ACTA ARITHMETICA
166.1 (2014)

A generalization of a theorem of Erdős–Rényi to m-fold sums and differences

by

Kathryn E. Hare and Shuntaro Yamagishi (Waterloo)

1. Introduction. Given a set $S \subseteq \mathbb{N}$, we define $R_S^m(n)$ to be the number of representations of the form $n = s_1 + \cdots + s_m$, where $s_i \in S$ and $s_1 \leq \cdots \leq s_m$. We say that the set S is *of type* $B_m(g)$ if

$$R_S^m(n) \leq g$$

for all n. In [10], Vu gives a brief history of the topic, which we paraphrase here. In 1932, Sidon, in connection with his work in Fourier analysis, investigated power series of type $\sum_{i=1}^{\infty} z^{a_i}$ when $(\sum_{i=1}^{\infty} z^{a_i})^m$ has bounded coefficients [9]. This leads to the study of sets of type $B_m(g)$. One classical question in this area is the following (see [7]):

"Let S be a set of type $B_m(g)$. How fast can $S(n)$ grow, where $S(n)$ is the number of elements of S not exceeding n?"

In [3], Erdős and Rényi gave an answer to this question for $m = 2$. This result was discussed in great detail in the monograph of Halberstam and Roth [5].

Theorem 1.1 (Erdős–Rényi). *For any $\varepsilon > 0$, there exists $g = g(\varepsilon)$ and a set $S \subseteq \mathbb{N}$ of type $B_2(g)$ such that*

$$S(n) > n^{1/2-\varepsilon}$$

for sufficiently large n.

The result is best possible up to the ε term in the exponent. Erdős–Rényi used a probabilistic argument, and their proof was presented in [5] in a more rigorous and carefully written form. This theorem can be generalized from 2-fold sums to the following theorem for arbitrary m-fold sums, as was noted

2010 *Mathematics Subject Classification*: Primary 11K31, 11B83; Secondary 43A46.
Key words and phrases: sequences, additive number theory, probabilistic methods, thin sets.

DOI: 10.4064/aa166-1-5

in [4] and [5] (without proof), and also by Vu who also observed that it can be deduced as a consequence of a more general result proven in [10].

THEOREM 1.2. *For any positive integer $m \geq 2$ and any $\varepsilon > 0$, there exists $g = g(\varepsilon, m)$ and a set $S \subseteq \mathbb{N}$ of type $B_m(g)$ such that*

$$S(n) > n^{1/m-\varepsilon}$$

for sufficiently large n.

Given a set $E(\omega) \subseteq \mathbb{N}$ we define $r_N^{(m)}(\omega)$ to be the number of ways to represent $N \in \mathbb{Z}$ as a combination of sums *and* differences of m distinct elements of $E(\omega)$. In this paper, we prove the existence of a "thick" set $E(\omega)$ and a positive constant K such that $r_N^{(m)}(\omega) < K$ for all $N \in \mathbb{Z}$. Hence, our theorem is a (partial) generalization of Theorem 1.2. The caveat here is that with $r_N^{(m)}(\omega)$ we do not allow repeated elements in the representation, for otherwise every infinite set will admit integers N with $r_N^{(m)}(\omega) = \infty$. (Take $N = 0$ when m is even, for instance.)

Our main result is the following:

THEOREM 1.3. *For any positive integer $m \geq 2$ and $\varepsilon > 0$, there exists $K = K(\varepsilon, m)$ and a set $E(\omega) \subseteq \mathbb{N}$ such that*

$$r_N^{(m)}(\omega) < K$$

for all $N \in \mathbb{Z}$, and

$$\operatorname{card}(E(\omega) \cap \{1, \ldots, n\}) \gg n^{1/m-\varepsilon}$$

for sufficiently large n.

We will also prove analogous results for $\bigoplus_0^\infty \mathbb{Z}(q)$, $\bigoplus_0^\infty \mathbb{Z}(q_n)$ for $\{q_n\}$ increasing integers, and $\mathbb{Z}(q^\infty)$ where q is prime. Here $\mathbb{Z}(m)$ denotes the cyclic group of order $m \in \mathbb{N}$ and $\mathbb{Z}(q^\infty)$ is the group of all q^nth roots of unity. The notation $\bigoplus_0^\infty$ means the countable direct sum.

In Section 4, we give an application of our results to harmonic analysis. A subset E of a discrete abelian group with dual group X is called a $\Lambda(q)$ *set* (for some $q > 2$) if whenever $f \in L^2(X)$ and the Fourier transform of f is non-zero only on E, then $f \in L^q(X)$. A *completely bounded* $\Lambda(q)$ set is defined in a similar spirit, but is more complicated and we refer the reader to Section 4 for the definition. We prove that for any integer $m \geq 2$ and $\varepsilon > 0$, every infinite discrete abelian group contains a set that is completely bounded $\Lambda(2m)$, but not $\Lambda(2m + \varepsilon)$.

We use Vinogradov's well-known notation $\ll$ and $\gg$.

2. Preliminaries. Let G be any one of $\mathbb{Z}$, $\bigoplus_0^\infty \mathbb{Z}(q)$ where $q \in \mathbb{N}$, $\mathbb{Z}(q^\infty)$ where q is prime, or $\bigoplus_0^\infty \mathbb{Z}(q_n)$ where $\{q_n\}$ are strictly increasing odd integers. (The case when not all q_n are odd requires a notational adaptation that we will leave for the reader.) We define G' to be $\mathbb{N}$ if $G = \mathbb{Z}$ and $G' = G \setminus \{0\}$ otherwise.

