Lacunarity and the Bohr Topology

Kenneth Kunen* and Walter Rudin
Department of Mathematics, Van Vleck Hall
University of Wisconsin, Madison, WI 53706, U.S.A.

June 17, 1998

Abstract

If G is an abelian group, then $G^{\#}$ denotes G equipped with the weakest topology that makes every character of G continuous. This is the Bohr topology of G. If $G = \mathbb{Z}$, the additive group of the integers, and A is a Hadamard set in $\mathbb{Z}$, it is shown that: (i) $A - A$ has 0 as its only limit point in $\mathbb{Z}^{\#}$, (ii) No Sidon subset of $A - A$ has a limit point in $\mathbb{Z}^{\#}$, (iii) $A - A$ is a $\Lambda(p)$ set for all $p < \infty$. This leads to an explicit example of a set which is $\Lambda(p)$ for all $p < \infty$ and is dense in $\mathbb{Z}^{\#}$. If $f(x)$ is a quadratic or cubic polynomial with integer coefficients, then the closure of $f(\mathbb{Z})$ in the Bohr compactification of $\mathbb{Z}$ is shown to have Haar measure 0. Every infinite abelian group G contains an I_0 set A of the same cardinality as G such that 0 is the only limit point of $A - A$ in $G^{\#}$.

1 Introduction

Let G be an abstract abelian group, with the discrete topology. We use Γ_G, or just Γ, to denote the group of characters, or homomorphisms from G into the circle group $\mathbb{T}$. Γ is a compact abelian group, and, by the Pontryagin Duality Theorem, we may identify G with the character group of Γ (that is, the *continuous* homomorphisms into $\mathbb{T}$), by identifying each $x \in G$ with the map $\gamma \mapsto \gamma(x)$. We may also *ignore* the topology on Γ, view Γ as a discrete

*email: kunen@math.wisc.edu; author supported by NSF Grant DMS-9704520.

group, and form *its* character group, denoted by $bG = \Gamma_{\Gamma_G}$, consisting of *all* homomorphisms from Γ_G into $\mathbb{T}$. Then bG is the *Bohr compactification* of G. The same identification now makes G into a dense subgroup of bG. The subspace topology on $G \subseteq bG$ is called the *Bohr topology*, and $G^\#$ denotes the group G given this topology.

More concretely, basic neighborhoods of 0 in $G^\#$ are of the form

$$W(\epsilon; \gamma_1, \ldots, \gamma_n) = \{x \in G : |\gamma_1(x) - 1| < \epsilon \ \& \ \cdots \ \& \ |\gamma_n(x) - 1| < \epsilon\} \ ,$$

where n is finite and $\gamma_1, \ldots, \gamma_n \in \Gamma$. Basic neighborhoods of other elements are obtained by translation. Thus, the topology of $G^\#$ is the weakest one which makes all the characters of G continuous. When $G = \mathbb{Z}$, the group of integers, then $\Gamma = \mathbb{T}$, and the characters are all of the form $x \mapsto e^{ix\theta}$ for some real θ.

Basic properties of $G^\#$ can be deduced directly from this description. For example, *every* group homomorphism Φ from G to another abelian group K is continuous, viewed as a map from $G^\#$ to $K^\#$. To prove this, it is sufficient to prove that Φ is continuous at 0, which follows from the fact that the inverse image of a basic neighborhood of 0 in K – that is, $\Phi^{-1}(W(\epsilon; \gamma_1, \ldots, \gamma_n))$ – is just $W(\epsilon; \gamma_1 \circ \Phi, \ldots, \gamma_n \circ \Phi))$, which is open in $G^\#$. It follows that *every* subgroup H of G is closed in $G^\#$, since $H = \Phi^{-1}\{0\}$, where $\Phi : G \to G/H$.

Now, bG may be characterized abstractly by its properties: bG is the unique (up to continuous isomorphism) compact group Y such that G is dense in Y and every character of G extends to a continuous character of Y. From this, it is easy to see that if H is a subgroup of G, then bH is a closed subgroup of bG: Let X be the closure of H in bG. Then H is dense in X, and every character γ of H extends to X by extending γ first to a character of G (which is possible since $\mathbb{T}$ is divisible), and then extending to bG. Hence, X is bH.

These basic constructions are contained in texts on harmonic analysis, such as [4][10][20]. In addition, the literature contains some more detailed structural information about $G^\#$ and bG, which we review briefly.

Definition 1.1 *$A \subseteq G$ is called an I_0-*set*, or an* interpolation set*, iff for all $E \subseteq A$, the closures of E and of $A \backslash E$ are disjoint in bG.*

This is the same as saying that every bounded real-valued function on A may be extended to a continuous function on bG; or, equivalently, to an almost periodic function on G (since the almost periodic functions are exactly the restrictions of such continuous functions to G). So, the I_0 sets are the subsets of G which are relatively discrete in the topology $G^\#$ and are C^*-embedded in bG. For more details, see Kahane [11] Chapitre X§2. In general, a subset A of a compact Hausdorff space X is said to be C^*-embedded in X iff every bounded $f \in C(A)$ can be extended to a function in $C(X)$; in the special case at hand, when A is discrete in its relative topology, this is equivalent to saying that $\overline{E} \cap \overline{A \backslash E} = \emptyset$ for all $E \subseteq A$. For more on these notions, see Gillman and Jerison [5].

Theorem 1.2 (Hartman and Ryll-Nardzewski [9]) *In every abelian group G, there is an I_0-set $A \subseteq G$ with $|A| = |G|$.*

Here, we are using $|X|$ for the cardinality of the set X.

Of course, when G is finite, we may take $A = G$. When G is infinite, the proof splits into cases, with the hardest case being $G = \mathbb{Z}$.

If A is an I_0 set, then its closure in bG is homeomorphic to βA (the Čech compactification of A with the discrete topology). So, if A is an infinite I_0 set, it will have $2^{2^{|A|}}$ limit points in bG. All of these limit points lie outside of G, however, by:

Theorem 1.3 *If $A \subseteq G$ is an I_0-set, then no element of G is a limit point of A in $G^\#$.*

This theorem was first discovered by Ryll-Nardzewski [21]. A different proof is due to L. T. Ramsey [17]. Ramsey's method of proof was discovered independently by Arkhangel'skii (see [1]) in the context of C_p theory; this applies because $G^\#$ is a subspace of $C_p(\Gamma)$. See [7] for more on the relations between C_p theory and Bohr topologies.

