}\, \mu| \leq m$,

(ii) $\Pr(|\hat{\mu}(\chi)| \geq \varepsilon) \leq 4 \exp(-\varepsilon^2 m/8)$ *for all* $1 \neq \chi \in \hat{G}$,

(iii) $\hat{\mu}(0) = 1$.

Proof. Let $X_1, X_2, \ldots, X_m$ be chosen randomly as described in Section 1. Take $\mu = m^{-1} \sum_{j=1}^{m} \delta_{xj}$. Conditions (i) and (iii) are satisfied automatically and (ii) holds because, as in the proof of Theorem 1.2(ii) we have

$$\Pr(|\hat{\mu}(\chi)| \geq \varepsilon) = \Pr\left(\sum_{j=1}^{m} \chi(X_j) \mid \geq \varepsilon m\right) \leq 4 \exp(-\varepsilon^2 m/8)$$

LEMMA 3.2. *Suppose μ is a random measure with range in $M(G)$ such that*

$$\Pr(|\hat{\mu}(\chi)| \geq \varepsilon) \leq B \exp(-\varepsilon^2 \tau^2)$$

for all $1 \neq \chi \in \hat{G}$ *for some* $B, \tau > 0$. *Then, given* $\lambda \geq 1$, *we can find a measure* μ' *in the range of* μ *such that* $\hat{\mu}' = g_1 + g_2$ *with*

(i) $|g_1(\chi)| \leq \lambda\tau^{-1}$ *for all* $1 \neq \chi \in \hat{G}$,

(ii) $\sum_{\chi \in \hat{G}} |g_2(\chi)|^2 \leq 2\, Bn\lambda^2\tau^{-2} \exp(-\lambda^2)$.

Proof. Take

$$g_1(1) = \hat{\mu}(1),$$

$$g_1(\chi) = \hat{\mu}(\chi) \quad \text{for} \quad |\hat{\mu}(\chi)| \leq \lambda\tau^{-1},$$

$$g_1(\chi) = \frac{\lambda\tau^{-1}}{|\mu(\chi)|}\hat{\mu}(\chi) \quad \text{otherwise} \quad (1 \neq \chi \in \hat{G}),$$

and $g_2 = \hat{\mu} - g_1$. Then g_1 automatically satisfies condition (i). On the other hand:

$$\begin{aligned}
\mathscr{E} \sum_{\chi \in \hat{G}} |g_2(\chi)|^2 &= \sum_{\chi \in \hat{G}} \mathscr{E}\, |g_2(\chi)|^2 \\
&\leq \sum_{\chi \in \hat{G}} \sum_{r=0}^{\infty} ((r+1)\lambda\tau^{-1})^2 \Pr(r\lambda t^{-1} \leq |g_2(\chi)| < (r+1)\lambda\tau^{-1}) \\
&\leq \sum_{\chi \in G} \sum_{r=0}^{\infty} ((r+1)\lambda\tau^{-1})^2 \Pr(r\lambda\tau^{-1} \leq |g_2(\chi)|) \\
&= \sum_{\chi \in \hat{G}} \sum_{r=0}^{\infty} ((r+1)\lambda\tau^{-1})^2 \Pr((r+1)\lambda\tau^{-1} \leq |\hat{\mu}(\chi)|) \\
&\leq \sum_{\chi \in \hat{G}} \sum_{r=1}^{\infty} A\lambda^2\tau^{-2}r^2 \exp(-\lambda^2 r^2) \\
&= \mathrm{Bn}\, \lambda^2\tau^{-2} \exp(-\lambda^2) \sum_{r=1}^{\infty} r^2 \exp(-\lambda^2(r^2-1)) \\
&\leq Bn\lambda^2\tau^{-2} \exp(-\lambda^2) \sum_{r=1}^{\infty} r^2 \exp(-(r^2-1)) \\
&\leq 2Bn\lambda^2\tau^{-2} \exp(-\lambda^2).
\end{aligned}$$

Thus condition (ii) must hold for some μ' in the range of μ and we are done.

LEMMA 3.3 (Standard Fourier Transforms). *Given* $f \in C(\hat{G})$ *we can find a unique* $\mu \in M(G)$ *such that* $\hat{\mu}(\chi) = f(\chi)$ *for all* $\chi \in G$. *Further*

(i) $\sum_{g \in G} |\mu(g)|^2 = n^{-1} \sum_{\chi \in \hat{G}} |f(\chi)|^2$,

(ii) $\|\mu\| \leq \sqrt{(\sum_{\chi \in \hat{G}} |f(\chi)|^2)}$.

Proof. Direct, and standard verification. We have $\mu(g) = n^{-1}\sum_{\chi\in\hat{G}} f(\chi)\chi(g)$. Condition (ii) follows from an application of Schwartz's inequality

$$\|\mu\| = \sum_{g\in G} |\mu(g)| = \sum_{g\in G} 1 = |\mu(g)| \leq \sqrt{(\sum_{g\in G} 1^2 \cdot \sum_{g\in G} |\mu(g)|^2)} = \sqrt{n}\sqrt{(\sum |\mu(g)|^2)}$$

LEMMA 3.4. *Given $\mu \in M(G)$ and $K \geq 1$, we can find a random measure $\mu'' \in M(G)$ such that*

(i) $|\text{supp } \mu''| \leq 2\|\mu\| K^{-1}$, $\|\mu''\| \leq 2\|\mu\|$,

(ii) $\Pr(|\hat{\mu}''(\chi) - \hat{\mu}(\chi)| \geq \varepsilon) \leq 8 \exp(-\varepsilon^2/(100 \text{ K} \|\mu\|))$.

Lemma 3.4 is a direct consequence of a more natural but slightly less manageable result.

LEMMA 3.5. *Given $\mu \in M(G)$ and $K \geq 1$, we can find a random measure $\mu' \in M(G)$ such that:*

(i) *If σ belongs to the range of μ' then for each $g \in G$ we have either $\sigma(g) = 0$ or $|\sigma(g)| \geq K$.*

(ii) $\mathscr{E}\|\mu'\| = \|\mu\|$.

(iii) $\Pr(|\hat{\mu}'(\chi) - \hat{\mu}(\chi)| \geq \varepsilon) \leq 4 \exp(-\varepsilon^2/(100 \text{ K} \|\mu\|))$

for all $0 \leq \varepsilon \leq 3\|\mu\|$.

