COLLOQUIUM MATHEMATICUM

VOL. LXIX 1995 FASC. 1

ON PARTITIONING SIDON SETS WITH QUASI-INDEPENDENT SETS

BY

K. J. HARRISON (MURDOCH, WESTERN AUSTRALIA) AND
L. THOMAS RAMSEY (HONOLULU, HAWAII)

Sidon subsets have been characterized by Pisier as having proportional quasi-independent subsets [8]. There remains the open problem of whether Sidon subsets of $\mathbb{Z}$ must be finite unions of quasi-independent sets. Grow and Whicher produced an interesting example of a Sidon set whose Pisier proportionality was $1/2$ but the set was not the union of two quasi-independent sets [3]. On the other hand, the present paper provides probabilistic evidence in favor of an affirmative answer with a construction of random Sidon sets which borrows heavily from ideas of Professors Katznelson and Malliavin [6, 4, 5]. Katznelson provided a random construction of integer Sidon sets which, almost surely, were not dense in the Bohr compactifaction of the integers [4, 5]. This paper presents a modification of that construction and emphasizes a stronger conclusion which is implicit in the earlier construction: almost surely, the random sets are finite unions of quasi-independent sets (also of N-independent sets, defined below). In this paper, random subsets of size $O(\log n_j)$ are chosen from disjoint arithmetic progressions of length n_j (the maximum density allowed for a Sidon set), with $n_j \to \infty$ fast enough and the progressions rapidly dilated as $j \to \infty$.

This paper concludes with several deterministic results. If every Sidon subset of $\mathbb{Z}\setminus\{0\}$ is a finite union of quasi-independent sets, then the required number of quasi-independent sets is bounded by a function of the Sidon constant. Analogs of this result are proved for all Abelian groups, and for other special Sidon sets (the N-independent sets). Throughout this paper, unspecified variables denote positive integers.

Definition. A subset $F \subset \mathbb{Z}$ is said to be *N-independent* if and only if, for all integers $\alpha_x \in [-N, N]$, with $\alpha_x \neq 0$ for at most finitely many x,

1991 *Mathematics Subject Classification*: Primary 43A56.
Key words and phrases: Sidon, quasi-independent, dissociate, N-independent.

$$\sum_{x\in F}\alpha_x x = 0 \to \sum_{x\in F}|\alpha_x| = 0.$$

That is, among all linear relations with integer coefficients from $[-N, N]$, only the trivial relation holds. (This definition differs from that of J. Bourgain, for whom N-independence is a weaker form of quasi-independence.)

When $N = 1$ such sets are called *quasi-independent* and are Sidon [8]; when $N = 2$ they are called *dissociate* [7].

THEOREM 1. *Let $K \in \mathbb{R}^+$, let integers M_j and p_j satisfy*

$$0 \le p_j \le K\log(j^2) \tag{1}$$

and

$$M_j > K\sum_{q<j} M_q q^3 \log(q^2), \tag{2}$$

and set Q_j equal to $M_j \cdot \{1,\ldots,j^2\}$. For each j, and each $i \in [1, p_j]$, choose $g_{j,i}$ from Q_j independently with uniform probability. Given N, let $\lambda \in (0, 1/2]$ so that

$$W(N,K,\lambda) = K[\lambda\log(2N/\lambda) + (\lambda-1)\log(1-\lambda)] < 1/2. \tag{3}$$

Then, for almost all choices of $\{g_{j,i}\}$, the index set for the random variables can be partitioned into $\lceil 1/\lambda\rceil + 1$ sets of which one is finite and the rest index N-independent subsets of $\mathbb{Z}$.

Remark 1. Note that $\{x\}$ is N-independent when $x \neq 0$. Since $0 \notin Q_j$, the finite set in Theorem 1 is also a finite union of N-independent sets. Since N-independent sets are Sidon [8], as are the unions of finitely many Sidon sets [7], almost all choices produce a Sidon set.

Remark 2. $W(N,K,\lambda)$ is a non-decreasing function of $\lambda \in (0, 1/2]$:

$$\frac{\partial W(N,K,\lambda)}{\partial\lambda} = K\log(2N) + K\log((1-\lambda)/\lambda) > 0.$$

Since $\lim_{\lambda\to 0^+} W(N,K,\lambda) = 0$, there is a maximum $\lambda(N,K) \in (0, 1/2]$ such that

$$W(N,K,\lambda(N,K)) \le 1/2.$$

The theorem applies to any λ in the non-empty interval $(0, \lambda(N,K))$.

Likewise, $W(N,K,\lambda)$ is linear in K with a positive slope for $\lambda \in (0, 1/2]$. In that case, there is a unique $K(N,\lambda) > 0$ such that $W(N, K(N,\lambda), \lambda) = 1/2$. For example, $K(N, 1/2) = \log(8N)^{-1}$. The theorem applies to any K in the non-empty interval $(0, K(N,\lambda))$.

Condition (2) implies the next lemma.