In somewhat the opposite direction, K. P. Hart and J. van Mill [8] showed that if G is an infinite boolean group $(\forall x(x + x = 0))$, then there is an infinite $E \subseteq G$ such that 0 is a limit point of E and every point of E other then 0 is isolated in E. Their E was of the form $A - A = A + A$, where A was an independent subset of G. In fact, there is such an E for every G. We shall show (after proving Lemma 3.7):

Theorem 1.4 *Every infinite abelian group G contains a subset A such that $|A| = |G|$ and:*

1. *A is an I_0-set.*
2. *0 is the unique limit point of $A - A$ in $G^\#$.*
3. *If the index of $\{x \in G : x + x = 0\}$ in G equals $|G|$, then $A + A$ has no limit points in $G^\#$.*

Regarding item 2, note:

Lemma 1.5 *If A is any infinite subset of the abelian group G, then 0 is a limit point of $A - A$ in $G^{\#}$.*

Proof. By compactness, A has some limit point p in bG. Then $0 = p - p$ must be a limit point of $A - A$. $\square$

Note that the additional assumption in Theorem 1.4.3 is exactly what is required. If the index of $B = \{x \in G : x + x = 0\}$ in G is less than $|G|$, and $|A| = |G|$, then infinitely many elements of A lie in some coset, $B + c$, which implies, as in the proof of Lemma 1.5, that $c + c$ is a limit point of $A + A$.

As with Theorem 1.2, the proof of Theorem 1.4 splits into cases. If $G = \mathbb{Z}$, then A can be any Hadamard set (see Definition 2.2), as we show in Section 2. Then, in Section 3, we handle the other cases by examining more closely how the algebraic structure of an abelian group G affects the character group Γ_G. This structure theory is also applied with $G = \mathbb{T}$ to describe the topology of $b\mathbb{Z}$. In Section 4, we study uniformly distributed sequences in Γ_G. In Section 5, this knowledge is applied to describe the topology on sequences defined by polynomial functions. For example (Theorem 5.4), if $f(x)$ is a non-constant polynomial with integer coefficients, then its range is dense in itself in $\mathbb{Z}^{\#}$. When $f(x) = x^k$, its range is also closed in $\mathbb{Z}^{\#}$ (Theorem 5.5), but this is not true for all polynomials. For example, it is true for some, but not all, quadratic polynomials (Theorem 5.6). Questions about the Haar measure of the closure (in $b\mathbb{Z}$) of the range of a polynomial are taken up in Section 6.

In Section 7, we study $\Lambda(p)$ sets and Sidon sets in $\mathbb{Z}$. In Lemma 1.5 above, if A is an I_0 set, one can get a fairly simple description of the topology of $A - A$; see Lemma 7.2. Now, if A is a Hadamard set, then $A - A$ is a $\Lambda(p)$ set for all $p < \infty$; we use a similar argument, plus our description of the topology, to construct another $\Lambda(p)$ set which is dense in $\mathbb{Z}^{\#}$. It is well-known that $A - A$ is not a Sidon set. In fact, we shall show that every Sidon subset of $A - A$ is discrete in $\mathbb{Z}^{\#}$. It is still unknown whether there is a non-discrete Sidon set.

2 Hadamard Sets

The following general result will be useful in proving theorems about $A - A$:

Lemma 2.1 *If $A, B \subseteq G$ are both I_0 sets, and $x \in G$ is a limit point of $A - B$ in $G^{\#}$, then x is also a limit point of $(A \backslash P) - (B \backslash Q)$ for all finite $P \subset A$ and $Q \subset B$.*

Proof. If not, then x would be a limit point of either $P - B$ or $A - Q$, and hence of either $\{p\} - B$ for some $p \in P$, or $A - \{q\}$ for some $q \in Q$. But these sets are also I_0 sets, so we contradict Theorem 1.3. $\square$

We now turn to subsets of $\mathbb{Z}$.

Definition 2.2 *For $M \in \mathbb{R}$, a subset $A \subset \mathbb{Z}$ satisfies the* Hadamard condition with ratio M *iff $A = \{a_n : n \in \mathbb{N}\}$, where $0 < a_0 < a_1 < \cdots$ and each $a_{n+1}/a_n \geq M$. A is a* Hadamard set *iff it satisfies the Hadamard condition with some ratio $M > 1$.*

Theorem 2.3 *If $A \subset \mathbb{Z}$ is a Hadamard set, then:*

1. *A is an I_0-set.*
2. *0 is the unique limit point of $A - A$ in $\mathbb{Z}^{\#}$.*
3. *$A + A$ has no limit points in $\mathbb{Z}^{\#}$.*

The fact that A is an I_0-set is well-known (see, e.g., Kahane [11] Chapitre X§§2,3), but we include the proof, since all three parts follow by the following general technique for constructing characters, which might be useful for other "thin" sets of integers.

General Construction. For now, assume only that $A = \{a_n : n \in \mathbb{N}\} \subset \mathbb{Z}$ and that $0 < a_0 < a_1 < \cdots$. Say we are given "target angles" t_n for $n \in \mathbb{N}$, and we would like to construct a character φ such that $\varphi(a_n) \sim e^{it_n}$ for each n. So, $\varphi(x) = e^{ix\theta}$, for some θ to be determined, and we would like each $a_n\theta \sim t_n (\mathrm{mod}\ 2\pi)$. To do this, we find θ_n for $n \in \mathbb{N}$, with each $a_n\theta_n = t_n + 2\pi k_n$, where the $k_n \in \mathbb{Z}$ will be chosen inductively. Let $\delta_n = \theta_{n+1} - \theta_n$; we try to keep these small so that the θ_n converge rapidly. We can let $k_0 = 0$ and $\theta_0 = t_0/a_0$. Given k_n (and hence θ_n), we choose an integer k_{n+1} and then set $\theta_{n+1} = t_{n+1}/a_{n+1} + 2\pi k_{n+1}/a_{n+1}$. As k_{n+1} varies over $\mathbb{Z}$, these possible values for θ_{n+1} are spaced $2\pi/a_{n+1}$ apart, so we can always choose k_{n+1} so that $|\delta_n| = |\theta_{n+1} - \theta_n| \leq \pi/a_{n+1}$. Assuming only that $\sum_n \frac{1}{a_n} < \infty$, we know that the θ_n converge to some limit θ. If we set

$$L_n = \pi a_n \left[\frac{1}{a_{n+1}} + \frac{1}{a_{n+2}} + \cdots\right] \quad ,$$

we have

$$|a_n\theta - t_n - 2\pi k_n| = |a_n\theta - a_n\theta_n| \leq a_n[|\delta_n| + |\delta_{n+1}| + \cdots] \leq L_n \quad .$$