Proof of Lemma 3.4 *from Lemma* 3.5. Take μ' as in Lemma 3.5. We have

$$\Pr(\|\mu'\| > 2\|\mu\|)\, 2\|\mu\| \leq \mathscr{E}\|\mu'\| = \|\mu\|$$

so $\Pr(\|\mu'\| \leq 2\|\mu\|) \geq 1/2$. Take μ'' to be a random measure in $M(G)$ defined by

$$\begin{aligned} \Pr(\mu'' = \sigma) &= \Pr(\mu' = \sigma \mid \|\mu'\| \leq 2\|\mu\|) \quad &&\text{for} \quad \|\sigma\| \leq 2\|\mu\| \\ &= 0 &&\text{otherwise} \end{aligned}$$

(That is to say

$$\begin{aligned} \Pr(\mu'' = \sigma) &= \frac{\Pr(\mu' = \sigma)}{\Pr(\|\mu'\| \leq 2\|\mu\|)} \quad &&\text{for} \quad \|\sigma\| \leq 2\|\mu\| \\ &= 0 &&\text{otherwise.)} \end{aligned}$$

Automatically $\|\mu''\| = 2\|\mu\|$ and, since $\sigma \in$ range μ'' implies $\sigma \in$ range μ', condition (i) of Lemma 3.5 gives $|\text{supp } \mu''| \leq 2\|\mu\| K^{-1}$. Thus μ'' satisfies condition (i) of Lemma 3.4. To prove condition (ii) of Lemma 3.4, we note first that if $\varepsilon > 3\|\mu\|$, then, since

$$|\hat{\mu}''(\chi) - \hat{\mu}(\chi)| \leq \|\mu''\| + \|\mu\| \leq 3\|\mu\|,$$

we have

$$\Pr(|\hat{\mu}''(\chi)-\hat{\mu}(\chi)|\geq\varepsilon)=0\leq 8\exp(-\varepsilon^2/100\mathrm{K}\,\|\mu\|).$$

On the other hand, if $0\leq\varepsilon\leq 3\|\mu\|$, we have, since

$$\Pr(\mu''=\sigma)\leq\frac{\Pr(\mu'=\sigma)}{\Pr(\|\mu'\|\leq 2\|\mu\|)}\leq 2\Pr(\mu'=\sigma),$$

that condition (iii) of Lemma 3.4 gives

$$\begin{aligned}\Pr(|\hat{\mu}''(\chi)-\hat{\mu}(\chi)|\geq\varepsilon)&\leq 2\Pr(|\hat{\mu}''(\chi)-\hat{\mu}(\chi)|\geq\varepsilon)\\&\leq 8\exp(-\varepsilon^2/(100\mathrm{K}\,\|\mu\|))\end{aligned}$$

and we are done.

Proof of Lemma 3.4. Let $\mu'=\sum_{g\in G}\mu'(g)\delta_g$, where the $\mu'(g)$ are independent random variables in $\mathbf{C}$ defined as follows. If $|\mu(g)|\geq K$ or $\mu(g)=0$ then we take $\mu'(g)=\mu(g)$. If $K>|\mu(g)|>0$ then we write $\alpha(g)=\mu(g)/|\mu(g)|$ and take

$$\Pr(\mu'(g)=\alpha(g)K)=|\mu(g)|/K,\qquad \Pr(\mu'(g)=0)=1-|\mu(g)|/K.$$

Thus condition (i) holds automatically.

Again

$$\mathscr{E}(\|\mu'\|)=\mathscr{E}\left(\sum_{g\in G}|\mu(g)|\right)=\sum_{g\in G}\mathscr{E}|\mu(g)|=\sum_{g\in G}|\mu(g)|=\|\mu\|$$

so condition (ii) also holds.

To prove (iii) we follow Lemma 1.3. Let $X(g)=(\mu'(g)-\mu(g))\chi(g)$. If $|\mu(g)|\geq K$ or $\mu(g)=0$, then $X(g)=0$. If $K\geq|\mu(g)|\geq 0$, then

$$\begin{aligned}|\mathscr{E}(\operatorname{Re}X(g))^r|&\leq\mathscr{E}|X(g)|^r\\&\leq K^r\frac{|\mu(g)|}{K}+\left(1-\frac{\mu(g)|}{K}\right)|\mu(g)|^r\\&\leq K^{r-1}|\mu(g)|+|\mu(g)|^r\\&\leq 2K^{r-1}|\mu(g)| \qquad (r\geq 1)\end{aligned}$$

whilst

$$\mathscr{E}\operatorname{Re}X(g)=\operatorname{Re}\left(\alpha(g)\left(\alpha(g)K\frac{|\mu(g)|}{K}-\mu(g)\right)\right)=\operatorname{Re}0=0.$$

Thus, irrespective of the value of $\mu(g)$, we have

$$|\mathscr{E}(\operatorname{Re}X(g))^r|\leq 2K^{r-1}|\mu(g)|\quad(r\geq 1),\quad \mathscr{E}\operatorname{Re}X(g)=0.$$

It follows that, if $1 \geq K\lambda \geq 0$,

$$\begin{aligned}
\mathscr{E} \exp(\lambda \operatorname{Re} X(g)) &= \sum_{r=0}^{\infty} \frac{\lambda^r \mathscr{E}(\operatorname{Re} X(g))^2}{r!} \\
&= 1 + \sum_{r=2}^{\infty} \frac{\lambda^r \mathscr{E}(\operatorname{Re} X(g))^r}{r!} \\
&\leq 1 + 2K|\mu(g)|\lambda^2 \sum_{r=2}^{\infty} \frac{(K\lambda)^{r-2}}{r!} \\
&\leq 1 + 2K|\mu(g)|\lambda^2 \sum_{r=2}^{\infty} \frac{1}{r!} \\
&\leq 1 + 4K|\mu(g)|\lambda^2 \\
&\leq \exp(4K|\mu(g)|\lambda^2).
\end{aligned}$$

Now $\hat{\mu}'(\chi) - \hat{\mu}(\chi) = \sum_{g \in G} (\mu'(g) - \mu(g))\chi(g) = \sum_{g \in G} X(g)$ so

$$\begin{aligned}
\mathscr{E} \exp(\lambda \operatorname{Re}(\hat{\mu}'(\chi) - \mu(\chi))) &= \mathscr{E} \exp\left(\lambda \sum_{g \in G} \operatorname{Re} X(g)\right) \\
&= \prod_{g \in G} \mathscr{E} \exp(\lambda \operatorname{Re} X(g)) \\
&\leq \prod_{g \in G} \exp(4K|\mu(g)|\lambda^2) \\
&= \exp\left(4K \sum_{g \in G} |\mu(g)|\lambda^2\right) \\
&= \exp(4K\|\mu\|\lambda^2)
\end{aligned}$$

and

$$\Pr(\operatorname{Re}(\hat{\mu}'(\chi) - \hat{\mu}(\chi)) \geq 2\varepsilon^{-1/2}) \leq \exp(4K\|\mu\|\lambda^2 - 2\varepsilon^{-1/2}\lambda)$$

provided that $1 \geq K\lambda \geq 0$.

Suppose now that $0 \leq \varepsilon \leq 3\|\mu\|$. Setting $\lambda = \varepsilon/(10K\|\mu\|)$, we have $0 \leq \lambda K \leq 1$ and so

$$\Pr(\operatorname{Re}((\hat{\mu}'(\chi) - \hat{\mu}(\chi)) \geq 2^{-1/2}\varepsilon) \leq \exp(-\varepsilon^2/(100K\|\mu\|)).$$

Exactly similar estimates give

$$\Pr(\operatorname{Re}(\omega(\hat{\mu}'(\chi) - \hat{\mu}(\chi)) \geq 2^{-1/2}\varepsilon) \leq \exp(-\varepsilon^2/(100K\|\mu\|))$$

for $\omega = 1, i, -i$. Thus

$$\Pr(|\hat{\mu}'(\chi) - \hat{\mu}(\chi)| \geq \varepsilon) \leq 4\exp(-\varepsilon^2/(100K\|\mu\|))$$

for all $0 \leq \varepsilon \leq 3\|\mu\|$ and we have obtained condition (iii).

The proof of our main theorem now follows after a little reorganisation.