LEMMA 2. *Let $K \in \mathbb{R}^+$, integers M_j satisfy condition* (2), $Q_j = M_j \cdot \{1, \ldots, j^2\}$, *and S_j be a subset of Q_j with at most $K \log(j^2)$ points. A set $E \subset \bigcup_{j=N}^{\infty} S_j$ is N-independent if and only if, for all $j \ge N$, the sets $E \cap S_j$ are N-independent.*

Proof. The "only if" follows from the fact that any subset of an N-independent set is likewise N-independent. Consider the contrapositive of the converse. Assume that E is not N-independent and let α be the coefficient sequence for a non-trivial "N-relation" in E. Let J be the largest integer for which there is some $x \in S_J$ with $\alpha_x \ne 0$. If $J = N$, then α is supported in $E \cap S_N$; hence $E \cap S_N$ is not N-independent. Suppose that $J > N$. Then

$$0 = \sum_{N \le q < J} \sum_{x \in E \cap S_q} \alpha_x x + \sum_{x \in E \cap S_J} \alpha_x x.$$

For $x \in S_q$, $|x| \le q^2 M_q$. Thus

$$\begin{aligned}\Big| \sum_{N \le q < J} \sum_{x \in E \cap S_q} \alpha_x x \Big| &\le \sum_{N \le q < J} \sum_{x \in E \cap S_q} |\alpha_x x| \le N \sum_{N \le q < J} \sum_{x \in E \cap S_q} |x| \\ &\le N \sum_{N \le q < J} K \log(q^2) q^2 M_q \le K \sum_{N \le q < J} \log(q^2) q^3 M_q \\ &< M_J, \qquad \text{by condition (2).}\end{aligned}$$

Thus

$$\Big| \sum_{x \in E \cap S_J} \alpha_x x \Big| = \Big| - \sum_{N \le q < J} \sum_{x \in E \cap S_q} \alpha_x x \Big| < M_J.$$

However, each $x \in S_J$ is a multiple of M_J; therefore

$$\sum_{x \in E \cap S_J} \alpha_x x = 0.$$

Since $\alpha_x \ne 0$ for at least one $x \in E \cap S_J$, it follows that $E \cap S_J$ is not N-independent. Thus, whether $J = N$ or $J > N$, $E \cap S_J$ is not N-independent. ■

LEMMA 3. *Assume the hypotheses and notations of Theorem* 1. *Let $\{x_i\}_{i=1}^{p_j}$ range over random selections from Q_j. Let P_j denote this proposition: for all $\alpha = \{\alpha_i\}_{i=1}^{p_j}$, with α_i an integer in $[-N, N]$, the equality $\sum_{i=1}^{p_j} \alpha_i x_i = 0$ implies that $\sum_{i=1}^{p_j} |\alpha_i| = 0$ or that there are more than $\lceil \lambda p_j \rceil$ coefficients which are non-zero. Then the probability of P_j being false is at most $C \log(j) j^{2W-2}$, where W is defined in expression* (3) *of Theorem* 1 *and $C = 8NK(1 - \lambda)$.*

Before describing the proof of Lemma 3, here is the proof of Theorem 1.

Proof of Theorem 1. By Lemma 3, the probability of P_j failing for infinitely many positive integers j is at most

$$\lim_{t\to\infty}\sum_{q>t} C\log(q)q^{2W-2},$$

which is 0 since $W < 1/2$ (by an integral comparison test). Thus, almost surely, P_j is true for all but finitely many j's. P_j implies that any set of at most $\lceil\lambda p_j\rceil$ indices i must index distinct elements forming an N-independent set. Therefore, for $p_j > 0$, one can partition the p_j indices (j,i) into $\lceil p_j/\lceil\lambda p_j\rceil\rceil$ subsets each of which indexes an N-independent subset of Q_j. Consequently, for $p_j > 0$,

$$\left\lceil\frac{p_j}{\lceil\lambda p_j\rceil}\right\rceil \le \left\lceil\frac{p_j}{\lambda p_j}\right\rceil = \lceil 1/\lambda\rceil.$$

[This partition bound holds trivially if $p_j = 0$.] By Lemma 2, the union of N-independent subsets from distinct Q_j's, $j \ge N$, remains N-independent. Thus, almost surely, the index set for the random variables $\{g_{i,j}\}$ is a union of at most $\lceil 1/\lambda\rceil$ sets which index N-independent sets together with a finite set; the finite set comes from the finite number of j's where $j < N$ or where P_j fails to be true. ■

LEMMA 4. *From a finite subset Q of real numbers of size n, choose p points at random, $\{g_i\}_{i=1}^p$, uniformly and independently. For any coefficient sequence $\alpha = \{\alpha_i\}_{i=1}^p$, let C_α denote the probability that*

$$0 = \mathcal{R}(\alpha) = \sum_{i=1}^p \alpha_i g_i.$$

If $\sum_{i=1}^p |\alpha_i| > 0$, then $C_\alpha \le n^{-1}$.

Proof. Suppose first that exactly one coefficient, say α_j, is non-zero. Then $\mathcal{R}(\alpha) = 0$ if and only if $g_j = 0$. This has probability 0 if $0 \notin Q$ and $1/n$ if $0 \in Q$. Next, suppose that at least two coefficients are non-zero. Let t be the last integer such that $\alpha_t \ne 0$. Then, $\mathcal{R}(\alpha) = 0$ if and only if

$$g_t = -(\alpha_t)^{-1}\sum_{i=1}^{t-1}\alpha_i g_i.$$

Set the right-hand side above equal to $\mathcal{R}^*(\alpha)$. By the joint independence of the random variables g_i, $1 \le i \le p$, g_t is independent of $\mathcal{R}^*(\alpha)$. Also, $P(g_t = y)$ is either $1/n$ or 0; the latter if $y \in Q$ and the former if not. Hence

$$\begin{aligned} P(\mathcal{R}(\alpha) = 0) &= \sum_{x\in\mathbb{R}} P(g_t = -x)P(\mathcal{R}^*(\alpha) = x) \\ &\le (1/n)\sum_{x\in\mathcal{R}} P(\mathcal{R}^*(\alpha) = x) = 1/n\cdot 1 = 1/n. \ \blacksquare \end{aligned}$$