So, we have constructed φ such that each $\varphi(a_n)$ lies on the arc of length $2L_n$ centered at e^{it_n}. Of course, this is useless unless $L_n < \pi$.

Lemma 2.4 *Suppose A satisfies the Hadamard condition with ratio M.*

1. *If $M > 3$, then A is an I_0-set.*
2. *If $M \geq 7$, then 0 is the only limit point of $A - A$ in $\mathbb{Z}^{\#}$.*

Proof. We now have

$$|a_n\theta - t_n - 2\pi k_n| \leq \pi\left[\frac{1}{M} + \frac{1}{M^2} + \cdots\right] = \frac{\pi}{M-1} \quad .$$

For (1), fix any $E \subseteq \mathbb{N}$, and apply the general construction, letting t_n be 0 for $n \in E$ and π for $n \notin E$. Then $\frac{\pi}{M-1} = \frac{\pi}{2} - \epsilon$ for some $\epsilon > 0$, and we have constructed φ so that $\varphi(a_n)$ lies in the arc $\{e^{ix} : -\pi/2 + \epsilon \leq x \leq \pi/2 - \epsilon\}$ when $n \in E$, and in the disjoint arc, $\{e^{ix} : \pi/2 + \epsilon \leq x \leq 3\pi/2 - \epsilon\}$ when $n \notin E$. So, for every $E \subseteq \mathbb{N}$, the sets $\{a_n : n \in E\}$ and $\{a_n : n \notin E\}$ have disjoint closures in $b\mathbb{Z}$ (since we have found a continuous function φ which maps them into disjoint closed sets); hence, A is an I_0-set.

For (2), suppose $r \neq 0$ were a limit point of $A - A$. Since $A - A = -(A - A)$, we may assume that $r > 0$. Let $Q \subset A$ be finite so that if $b_1 = \min(A \backslash Q)$, then $b_1/r \geq M$. So, $B = \{r\} \cup (A\backslash Q)$ satisfies the Hadamard condition with ratio M, and $r = b_0$. Let $t_0 = \pi$ and $t_n = 0$ for $n > 0$, and apply the general construction to B to get φ. We have $\pi/(M-1) \leq \pi/6$, so $r = \varphi(b_0)$ lies in the arc $\{e^{ix} : 5\pi/6 \leq x \leq 7\pi/6\}$, while for $m, n > 0$, each $\varphi(b_m - b_n)$ lies in the arc $\{e^{ix} : -\pi/3 \leq x \leq \pi/3\}$. But this contradicts the fact that, by Lemma 2.1, r is a limit point of $\{(b_m - b_n) : m, n > 0\}$. $\square$

To handle smaller values of M, we need:

Definition 2.5 *If $K, L > 1$, then A satisfies the* compound Hadamard condition with ratios K, L *iff $a_{n+1}/a_n \geq K$ when n is even, and $a_{n+1}/a_n \geq L$ when n is odd.*

Lemma 2.6 *Suppose that A satisfies the compound Hadamard condition with ratios $K, L > 1$. Let $A_0 = \{a_{2n} : n \in \mathbb{N}\}$ and $A_1 = \{a_{2n+1} : n \in \mathbb{N}\}$. Then*

1. *If $(L + K + 2)/(KL - 1) < 1$, then A_0 and A_1 have disjoint closures in $b\mathbb{Z}$.*
2. *If $(2L + K + 3)/(KL - 1) < 1$, then the closures of $A_0 - A_1$ and $A_1 - A_0$ in $\mathbb{Z}^{\#}$ contain neither a_0 nor $-a_0$.*

Proof. We now have

$$|a_n\theta - t_n - 2\pi k_n| \leq \pi[\tfrac{1}{K} + \tfrac{1}{KL} + \tfrac{1}{K^2L} + \tfrac{1}{K^2L^2}\cdots] = \tfrac{\pi(L+1)}{KL-1} \qquad (n \text{ even})$$
$$|a_n\theta - t_n - 2\pi k_n| \leq \pi[\tfrac{1}{L} + \tfrac{1}{KL} + \tfrac{1}{KL^2} + \tfrac{1}{K^2L^2}\cdots] = \tfrac{\pi(K+1)}{KL-1} \qquad (n \text{ odd})$$

For (1), let t_n be 0 if n is even and π if n is odd, and construct φ as in the proof of lemma 2.4. Then $\varphi(A_0)$ and $\varphi(A_1)$ lie on subarcs of $\mathbb{T}$, centered at 1 and -1 respectively, with lengths $\frac{2\pi(L+1)}{KL-1}$ and $\frac{2\pi(K+1)}{KL-1}$ respectively. Our assumption on K and L implies that these lengths add up to less than 2π, so that the arcs are disjoint.