LEMMA 3.6_1. *Let G be a finite Abelian group with n elements. Suppose*

$n/8 > A > 2$ and $1 \geq \eta > 0$ given. Then we can find a $\mu_1 \in M^+(G)$ and an $f_1 \in C(G)$ such that

(i)$_1$ $|\text{supp}\, \mu_1| \leq nA^{-1}2^{-1}$,
(ii)$_1$ $\|\mu_1\| = 1$,
(iii)$_1$ $|\hat{\mu}_1(\chi) + f_1(\chi)| \leq 2^{-2}\, 10(\log A\eta^{-1})^{1/2}(n/A)^{-1/2}$ *for all* $1 \neq \chi \in \hat{G}$,
(iv)$_1$ $\sum_{\chi \in \hat{G}} |f_1(\chi)|^2 \leq 2^{-16}\eta^2$.

LEMMA 3.6$_r$. *Suppose G, A, η as in Lemma 3.6$_1$. Suppose we are given an $f_{r-1} \in C(G)$ such that*

(iv)$_{r-1}$ $\sum_{\chi \in G} |f_{r-1}(\chi)|^2 \leq 2^{-8r}\eta^2$.

Then we can find a $\mu_r \in M(G)$ and an $f_r \in C(G)$ such that

(i)$_r$ $|\text{supp}\, \mu_r| \leq nA^{-1}\, 2^{-r}\eta$,
(ii)$_r$ $\|\mu_r\| \leq 2^{-r}\eta$,
(iii)$_r$ $|\hat{\mu}_r(\chi) - f_{r-1}(\chi) + f_r(\chi)| \leq 2^{-r-1}\, 10^4(\log A\eta^{-1})^{1/2}(n/A)^{-1/2}$ *for all* $1 \neq \chi \in G$,
(iv)$_r$ $\sum_{\chi \in G} |f_r(\chi)|^2 \leq 2^{-8(t+1)}\eta^2$, $r = 2$.

Proof of 3.6$_1$. By Lemma 3.1 with $m = [n/2A]$ (so $m \geq nA^{-1}4^{-1}$), we can find a random measure $\mu \in M^+(G)$ with $\|\mu\| = 1$ such that

(i) $|\text{supp}\, \mu| \leq m \leq n\, A^{-1}2^{-1}$,
(ii) $\Pr(|\hat{\mu}(\chi)| \geq \varepsilon) \leq 4\exp(-\varepsilon^2 m/8) \leq 4\exp(-\varepsilon^2 n/(32A))$.

Applying Lemma 3.2 with $B = 4$, $\tau = (n/32A)^{1/2}$,

$$\lambda = \tau\, 2^{-2}\, 10^4(\log A\, \eta^{-1})^{1/2}(n/A)^{-1/2},$$

$f_1 = g_2$ and $\mu_1 = \mu'$, we see that there exists a μ_1 in the range of μ and an $f_1 \in C(G)$ such that

(iii)$_1$ $$|\hat{\mu}_1(\chi) + f_1(\chi)| \leq 2^{-2}\, 10^4(\log A\eta^{-1})^{1/2}(n/A)^{-1/2},$$

(iv)$_1$ $$\begin{aligned}\sum_{\chi \in \hat{G}} |f_1(\chi)|^2 &\leq 2Bn\lambda^2\tau^{-2}\exp(-\lambda^2)\\ &\leq 8n(2^{-2}\, 10^4(\log A\eta^{-1})^{1/2}(n/A)^{-1/2})^2\\ &\quad\times \exp(-n/32A(2^{-2}\, 10^4(\log A^{-1})^{1/2}(n/A)^{-1/2})^2)\\ &\leq 2^{-1}\, 10^8(\log A\eta^{-1})A\exp(-10^2\log A\eta^{-1})\\ &\leq 2^{-1}\, 10^8\, A(\log A\eta^{-1})(A\eta^{-1})^{-100}\\ &\leq 2^{-16}\eta^2\end{aligned}$$

because $A \geq 2$, $1 \geq \eta > 0$. Since μ_1 belongs to the range of μ the remaining conditions of Lemma 3.6$_1$ are automatically satisfied.

Proof of Lemma 3.6$_r$. From condition *(iv)*$_{r-1}$ and a direct application of

Lemma 3.3 with $f=f_{r-1}$, $\mu=\sigma_r$ we know that there exists a $\sigma_r \in M(G)$ with

(v)$_r$ $\hat{\sigma}_r(\chi)=f_{r-1}(\chi)$ for all $\chi \in \hat{G}$,
(vi)$_r$ $\|\sigma_r\| \leq 2^{-4r}\eta$.

Next, using Lemma 3.4 with $\mu=\sigma_r$, $K=A\,n^{-1}$ and $\mu''=\sigma_r'$, we can find a random measure $\sigma_r' \in M(G)$ such that

(vii)$_r$ $|\text{supp}\, \sigma_r'| \leq 2\|\sigma_r\|(An^{-1})^{-1} \leq 2^{-4r+1}\eta\, A^{-1}\eta \leq n\, A^{-1}2^{-r}\eta$,
(viii)$_r$ $\|\sigma_r'\| \leq 2\|\sigma_r\| \leq 2^{-r}\eta$,
(ix)$_r$ $\Pr(|(\sigma_r'-\sigma_r)\hat{}(\chi)| \geq \varepsilon) \leq 8 \exp(-\varepsilon^2/(100\, An^{-1}2^{-4r}\eta))$.

Applying Lemma 3.2 with $B=8$, $\tau=(2^{4r}n/100\, A\eta)^{1/2}$,

$$\lambda=\tau\, 2^{-r-1}\, 10^4(\log A\eta^{-1})^{1/2}(n/A)^{-1/2},$$

$\mu=\sigma_r'-\sigma_r$, $f_r=-g_2$ and $\mu_r=\mu''+\sigma_r$, we see that there exists a μ_r in the range of σ_r' and an $f_r \in C(G)$ such that (using $(v)_r$)

$$\begin{aligned}
\text{(iii)}_r\quad |\hat{\mu}_r(\chi)-f_{r-1}(\chi)+f_r(\chi)| &= |\mu''(\chi)-\hat{\sigma}_r(\chi)+\hat{\sigma}_r(\chi)+f_r(\chi)| \\
&= |\mu''(\chi) \mp g_2(\chi)| \\
&\leq 2^{-r-1}\, 10^4(\log A\eta^{-n})^{1/2}(n/A)^{-1/2},
\end{aligned}$$

and

$$\begin{aligned}
\text{(iv)}_r\quad \sum_{\chi \in \hat{G}} |f_r(\chi)|^2 &\leq 2B_n\lambda^2\tau^{-2}\exp(-\lambda^2) \\
&\leq 16n(2^{-r-1}10^4(\log A\eta^{-1})^{1/2}(n/A)^{-1/2})^2 \\
&\quad \times \exp\left(-\frac{2^{4m}}{100\, A\eta}\left(2^{-r-1}\, 10^4(\log A\eta^{-1})^{1/2}\left(\frac{n}{A}\right)^{-1/2}\right)^2\right) \\
&\leq 2^{-r+2}\, 10^8(\log A\eta^{-1})A \exp(-10^2\, 2^{3r-2}\eta^{-1}\log A\eta^{-1}) \\
&\leq 2^{-r+2}\, 10^8\, A(\log A\eta^{-1})(A\eta^{-1})^{-100(r+1)} \\
&\leq 2^{-8(r+1)}
\end{aligned}$$

because $A \geq 2$, $1 \geq \eta > 0$ and $2^{3r-2} \geq r+1$. Since μ_r belongs to the range of σ_r', conditions (i)$_r$ and (ii)$_r$ follow from (vii)$_r$ and (viii)$_r$.