LEMMA 5. *Let* $\phi(s) = s\log(s) + (1-s)\log(1-s)$, *for* $s \in (0,1)$. *For* $\lambda \in (0,1)$, $p \in \mathbb{Z}^+$, *and* $t \in (-\lambda, 1-\lambda) \cap [-1/p, 1/p]$,

$$-p\phi(\lambda+t) \le |\phi'(\lambda)| - p\phi(\lambda).$$

Proof. Since ϕ'' is positive, this follows from Taylor's Remainder Theorem. For $\lambda \in (0,1)$ and $t \in (-\lambda, 1-\lambda)$,

$$\phi(\lambda+t) = \phi(\lambda) + \phi'(\lambda)t + \frac{\phi''(u)}{2}t^2,$$

for some u between λ and $\lambda+t$. One has $\phi'(u) = \log(u) - \log(1-u)$ and $\phi''(u) = u^{-1} + (1-u)^{-1} > 0$ for $u \in (0,1)$. Since both λ and $\lambda+t$ are in $(0,1)$ the remainder term is non-negative and thus

$$\phi(\lambda+t) \ge \phi(\lambda) + \phi'(\lambda)t.$$

Therefore, to prove this lemma, it suffices to have

$$-p\phi'(\lambda)t \le |\phi'(\lambda)|.$$

Suppose that $\lambda \le 1/2$. Then $\phi'(\lambda) = \log[\lambda/(1-\lambda)] \le 0$. It follows from $t \le 1/p$ that

$$[-p\phi'(\lambda)]t \le [-p\phi'(\lambda)](1/p) = -\phi'(\lambda).$$

If $\lambda > 1/2$, then $\phi'(\lambda) > 0$. It follows from $t \ge -1/p$ that

$$[-p\phi'(\lambda)]t \le [-p\phi'(\lambda)](-1/p) = \phi'(\lambda). \ \blacksquare$$

Proof of Lemma 3. Let p denote p_j. If $\lambda p \le 1$, P_j is always true because $0 \notin Q_j$ and hence any "N-relation" requires at least two points of Q_j. So assume $\lambda p > 1$. The number of quasi-relations excluded by P_j is

$$D(p) = \sum_{w=1}^{\lceil \lambda p \rceil} \binom{p}{w} (2N)^w. \tag{4}$$

To see equation (4), think of a quasi-relation α with exactly s non-zero coefficients. There are $\binom{p}{s}$ locations for the non-zero coefficients; for each placement, there are $2N$ choices of a non-zero integer from $[-N, N]$.

Use Stirling's approximation to factorials [1] to estimate $\binom{p}{sp}$ with $sp = \lceil \lambda p \rceil$:

$$\binom{p}{sp} \le \frac{p^p\sqrt{2\pi p}}{e^p} \cdot \frac{e^{sp}}{(sp)^{sp}\sqrt{2\pi sp}} \cdot \frac{e^{p-sp}}{(p-sp)^{p-sp}\sqrt{2\pi(p-sp)}} * T \tag{5}$$

where

$$T \le e^{1/(12p)} * e^{1/(12ps)} * e^{1/[12(p-ps)]} \le e^{11/72} \le 1.17.$$

After removing common factors of the form e^x and p^x, one has

$$\begin{aligned}
\binom{p}{sp} &\le \sqrt{2\pi p} * \frac{1}{s^{sp}\sqrt{2\pi sp}} * \frac{1}{(1-s)^{p-sp}\sqrt{2\pi(p-sp)}} * T \\
&\le \frac{T}{\sqrt{2\pi sp}} * \frac{\sqrt{p}}{\sqrt{p-sp}} * s^{-sp}(1-s)^{sp-p} \\
&\le \frac{T}{\sqrt{2\pi sp}} * \frac{\sqrt{2p}}{\sqrt{p-1}} * \ e^{-p\cdot[s\log(s)+(1-s)\log(1-s)]}, \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{since } p-sp \ge (p-1)/2, \\
&\le \frac{T}{\sqrt{\pi}} * \frac{\sqrt{p}}{\sqrt{2(p-1)}} * \ e^{-p\cdot\phi(s)}, \qquad \text{since } sp \ge 2, \\
&< e^{-p\phi(s)}, \qquad\qquad\qquad\qquad\quad \text{since } p > 2.
\end{aligned}$$

View $\phi(s)$ with $s = \lambda + t$ as in Lemma 5:

$$\binom{p}{sp} \le \frac{1-\lambda}{\lambda} e^{-p\phi(\lambda)}.$$

Now return to $D(p)$. Since $\lambda \le 1/2$, the binomial coefficients in equation (4) are dominated by the last one. Also, $\lambda p > 1$ and hence $\lceil \lambda p \rceil < \lambda p + 1 < 2\lambda p$. Therefore

$$\begin{aligned}
D(p) &\le (\lceil \lambda p \rceil) \binom{p}{sp} (2N)^{\lceil \lambda p \rceil} \\
&< (2\lambda p) \cdot \frac{1-\lambda}{\lambda} e^{-p\phi(\lambda)} \cdot (2N) e^{\lambda p \log(2N)} \\
&= 4Np(1-\lambda)e^{p(W/K)}, \qquad \text{by equation (3).}
\end{aligned}$$