For (2), let $t_0 = \pi$ and $t_n = 0$ for $n > 0$. Then $arg(\varphi(a_0))$ and $arg(\varphi(-a_0))$ are within $\pi(L+1)/(KL-1)$ of π and $arg(\varphi(d))$ is within $\pi(L+K+2)/(KL-1)$ of 0 for any d in $D = (A_0 - A_1) \cup (A_1 - A_0)$, so the condition on K, L implies that we have mapped $\{a_0, -a_0\}$ and D to disjoint arcs. $\square$

Proof of Theorem 2.3. Assume that each $a_{n+1}/a_n > M$, where $M > 1$ For each $s \in \mathbb{N}$, we may partition A into sets A_ℓ for $\ell < s$, where

$$A_\ell = \{a_{ns+\ell} : n \in \mathbb{N}\} \ .$$

Then each A_ℓ satisfies the Hadamard condition with ratio M^s. If s is chosen so large that $M^s > 3$, then by Lemma 2.4.1, each A_ℓ is an I_0-set. So, to prove that A is an I_0-set, we must show that A_j and A_ℓ have disjoint closures in $b\mathbb{Z}$ whenever $0 \leq j < \ell < s$. Let $c = \ell - j$. Then $A_j \cup A_\ell$ satisfies a compound Hadamard condition, with $K = M^c$ and $L = M^{s-c}$, where $c \in [1, s-1]$. Choose s so large that $f(s,c) = (M^c + M^{s-c} + 2)/(M^s - 1) < 1$ for all $c \in [1, s-1]$; this is possible because $f(s,c) \leq f(s,1) = f(s,s-1)$ for all $c \in [1, s-1]$, and $f(s,1) \to 1/M < 1$ as $s \to \infty$. Now apply Lemma 2.6.1 to A_j and A_ℓ.

Now, we fix a positive $r \in \mathbb{Z}$, assume r is a limit point of $A - A$, and derive a contradiction. Assuming s was chosen so that $M^s \geq 7$, we know that r is not a limit point of any $A_\ell - A_\ell$ by Lemma 2.4.2, so either r or $-r$ is a limit point of some $A_\ell - A_j$, where $0 \leq j < \ell < s$. Now, assume also that s was chosen so large that $(2M^c + M^{s-c} + 3)/(M^s - 1) < 1$ for all $c \in [1, s/2]$. If $k > r$, and we set $B = \{r\} \cup (A_j \cap (k, \infty)) \cup (A_\ell \cap (k, \infty))$ and list B in increasing order as $\{b_n : n \in \mathbb{Z}\}$, then $b_0 = r$. Furthermore, if $B_0 = \{b_{2n} : 0 < n \in \mathbb{N}\}$ and $B_1 = \{a_{2n+1} : n \in \mathbb{N}\}$, then one of B_0, B_1 will be contained in A_j and the other in A_ℓ, so by Lemma 2.1, either r or $-r$ is a limit point of either $B_0 - B_1$ or $B_1 - B_0$. Let c be the smaller of $\ell - j$ and $s - (\ell - j)$; so $c \leq s/2$. Now fix k

so that B satisfies the compound Hadamard condition with ratios M^{s-c}, M^c (that is, $B_0 \subseteq A_\ell$ if $c = \ell - j$, and $B_0 \subseteq A_j$ if $c = s - (\ell - j)$). Then, Lemma 2.6.2 implies that r is not limit point of either $B_0 - B_1$ or $B_1 - B_0$.

Finally, if r is any element of $\mathbb{Z}$, a similar argument shows that r is not a limit point of $A + A$. If M is large, we can choose φ such that $\varphi(r) \sim 1$ and $\varphi(a_n) \sim i$ for each n, so that $\varphi(a_m + a_n) \sim -1$. Then, for smaller M, we partition A as in the $A - A$ proof. $\square$

3 Abelian Groups

We shall use some structure theory for abelian groups to study their character groups and their Bohr topologies. The material through Lemma 3.7 is known or follows easily from known results (see Kaplansky [12], or Appendix A of Hewitt and Ross [10]), but we include proofs to show that what we need can be derived quickly from what is available in college algebra texts, without going deeply into abelian group theory. We first note that one can often construct characters with specific properties by prescribing their values on an independent set:

Definition 3.1 *If $S \subseteq G$, then $\langle S \rangle$ is the subgroup of G generated by S. $A \subseteq G$ is* independent *iff $0 \notin A$ and $\langle X \rangle \cap \langle A \backslash X \rangle = \{0\}$ for all $X \subseteq A$.*

Lemma 3.2 *Suppose that A is an independent subset of the abelian group G and $\varphi_0 : A \to \mathbb{T}$ is any map such that $(\varphi_0(x))^n = 1$ whenever $x \in A$ has some finite order, n. Then there is a character φ of G which extends φ_0.*

This makes the proof of Theorem 1.4 easy in the case that there is a large independent set:

Corollary 3.3 *Suppose that A is an infinite independent subset of the abelian group G. Then A is an I_0-set, and 0 is the unique limit point of $A - A$ in $G^\#$. Furthermore, if A contains no elements of order 2, then $A + A$ has no limit points in $G^\#$.*

Proof. To see that A is an I_0-set, fix $E \subseteq A$; then by independence and Lemma 3.2, there is a character φ which maps E to 1 and $A \backslash E$ to the arc $\{e^{ix} : \pi/2 \leq x \leq 3\pi/2\}$, so that E and $A \backslash E$ have disjoint closures in bG.

Next, suppose $r \in G$ is a limit point of $A - A$ in $G^\#$. Let $H = \langle A \rangle$. Since every subgroup is closed in $G^\#$, we have $r \in H$, so $r \in \langle C \rangle$ for some finite

$C \subset A$. Let $A' = A \backslash C$. By Lemma 2.1, r is also a limit point of $A' - A'$. Then, if $r \neq 0$, we can apply independence of $\{r\} \cup A'$ to get a character φ with $\varphi(r) \neq 1$ and $\varphi(x) = 1$ for all $x \in A'$, and hence all $x \in A' - A'$, which yields a contradiction.

Finally, the same argument shows that $A + A$ can have no limit point in $G^{\#}$ except possibly 0. But, now, since A contains no element of order 2, we may get a character φ to map all elements of A to the arc $\{e^{ix} : 2\pi/5 \leq x \leq 2\pi/3\}$, and hence all elements of $A + A$ to the arc $\{e^{ix} : 4\pi/5 \leq x \leq 4\pi/3\}$, which does not contain $1 = \varphi(0)$. $\square$

In some cases, large independent sets are easily produced by Corollary 3.5.