Proof of Theorem 2.3B. Construct μ_1, f_1 as in Lemma 3.6(i). We now use Lemma 3.6$_r$ to construct inductively μ_r and f_r for $r=2,3,\ldots$. Since $nA^{-1}2^{-r}\eta \to 0$, we can find an N such that $0 \leq nA^{-1}2^{-r}\eta \leq \frac{1}{2}$ for all $r \geq N$ and so by condition (i)$_r$ we have $|\text{supp}\, \mu_r| \leq \frac{1}{2}$, i.e. $\mu_r=0$ for all $r \geq N$. Let $\sigma=\sum_{r=2}^{N}\mu_r$. then by condition (ii)$_r$ we know that

$$\|\sigma\| \leq \sum_{r=2}^{N}\|\mu_r\| \leq \eta/2.$$

Since $\mu_1 \in M^+(G)$, $\|\mu_1\|=1$, we may set $\mu=(\mu_1+\sigma)/\|\mu_1+\sigma\|$ and obtain a measure $\mu \in M(G)$ with $\|\mu\|=1$ and $\hat{\mu}(0) \geq 1-\eta$.

Clearly supp $\mu \subset \bigcup_{r=1}^{N}$ supp μ_r so $|\text{supp }\mu| \le \sum_{r=1}^{N} |\text{supp }\mu_r|$ and condition (i)$_r$ gives $|\text{supp }\mu| \le n A^{-1}$. All that remains therefore is to verify condition (ii). Choose $M \ge N$ such that

$$2^{-8(M+1)}\eta^2 \le (2^{-1}10^4(\log A\eta^{-1})^{1/2}(n/A)^{-1/2})^2.$$

Then, using (iv)$_M$, we see that

$$f_M(\chi) \le 2^{-1}10^4(\log A\eta^{-1})^{1/2}(n/A)^{-1/2}$$

for all $\chi \in \hat{G}$ and so, using (iii)$_r$, we have

$$\begin{aligned}
\hat{\mu}(\chi) &= \left|\sum_{r=1}^{M} \hat{\mu}_r(\chi)\right| \\
&= \left|\sum_{r=1}^{M} \hat{\mu}_r(\chi) - f_M(\chi)\right| + |f_M(\chi)| \\
&\le \left|\sum_{r=2}^{M} (\hat{\mu}_r(\chi) - f_{r-1}(\chi) + f_r(\chi)) + \hat{\mu}_1(\chi)\right| + |f_M(\chi)| \\
&\le |\hat{\mu}_1(\chi)| + \sum_{r=2}^{M} |\hat{\mu}_r(\chi) - \hat{f}_{r-1}(\chi) + f_r(\chi)| + |f_M(\chi)| \\
&\le \left(\sum_{r=1}^{M} 2^{-r-1} + 2^{-1}\right) 10^4(\log A\eta^{-1})^{1/2}(n/A)^{-1/2} \\
&\le 10^4 (\log A\eta^{-1})^{1/2}(n/A)^{-1/2},
\end{aligned}$$

for all $1 \ne \chi \in \hat{G}$ and we are done.

We note that the measure μ we have constructed is real. Further with a little extra care (essentially by re-defining $\mu'(g)$ in Lemma 3.4 so that if

$$pK > |\mu(g)| \ge (p-1)K$$

then

$$\Pr(\mu'(g) = p\alpha(g)K) = \frac{|\mu(g)| - (p-1)K}{K},$$

$$\Pr(\mu'(g) = (p-1)\alpha(g)K = \frac{pK - |\mu(g)|}{K}$$

we can obtain a minor refinement of our theorem.

THEOREM 2.3C. *In Theorem* 2.3*A and* 2.3*B we may replace condition* (i) *by the stronger condition:*

(i)′ $\mu(g)$ *is an integral multiple of* An^{-1} *for each* $g \in G$.

Unfortunately this result is not really a true analogue of the corresponding condition in the Rudin Shapiro theorem. A true analogue would be

(i)″ (g) takes one of the values An^{-1}, 0 or $-An^{-1}$
but I have not succeeded in obtaining this.

4. Measures on the circle

At the beginning of Section 2, we claimed that Lemma 2.1 paralleled exactly the probabilistic calculations used by Salem to obtain results of the following form.

THEOREM 4.1. *Let h be a positive concave function on $[0, \infty)$ with $h(0)=0$. Let $\omega_n \to \infty$. Then there exists a closed set E with Hausdorff h-measure* 0 *and $\mu \in M^+(E)$ a non-zero measure (indeed the L measure of E) such that*

$$|\hat{\mu}(n)| = O((\omega_{|n|} \log |n|\, h(|n|^{-1}))^{1/2} \quad as \quad |n| \to \infty.$$

To support this claim, if the reader has not already granted it, and to show that our theorem does in fact give some new results, we shall show, in Section 5, how, using Theorem 2.3 instead of Lemma 2.1, we get the following result.

THEOREM 5.1. *Let h be a positive concave function on $[0, \infty)$ with $h(0)=0$. Let $\omega_n \to \infty$. Then there exists a closed translational set E with Hausdorff h-measure* 0 *and $\mu \in M(E)$ a non-zero translational measure such that*

$$|\hat{\mu}(n)| = O((\omega_{|n|} \log(|n|\, h(|n|^{-1}))\, h(|n|^{-1}))^{1/2}) \quad as \quad |n| \to \infty$$

The version of Theorem 2.3 that we shall use for the circle is the following.

LEMMA 4.2. *Suppose $N \geq 10^4$ an integer. Then there exists an $A(N) \geq 1$ such that, given any $\eta > 0$, any integer $K \geq 8N^6$ and any function*

$$\psi: \mathbf{Z} \to \mathbf{R}^+ \quad with \quad \frac{\psi(n)n}{\log n} \to \infty \quad as \quad n \to \infty$$

we can find a $P(\psi, \kappa, N, \eta)$ with the following property. Given $M \geq P(\psi, K, N, \eta)$, we can find a $\mu(M, \psi, K, N, \eta) \in M(\mathbf{T})$ such that

(i) $\|\mu\| \leq 1$,
(ii) $|\hat{\mu}(0) - 1| \leq \eta$,
(iii) $\operatorname{supp} \mu \subseteq \{2\pi u/M : u \in \mathbf{Z}\} \cap [-\pi(N^{-1} - N^{-6}), \pi(N^{-1} - N^{-6})]$,
(iv) $\operatorname{card} \operatorname{supp} \mu \leq \psi(M)M$,
(v) $|\hat{\mu}(lN + s)| \leq 2(|s|+1)/|lN + s|$ *for* $0 \neq |lN + s| \leq N^5$,
(vi) $|\hat{\mu}(s)| \leq 2N/|s|$ *for* $N^5 \leq |s| \leq K$
(viii) $|\hat{\mu}(s)| \leq A(N)(\log(\psi(M)\eta)^{-1})^{1/2}(\psi(M)M)^{-1/2} + 10^5 N^{30} |s|^{-4}$ *for* $K \leq |s| \leq M/2$.

Remark. After reading our proof of Theorem 2.4 the reader may very well be prepared to take on trust the details of the transfer from Theorem 2.3 about measures supported on finite subgroups of the circle. Or she may well be able to give her own proof in less time than it takes to unravel mine. If not, the details which are messy rather than difficult are given below and form the remainder of this section.