By Lemma 4, the probability of P_j failing is at most $D(p)|Q_j|^{-1}$. With $|Q_j| = j^2$, $p = p_j \le K\log(j^2)$, and $W \ge 0$, one has

$$\begin{aligned}
P(P_j \text{ failing}) &\le 4N(1-\lambda)K\log(j^2)e^{K\log(j^2)(W/K)} j^{-2} \\
&= C\log(j) j^{2W-2},
\end{aligned}$$

where $C = 8N(1-\lambda)K$. ∎

The efficiency of the proof. The proof does not provide elegant estimates for λ in terms of *a priori* values of N and K. To evaluate the efficiency of the proof, assume that $p_j = \lfloor K\log(j^2) \rfloor$ (the maximum density allowed by condition (1) of Theorem 1).

One can view the choice of $K\log(j^2)$ points as approximately K/K_0 choices of sets of size $K_0\log(j^2)$. Let $K_0 = K(N, 1/2)$. (By using Lagrange multipliers to find the maximum of $K\lambda$ subject to $\lambda \in [0, 1/2]$ and $W(N, K, \lambda) = 1/2$, one can show that the maximum occurs at the boundary of this manifold with $\lambda = 1/2$. Thus, $K_0 = K(N, 1/2)$ is optimal for this comparison argument.) The details require some explanation. Assume first that K is not an integer multiple of K_0. Then one may find $K_0' \in (0, K_0)$ for which $W(N, K_0', 1/2) < 1/2$, $\lceil K/K_0 \rceil = \lceil K/K_0' \rceil$, and K is not an integer multiple of K_0'. Then the number of N-independent sets required for sets chosen from Q_j's with large j is

$$2 \limsup_j \left\lceil \frac{\lfloor K \log(j^2) \rfloor}{\lfloor K_0' \log(j^2) \rfloor} \right\rceil \leq 2 \limsup_j \left\lceil \frac{K \log(j^2)}{K_0' \log(j^2) - 1} \right\rceil = 2\lceil K/K_0 \rceil.$$

Thus at most $2\lceil \log(8N)K \rceil$ N-independent sets are required for all but finitely many j's (almost surely). If K is an integer multiple of K_0, one can not choose $K_0' < K_0$ without making $\lceil K/K_0' \rceil$ greater than $\lceil K/K_0 \rceil$. In this case, the limsup is $\lceil 1 + K/K_0 \rceil$. In summary, the number of N-independent sets required for all but finitely many j's, almost surely, is bounded by

$$2\lfloor 1 + \log(8N)K \rfloor.$$

In the case of $N = 2$ and $K = 1.80 > \log(2)^{-1}$ (the latter is the asymptotic density of a quasi-independent set, as proved below), random sets chosen with a density greater than that of a quasi-independent set are a union of no more than 10 dissociate sets (for all but finitely many j's, almost surely). The authors venture no guesses as to whether this is universally true of quasi-independent sets; the quasi-independent set $\{1, 6, 10, 12, 14\}$ is an example where three dissociate sets are required and the worst case known to date.

Fix $K > 0$, let $N \to \infty$, and consider $\lceil 1/\lambda(N, K)^- \rceil$ for some $\lambda(N, K)^- \in (0, \lambda(N, K))$ to be described. If $\lambda \in (0, 1/2]$ and

$$W(N, K, \lambda) = K[\lambda \log(2N/\lambda) + (\lambda - 1) \log(1 - \lambda)] \leq 1/2,$$

then $K\lambda \log(2N) \leq 1/2$ and thus $\lambda \leq 1/(2K \log(2N))$. It follows that $\lambda(N, K) \to 0$ as $N \to \infty$. One has

$$(\lambda - 1) \log(1 - \lambda) < \lambda \quad \text{for } \lambda \in (0, 1),$$

with

$$\lim_{\lambda \to 0^+} (\lambda - 1) \log(1 - \lambda)/\lambda = 1.$$

If $W^*(N, K, \lambda)$ is defined as $K\lambda[1 + \log(2N/\lambda)]$, one has $W(N, K, \lambda) < W^*(N, K, \lambda)$ for $\lambda \in (0, 1)$. Let $\lambda(N, K)^-$ be the last $\lambda \in (0, 1/2]$ such that $W^*(N, K, \lambda) \leq 1/2$. Since $W(N, K, \lambda) < W^*(N, K, \lambda)$ for $\lambda \in (0, 1)$, one has $\lambda(N, K)^- < \lambda(N, K)$. As shown earlier,

$$\lambda(N, K)^- < \lambda(N, K) \leq 1/(2K \log(2N)).$$

Also, $\lim_{N \to \infty} W^*(N, K, (4K \log(2N))^{-1}) = 1/4 < 1/2$. Consequently, for

N large enough,

$$1/(4K\log(2N)) < \lambda(N,K)^- < 1/(2K\log(2N))$$

and one may write

$$\lambda(N,K)^- = ((2+\varepsilon_N)K\log(2N))^{-1} \quad \text{for some } \varepsilon_N \in (0,2).$$