If $\psi \in \bigoplus_0^\infty \mathbb{Z}(q)$, then $\psi = (\psi_i)_{i=0}^\infty$, where each ψ_i is in $\mathbb{Z}(q)$ and all but finitely many ψ_i are zero. Given $\psi = (\psi_i)_{i=0}^\infty$, we call the maximum i such that $\psi_i \neq 0$ the *degree* of ψ (written $\deg \psi$). We also let $\deg 0 = -\infty$. By choosing the representative $0 \leq \psi_i < q$ for each i, we can identify $\psi \neq 0$ with the natural number $\psi_0 + \psi_1 q + \cdots + \psi_d q^d$, where $d = \deg \psi$. This gives a one-to-one correspondence between $\bigoplus_0^\infty \mathbb{Z}(q)$ and $\mathbb{N} \cup \{0\}$. Notice there are $q^{d+1} - q^d$ elements of degree d for each $d \geq 0$.

If $\psi \in \mathbb{Z}(q^\infty)$ and $\psi \neq 0$, then ψ is the argument of a primitive q^Mth root of unity for a unique choice of M; in other words, $\psi = j/q^M$ where $j \in \{1, \ldots, q^M - 1\}$ and $q \nmid j$. We let $\deg \psi = M - 1$ and $\deg 0 = -\infty$. Again, for each $d \geq 0$, there are $q^{d+1} - q^d$ elements of degree d. We can identify $\mathbb{Z}(q^\infty)$ with $\mathbb{N} \cup \{0\}$ by assigning 0 to 0, and elements of degree d to $\{q^d, q^d + 1, \ldots, q^{d+1} - 1\}$ for each $d \geq 0$ in the natural way.

In the case that $G = \bigoplus_0^\infty \mathbb{Z}(q_n)$ where q_n are strictly increasing odd integers we choose representatives from $\{-(q_n - 1)/2, \ldots, (q_n - 1)/2\}$ for each $\mathbb{Z}(q_n)$. We define the degree of $\psi = (\psi_i)_{i=0}^\infty$ in the same manner as for $\bigoplus_0^\infty \mathbb{Z}(q)$. We will identify the $2q_0 \cdots q_{d-1}$ characters $\psi = (\psi_i)$ which have degree d and dth coordinate $\psi_d = \pm r$, $r \in \mathbb{N}$, with the integers in the interval $[(2r-1)q_0 \cdots q_{d-1}, (2r+1)q_0 \cdots q_{d-1})$ (where, if $d = 0$, we understand $q_0 \cdots q_{d-1} = 1$). Hence, the characters of degree d are assigned to integers in $\{q_0 \cdots q_{d-1}, \ldots, q_0 \cdots q_d - 1\}$.

Thus, for any of the four choices of G above, we have $G' = \{\chi_n\}_{n=1}^\infty$ where χ_n is the non-zero element of G uniquely associated with the integer n.

Given real numbers α_n with $0 < \alpha_n < 1$, we let Y_n, $n = 1, 2, \ldots$, be independent Bernoulli random variables defined on a probability space (Ω, M, P), with $P(Y_n = 1) = \alpha_n$ and $P(Y_n = 0) = 1 - \alpha_n$. For each of the groups G we define random subsets

$$E(\omega) = E(\omega, G) = \{\chi_n \in G' : Y_n(\omega) = 1\}.$$

Throughout the paper we will be specifying a positive number s and putting

$$\alpha_n = n^{-s} \quad \text{when } G = \mathbb{Z},\ \bigoplus_0^\infty \mathbb{Z}(q) \text{ or } \mathbb{Z}(q^\infty) \tag{2.1}$$

and

$$\alpha_n = \begin{cases} n^{-s} & \text{if } q_0 \cdots q_{d-1} < n \leq (2\lfloor \frac{q_d}{8m} \rfloor + 1) q_0 \cdots q_{d-1} \text{ and } q_d > 8m, \\ 0 & \text{else} \end{cases} \tag{2.2}$$

when $G = \bigoplus_0^\infty \mathbb{Z}(q_n)$.

Note we have $\alpha_n \leq n^{-s}$ for all n in the last case as well.

Let $m \geq 2$ be a positive integer. For $t \in \{0, 1, \ldots, m\}$, we define

$$r_{N,t}^{(m)}(\omega) := \operatorname{card}\Big\{(a_1, \ldots, a_m) : \chi_{a_i} \in E(\omega),\ \sum_{i=1}^{t} \chi_{a_i} - \sum_{i=t+1}^{m} \chi_{a_i} = \chi_N,$$
$$a_1 < \cdots < a_t,\ a_{t+1} < \cdots < a_m,\ a_i \neq a_j \text{ for } i \neq j\Big\}.$$

For clarification, we note that when $t = 0$ and $t = m$, we mean to consider the expressions $-\sum_{i=1}^{m} \chi_{a_i} = \chi_N$ and $\sum_{i=1}^{m} \chi_{a_i} = \chi_N$, respectively, with $a_1 < \cdots < a_m$. We also define

$$r_N^{(m)}(\omega) := \sum_{t=0}^{m} r_{N,t}^{(m)}(\omega). \tag{2.3}$$

Lastly, we recall a fact about elementary symmetric functions that will be useful later.

Lemma 1. *Let $\{y_k\}_{k>0}$ be a sequence of non-negative numbers. For each $d \in \mathbb{N}$, we write*

$$\sigma_d = \sum_{k_1 < \cdots < k_d} y_{k_1} \cdots y_{k_d};$$

in other words, σ_d is the dth elementary symmetric function of the y_k. Then

$$\sigma_d \leq \sigma_1^d / d!.$$

Proof. See [5, p. 147, Lem. 13]. ∎

3. m-fold sums and differences. Our main result, Theorem 1.3, follows fairly easily from Theorem 3.3 below. This will be proven by induction, with the base case taken care of in Corollary 3.2 (following Proposition 3.1). Unless we specify otherwise in the statement of the results, in this section G can be considered to be any one of $\mathbb{Z}$, $\bigoplus_0^\infty \mathbb{Z}(q)$, $\mathbb{Z}(q^\infty)$ or $\bigoplus_0^\infty \mathbb{Z}(q_n)$.