Lemma 3.4 *If $A \subseteq G$ is a maximal independent set and $x \neq 0$, then $mx \in A$ for some m.*

Corollary 3.5 *If G is an uncountable torsion-free abelian group and $A \subseteq G$ is a maximal independent set, then $|A| = |G|$.*

Proof. For $m \neq 0$, let $D_m = \{x \in G : mx \in A\}$. Since G is torsion-free, the map $x \mapsto mx$ is 1-1, so $|D_m| \leq |A|$. Applying the lemma, $G \backslash \{0\} = \bigcup_m D_m$, so $|A|$ must be $|G|$. $\square$

To handle the general case, we need to look more carefully at the torsion elements. If G is an abelian group, we denote the order of an element $x \in G$ by $ord(x) \in \{1, 2, \ldots \infty\}$. For prime p, a *p-group* is a group such that $ord(x)$ is a power of p for all elements of G. For any abelian G, $F = F_G = \{x \in G : ord(x) < \infty\}$ denotes the *torsion subgroup* of G. This F may be expressed uniquely as $F = \bigoplus_{p \in P} F_p$, where P is the set of primes and each F_p is a p-group; the F_p are the *primary components* of G (or, of F).

Among the p-groups are the cyclic groups $\mathbb{Z}_{p^k}$ for $k = 0, 1, 2, \ldots$. Each $\mathbb{Z}_{p^k}$ is isomorphic to the set of $x \in \mathbb{T}$ of order p^j for some $j \leq k$. We use $\mathbb{Z}_{p^\infty}$ to denote the set of $x \in \mathbb{T}$ of order p^j for some $j \in \mathbb{N}$. The detailed structure theory of p-groups involves Ulm invariants (see [12]). For now we need only

Lemma 3.6 *Let G be an infinite abelian p-group and let $\kappa = |\{x \in G : ord(x) = p\}|$. Then:*

1. $|G| = \max(\kappa, \aleph_0)$.
2. *If κ is finite, then G contains an isomorphic copy of $\mathbb{Z}_{p^\infty}$.*

Proof. View G as a tree, whose root is the element 0. The set of children of the node 0 is $\{y : ord(y) = p\}$, and the set of children of the node $x \neq 0$ is $\{y : py = x\}$. Since any two children of a given node must differ by an element of order p, each node has no more than $\kappa+1$ children; hence $|G| = \max(\kappa, \aleph_0)$. For finite κ, all the levels of the tree are finite, so, by König's Lemma, there is a path $C = \{x_j : j \in \mathbb{N}\}$ through the tree. Then $ord(x_j) = p^j$ and $px_{j+1} = x_j$, so $\langle C \rangle$ is isomorphic to $\mathbb{Z}_{p^\infty}$. $\square$

To prove Theorem 1.4, we need to show that every infinite G contains an independent set of size $|G|$, except in two special cases which we can handle separately.

Lemma 3.7 *Let G be an abelian group with $\kappa = |G| \geq \aleph_0$, and let $B = \{x \in G : x + x = 0\}$:*

1. *If $\kappa > \aleph_0$, then there is an independent $A \subseteq G$ with $|A| = \kappa$.*
2. *If $\kappa = \aleph_0$, then at least one of the following holds:*
   a. *There is an infinite independent $A \subseteq G$.*
   b. *G contains a subgroup isomorphic to $\mathbb{Z}$.*
   c. *G contains a subgroup isomorphic to some $\mathbb{Z}_{p^\infty}$.*

Furthermore, if $|G/B| = \kappa$, then the set A in cases 1 or 2a can be taken to contain no elements of order 2.

Proof. Let F be the torsion subgroup. Either $|F| = \kappa$ or $|G/F| = \kappa$ (or both).

If $|G/F| = \kappa$ then G does contain a copy of $\mathbb{Z}$ (since $F \neq G$), so we are done unless $\kappa > \aleph_0$, in which case we apply Corollary 3.5 to get an independent subset of G/F of the form $\{F + a_\alpha : \alpha \in \kappa\}$; here, we view elements of G/F as cosets of F. Then $\{a_\alpha : \alpha \in \kappa\}$ is an independent subset of G.

If $|F| = \kappa$, decompose F into its primary components as $F = \bigoplus_{p \in P} F_p$, and let $H_p = \{x \in F_p : ord(x) = p\}$. Then $H_p \cup \{0\}$ is a vector space over $\mathbb{Z}_p$, so choose $A_p \subseteq H_p$ such that A_p is a basis for $H_p \cup \{0\}$. Then each A_p is independent in G, and hence $A = \bigcup_{p \in P} A_p$ is also independent (since each $A_p \subseteq F_p$). We are done if $|A| = \kappa$, so assume that $|A| < \kappa$. If κ is uncountable, let $\lambda = \max(|A|, \aleph_0)$. Each $|A_p| \leq \lambda$, so $|H_p| \leq \lambda$, and then $|F_p| \leq \lambda$ by Lemma 3.6.1, but then $|F| \leq \lambda$; this is a contradiction because $\lambda < \kappa$. So, $\kappa = \aleph_0$ and A is finite, so each A_p is finite and only finitely many of the A_p are non-empty. Since $F_p = \{0\}$ whenever $A_p = \emptyset$, we may fix p such that F_p is infinite. But since H_p is finite, this F_p will contain a $\mathbb{Z}_{p^\infty}$ by Lemma 3.6.2.

Finally, if $|G/B| = \kappa$, we can apply the same argument to G/B to get an independent subset of G/B of the form $\{B + a_\alpha : \alpha \in \kappa\}$. Then $\{a_\alpha : \alpha \in \kappa\}$ is an independent subset of G containing no element of order 2. Observe that if G/B contains a copy of $\mathbb{Z}$ or $\mathbb{Z}_{p^\infty}$, then the same is true of G. $\square$

Proof of Theorem 1.4. By Lemma 3.7, there are three cases. In Cases 1 and 3, we use the fact that whenever H is a subgroup of G, we may regard bH as a closed subgroup of bG, so that any I_0 subset of H is also an I_0 subset of G.

Case 1: G is countable and contains a subgroup isomorphic to $\mathbb{Z}$: Apply Theorem 2.3 to get A contained in that subgroup.

Case 2: G contains an independent subset of cardinality $|G|$: Apply Corollary 3.3.