By solving $W^*(N,K,\lambda(N,K)^-) = 1/2$ with $\lambda(N,K)^-$ in this form, one finds that

$$\begin{aligned}\varepsilon_N &= 2[1+\log(2+\varepsilon_N)+\log(K)+\log(\log(2N))]/\log(2N)\\ &\le 2[1+\log(4)+\log(K)+\log(\log(2N))]/\log(2N).\end{aligned}$$

Therefore,

$$\lceil 1/\lambda(N,K)^-\rceil = \lceil (2+\varepsilon_N)K\log(2N)\rceil,$$

with $\lim_{N\to\infty}\varepsilon_N = 0$. By the previous equation for ε_N,

$$\begin{aligned}&\lceil 1/\lambda(N,K)^-\rceil\\ &\quad = \lceil 2K\,\{\log(2N)+\log(\log(2N))+\log(K)+1+\log(2+\varepsilon_N)\}\rceil.\end{aligned}$$

A lower bound for $1/\lambda$ will follow from the next proposition.

PROPOSITION 6. *Let m_j be the maximum cardinality of an N-independent subset of any arithmetic progression of the form $S_j = k\cdot\{1,\ldots,j\}$ with $k \ne 0$. Then*

$$\lim_{j\to\infty}\frac{m_j}{\log(j)} = \frac{1}{\log(N+1)}.$$

Proof. It is clear that m_j does not depend upon the dilation factor k, so we may set $k=1$ for simplicity. The set $\{1, N+1, (N+1)^2, \ldots, (N+1)^t\}$ is N-independent in S_j, where $t = \lfloor \log(j)/\log(N+1)\rfloor$. Thus,

$$\liminf_{j\to\infty}\frac{m_j}{\log(j)} \ge \frac{1}{\log(N+1)}.$$

Second, any N-independent subset E has the property that, for distinct coefficient sequences α and α' from $\{0,1,\ldots,N\}^E$,

$$\sum_{x\in E}\alpha_x x \ne \sum_{x\in E}\alpha'_x x.$$

If $E\subset S_j$ is N-independent of cardinality m_j, there are $(N+1)^{m_j}$ of these sums in $[0, N\sum_{x\in E}x]$. Thus, for $m_j > 1$,

$$(N+1)^{m_j} \le 1 + N\sum_{x\in E}x < 1 + Njm_j.$$

Thus $(N+1)^{m_j} \le Njm_j$ (for $m_j > 1$) and

$$m_j\log(N+1) - \log(m_j) \le \log(j) + \log(N).$$

It follows that
$$\frac{m_j}{\log(j)}\left[\log(N+1)-\frac{\log(m_j)}{m_j}\right]\le 1+\frac{\log(N)}{\log(j)}.$$
Since $m_j \to \infty$ as $j \to \infty$,
$$\lim_{j\to\infty}\frac{\log(m_j)}{m_j}=0$$
and hence
$$\begin{aligned}\log(N+1)\limsup_{j\to\infty}\frac{m_j}{\log(j)} &= \limsup_{j\to\infty}\left\{\frac{m_j}{\log(j)}\left[\log(N+1)-\frac{\log(m_j)}{m_j}\right]\right\}\\ &\le \limsup_{j\to\infty}\left[1+\frac{\log N}{\log(j)}\right]=1.\end{aligned}$$
Consequently,
$$\limsup_{j\to\infty}\frac{m_j}{\log(j)}\le\frac{1}{\log(N+1)}. \ \blacksquare$$

Proposition 6 implies that, for any choice of $\lambda(N,K)^-$ from $(0,\lambda(N,K))$,
$$\lceil 1/\lambda(N,K)^-\rceil \ge K\log(N+1).$$
First, by Proposition 6, if $K\log(j^2)$ distinct points are chosen from Q_j (of size j^2) and m_j is the maximum size of an N-independent subset of Q_j, the number of N-independent subsets required to cover those points is at least
$$\lim_{j\to\infty}\frac{\lfloor K\log(j^2)\rfloor}{m_j}=\lim_{j\to\infty}\frac{\log(j^2)}{m_j}\cdot\frac{K\log(j^2)-1}{\log(j^2)}=K\log(N+1).$$
Second, note that Lemma 3 implies that almost all the random choices of Theorem 1 produce distinct elements of Q_j for all but finitely many j. Hence the above estimate applies to $\lceil 1/\lambda(N,K)^-\rceil$.

Some deterministic observations. For Sidon sets and M-independent sets, the question of whether they are a finite union of N-independent sets is "finitely determined". To make this precise, the following definition is offered.

DEFINITION. For subsets $E\subset\mathbb{Z}$, let $\mu(E,m)=\infty$ if E is not a finite union of m-independent sets; otherwise, let $\mu(E,m)$ be the minimum number of m-independent sets of which E is the union.

As in [7], let $\alpha(E)$ denote the Sidon constant of E for Sidon subsets of $\mathbb{Z}$, and ∞ otherwise.