Proof. Without real loss of generality, we may suppose $\psi(n) \leq 1/8$ since the proof is, if anything, easier if $\limsup \psi(n) > 0$ and in any case we shall only be interested in the case when $\psi(n) \to 0$ as $n \to \infty$. We also suppose, without any loss of generality, that $1/8 \geq \eta > 0$.

Let q be an infinitely differentiable positive function $q: \mathbf{R} \to \mathbf{R}^+$ with

$$\operatorname{supp} q \subseteq [-\pi, \pi], \quad \int_{-\infty}^{\infty} q(t)dt = 2\pi \quad \textit{and} \quad \sup_{t \in \mathbf{R}} |q^{(4)}(t)| \leq 10^5.$$

Set $h(t) = N^6 q(N^6 t)$ for $t \in [-\pi N^{-6}, \pi N^{-6}]$, $h(t) = 0$ otherwise. By a slight abuse of notation, we may consider h as a function $\mathbf{T} \to \mathbf{R}^+$ and we shall do this. Let $\sigma \in M(\mathbf{T})$ be Lebesgue measure on

$$[-\pi(N^{-1} - 3N^{-6}), \pi(N^{-1} - 3N^{-6})]$$

normalised to give $\|\sigma\| = 1$, and set $f = \sigma * h$. Automatically:

(viii) $f(t) \geq 0$ for all $t \in \mathbf{T}, \int_{-\pi}^{\pi} f(t)\,\mathrm{d}t = 2\pi$ and f is infinitely differentiable,
(ix) $\operatorname{supp} f \subseteq \operatorname{supp} \sigma + \operatorname{supp} h \subseteq [-\pi(N^{-1} - 2N^{-6}), \pi(N^{-1} - 2N^{-6})]$.

Next we estimate $\hat{f}(r)$. Since

$$|\hat{\sigma}(r)| = \left| \frac{1}{2\pi(N^{-1} - 3N^{-6})} \int_{-\pi(N^{-1}-3N^{-6})}^{\pi(N^{-1}-3N^{-6})} \exp irt\,\mathrm{d}t \right|$$
$$= \frac{1}{\pi(N^{-1} - 3N^{-6})} \left| \frac{\sin \pi r(N^{-1} - 3N^{-6})}{r} \right|$$

we have the trivial estimates $\hat{\sigma}(r) \leq N/r$ for all $r \neq 0$, and, provided $|l| \leq N^4$, $0 \neq lN + s$,

$$|\hat{\sigma}(lN+s)| = \frac{1}{\pi(N^{-1} - 3N^{-6})} \frac{|\sin(\pi s(N^{-1} - 3N^{-6}) - 3l\pi N^{-5})|}{|lN+s|}$$
$$\leq \frac{1}{\pi(N^{-1} - 3N^{-6})} \frac{|\pi s(N^{-1} - 3N^{-6}) - 3l\pi N^{-5}|}{|lN+s|}$$
$$\leq \frac{|s|}{|lN+s|} + \frac{3\,|l|\,N^{-5}}{|lN+s|\;\pi(N^{-1} - 2N^{-6})}$$
$$\leq \frac{|s|}{|lN+s|} + \frac{3N^4 N N^{-5}}{|lN+s|\;\pi(1 - 2N^{-5})}$$
$$\leq \frac{|s|+1}{|lN+s|}.$$

Thus $|\hat{\sigma}(lN+s)| \leq (|s|+1)/|lN+s|$ whenever $0 \neq |lN+s| \leq N^5$ and we have the estimates

(x) $|\hat{f}(lN+s)| = |\hat{\sigma}(lN+s)|\,|h(lN+s)| \leq (|s|+1)/|lN+s|$ for all s, l integers with $0 \neq |lN+s| \leq N^5$,
(xi) $|\hat{f}(r)| \leq N/|r|$ for all $r \neq 0$.

Further, since

$$\sup_{t\in\mathbf{T}} |h^{(4)}(t)| \le N^{30} \sup_{t\in\mathbf{R}} |q^{(4)}(t)| \le 10^5 N^{30},$$

it follows that $|\hat{h}(r)| \le 10^5 N^{30}/r^4$ and so

(xii) $|\hat{f}(r)| = |\hat{\sigma}(r)|\,|\hat{h}(r)| \le 10^5 N^{30}/r^4$ for all $r \ne 0$.

It follows from (xii) (or directly from the fact that f is differentiable) that $\sum_{r=-\infty}^{\infty} |\hat{f}(r)| < \infty$. Set $A(N) = 10^8(\sum_{r=-\infty}^{\infty} |\hat{f}(r)| + 1)$.

Let $M \ge K$ be an integer. Consider the group G consisting of the M-*th* roots of unity. By Theorem 2.3B we can find a $\tau_M' \in M(G)$ with $\|\tau_M'\| \le 1 + \eta/2$ such that

(xiii)′ card supp $\tau_M' \le \psi(M)M$,
(xiv)′ $|\hat{\tau}_M'(\chi)| \le 10^4(\log 4\psi(M)\eta)^{-1})^{1/2}(\psi(M)M)^{-1/2}$,
(xv)′ $\hat{\tau}_M'(0) = 1$.

Since G embeds in a natural way in $\mathbf{T}$, there is a measure $\tau_M \in M(\mathbf{T})$ corresponding to τ_M' with

(xvi) supp $\tau_M' \subseteq \{2\pi u/M \colon u \in Z\}$

and $\|\tau_M\| \le 1 + \eta/2$ such that

(xiii) $|\text{supp } \tau_M| \le \psi(M)M$,
(xiv) $|\hat{\tau}_M(r)| \le 10^4(\log(4\psi(M)\eta)^{-1})^{1/2}(\psi(M)M)^{-1/2}$
$\le 4.10^4(\log(\psi(M)\eta)^{-1})^{1/2}(\psi(M)M)^{-1/2}$ for $r \ne 0$,
(xv) $\hat{\tau}_M(0) = 1$.

Set $f_\lambda(t) = f(t+\lambda)$ for $t \in \mathbf{T}$, $\lambda \in \mathbf{T}$ and consider $\tau_{\lambda M} = f_\lambda \tau_M$.
Since f is positive,

$$\begin{aligned}
\int_{-\pi}^{\pi} \|\tau_{\lambda M}\|\, d\lambda &= \int_{-\pi}^{\pi} \sum_{u=1}^{M} |\tau_{\lambda M}(2\pi\, u/M)|\, d\lambda \\
&= \int_{-\pi}^{\pi} \sum_{u=1}^{M} f_\lambda(2\pi\, u/M)\, |\tau_M(2\pi\, u/M)|\, d\lambda \\
&= \sum_{u=1}^{M} |\tau_M(2\pi\, u/M)| \int_{-\pi}^{\pi} f_\lambda(2\pi\, u/M)\, d\lambda \\
&\le 1 + \eta/2.
\end{aligned}$$

Thus we can find a $\lambda(M)$ with $\|\tau_{\lambda(M)M}\| \le 1 + \eta/2$. Take $u(M) \in \mathbf{Z}$ such that

$$2\pi u(M)/M \le \lambda(M) < 2\pi(u(M)+1)/M$$

and set $\mu_M = \tau_{\lambda(M)M} * \delta_{2\pi u(M)/M}$.

We note at once that

(i)′ $\|\mu\|_M = \|\tau_{\lambda(M)M}\| \le 1 + \eta/2$.