Case 3: G is countable and contains a subgroup isomorphic to $\mathbb{Z}_{p^\infty}$: We may assume that G is $\mathbb{Z}_{p^\infty}$, written additively. Let d be p if $p \geq 3$ and let $d = 4$ if $p = 2$. Let $A = \{a_n : n \in \mathbb{N}\}$, where $ord(a_0) = d$ and $da_{n+1} = a_n$. Although A is not independent, we have enough freedom in defining characters inductively on the a_n to repeat the arguments of the other two cases. Specifically, since $d \geq 3$, whenever we are given arcs $K_n \subset \mathbb{T}$ of length $2\pi/3$, we may find a character φ of $\mathbb{Z}_{p^\infty}$ such that $\varphi(a_n) \in K_n$ for all n.

Using this, we may show that A is an I_0 set: Fix any $E \subseteq \mathbb{N}$, and choose φ such that $\varphi(a_n) \in \{e^{ix} : -\pi/3 \leq x \leq \pi/3\}$ for $n \in E$ and $\varphi(a_n) \in \{e^{ix} : 2\pi/3 \leq x \leq 4\pi/3\}$ for $n \notin E$. This shows that $\{a_n : n \in E\}$ and $\{a_n : n \notin E\}$ have disjoint closures in bG. Likewise, we may show that 0 is not in the closure of $A + A$, by defining φ so that $\varphi(a_n) \in \{e^{ix} : \pi/6 \leq x \leq 5\pi/6\}$ for all n, so that $\varphi(b) \in \{e^{ix} : \pi/3 \leq x \leq 5\pi/3\}$ for all $b \in A + A$.

Finally, fix $c \neq 0$ in $\mathbb{Z}_{p^\infty}$, and we show that c cannot be a limit point of $A - A$ or $A + A$. Let ψ be the "usual" isomorphic embedding of $\mathbb{Z}_{p^\infty}$ into $\mathbb{T}$; so, $\psi(a_n) = e^{2\pi i/d^{n+1}}$. Since $\psi(c) \neq 1$ and $\psi(a_n) \to 1$, there must be an $N \in \mathbb{N}$ such that $\psi(c)$ is not in the closure of $\{\psi(a_n \pm a_m) : m, n \geq N\}$, so that c is not in the closure of $\{a_n \pm a_m : m, n \geq N\}$. But then, by Lemma 2.1, c is not a limit point of $A + A$ or $A - A$. $\square$

We now describe the topology of the character group in more detail.

Definition 3.8 *In* Γ_G,

$$U(\epsilon; x_1, \ldots, x_n) = \{\gamma : |\gamma(x_1) - 1| < \epsilon \ \& \ \cdots \ \& \ |\gamma(x_n) - 1| < \epsilon\} \ .$$

These sets form a base at 0 in Γ_G, but so do sets of a somewhat simpler form.

Lemma 3.9 *In Γ_G, a base at 0 is given by sets of the form:*

$$\Delta \cap U(\epsilon; x_1, \ldots, x_n) \quad ,$$

where Δ is a closed subgroup of Γ of finite index and $x_1, \ldots, x_n$ are independent elements of G of infinite order.

Proof. Note that every closed subgroup of finite index is also open, so that all sets of the stated form are indeed neighborhoods of 0. Now, let $U(\epsilon; y_1, \ldots, y_m)$ be any basic neighborhood of 0. Since $\langle y_1, \ldots, y_m \rangle$ is isomorphic to a product of cyclic groups, we can find independent $x_1, \ldots, x_n, z_1, \ldots, z_r$ such that $\langle y_1, \ldots, y_m \rangle = \langle x_1, \ldots, x_n, z_1, \ldots, z_r \rangle$, where each $ord(x_j)$ is infinite and each $ord(z_j)$ is finite. Choose N large enough so that each y_j is (uniquely) of the form $c_1 x_1 + \cdots c_n x_n + w$, where $w \in \langle z_1, \ldots, z_r \rangle$ and $N \geq |c_1| + \cdots + |c_n|$. Let $\Delta = \{\gamma : \gamma(z_1) = \cdots = \gamma(z_r) = 1\}$. We are done if we can show that $\Delta \cap U(\epsilon/N; x_1, \ldots, x_n) \subseteq U(\epsilon; y_1, \ldots, y_m)$. So, fix $\gamma \in \Delta \cap U(\epsilon/N; x_1, \ldots, x_n)$, and fix any $y_j = c_1 x_1 + \cdots c_n x_n + w$. Since $\gamma(w) = 1$, we have

$$|\gamma(y_j) - 1| = |\prod_1^n (\gamma(x_\ell))^{c_\ell} - 1| \leq \sum_1^n |c_\ell||\gamma(x_\ell) - 1| < \sum_1^n |c_\ell| \frac{\epsilon}{N} \leq \epsilon \quad .$$

Hence $\gamma \in U(\epsilon; y_1, \ldots, y_m)$. We have used here the inequality $|(\prod_1^n \alpha_\ell) - 1| \leq \sum_1^n |\alpha_\ell - 1|$, which holds whenever all the $\alpha_\ell \in \mathbb{T}$. $\Box$

In particular, we may apply this with $G = \mathbb{T}$ and $\Gamma = b\mathbb{Z}$ to get a description of the topology of $b\mathbb{Z}$ and hence of $\mathbb{Z}^\#$. In this case, it is somewhat simpler to apply the exponential map and index the neighborhoods by angles, rather than elements of $\mathbb{T}$.

Lemma 3.10 *For $\theta_1, \ldots, \theta_n \in \mathbb{R}$: $e^{i\theta_1}, \ldots, e^{i\theta_n}$ are independent elements of $\mathbb{T}$ of infinite order iff the reals $1, \theta_1/\pi, \ldots, \theta_n/\pi$ are linearly independent over the rationals.*

Definition 3.11 *In $\mathbb{Z}^\#$,*

$$V(\epsilon; \theta_1, \ldots, \theta_n) = \{a : |e^{ia\theta_1} - 1| < \epsilon \ \& \ \cdots \ \& \ |e^{ia\theta_n} - 1| < \epsilon\} \quad .$$

Lemma 3.12 *In $\mathbb{Z}^{\#}$, a basis at 0 is given by sets of the form:*

$$m\mathbb{Z} \cap V(\epsilon; \theta_1, \ldots, \theta_n) \quad ,$$

where m is a positive integer and the reals $1, \theta_1/\pi, \ldots, \theta_n/\pi$ are linearly independent over the rationals.