THEOREM 7. *If the m-independent subsets of $\mathbb{Z}$ are unions of finitely many n-independent subsets*, *then there is a uniform bound on the number of n-independent subsets which are required.*

THEOREM 8. *If every Sidon subset of* $\mathbb{Z}\setminus\{0\}$ *is the union of finitely many* m*-independent subsets*, *then then there is an increasing function* $\phi : [1,\infty)\to\mathbb{Z}^+$ *such that*, *for Sidon subsets* E *of* $\mathbb{Z}\setminus\{0\}$ *with* $\alpha(E)\le r$,

$$\mu(E,m)\le\phi(r). \tag{6}$$

The restriction to $r\ge 1$ is due to the fact that $\alpha(E)\ge 1$ for all $E\subset\mathbb{Z}$ (cf. [7]). The proofs of Theorems 7 and 8 will be facilitated by the following lemmas. The proof of the first follows closely from the definitions.

LEMMA 9. *For subsets* E *and* F *of* $\mathbb{Z}$, *if* $F\subset E$ *then* $\alpha(F)\le\alpha(E)$ *and* $\mu(F,m)\le\mu(E,m)$. *Also*, *for* $m\le n$, $\mu(E,m)\le\mu(E,n)$.

LEMMA 10. *For* $k\ne 0$ *and* $E\subset\mathbb{Z}$, $\alpha(E)=\alpha(kE)$ *and* $\mu(E,m)=\mu(kE,m)$.

Proof. That $\alpha(E)=\alpha(kE)$ is well known. For $k\ne 0$, $F\subset\mathbb{Z}$ is m-independent if and only if kF is m-independent. Thus, if E is partitioned into F_i's which are m-independent, then kE is partitioned by kF_i's which remain m-independent and vice versa. ∎

LEMMA 11. *For* $E\subset\mathbb{Z}$,

$$\mu(E,m)=\sup\{\mu(F,m)\mid F\subset E\ \&\ F \text{ is finite}\}. \tag{7}$$

Proof. Let t equal the right-hand side of equation (7). By Lemma 9, $\mu(E,m)\ge t$. Next, the reversed inequality will be proved. Let $E_s = E\cap[-s,s]$. Then

$$E=\bigcup_s E_s$$

and there are m-independent subsets $I_{q,s}$ (possibly equal to $\emptyset$) such that

$$E_s=\bigcup_{q\le t} I_{q,s}.$$

Without loss of generality, it may be assumed that the $I_{q,s}$'s are disjoint for distinct q's. Hence

$$\chi_{E_s}=\sum_{q=1}^{t}\chi_{I_{q,s}}. \tag{8}$$

By a weak-limit argument, or by using Alaoglu's Theorem in $\ell_\infty(\mathbb{Z}) = \ell_1(\mathbb{Z})^*$, there is a subsequence s_j such that

$$\lim_{j\to\infty}\chi_{I_{q,s_j}}=f_q \quad \text{for } 1\le q\le t,$$

pointwise on $\mathbb{Z}$ (or weak-* in $\ell_\infty(\mathbb{Z})$).

Necessarily, $f_q = \chi_{I_q}$ for some set $I_q \subset \mathbb{Z}$. By equation (8),

$$\sum_{q=1}^{t} \chi_{I_q} = \lim_{j\to\infty} \sum_{q=1}^{t} \chi_{I_{q,s_j}} = \lim_{j\to\infty} \chi_{E_{s_j}} = \chi_E.$$

Thus, E is the disjoint union of the I_q's. To prove that the I_q's are m-independent, suppose that I_q is not m-independent for some q. Then there is an "m-relation", specifically a finite set $W \subset I_q$ and integer coefficients $\alpha_x \in [-m, m]$ with $\alpha_x \neq 0$ such that

$$\sum_{x\in W} \alpha_x x = 0.$$

Because $\chi_{I_{q,s_j}}$ converges pointwise to χ_{I_q} on $\mathbb{Z}$ and W is finite, there is some j_0 such that $W \subset I_{q,s_j}$ for all $j \geq j_0$. That would make I_{q,s_j} fail to be m-independent, contrary to the hypotheses. So, I_q must be m-independent and hence $\mu(E, m) \leq t$. ∎

Proof of Theorem 7. Assume that no uniform bound holds. That is, for each t, there is an m-independent subset $E_t \subset \mathbb{Z}$ such that $\mu(E_t, n) \geq t$. By Lemma 11 there is a finite subset $F_t \subset E_t$ such that $\mu(F_t, n) \geq t$ (and of course remains m-independent). Let

$$F = \bigcup_t k_t F_t,$$

where the k_t's are positive integers which increase rapidly enough to make F be m-independent. This will contradict the hypotheses, because Lemmas 9 and 10 imply that for all t,

$$\mu(F, n) \geq \mu(k_t F_t, n) = \mu(F_t, n) \geq t.$$

One may choose k_t as follows. Let $k_1 = 1$. Given k_s for $s \leq t$, let D_t denote the maximum absolute value of the elements

$$\sum_{s\leq t} \sum_{x\in k_s F_s} \alpha_x x, \qquad \text{where } \alpha_x \text{ an integer in } [-m, m] \text{ for all } x.$$

Choose $k_{t+1} > D_t$. Here's an argument that F is then m-independent.