We begin with some observations utilized in the proof of the next lemma: Suppose $\chi_n = \sum_{i=1}^{m} \varepsilon_i \chi_{n_i}$, where $\varepsilon_i = \pm 1$, n_i are distinct and all $\alpha_{n_i} \neq 0$.

When $G = \mathbb{Z}$, we have $\max_{1 \leq i \leq m} |n_i| \geq |n|/m$.

When $G = \bigoplus_0^\infty \mathbb{Z}(q)$, $\mathbb{Z}(q^\infty)$ (resp. $\bigoplus_0^\infty \mathbb{Z}(q_n)$) and $\deg \chi_n = d$, then $q^d \leq n \leq q^{d+1}$ (resp. $q_0 \cdots q_{d-1} \leq n \leq q_0 \cdots q_d$). Since $\deg(\chi_a \pm \chi_b) \leq \max\{\deg \chi_a, \deg \chi_b\}$, it follows that $\max_{1 \leq i \leq m} \deg \chi_{n_i} \geq \deg \chi_n$.

When $G = \bigoplus_0^\infty \mathbb{Z}(q_n)$ and $\chi_n = (\chi_{n,j})_{j=1}^{\infty}$ with degree $d \geq 0$, then

$$n \leq (2|\chi_{n,d}| + 1) q_0 \cdots q_{d-1}.$$

If $\max_{1 \leq i \leq m} \deg \chi_{n_i} = \deg \chi_n$ (which can occur only if $q_d > 8m$ as we are assuming all α_{n_i} are non-zero), then the modulus of the dth coordinate of χ_{n_i} is at least $\lfloor |\chi_{n,d}|/m \rfloor$ for some χ_{n_i} of maximal degree. This is because addition in the dth coordinate on the terms where $\alpha_{n_i} \neq 0$ is the same as in $\mathbb{Z}$ (recall (2.2)). Thus (whether $\max_{1\le i\le m}\deg\chi_{n_i} > \deg\chi_n$ or $\max_{1\le i\le m}\deg\chi_{n_i} = \deg\chi_n$) there must be some i such that

$$n_i \ge (2\lfloor|\chi_{n,d}|/m\rfloor - 1)q_0\cdots q_{d-1} \ge \frac{|\chi_{n,d}|}{m}q_0\cdots q_{d-1}.$$

LEMMA 2. *Given $m\ge 2$, we let $s=(m-1)/m+\theta$ where $0<\theta<1/m$, and let α_n be as in* (2.1) *and* (2.2). *Fix $\varepsilon_1,\dots,\varepsilon_m\in\{\pm 1\}$. Then*

$$\sum_{\substack{(n_1,\dots,n_m)\in\mathbb{N}^m\\ \sum_{i=1}^m \varepsilon_i\chi_{n_i}=\chi_n}} \alpha_{n_1}\cdots\alpha_{n_m} \le \begin{cases} C_m & \text{if } n=0,\\ C_m/|n|^{m\theta} & \text{if } n\ne 0,\end{cases} \tag{3.1}$$

where C_m is a positive constant dependent only on G, m and s.

Proof. We only give the proof for $G=\bigoplus_0^\infty \mathbb{Z}(q)$ and $\bigoplus_0^\infty\mathbb{Z}(q_n)$ as the other cases can be obtained by similar calculations. We use the fact that $\sum_{n\le A} n^{-s}\ll A^{1-s}$ in both these cases.

CASE $G=\bigoplus_0^\infty\mathbb{Z}(q)$. If $n\ne 0$, let $t_0\ge 0$ be such that $n\in[q^{t_0},q^{t_0+1})$. If $n=0$, we let $t_0=0$. In either case, we have $\max_{1\le i\le m}\deg\chi_{n_i}\ge t_0$ for any choice of $(n_1,\dots,n_m)$ in the summand of (3.1). Therefore, we can simplify and bound the sum (3.1) as follows:

$$\begin{aligned}\sum_{\substack{(n_1,\dots,n_m)\in\mathbb{N}^m\\ \sum_{i=1}^m \varepsilon_i\chi_{n_i}=\chi_n}} \alpha_{n_1}\cdots\alpha_{n_m} &\le \sum_{t=t_0}^\infty \sum_{\substack{\sum_{i=1}^m \varepsilon_i\chi_{n_i}=\chi_n\\ \max n_i\in[q^t,q^{t+1})}} \alpha_{n_1}\cdots\alpha_{n_m}\\ &\le \sum_{t=t_0}^\infty \frac{1}{q^{ts}} \sum_{\substack{n_i<q^{t+1}\\ 1\le i<m}} \alpha_{n_1}\cdots\alpha_{n_{m-1}} \le \sum_{t=t_0}^\infty \frac{1}{q^{ts}}\Big(\sum_{n<q^{t+1}}\alpha_n\Big)^{m-1}.\end{aligned}\tag{3.2}$$

As $\alpha_n\le n^{-s}$ we deduce that

$$\sum_{\substack{(n_1,\dots,n_m)\in\mathbb{N}^m\\ \sum_{i=1}^m \varepsilon_i\chi_{n_i}=\chi_n}} \alpha_{n_1}\cdots\alpha_{n_m} \le C_m q^{-t_0 m\theta},$$

which is equivalent to the inequality we desired to show.