Since supp $\mu_M = \operatorname{supp} \tau_{\lambda(M)M} + 2\pi u(M)/M$ and supp $\tau_{\lambda(M)} \subseteq \operatorname{supp} \tau_M$, it follows from (xvi) and (xiii) that

(iv)′ card supp $\mu_M \leq \psi(M)M$,
(iii)$'_a$ supp $\mu \subseteq \{2\pi u/M\colon u \in \mathbf{Z}\}$.

Again, supp $\tau_{\lambda(M)} \subseteq \operatorname{supp} f_{\lambda(M)} = \operatorname{supp} f + \lambda(M)$ and

$$|\lambda(M) - 2\pi u(M)/M| \leq 2\pi/M \leq \pi N^{-6},$$

so by (ix),

(iii)$'_b$ supp $\mu_M \subseteq [-\pi(N^{-1} - N^{-6}), \pi(N^{-1} - N^{-6})]$.

We now have to estimate $\hat{\mu}_M(r)$. Observe first that $|\hat{f}_\lambda(s)| = |\hat{f}(s)|$ for all $s \in \mathbf{Z}$ and so, writing

$$b_M = \frac{A(N)}{2} (\log (\psi(M)\eta)^{-1})^{-1/2} (\psi(M)M)^{-1/2},$$

$\gamma_r = 1$ for $r \neq 0$, $\gamma_0 = 0$, we have, using (xii), (viii) (to obtain $\hat{f}(0) = 1$) and (xiv) that

$$\begin{aligned}
|\hat{\tau}_{\lambda(M)M}(r) - \hat{f}_{\lambda(M)}(r)| &= \left| \sum_{s=-\infty}^{\infty} \hat{\tau}_M(r+e)\hat{f}_{\lambda(M)}(-s) - \hat{\tau}_M(0)\hat{f}_{\lambda(M)}(r) \right| \\
&\leq \sum_{s \neq r} |\hat{\tau}_M(r+s)|\, |\hat{f}_{\lambda(M)}(-s)| \\
&= \sum_{s \in \{-r+kM:\, k \in \mathbf{Z}\},\, s \neq 0} |\hat{\tau}_M(r+s)|\, |\hat{f}_{\lambda(M)}(-s)| \\
&\quad + \sum_{s \in \{-r+kM:\, k \in \mathbf{Z}\},\, s \neq 0,\, -r} |\hat{\tau}_M(r-s)|\, |\hat{f}_{\lambda(M)}(-s)| \\
&\quad + |\hat{\tau}_M(r)|\, |\hat{f}_{\lambda(M)}(0)|\, \gamma_r \\
&\leq 4.10^4 (\log (\psi(M)\eta)^{-1})^{1/2} (\psi(M)M)^{-1/2} \\
&\quad \times \sum_{s \in \{r+kM:\, k \in Z\},\, s \neq 0} |\hat{f}_{\lambda(M)}(-s)| \\
&\quad + \sum_{k \neq 0} \frac{10^5 N^{30}}{(kM+r)^4} \\
&\qquad + 4.10^4 (\log (\psi(M)\eta)^{-1})^{1/2} (\psi(M)M)^{-1/2} \\
&\leq \frac{b_M}{2} + \frac{10^8 N^{30}}{M^4}
\end{aligned}$$

for all $|r| < M/2$. But

$$M^{5/2}(\psi(M))^{-1/2}(\log (\psi(M)\eta)^{-1})^{-1/2} \to \infty \quad \text{as} \quad M \to \infty.$$

So provided only that M is sufficiently large (say $M \geq Q(\psi, N, \eta)$), we have

$$\frac{10^8 N^{30}}{M^4} \leq \frac{b_M}{2}$$

and so

(xvii) $|\hat{\tau}_{\lambda(M)M}(r) - \hat{f}_\lambda(r)| \leq b_M + |\hat{\tau}_M(r)|$.

For the remainder of the proof we shall always take $M \geq Q(\psi, N, \eta)$. Note that $b_M \to 0$ as $M \to \infty$.

When $r = 0$ then $\hat{f}_\lambda(0) = \hat{f}(0) = 1$ and $\hat{\mu}_M(0) = \hat{\tau}_{\lambda(M)M}(0)$ so (xvii) gives

(ii)′ $|\hat{\mu}_M(0) - 1| \leq b_M \to 0$ as $M > \infty$.

In general $|\hat{\mu}_M(r)| = |\hat{\tau}_{\lambda(M)M}(r)|| \hat{f}_\lambda(r)|$ so that (vii) gives

(xviii) $|\hat{\mu}_M(r)| \leq b_M + |\hat{f}(r)|$.

Thus, using (x) and (xi), we have

(v)′ $\limsup_{M\to\infty} |\hat{\mu}_M(lN + s)| = (|s| + 1)/|lN + s|$ for $0 \neq |lN + s| \leq N^5$,

(vi)′ $\limsup_{M\to\infty} |\hat{\mu}_M(s)| \leq N/|s|$ for $s \neq 0$,

whilst by (xi) we have

(vii)′ $|\hat{\mu}_M(s)| \leq b_M + 10^5 N^{30}/s^4$ for all $s \neq 0$.

It follows by the formulae (i)′, (ii)′, (iii)$'_a$, (iii)$'_b$, (iv)′, (v)′, (vi)′, (vii)′ just obtained that $\mu = \mu_M/\|\mu\|_M$ will satisfy the conditions of Lemma 4.2 provided only that M is large enough (say $M \geq P(\psi, K, N, \eta)$) and we are done.

Let us briefly recap the proof above. Ignoring the introduction of $\lambda(M)$ and $u(M)$ as a peripheral step which could, indeed, have been avoided, we consider $\mu_M = f\tau_M$. Formulae (xiv) and (xv) mean that $\tau_M \to 1$ in a distributional sense and so $\hat{\mu}_M(r) \to \hat{f}(r)$ as $M \to \infty$. Thus for r very small compared with M, $\hat{\mu}_M(r)$ behaves like $\hat{f}(r)$. On the other hand, if f is smooth, we may hope that $\hat{\mu}_M(r)$ will behave rather like $\hat{\tau}_M(r)$ for large r and this is the content of condition (vii). (Note, however, that since $\hat{\mu}_M(r)$ is periodic with period M, the condition "r large" must be qualified by "but not close to a multiple of M".) Provided that the gap between r large and r small can be bridged satisfactorily, all that remains is to choose f with nice properties.

For reasons connected with the nature of the inductive proof in Section 5 we require very tight control over the size of $\hat{\mu}_M(r)$ and so of $\hat{f}(r)$ when r is close to a multiple of N. Bearing in mind that supp μ_M and so supp f is to be contained in an interval comparable with $[-1/N, 1/N]$, it is natural to take f to be a multiple of the characteristic function ξ of $[-\pi/N, \pi/N]$. (In the actual construction we use an interval $[-\pi/N + \delta, \pi/N - \delta]$ where δ is very small, but this is to get the technical refinement

$$\operatorname{supp} \mu \subseteq [-\pi(N^{-1}-N^{-6}), \pi(N^{-1}-N^{-6})]$$

rather than the obvious $\operatorname{supp} \mu \subseteq [-2\pi N^{-1}, 2\pi N^{-1}]$.) Since ξ is not smooth, we convolve it with a smooth function h of small support. The resulting function $f=\sigma * h$ has $\hat{f}(r)$ very small when r is close to a multiple of N (conditions (v) and (vi)) but is smooth, so that the arguments establishing (vii) can still go through.