Suppose that F is not m-independent. Then there is a non-empty, finite set $W \subset F$ and integers $\alpha_x \in [-m, m]$ with $\alpha_x \neq 0$ such that

$$\sum_{x\in W} \alpha_x x = 0. \tag{9}$$

Because W is finite and non-empty, there is a maximum t such that $W \cap k_t F_t \neq \emptyset$. If $t = 1$, then W is a subset of $k_1 F_1$ and $k_1 F_1$ fails to be m-independent (which contradicts the m-independence of F_1). So $t > 1$, and equation (9) can be rewritten as

$$\sum_{x\in W\cap k_tF_t}\alpha_x x = -\sum_{s<t}\sum_{x\in W\cap k_sF_s}\alpha_x x. \tag{10}$$

If $\sum_{x\in W\cap k_tF_t}\alpha_x x\neq 0$, then it is a non-zero multiple of k_t and

$$k_t\le\Big|\sum_{x\in W\cap k_tF_t}\alpha_x x\Big| = \Big|-\sum_{s<t}\sum_{x\in W\cap k_sF_s}\alpha_x x\Big|\le D_{t-1}.$$

This contradiction proves that

$$\sum_{x\in W\cap k_tF_t}\alpha_x x = 0.$$

Since $\alpha_x\neq 0$ for at least one $x\in k_tF_t$, k_tF_t fails to be m-independent. However, since $k_t>0$, this contradicts the m-independence of F_t. ∎

Proof of Theorem 8. Suppose that, for every $r\ge 1$,

$$\sup\{\mu(E,m)\mid E\subset(\mathbb{Z}\setminus\{0\})\ \&\ \alpha(E)\le r\}<\infty. \tag{11}$$

Then let $\phi(r)$ be that supremum; it is clearly increasing with r and meets the requirements of the theorem. Suppose, on the contrary, that there is some $r\ge 1$ for which inequality (11) is false. Then, for each t, there is some $E_t\subset\mathbb{Z}\setminus\{0\}$ for which $\alpha(E_t)\le r$ and $\mu(E_t,m)\ge t$. By Lemma 11, there is a finite subset $F_t\subset E_t$ for which $\mu(F_t,m)\ge t$ (and, of course, $\alpha(F_t)\le r$). As in the proof of Theorem 7, let

$$F=\bigcup_t k_tF_t,$$

for a rapidly increasing sequence of positive integers, $\{k_t\}_t$. For all t,

$$\mu(F,m)\ge\mu(k_tF_t,m)=\mu(F_t,m)\ge t.$$

Thus, F will not be a finite union of m-independent sets. If F is Sidon, this will contradict the hypotheses of Theorem 8.

To make F be Sidon, let $k_1=1$; for $t>1$, let $k_t>\pi^2 2^t M_{t-1}$, where M_t is the maximum absolute value of an element of $\bigcup_{s<t}k_sF_s$. Then, as in the proof of Proposition 12.2.4, pages 371–372 of [2], $\{k_tF_t\}_t$ is a sup-norm partition for F: if p_t is a k_tF_t-polynomial (on T) and is non-zero for at most finitely many t, then

$$\sum_{j=1}^{\infty}\|p_j\|_\infty\le 2\pi\Big\|\sum_{j=1}^{\infty}p_j\Big\|_\infty.$$

Recall that $B(F)$ (the restrictions to F of Fourier transforms of bounded Borel measures on T) is the Banach space dual of $\mathrm{Trig}_F(T)$ (the trigonometric polynomials with spectrum in F). For $p\in\mathrm{Trig}_F(T)$, let p_j denote its summand in $\mathrm{Trig}_{k_jF_j}(T)$ under the natural decomposition. Then for $f \in B(F)$,

$$\begin{aligned}
|\langle f, p\rangle| &= \Big|\sum_{j=1}^{\infty}\langle f, p_j\rangle\Big| \le \sum_{j=1}^{\infty}|\langle f, p_j\rangle| \\
&\le \sum_{j=1}^{\infty}\|f|_{k_jF_j}\|_{B(k_jF_j)}\|p_j\|_\infty \\
&\le (\sup_t \|f|_{k_tF_t}\|_{B(k_tF_t)})\sum_{j=1}^{\infty}\|p_j\|_\infty \\
&\le (r\sup_t \|f|_{k_tF_t}\|_\infty)(2\pi\|p\|_\infty), \qquad \text{since } \alpha(k_tF_t) \le r, \\
&\le (2\pi r\|f\|_\infty)\|p\|_\infty.
\end{aligned}$$

Thus, $\|f\|_{B(F)} \le 2\pi r\|f\|_\infty$. By the definition of Sidon constant, $\alpha(F) \le 2\pi r$ and thus F is Sidon. ∎

One can extend the idea of m-independence to arbitrary abelian groups, by additionally restricting α_x to $[-p, p)$ when $2p$ is the order of x, and to $[-(p-1)/2, (p+1)/2)$ when the order of x is p and odd. Then Theorems 7 and 8 have more universal versions.

THEOREM 12. *Suppose that, for some integers m and n and all abelian groups G, m-independent sets are the finite unions of n-independent sets. Then, independent of the group G, there is a uniform bound on the number of n-independent sets required.*

THEOREM 13. *Suppose there is an integer m such that, for all abelian groups G and all Sidon subsets E of $G \setminus \{0\}$, E is a finite union of m-independent sets. Then there is an increasing function $\phi : [0, \infty) \to \mathbb{Z}^+$ such that, if $E \subset (G\setminus\{0\})$ for any abelian group G and $\alpha(E) \le r$, then $\mu(E, m) \le \phi(r)$.*