CASE $G=\bigoplus_0^\infty\mathbb{Z}(q_n)$. Since $\alpha_{n_1}\cdots\alpha_{n_m}\ne 0$ if and only if all $\alpha_{n_j}\ne 0$, the comments preceding the statement of the lemma imply that if $\deg\chi_n = d\ge 0$ (the case $n=0$ will be left for the reader), then we may rewrite the sum as

$$\sum_{\substack{(n_1,\dots,n_m)\in\mathbb{N}^m\\ \sum_{i=1}^m \varepsilon_i\chi_{n_i}=\chi_n}} \alpha_{n_1}\cdots\alpha_{n_m} = \sum_{k=0}^\infty \sum_{\substack{\sum_{i=1}^m \varepsilon_i\chi_{n_i}=\chi_n\\ \max n_i\in[2^k,2^{k+1})q_0\cdots q_{d-1}|\chi_{n,d}|/m}} \alpha_{n_1}\cdots\alpha_{n_m}$$

$$\leq \sum_{k=0}^{\infty}(2^k q_0\cdots q_d|\chi_{n,d}|/m)^{-s}\Big(\sum_{j\leq 2^{k+1}q_0\cdots q_{d-1}|\chi_{n,d}|/m}\alpha_j\Big)^{m-1}$$
$$\ll \sum_{k=0}^{\infty}(2^k q_0\cdots q_{d-1}|\chi_{n,d}|/m)^{-s}(2^{k+1}q_0\cdots q_{d-1}|\chi_{n,d}|/m)^{(1-s)(m-1)}$$
$$\ll \sum_{k=0}^{\infty}(2^k q_0\cdots q_{d-1}|\chi_{n,d}|/m)^{-\theta m}.$$

The final expression is comparable to $n^{-\theta m}$. ∎

We will first study $r_N^{(m)}(\omega)$ with $m=2$.

Proposition 3.1. *Let $s=1/2+\theta$ where $0<\theta<1/2$. Then, for any $\varepsilon>0$, there exists $K=K(G,s)$ such that*

$$\sum_N P(\{\omega\in\Omega : r_N^{(2)}(\omega)\geq K\})<\varepsilon.$$

Proof. By definition, we have

$$r_N^{(2)}(\omega)=\operatorname{card}\{(a,b):\chi_a,\chi_b\in E(\omega),\ \pm(\chi_a+\chi_b)=\chi_N,\ a<b,\text{ or }\chi_a-\chi_b=\chi_N,\ a\neq b\}. \tag{3.3}$$

If $\chi_{a'}+\chi_{b'}=\chi_N$ and $\chi_{a'}+\chi_{c'}=\chi_N$, then $b'=c'$, and similarly if we consider subtraction. Thus, given any $\chi_{a'}$ there are at most four ways in which $\chi_{a'}$ could appear as one of χ_a or χ_b in the three equations considered in (3.3). Hence, if $r_N^{(2)}(\omega)\geq K$, then there exist at least $\lfloor K/4\rfloor$ pairs (a_i,b_i), $1\leq i\leq\lfloor K/4\rfloor$, counted in (3.3), such that every element of the set $\{a_i,b_j\}_{1\leq i,j\leq\lfloor K/4\rfloor}$ is distinct. By the pigeon-hole principle, one of the three equations considered in (3.3) must be satisfied by at least one third of these $\lfloor K/4\rfloor$ pairs. Without loss of generality, we suppose it is the equation $\chi_a+\chi_b=\chi_N$ with $a<b$, as the other two cases can be treated in a similar manner. Let $L=\lfloor K/12\rfloor$. By independence, we have

$$\begin{aligned}P(\{\omega\in\Omega : r_N^{(2)}(\omega)\geq K\})&\leq P(\{\omega\in\Omega:\text{there exist } L \text{ pairs } (a_i,b_i)\\&\qquad\text{such that } \chi_{a_i},\chi_{b_i}\in E(\omega),\chi_{a_i}+\chi_{b_i}=\chi_N,\\&\qquad a_i<b_i,\ \text{and } a_i,b_j \text{ all distinct}\})\\&\leq\sum_{S(L)}\prod_{i=1}^{L}P(\{\omega\in\Omega_m:\chi_{a_i},\chi_{b_i}\in E(\omega)\}),\end{aligned} \tag{3.4}$$

where $S(L)$ is the collection of all L distinct pairs, (a_i,b_i), $1\leq i\leq L$, such that $\chi_{a_i}+\chi_{b_i}=\chi_N$ and $a_i<b_i$.

Since the last inequality of (3.4) gives us an Lth elementary symmetric function, we can bound it by Lemmas 1 and 2:

$$P(\{\omega \in \Omega : r_N^{(2)}(\omega) \geq K\}) \leq \frac{1}{L!}\Big(\sum_{S(1)} \alpha_a \alpha_b\Big)^L \leq \begin{cases} \frac{1}{L!}C^L & \text{if } N = 0, \\ \frac{1}{L!}C^L/|N|^{2\theta L} & \text{if } N \neq 0, \end{cases}$$

for some positive constant C. As $\theta > 0$, we obtain

$$\sum_{N=-\infty}^{\infty} P(r_N^{(2)}(\omega) \geq K) \leq 2 \sum_{N=2}^{\infty} \frac{1}{L!} C^L \frac{1}{|N|^{2\theta L}} + 3\frac{1}{L!}C^L < \varepsilon, \tag{3.5}$$

for L large enough. Notice that if $G = \bigoplus_0^\infty \mathbb{Z}(q)$ or $\mathbb{Z}(q^\infty)$ or $\bigoplus_0^\infty \mathbb{Z}(q_n)$, then we only need to take the sum on the left side of (3.5) from $N = 0$ to ∞. ∎

Corollary 3.2. *Let $s = 1/2 + \theta$ and $0 < \theta < 1/2$. Given any $\varepsilon > 0$, there exist $K = K(G, s)$ and $\Omega_2 \subseteq \Omega$ such that $P(\Omega_2) \geq 1 - \varepsilon$ and $r_N^{(2)}(\omega) < K$ for all N and all $\omega \in \Omega_2$.*

Proof. By Proposition 3.1, we can find K with $\sum_N P(r_N^{(2)}(\omega) \geq K) < \varepsilon$. Let $\Omega_2 = \{\omega \in \Omega : r_N^{(2)}(\omega) < K \text{ for all } N\}$. Then

$$\begin{aligned} P(\Omega_2^c) &= P(\{\omega \in \Omega : \text{there exists } N \text{ such that } r_N^{(2)}(\omega) \geq K\}) \\ &\leq \sum_N P(r_N^{(2)}(\omega) \geq K) < \varepsilon. \ \blacksquare \end{aligned}$$

We complete the induction argument in the following proof. The argument is similar to the base case, but slightly more involved due to the larger value of m. We will then prove the required density property of the subsets in Corollary 3.6.