We now use structure theory to describe the characters which are 1-1 on G.

Definition 3.13 *If G is any discrete abelian group with character group Γ, then $\Omega = \Omega_\Gamma$ is the set of $\gamma \in \Gamma$ such that γ maps G 1-1 into $\mathbb{T}$.*

Equivalently, such γ have kernel equal to $\{0\}$.

Lemma 3.14 *$\gamma \in \Omega$ iff $ord(x) = ord(\gamma(x))$ for all $x \in G$.*

In particular, $arg(\gamma(x))/\pi$ is irrational whenever $ord(x) = \infty$ and $\gamma \in \Omega$.

Theorem 3.15 *$\Omega_\Gamma \neq \emptyset$ iff $|G| \leq 2^{\aleph_0}$ and, for each prime p, the primary component F_p of G is isomorphic to $\mathbb{Z}_{p^k}$ for some $k = k_p \in \{0, 1, 2, \ldots, \infty\}$.*

Proof. If $\gamma \in \Omega$, then $|G| = |\gamma(G)| \leq |\mathbb{T}| = 2^{\aleph_0}$. Also, the fact that F_p is isomorphic to some subgroup of $\mathbb{T}$ forces F_p to be of the form $\mathbb{Z}_{p^k}$.

Conversely, if each F_p is isomorphic to some $\mathbb{Z}_{p^k}$, we may easily define a 1-1 character ψ_0 on F (since it is sufficient to make it 1-1 on each F_p). Now, the quotient G/F is torsion-free, and we may also assume it is divisible, since every torsion-free abelian group is contained in a divisible abelian group of the same cardinality (see Exercise 5 on p. 12 of Kaplansky [12]). Let A be a basis for G/F (viewed as a vector space over the rationals). Say $A = \{F + a_\alpha : \alpha \in \kappa\}$. Since $\kappa \leq 2^{\aleph_0}$, we may choose $\{d_\alpha : \alpha \in \kappa\} \subset [0, 1]$ so that $\{1\} \cup \{d_\alpha : \alpha \in \kappa\}$ is linearly independent over the rationals. We then extend ψ_0 to a 1-1 character ψ by defining $\psi(x + a_\alpha) = \psi_0(x)e^{\pi i d_\alpha}$ whenever $x \in F$. $\square$

In the case that Γ is a torus, $\mathbb{T}^J$, then G is a direct sum of $|J|$ copies of $\mathbb{Z}$, so the theorem implies that $\Omega_\Gamma \neq \emptyset$ iff $|J| \leq 2^{\aleph_0}$. This is easier to see directly from the following explicit description of Ω, which follows from Lemma 3.14:

Lemma 3.16 *If $\Gamma = \mathbb{T}^J$, for some index set J, then $(e^{i\theta_j} : j \in J) \in \Omega$ iff the reals $\{1\} \cup \{\theta_j/\pi : j \in J\}$ are linearly independent over the rationals.*

When $J = \{1, \ldots, n\}$ is finite, we see that the elements of $\Omega_{\mathbb{T}^n}$ correspond nicely with the generators of the topology of $\mathbb{Z}^{\#}$ described in Lemma 3.12. This fortuitous coincidence will be useful later in proving Lemma 5.2. Also, we see that $\Omega_{\mathbb{T}^n}$ has Haar measure 1, but that easily generalizes to:

Theorem 3.17 *If G is countable and torsion-free, then $\lambda(\Omega) = 1$, where λ is the Haar measure on Γ.*

Proof. Let $I = \{z \in \mathbb{T} : ord(z) = \infty\}$; these are the z such that $arg(z)/\pi$ is irrational. For each $x \in G$, define $\Phi_x : \Gamma \to \mathbb{T}$ so that $\Phi_x(\gamma) = \gamma(x)$. Then Φ_x is a continuous homomorphism, and it maps Γ *onto* $\mathbb{T}$ (since $ord(x) = \infty$). Thus, the induced measure $\lambda\Phi_x^{-1}$ is the Haar measure on $\mathbb{T}$, so that $\lambda\Phi_x^{-1}(I) = 1$. Now, $\Omega = \bigcap_x \Phi_x^{-1}(I)$, which has measure 1 when G is countable. $\Box$

If G is torsion-free, then Ω depends on $|G|$: Ω is empty when $|G| > 2^{\aleph_0}$ (Theorem 3.15), and $\lambda(\Omega) = 1$, when $|G| \leq \aleph_0$ (Theorem 3.17). The third case for $|G|$ is covered by Theorem 3.18:

Theorem 3.18 *If G is torsion-free and $\aleph_1 \leq |G| \leq 2^{\aleph_0}$, then Ω has inner Haar measure 0 and outer Haar measure 1.*

Proof. We shall write Ω_G for Ω_{Γ_G}, denote the Haar measure on Γ_G by λ_G, and use $\mathcal{B}(\Gamma_G)$ for the collection of all Baire subsets of Γ_G. If H is a subgroup of G, define $\pi_H : \Gamma_G \to \Gamma_H$ so that $\pi_H(\gamma)$ is the restriction of γ to H. Observe that π_H maps *onto* Γ_H. Furthermore:

(1) If H is a countable subgroup of G and G/H is torsion-free then:
  - **(a)** For every $\delta \in \Gamma_H$, some $\gamma \in \pi_H^{-1}(\delta)$ is not 1-1; i.e., is in $\Gamma_G \backslash \Omega_G$.
  - **(b)** For every $\delta \in \Omega_H$, some $\gamma \in \pi_H^{-1}(\delta)$ is 1-1; i.e., is in Ω_G.

The proof of (b) is like the proof of Theorem 3.15, and the proof of (a) is easier.