Proof of Theorem 12. Suppose that, for every t, there is an m-independent subset E_t of some abelian group G_t such that $\mu(E_t, n) \ge t$. Let G be the infinite direct sum of the G_t's: $g \in G$ if and only if

$$g : \mathbb{Z}^+ \to \bigcup_t G_t$$

with $g(t) \in G_t$ for all t and $g(t) \ne 0$ for at most finitely many t [assume that the groups are presented additively]. Embed G_t into G canonically: $x \mapsto g_x$, where $g_x(t) = x$ and $g_x(s) = 0$ for $s \ne t$. View G_t as identical with its isomorphic embedding; E_t remains m-independent under the embedding and $\mu(E_t, n)$ is unchanged. It should be clear that

$$E = \bigcup_t E_t \subset G$$

is m-independent while

$$\mu(E, n) \geq \mu(E_t, n) \geq t, \qquad \text{for all } t.$$

So E is not the finite union of n-independent sets, contrary to the hypotheses. ∎

Proof of Theorem 13. As in the proof of Theorem 8, suppose that there is some $r \in [1, \infty)$ such that, for all t, there is an abelian group G_t and $E_t \subset G_t \setminus \{0\}$ for which $\alpha(E_t) \leq r$ and $\mu(E_t, m) \geq t$. As in the proof of Theorem 12, let G be the direct sum of the G_t's and view G_t as embedded in G. Under this embedding, neither $\alpha(E_t)$ nor $\mu(E_t, m)$ changes. Let

$$E = \bigcup_t E_t.$$

Then E is not the union of finitely many m-independent sets.

To see that E is a Sidon set, note that $\{E_t\}_t$ is a sup-norm partition of E. Specifically, if Γ is the compact group dual to G (G is given the discrete topology), then for $p \in \mathrm{Trig}_E(\Gamma)$, with p_j its natural summand in $\mathrm{Trig}_{E_j}(\Gamma)$,

$$\sum_{j=1}^{\infty} \|p_j\|_\infty \leq \pi \|p\|_\infty,$$

by Lemma 12.2.2, page 370 of [2]. To apply that lemma two things are required. First, no E_j may contain 0, which is true here. Second, in the language of [2], the ranges of $\{p_j\}_{j=1}^{\infty}$ are 0-additive: given $\{\gamma_j\}_{j=1}^{\infty}$ from Γ, there is some $\gamma \in \Gamma$ for which

$$\Big| p(\gamma) - \sum_{j=1}^{\infty} p_j(\gamma_j) \Big| = 0. \tag{12}$$

Here's a proof of equation (12). Γ is the infinite direct product of $\Gamma_t = \widehat{G}_t$: $\gamma \in \Gamma$ if and only if

$$\gamma : \mathbb{Z}^+ \to \bigcup_t \Gamma_t, \qquad \text{with } \gamma(t) \in \Gamma_t.$$

Let $\gamma \in \Gamma$ satisfy $\gamma(j) = \gamma_j(j)$. Note that for a character g used in p_j, $\langle g, \gamma \rangle$ is determined by $\gamma(j)$ because g is 0 in every other coordinate:

$$\begin{aligned} \langle g, \gamma \rangle &= \prod_s \langle g(s), \gamma(s) \rangle \\ &= \langle g(j), \gamma(j) \rangle = \langle g(j), \gamma_j(j) \rangle = \langle g, \gamma_j \rangle. \end{aligned}$$

Thus

$$p(\gamma) = \sum_{j=1}^{\infty} p_j(\gamma) = \sum_{j=1}^{\infty} p_j(\gamma_j).$$

Once it is known that E is sup-norm partitioned by the E_t's, then just as in the proof of Theorem 8 one has

$$\alpha(E) \le \pi \sup_t \alpha(E_t) \le \pi r.$$

This proves that E is Sidon. ∎

REFERENCES

[1] W. H. Beyer (ed.), *CRC Standard Mathematical Tables*, 28*th Edition*, CRC Press, Boca Raton, Florida, 1981, 58–59.

[2] C. C. Graham and O. C. McGehee, *Essays in Commutative Harmonic Analysis*, Springer, New York, 1979, 371–372.

[3] D. Grow and W. C. Whicher, *Finite unions of quasi-independent sets*, Canad. Math. Bull. 27 (4) (1984), 490–493.

[4] Y. Katznelson, *Suites aléatoires d'entiers*, Lecture Notes in Math. 336, Springer, 1973, 148–152.

[5] —, *Sequences of integers dense in the Bohr group*, Proc. Roy. Inst. Tech., June 1973, 73–86.

[6] Y. Katznelson et P. Malliavin, *Vérification statistique de la conjecture de la dichotomie sur une classe d'algèbres de restriction*, C. R. Acad. Sci. Paris Sér. A 262 (1966), 490–492.

[7] J. M. López and K. M. Ross, *Sidon Sets*, Marcel Dekker, New York, 1975, 19–44.

[8] G. Pisier, *Arithmetic characterization of Sidon sets*, Bull. Amer. Math. Soc. 8 (1983), 87–89.

SCHOOL OF MATHEMATICAL AND PHYSICAL SCIENCES
MURDOCH UNIVERSITY
SOUTH STREET
MURDOCH, WESTERN AUSTRALIA 6150
AUSTRALIA
E-mail: HARRISON@PRODIGAL.MURDOCH.EDU.AU

MATHEMATICS
KELLER HALL
2565 THE MALL
HONOLULU, HAWAII 96822
U.S.A.
E-mail: RAMSEY@MATH.HAWAII.EDU

Reçu par la Rédaction le 8.9.1994