Theorem 3.3. *Let $m \geq 2$ be a positive integer. If $s = (m-1)/m + \theta$ for $0 < \theta < 1/m$, then for all $\varepsilon > 0$ there exist $K_m = K_m(G, \varepsilon, s)$ and $\Omega_m \subseteq \Omega$ such that $P(\Omega_m) \geq 1 - \varepsilon$ and $r_N^{(m)}(\omega) < K_m$ for all N and all $\omega \in \Omega_m$.*

Proof. We proceed by induction. Corollary 3.2 gives us the base case. Suppose the statement holds for $m_0 < m$. Fix $\varepsilon > 0$. We may rewrite s as $s = (m_0 - 1)/m_0 + \theta'$ with $0 < \theta' < 1/m_0$. Thus, by the inductive hypothesis there exist K_{m_0} and Ω_{m_0} such that $P(\Omega_{m_0}) \geq 1 - \varepsilon/(2(m_0+2))$ and $r_N^{(m_0)}(\omega) < K_{m_0}$ for all N and for all $\omega \in \Omega_{m_0}$.

Let $\omega \in \Omega_{m_0}$ and fix $t \in \{0, 1, \ldots, m_0 + 1\}$ and an integer N. Suppose for each $i = 1, \ldots, K$ that

$$\chi_{a_1^{(i)}} + \cdots + \chi_{a_t^{(i)}} - (\chi_{a_{t+1}^{(i)}} + \cdots + \chi_{a_{m_0+1}^{(i)}}) = \chi_N, \tag{3.6}$$

with

$$a_1^{(i)} < \cdots < a_t^{(i)}, \quad a_{t+1}^{(i)} < \cdots < a_{m_0+1}^{(i)} \quad \text{and} \quad a_u^{(i)} \neq a_{u'}^{(i)} \quad \text{if } u \neq u'. \tag{3.7}$$

Assume there exist some $i_1, \dots, i_r$ and $s_1, \dots, s_r$ such that $a_{s_1}^{(i_1)} = a_{s_j}^{(i_j)}$ for all $j \in \{1, \dots, r\}$. Then, for each $j \in \{1, \dots, r\}$, we have

$$(3.8)\quad \chi_{a_1^{(i_j)}} + \dots + \chi_{a_t^{(i_j)}} - (\chi_{a_{t+1}^{(i_j)}} + \dots + \chi_{a_{m_0+1}^{(i_j)}}) + \varepsilon_j \chi_{a_{s_j}^{(i_j)}} = \chi_N + \varepsilon_j \chi_{a_{s_1}^{(i_1)}},$$

where ε_j is -1 if $s_j \le t$ and $+1$ if $s_j > t$, making the left hand side of (3.8) into a combination of m_0 terms. This gives us a total of r representations for $\chi_N + \chi_{a_{s_1}^{(i_1)}}$ and $\chi_N - \chi_{a_{s_1}^{(i_1)}}$ as a combination of m_0 terms. By the inductive hypothesis, we have $r \le 2K_{m_0}$. Therefore, it follows that each (m_0+1)-tuple $(a_1^{(i)}, \dots, a_{m_0+1}^{(i)})$, $1 \le i \le K$, has at most $2(m_0+1)K_{m_0}$ other (m_0+1)-tuples which it may possibly share an entry with. Hence, by reordering if necessary, there exists a subset of $L = \lfloor \frac{K}{2(m_0+1)K_{m_0}} \rfloor$ (m_0+1)-tuples $(a_1^{(l)}, \dots, a_{m_0+1}^{(l)})$, $1 \le l \le L$, which satisfy (3.6) and (3.7), and the additional condition that the elements of the set $\{a_j^{(l)}\}_{1 \le j \le m_0+1,\, 1 \le l \le L}$ are distinct.

From the discussion above, and by independence, we have

$$\begin{aligned}(3.9)\quad & P(\{\omega \in \Omega_{m_0} : r_{N,t}^{(m_0+1)}(\omega) \ge K\}) \\ & \le P\Big(\{\omega \in \Omega_{m_0} : \text{there exist } L\ (m_0+1)\text{-tuples } (a_1^{(l)}, \dots, a_{m_0+1}^{(l)}), \\ & \qquad 1 \le l \le L,\ \text{such that } \sum_{s=1}^{t} \chi_{a_s^{(l)}} - \sum_{s=t+1}^{m_0+1} \chi_{a_s^{(l)}} = \chi_N, \\ & \qquad \text{all } a_j^{(l)} \text{ are distinct, and } \chi_{a_j^{(l)}} \in E(\omega)\}\Big) \\ & \le \sum_{S(L)} \prod_{l=1}^{L} P(\{\omega \in \Omega_{m_0} : \chi_{a_j^{(l)}} \in E(\omega),\ 1 \le j \le m_0+1\}),\end{aligned}$$

where $S(L)$ is the collection of all L distinct (m_0+1)-tuples $(a_1^{(l)}, \dots, a_{m_0+1}^{(l)})$, $1 \le l \le L$, such that

$$\sum_{s=1}^{t} \chi_{a_s^{(l)}} - \sum_{s=t+1}^{m_0+1} \chi_{a_s^{(l)}} = \chi_N,$$

and $a_i^{(l)} \ne a_j^{(l)}$ if $i \ne j$.