5. Construction of a thin set

We are now in a position to complete the paper by giving the construction required to produce E and μ in Theorem 5.1.

THEOREM 5.1. *Let h be a positive concave function on $[0,\infty)$ with $h(0)=0$ and $h(t)\log t \to 0$. Let $\omega_n \to \infty$. Then there exists a closed translational set E with Hausdorff h-measure 0 and $\mu \in M(E)$ a non-zero translational measure such that*

$$|\hat{\mu}(n)| = O((\omega_{|n|} \log(|n|\, h(|n|^{-1}))h(|n|^{-1}))^{1/2} \quad \text{as} \quad |n| \to \infty.$$

The method we use to obtain Theorem 5.1 from Lemma 4.2 is more or less standard. The reader who does not want to wade through the details that follow but who does want to see how this sort of thing is done, could read [**1**] instead. In that paper Kahane obtains a result similar to Theorem 5.1 starting from the Rudin Shapiro theorem. Because of the simplicity of the Rudin Shapiro measures which removes the technical difficulties which we encounter and because of the lucidity of the authors thought, the paper is short and easy to read.

Without loss of generality, we may suppose $h(t) \le 10^{-1}t$ for all $t \ge 0$, $\omega_n \ge 2^{20}$ and ω_n monotonic increasing. We shall construct sets E_n, measures μ_n and positive integers $P(n)$, $Q(n)$ and $N(n)$ satisfying the following inductive conditions.

Inductive conditions.

$(\mathrm{i})_n$ $N(n) \ge 10^5(Q(n)+1)^5$.

$(\mathrm{ii})_n$ $Q(n) \ge 10^5 N(n-1)$ *if* $n \ge 1$.

$(\mathrm{iii})_n$ $N(n)E_n = \{0\}$.

$(\mathrm{iv})_n$ $E_n \subseteq E_{n-1} + [-\pi(1-2^{-n})N(n-1)^{-1}, \pi(1-2^{-n})N(n-1)^{-1}]$ *if* $n \ge 1$.

$(\mathrm{v})_n$ $\operatorname{card} E_n\, h(2\pi N(n)^{-1}) \le 2^{-n}$ *if* $n \ge 1$.

$(\mathrm{vi})_n$ $\operatorname{supp} \mu_n \subseteq E_n$.

$(\mathrm{vii})_n$ $\|\mu_n\| \le 1$.

$(\mathrm{viii})_n$ $|\hat{\mu}_n(0)| \ge \frac{1}{2} + 2^{-n-1}$.

$(\mathrm{ix})_n$ $|\hat{\mu}_n(r)| \le |\hat{\mu}_{n-1}(r)|$ *if* $n \ge 1$.

(x)$_n$ $|\hat{\mu}_n(r)|\leq 2^{-n}(\omega_{|r|}\log(|r|\,h(|r|^{-1}))^{1/2}$ for $N(n-1)-Q(n-1)\leq|r|$
$\leq N(n)-Q(n)$ *if* $n\geq 1$.

(xi)$_n$ $|\hat{\mu}_n(r)|\leq 2^{-n-8}(\omega_{N(n)}\log(N(n)\,h(N(n)^{-1})h(N(n)^{-1}))^{1/2}$
for $Q(n)\leq|r|\leq N(n)-Q(n)$.

(xii)$_n$ $\omega_{N(n)}\geq 2^{2n+20}$.

To see that the induction can be started, we note that (ii)$_0$, (iv)$_0$, (v)$_0$, (ix)$_0$ and (x)$_0$ are vacuous, whilst conditions (i)$_0$, (iii)$_0$, (vi)$_0$, (vii)$_0$, (viii)$_0$, (xi)$_0$, (xii)$_0$ are automatically satisfied if we put $Q(0)=P(0)=1$, $N(0)=10^7$, $E_0=\{2\pi u/N(0)\colon u\in\mathbf{Z}\}$ and $\mu_0=N(0)^{-1}\sum_{u=1}^{N(0)}\delta_{2\pi u/N(0)}$.

Proof of Theorem 5.1 (*subject to the completion of the inductive construction*). Suppose we have constructed $E(n)$, μ_n, $P(n)$, $Q(n)$ and $N(n)$ for $n=0,1,2,\ldots$ obeying the inductive conditions. By (vii)$_n$, $\|\mu_n\|$ is bounded, so the sequence μ_n has a weak $*$ limit point μ. By (viii)$_n$, $|\hat{\mu}(0)|\geq 1/2$ so μ is non zero. By (ix)$_n$ and $(x)_n$ we know that

$$|\hat{\mu}_n(r)|\leq 2^{-m+1}\,(\omega_{|r|}\log(|r|\,h(|r|^{-1}))\,h(|r|^{-1}))^{1/2}$$

for all $N(m-1)-Q(m-1)\leq|r|\leq N(m)-Q(m)$ and all $n\geq m$ so that

$$|\hat{\mu}(r)|\leq 2^{-m+1}\,(\omega_{|r|}\log(|r|\,h(|r|^{-1}))\,h(|r|^{-1}))^{1/2}$$

for all $N(m-1)-Q(m-1)\leq|r|\leq N(m)-Q(m)$. Thus, since $N(m)-Q(m)\to\infty$ as $m\to\infty$, we have

$|\hat{\mu}(r)=0\,(\omega_{|r|}\log(|r|\,h(|r|^{-1}))\,h(|r|^{-1}))^{1/2}$ *as* $|r|\to\infty$, as required.

On the other hand, writing E for the topological limit of the E_n, we know from (vi)$_n$ that supp $\mu\subseteq E$. Using (iv)$_n$ and the fact that $N(n+1)\geq 100\,N(n)$ we see that

$$\begin{aligned}E_r&\subseteq E_m+\sum_{n=m}^{r-1}[-\pi(1-2^{-n-1})N(n)^{-1},\,\pi(1-2^{-n-1})N(n)^{-1}]\\&=E_m+\left[-\pi\sum_{n=m}^{r-1}(1-2^{-n-1})N(n)^{-1},\,\pi\sum_{n=m}^{r-1}(1-2^{-n-1})N(n)^{-1}\right]\\&\subseteq E_m+[-\pi N(m)^{-1},\,\pi N(m)^{-1}]\end{aligned}$$

for all $r>m>0$ and so $E\subseteq E_m+[-\pi N(m)^{-1},\,\pi N(m)^{-1}]$. Thus E can be covered by card E_m intervals of length $2\pi N(m)^{-1}$. Since, by (v)$_m$, card $E_m h(2\pi N(m)^{-1})\to 0$ as $m\to\infty$, it follows that E has Hausdorff h-measure 0. We have not shown explicitly that E and μ are translational, but this will be implicit in the proof of the next lemma which shows that the induction required can be performed and so completes the proof.

LEMMA 5.2. *Given* E_n, μ_n, $P(n)$, $Q(n)$ *and* $N(n)$ *satisfying the inductive conditions* (i)$_n$, (ii)$_n$, (iv)$_n$, (viii)$_n$, (ix)$_n$, *and* (xii)$_n$, *we can find* E_{n+1}, μ_{n+1}, $P(n+1)$ *and* $N(n+1)$ *satisfying all the conditions* (i)$_{n+1}$ *to* (xii)$_{n+1}$.