Since the last inequality of (3.9) gives us an Lth elementary symmetric function, we can bound it by Lemmas 1 and 2:

$$\begin{aligned} P(\omega \in \Omega_{m_0} : r_{N,t}^{(m_0+1)}(\omega) \ge K\}) &\le \frac{1}{L!}\Big(\sum_{S(1)} \alpha_{a_1} \dots \alpha_{a_{m_0+1}}\Big)^L \\ &\le \begin{cases} \frac{1}{L!} C_{m_0+1}^L & \text{if } N = 0, \\ \frac{1}{L!} (C_{m_0+1}/|N|^{(m_0+1)\theta})^L & \text{if } N \ne 0, \end{cases}\end{aligned}$$

for some positive constant C_{m_0+1}.

For each $t \in \{0, 1, \ldots, m_0 + 1\}$, let $\widetilde{\Omega}_t = \{\omega \in \Omega_{m_0} : r_{N,t}^{(m_0+1)}(\omega) < K$ for all $N\}$. We can then follow the arguments of Proposition 3.1 and Corollary 3.2 and deduce the existence of K such that for any $t \in \{0, 1, \ldots, m_0 + 1\}$,

$$\begin{aligned} (3.10) \quad P(\widetilde{\Omega}_t^c) &\le P(\{\omega \in \Omega_{m_0} : \text{there exists } N \text{ such that } r_{N,t}^{(m_0+1)}(\omega) \ge K\}) \\ &\quad + P(\Omega/\Omega_{m_0}) \\ &\le \sum_N P(\{\omega \in \Omega_{m_0} : r_{N,t}^{(m_0+1)}(\omega) \ge K\}) + \frac{\varepsilon}{2(m_0+2)} < \frac{\varepsilon}{m_0+2}. \end{aligned}$$

If we let

$$K_{m_0+1} = (m_0+2)K \quad \text{and} \quad \Omega_{m_0+1} = \bigcap_{t=0}^{m_0+1} \widetilde{\Omega}_t,$$

the result follows by (2.3). ■

Corollary 3.4. *Let $m \ge 2$ be a positive integer. If $s = (m-1)/m + \theta$ for $0 < \theta < 1/m$, then for a.e. ω,*

$$\sup_N r_N^{(m)}(\omega) < \infty.$$

Proof. This follows easily from Theorem 3.3. ■

To prove Theorem 1.3 we make use of the following variant of the Strong law of large numbers (cf. [5, p. 140, Thm. 11]). We denote by $\operatorname{Exp}(Y)$ the expectation of the random variable Y.

Theorem 3.5. *Let $\{Y_i\}$ be simple, independent random variables and $S_N = \sum_{i=1}^N Y_i$. Assume $\operatorname{Exp}(Y_i) > 0$, $\lim_{N\to\infty} S_N = \infty$ and*

$$\sum_i \frac{\operatorname{Var} Y_i}{(\operatorname{Exp}(S_i))^2} < \infty.$$

Then $S_N/\operatorname{Exp}(S_N) \to 1$ as $N \to \infty$ a.e.

Corollary 3.6. *Let $m \ge 2$ be a positive integer. Given any $\varepsilon > 0$, there exists $K_m = K_m(G, \varepsilon)$ and a set $E(\omega) \subseteq G'$ such that*

$$r_N^{(m)}(\omega) < K_m$$

for all N, and there is a constant $c = c(G, m, \varepsilon)$ such that

$$\text{(3.11)} \qquad \operatorname{card}(\{\chi_1, \ldots, \chi_n\} \cap E(\omega)) \ge c n^{1/m-\varepsilon}$$

for all n when $G = \mathbb{Z}$, $\bigoplus_0^\infty \mathbb{Z}(q)$ or $\mathbb{Z}(q^\infty)$, and for infinitely many n when $G = \bigoplus_0^\infty \mathbb{Z}(q_j)$.

Proof. Let $s = (m-1)/m + \varepsilon$. The result follows easily from Theorem 3.5 when $G = \mathbb{Z}$, $\bigoplus_0^\infty \mathbb{Z}(q)$ or $\mathbb{Z}(q^\infty)$.

In the case that $G = \bigoplus_0^\infty \mathbb{Z}(q_n)$, let $\{j_i\}$ be the indices such that $\alpha_{j_i} \neq 0$. Put $Z_i = Y_{j_i}$ and $S_N = \sum_{i=1}^N Z_i$. Then $\operatorname{Var} Z_i \leq \operatorname{Exp}(Y_{j_i}) \leq j_i^{-s}$ and $\operatorname{Exp}(S_N) = \operatorname{Exp}(\sum_{i=1}^{j_N} Y_i)$. If we suppose $j_N \in [q_0 \cdots q_d, q_0 \cdots q_{d+1})$ (which implies $j_N \leq \big(2\lfloor \frac{q_{d+1}}{8m} \rfloor + 1\big) q_0 \cdots q_d$), then

$$\operatorname{Exp}(S_N) = \sum_{j<q_0\cdots q_d} \alpha_j + \sum_{j=q_0\cdots q_d}^{j_N} \alpha_j. \tag{3.12}$$

Provided d is suitably large, the first sum is at least

$$\begin{aligned}\sum_{j=q_0\cdots q_{d-1}}^{q_0\cdots q_d - 1} \alpha_j \geq \sum_{j=q_0\cdots q_{d-1}+1}^{q_0\cdots q_d/8m-1} j^{-s} &\gg (q_0 \cdots q_d/4m)^{1-s} - (q_0 \cdots q_{d-1})^{1-s} \\ &\gg (q_0 \cdots q_d)^{1-s}.\end{aligned}$$

If $q_0 \cdots q_d < j \leq j_N$, then we must also have $\alpha_j = j^{-s}$. Hence the second sum in (3.12) is equal to $\sum_{j=q_0\cdots q_d+1}^{j_N} j^{-s}$ and that is comparable to $j_N^{1-s} - (q_0 \cdots q_d)^{1-s}$. Putting these together shows that $\operatorname{Exp}(S_N) \gg j_N^{1-s}$.

One can also easily check that

$$\sum_{j \leq q_0 \cdots q_d} \alpha_j \ll j_N^{1-s},$$

so that $\operatorname{Exp}(S_N)$ is comparable to j_N^{1-s}. Thus Theorem 3.5 can again be applied to deduce that for a.e. ω,

$$S_N(\omega) = \operatorname{card}(E(\omega) \cap \{\chi_1, \ldots, \chi_{j_N}\}) \gg j_N^{1-s}.$$

In particular, for large d,

$$\begin{aligned}\operatorname{card}\Big(E(\omega) \cap \prod_{n=0}^d \mathbb{Z}(q_n)\Big) &= \operatorname{card}(E(\omega) \cap \{\chi_1, \ldots, \chi_{(2\lfloor q_d/8m \rfloor + 1) q_0 \cdots q_{d-1}}\}) \\ &\gg ((2\lfloor q_d/8m \rfloor + 1) q_0 \cdots q_{d-1})^{1-s} \gg (q_0 \cdots q_d)^{1-s}. \ \blacksquare\end{aligned}$$

4. Application to the existence of thin sets in harmonic analysis. In this section, G will denote any discrete abelian group with compact dual group X. The groups $\mathbb{Z}$, $\bigoplus_0^\infty \mathbb{Z}(q)$, $\bigoplus_0^\infty \mathbb{Z}(q_n)$, and $\mathbb{Z}(q^\infty)$ are examples of such discrete groups. The symbol $\widehat{f}$ denotes the Fourier transform of the integrable function f defined on X. A subset E of G is said to be a $\Lambda(p)$ *set* for $p > 2$ if there is a constant C_p such that $\|f\|_p \leq C_p \|f\|_2$ whenever f is an E-trigonometric polynomial, meaning $\widehat{f}$ is non-zero only on E. As $L^p(X) \subseteq L^q(X)$ if $p \geq q$, it follows that if E is $\Lambda(p)$, then it is $\Lambda(q)$ for all $q \leq p$.

This notion was introduced for subsets of $\mathbb{Z}$ by Rudin [8], who proved many important facts about $\Lambda(p)$ sets. In particular, he showed that if $E \subseteq \mathbb{Z}$ is $\Lambda(p)$, then for all integers a, d,

$$\operatorname{card}(E \cap \{a+d, \ldots, a+Nd\}) \ll N^{2/p}. \tag{4.1}$$

He also showed that if for some integer $m \geq 2$,

$$\sup_{n \in \mathbb{Z}} (\operatorname{card}\{(n_1, \ldots, n_m) \in E^m : n = n_1 + \cdots + n_m\}) < \infty, \tag{4.2}$$

then E is $\Lambda(2m)$. Rudin used these properties to construct examples of subsets of $\mathbb{Z}$ which were $\Lambda(2m)$ for a specified integer $m \geq 2$, but not $\Lambda(2m+\varepsilon)$ for any $\varepsilon > 0$. Hajela [4] extended Rudin's properties and constructions to various other discrete abelian groups, although only achieving the existence of "exact" $\Lambda(2m)$ sets for $m < q$ when $G = \bigoplus_0^\infty \mathbb{Z}(q)$ for q prime, and for $m = 2$ when $G = \mathbb{Z}(q^\infty)$. Later, Bourgain [1] completely settled this problem by using sophisticated probabilistic methods to prove the existence of exact sets $\Lambda(p)$ for all $p > 2$ and all infinite, discrete abelian groups G.

Using Pisier's operator space complex interpolation, Harcharras [6] introduced the notion of completely bounded $\Lambda(p)$ sets: Let $p > 2$. A set $E \subseteq G$ is called *completely bounded* $\Lambda(p)$ (cb$\Lambda(p)$ for short) if there is a constant C_p such that

$$\|f\|_{L^p(X,S_p)} \leq C_p \max\Big[\Big\|\Big(\sum_{\gamma \in E} \widehat{f}(\gamma)^* \widehat{f}(\gamma)\Big)^{1/2}\Big\|_{S_p}, \Big\|\Big(\sum_{\gamma \in E} \widehat{f}(\gamma) \widehat{f}(\gamma)^*\Big)^{1/2}\Big\|_{S_p}\Big]$$

for all S_p-valued, E-trigonometric polynomials defined on X. Here S_p denotes the Schatten p-class with $\|T\|_{S_p} = (\operatorname{tr}|T|^p)^{1/p}$ and

$$\|f\|_{L^p(X,S_p)} = \Big(\int_X \|f(x)\|_{S_p}^p \, dx\Big)^{1/p}.$$

Harcharras showed that completely bounded $\Lambda(p)$ sets are always $\Lambda(p)$, but not conversely. She also improved upon Rudin's condition (4.2) by establishing that $E \subseteq G$ is cb$\Lambda(2m)$ for integer $m \geq 2$ if

$$\sup_{\chi \in G} \Big(\operatorname{card}\Big\{(\chi_1, \ldots, \chi_m) \in E^m : \chi = \sum_{j=1}^m (-1)^j \chi_j \text{ with } \chi_j \text{ distinct}\Big\}\Big) < \infty. \tag{4.3}$$

We remark that this condition was new even for $\Lambda(2m)$ sets. Harcharras used this property to construct examples of subsets of $\mathbb{Z}$ that were cb$\Lambda(2m)$ but not $\Lambda(2m+\varepsilon)$ for any $\varepsilon > 0$.

Here we will generalize upon this result by using (4.3) to show that every infinite, discrete abelian group G admits a set that is cb$\Lambda(2m)$, but not $\Lambda(2m+\varepsilon)$ for any given $\varepsilon > 0$. This will use the work of the previous part of the paper, as well as the following known generalization of (4.1).