Proof. By Lemma 4.2, taking $\psi(r)=(2^{n+2}N(n)\,h(2\pi r^{-1})r)^{-1}$, we see that there exists an $A(n+1)$ such that, given $Q(n+1)\geq 8N(n)^6$, we can find an $L(n+1)$ such that, given $N(n+1)\geq L(n+1)$, we can find a $\sigma_{n+1}\in M(\mathbf{T})$ with

(1) $$\|\sigma_{n+1}\|\leq 1,$$

(2) $$|\hat{\sigma}_{n+1}(0)-1|\leq 1-2^{-n-3},$$

(3) $$\operatorname{supp}\sigma_{n+1}\subseteq\{2\pi u/N(n+1)\colon u\in\mathbf{Z}\}\cap[-\pi(N(n)^{-1}-N(n)^{-6}),\ \pi(N(n)^{-1}-N(n)^{-6})],$$

(4) $$\operatorname{card}\operatorname{supp}\sigma_{n+1}\leq 2^{-n-2}N(n)^{-1}(h(2\pi(N(n+1))^{-1}))^{-1},$$

(5) $$|\hat{\sigma}_{n+1}(lN(n)+s)|\leq\frac{2(|s|+1)}{|lN(n)+s|}\quad\textit{for}\quad 0\neq|lN(n)+s|\leq N(n)^5,$$

(6) $$|\hat{\sigma}_{n+1}(s)|\leq 2N(n)/|s|\quad\textit{for}\quad N(n)^5\leq|s|\leq Q(n+1),$$

(7) $$|\hat{\sigma}_{n+1}(s)|\leq A(n+1)\,(\log((N(n+1))\,h(N(n+1)^{-1}))\,h(N(n+1)^{-1}))^{1/2}\quad\textit{for}\quad Q(n+1)\leq|r|\leq N(n+1)-Q(n+1).$$

In particular, taking $Q(n+1)\geq 10^5N(n)$ and taking $N(n+1)$ to be a sufficiently large multiple of $N(n)$, we have

(7)′ $$|\hat{\sigma}_{n+1}(s)|\leq 2^{-n-4}(\omega_{N(n+1)}\log(N(n+1)\,h(N(n+1)^{-1}))\,h(N(n+1)^{-1}))^{1/2}\quad\textit{for}\quad Q(n+1)\leq|r|\leq N(n+1)-Q(n+1)$$

whilst conditions $(\mathrm{i})_{n+1}$, $(\mathrm{ii})_{n+1}$ and $(\mathrm{xii})_{n+1})$ are automatically satisfied.

Set $\mu_{n+1}=\mu_n*\sigma_{n+1}$ and $E_{n+1}=\operatorname{supp}\mu_{n+1}$. Since $N(n)E_n=\{0\}$, $N(n+1)$ is a multiple of $N(n)$, and $E_{n+1}\subseteq E_n+\operatorname{supp}\sigma_{n+1}$, the conditions $(\mathrm{iii})_{n+1}$ and $(\mathrm{iv})_{n+1}$ follow from (3). Again, since $\operatorname{card}E_{n+1}\leq\operatorname{card}E_n\operatorname{card}\operatorname{supp}\sigma_{n+1}$ and $(\mathrm{iii})_n$ shows that $\operatorname{card}E_n\leq N(n)$, condition $(\mathrm{v})_{n+1}$ is a direct consequence of (4). Condition $(\mathrm{vi})_{n+1}$ is automatic and condition $(\mathrm{vii})_{n+1}$ follows from (1) and $(\mathrm{vii})_n$ just as $(\mathrm{viii})_{n+1}$ follows from $(\mathrm{viii})_n$ and (2). Similarly, $(\mathrm{ix})_n$ is a consequence of (1) and (since $\omega_{|r|}\log(|r|\,h(|r|^{-1}))\,h(|r|^{-1})$ is monotonic decreasing) $(\mathrm{xi})_{n+1}$ is a consequence of (7)′.

Thus all that remains is to prove $(\mathrm{x})_n$. We split the range

$$N(n)-Q(n)\leq|r|\leq N(n+1)-Q(n+1)$$

into bits and prove $(*)_r$

$$|\hat{\mu}_{n+1}(r)|\leq 2^{-n-1}(\omega_{|r|}\log(|r|\,h(|r|^{-1}))\,h(|r|^{-1}))^{1/2}$$

for each bit separately.

(A) $N(n+1)-Q(n+1)\geq|r|\geq Q(n+1)$. $(*)_r$ is a consequence of $(\mathrm{xi})_n$.

(B) $Q(n+1)\geq|r|\geq N(n)^5$. We have

$$|\hat{\mu}_{n+1}(r)|\leq|\hat{\sigma}_{n+1}(r)|\leq\frac{2N(n)}{|r|}\leq|r|^{-1/2}$$

so $(*)_r$ holds.

(C) $r=lN(n)+s$ with $2\leq|l|\leq N(n)^4$, $Q(n)\leq|s|\leq N(n)-Q(n)$.

$$\begin{aligned}|\hat{\mu}_{n+1}(r)|&\leq|\hat{\sigma}_{n+1}(r)|\,|\hat{\mu}_n(r)|\\&=|\hat{\sigma}_{n+1}(lN(n)+s)|\,|\hat{\mu}_n(s)|\\&\leq\frac{4}{|l|}2^{-n-10}(\omega_{N(n)}\log(N(n)\,h(N(n)^{-1})\,h(N(n)^{-1}))^{1/2}\\&\leq 2^{-n-1}(\omega_{|r|}\log(|r|\,h(|r|^{-1}))\,h(|r|^{-1}))^{1/2}\end{aligned}$$

(since $|r|\leq 2\,|l|\,N(n)$), so $(*)_r$ holds.

(D) $r=lN(n)+s$ with $|l|\leq 1$, $Q(n)\leq|s|\leq N(n)-Q(n)$. By $(\mathrm{xi})_n$,

$$|\hat{\mu}_{n+1}(r)|\leq|\hat{\mu}_n(s)|\leq 2^{-n-1}\,(\omega_{|r|}\log(|r|\,h(|r|^{-1}))\,h(|r|^{-1}))^{1/2}$$

(since $|r|\leq 2N(n)$) so $(*)_r$ holds.

(E) $r=lN(n)+s$ with $1\leq|l|\leq N(n)^4$, $|s|\leq Q(n)$. By (5) and $(\mathrm{i})_n$,

$$|\hat{\mu}_{n+1}(r)|\leq|\hat{\sigma}_{n+1}(r)|\leq\frac{2(|s|+1)}{|lN(n)+s|}\leq|l|^{-1}N(n)^{-4/5}\leq|r|^{-1/2}$$

so $(*)_r$ holds.

We have proved Lemma 5.2 and so have proved Theorem 5.1.

References

1. J. P. Kahane, *Sur certains ensembles de Salem*, Acta Math. Acad. Sci. Hungar., vol. 21 (1970), pp. 87–89.
2. ———, *Séries de Fourier absolument convergentes*, Ergebnisse der Mathematik und ihrer Grenzgebiete Band 50, Springer Verlag Berlin, 1970.
3. J. P. Kahane and R. Salem, *Ensembles parfaits et séries trigonométriques*, Actualités Sci. Industr., No. 1301, Hermann Paris, 1963.
4. R. Kaufman, *Small subsets of finite abelian groups*, Ann. Inst. Fourier, vol. 18 (1968), fasc. 1, pp. 99–102.

University of Cambridge
Cambridge, England