LEMMA 3 ([2]). *If $E \subseteq G$ is a $\Lambda(p)$ set for some $p > 2$, then there is a constant C such that* $\operatorname{card}(E \cap Y) \leq CN^{2/p}$ *whenever $Y \subseteq G$ is either an arithmetic progression or a finite subgroup of cardinality N.*

Fix an integer $m \geq 2$ and $\varepsilon > 0$. We will first consider $G = \mathbb{Z}$, $\mathbb{Z}(q^\infty)$, $\bigoplus_0^\infty \mathbb{Z}(q)$ or $\bigoplus_0^\infty \mathbb{Z}(q_n)$, where the q_n are strictly increasing odd primes. We denote the elements of G' by $\{\chi_n\}_{n=1}^\infty$, as described in the previous section, and let $E(\omega)$ be the random sets defined previously, with $s = (m-1)/m + \theta$ where $\theta > 0$ is chosen so that $1 - s > 2/(2m + \varepsilon)$.

PROPOSITION 4.1. *For a.e. ω, $E(\omega)$ is* $\mathrm{cb}\Lambda(2m)$ *but not $\Lambda(2m + \varepsilon)$.*

Proof. In the notation of (2.3), Haracharras' condition could be expressed as

$$E(\omega) \text{ is } \mathrm{cb}\Lambda(2m) \quad \text{if } \sup_N r_N^{(m)}(\omega) < \infty$$

and we have already seen that $\sup_N r_N^{(m)}(\omega)$ is finite for a.e. ω by Corollary 3.4. Also, Corollary 3.6 shows that for a.e. ω,

$$\operatorname{card}(E(\omega) \cap \{\chi_1, \ldots, \chi_N\}) \gg N^{1-s}$$

when $G = \mathbb{Z}$, $\mathbb{Z}(q^\infty)$ or $\bigoplus_0^\infty \mathbb{Z}(q)$, and

$$\operatorname{card}(E(\omega) \cap \{\chi_1, \ldots, \chi_{q_0 \cdots q_N}\}) \gg (q_0 \cdots q_N)^{1-s}$$

for sufficiently large N when $G = \bigoplus_0^\infty \mathbb{Z}(q_n)$.

If $G = \mathbb{Z}$, then $\{\chi_1, \ldots, \chi_N\}$ is an arithmetic progression of length N. If $G = \mathbb{Z}(q^\infty)$ or $\bigoplus_0^\infty \mathbb{Z}(q)$, then $\{\chi_1, \ldots, \chi_{q^N-1}\}$ is a subset of a subgroup of cardinality q^N, and similarly for $G = \bigoplus_0^\infty \mathbb{Z}(q_n)$, but with q^N replaced by $q_0 \cdots q_N$. In all cases, the choice of s together with Lemma 3 implies that $E(\omega)$ is not $\Lambda(2m + \varepsilon)$ for a.e. ω. ∎

THEOREM 4.2. *Let $m \geq 2$ be an integer and $\varepsilon > 0$. Every infinite discrete abelian group G contains a set E that is* $\mathrm{cb}\Lambda(2m)$ *but not $\Lambda(2m + \varepsilon)$.*

Proof. As observed in [2], any such group G contains a subgroup isomorphic to one of $\mathbb{Z}$, $\mathbb{Z}(q^\infty)$, $\bigoplus_0^\infty \mathbb{Z}(q)$ for q prime, or $\bigoplus_0^\infty \mathbb{Z}(q_n)$, where the q_n are strictly increasing odd primes.

Observe that if G_0 is a subgroup of G and f is an S_p-valued G_0-polynomial, then f is constant on the cosets of $G_0^\perp$, the annihilator of G_0. The same is true for $\|f\|_{S_{2m}}$, for any integer m. It follows from this that if $E \subseteq G_0$ is a $\mathrm{cb}\Lambda(2m)$ set, then E viewed as a subset of G is also $\mathrm{cb}\Lambda(2m)$, and that $E \subseteq G_0$ is a $\Lambda(2m + \varepsilon)$ set if and only if E viewed as a subset of G is $\Lambda(2m + \varepsilon)$.

Hence it suffices to prove the theorem for the four subgroups listed above, and this was done in the previous proposition. ∎

Acknowledgments. This research is partially supported by NSERC.

References

[1] J. Bourgain, *Bounded orthogonal systems and the $\Lambda(p)$-set problem*, Acta Math. 162 (1989), 227–245.

[2] R. Edwards, E. Hewitt and K. Ross, *Lacunarity for compact groups I*, Indiana Univ. Math. J. 21 (1972), 787–806.

[3] P. Erdős and A. Rényi, *Additive properties of random sequences of positive integers*, Acta Arith. 6 (1960), 83–110.

[4] D. Hajela, *Construction techniques for some thin sets in duals of compact abelian groups*, Ann. Inst. Fourier (Grenoble) 36 (1986), no. 3, 137–166.

[5] H. Halberstam and K. F. Roth, *Sequences*, Springer, New York, 1983.

[6] A. Harcharras, *Fourier analysis, Schur multipliers on S^p and non-commutative $\Lambda(p)$-sets*, Studia Math. 137 (1999), 203–260.

[7] C. Pomerance and A. Sárközy, *Combinatorial number theory*, Chapter 20 of Handbook of Combinatorics, R. Graham et al. (eds.), North-Holland, Amsterdam, 1995, 967–1018.

[8] W. Rudin, *Trigonometric series with gaps*, J. Math. Mech. 9 (1960), 203–227.

[9] S. Sidon, *Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier-Reihen*, Math. Ann. 106 (1932), 536–539.

[10] V. H. Vu, *On a refinement of Waring's problem*, Duke Math. J. 105 (2000), 107–134.

Kathryn E. Hare, Shuntaro Yamagishi
Department of Pure Mathematics
University of Waterloo
Waterloo, ON, Canada N2L 3G1
E-mail: kehare@uwaterloo.ca
syamagis@uwaterloo.ca

Received on 1.11.2013
and in revised form on 18.6.2014 (7632)