Since Haar measure is completion regular (see Halmos [6], Theorem H, Section 64), Theorem 3.18 follows if we can prove that $\lambda_G(E) = 0$ whenever $E \in \mathcal{B}(\Gamma_G)$ and either $E \subseteq \Omega_G$ or $E \subseteq \Gamma_G \backslash \Omega_G$. We do this using:

(2) If $E \in \mathcal{B}(\Gamma_G)$ then there is a countable subgroup $H \subset G$ and an $\widetilde{E} \in \mathcal{B}(\Gamma_H)$ such that G/H is torsion-free and $E = \pi_H^{-1}(\widetilde{E})$.

Now, assuming (2), we are done: Assume $E \in \mathcal{B}(\Gamma_G)$. If $E \subseteq \Omega_G$, then $\widetilde{E} = \emptyset$ and hence $E = \emptyset$ by (1)(a). If $E \subseteq \Gamma_G \backslash \Omega_G$, then $\widetilde{E} \subseteq \Gamma_H \backslash \Omega_H$ by (1)(b), so $\lambda_H(\widetilde{E}) = 0$ by Theorem 3.17, so that $\lambda_G(E) = 0$ because $\lambda_H = \lambda_G \pi_H^{-1}$.

To prove (2): E is a countable boolean combination of closed G_δ sets $F_0, F_1, \ldots$, and each $F_n = g_n^{-1}\{0\}$, where $g_n \in C(\Gamma_G)$. There is then a countable set S of characters of Γ_G (i.e., $S \subset G$) such that each g_n is in the closed subalgebra of $C(G)$ generated by S. Then, let H be the set of all $x \in G$ such that $nx \in \langle S \rangle$ for some $n \neq 0$. H is countable because $\langle S \rangle$ is countable and G is torsion-free, so that for each x, there is at most one n with $nx \in \langle S \rangle$. Then, let $\widetilde{E} = \pi_H(E)$; the construction of H ensures that $\pi_H^{-1}\pi_H(E) = E$. $\square$

4 Uniform Distribution

We begin with some general results on uniformly distributed sequences, and then use these to study sequences in $\mathbb{Z}^\#$.

Definition 4.1 *A sequence $(x_n : n \in \mathbb{N})$ from a compact group X is* uniformly distributed *iff*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{j<N} f(x_j) = \int_X f \, d\lambda \qquad (UD)$$

for all $f \in C(X)$, where λ is the Haar probability measure on X.

We must be careful to distinguish the sequence $(x_n : n \in \mathbb{N})$ from the set $\{x_n : n \in \mathbb{N}\}$ in our notation here, since the property depends on the order of enumeration.

Clearly, for any X, the existence of a uniformly distributed sequence in X implies that X is separable. It does not imply that X is second countable, even in the special case when the elements of this sequence are all powers of a given element; see Lemma 4.8 below. First, some elementary facts:

Lemma 4.2 *If X, Y are compact groups, Φ is a continuous homomorphism from X into Y, and $(x_n : n \in \mathbb{N})$ is uniformly distributed in X, then $(\Phi(x_n) : n \in \mathbb{N})$ is uniformly distributed in $\Phi(X)$.*

Proof. If λ is the Haar measure on X, then the induced measure $\lambda\Phi^{-1}$ is the Haar measure on the compact group $\Phi(X)$. $\square$

Lemma 4.3 *If X is a group of order $m < \infty$, then $(x_n : n \in \mathbb{N})$ is uniformly distributed in X iff $\{n : x_n = y\}$ has asymptotic density $1/m$ for each $y \in X$.*

Lemma 4.4 *If $(\gamma_n : n \in \mathbb{N})$ is a sequence in $\Gamma = \Gamma_G$, then the following are equivalent:*

a. $(\gamma_n : n \in \mathbb{N})$ is uniformly distributed in Γ.

b. For all $x \in G \backslash \{0\}$, $\lim_{N\to\infty} \frac{1}{N} \sum_{j<N} \gamma_j(x) = 0$.

Proof. (b) is equivalent to postulating (UD) whenever $f : \Gamma \to \mathbb{T} \subset \mathbb{C}$ is a character of Γ. Then, use the fact that the set of finite linear combinations of characters is dense in $C(\Gamma)$. $\square$

Corollary 4.5 *$(z_n : n \in \mathbb{N})$ is uniformly distributed in $\mathbb{T}$ iff for all non-zero $k \in \mathbb{Z}$, $\lim_{N\to\infty} \frac{1}{N} \sum_{n<N} (z_n)^k = 0$*

Definition 4.6 *Suppose $S : \mathbb{N} \to \mathbb{Z}$ and $\gamma \in X$, where X is a compact group. Then γ is S-*uniform *iff the sequence $(\gamma^{S(n)} : n \in \mathbb{N})$ is uniformly distributed in X.*

The existence of any such γ forces X to be abelian, since it contains the dense abelian subgroup $\langle\gamma\rangle$. We thus may as well assume that $X = \Gamma = \Gamma_G$, the character group of the discrete abelian group G. The following criterion for γ to be S-uniform is simplest when G is torsion-free, since then item b.2 can be deleted:

Theorem 4.7 *The following are equivalent for any $\gamma \in \Gamma = \Gamma_G$ and any $S : \mathbb{N} \to \mathbb{Z}$:*

a. γ is S-uniform in Γ.

b. All three of the following hold:

1. $\gamma(x)$ is S-uniform in $\mathbb{T}$ whenever $ord(x) = \infty$.

2. The sequence $n \mapsto S(n) \pmod m$ is uniformly distributed in $\mathbb{Z}_m$ for all finite m such that G contains an element of order m.

3. $\gamma \in \Omega_\Gamma$.

Proof. Define $\Phi_x(\gamma) = \gamma(x)$, so that $\Phi_x(\gamma^{S(n)}) = \gamma^{S(n)}(x) = \gamma(x)^{S(n)}$.

To prove $a \Rightarrow b$, assume that γ is S-uniform in Γ. By Lemma 4.4

$$\lim_{N\to\infty} \frac{1}{N} \sum_{j<N} \gamma(x)^{S(n)} = 0 \qquad (*)$$

for all $x \neq 0$; in particular, $\gamma(x) \neq 1$, so $\gamma : G \to \mathbb{T}$ is 1-1, proving $b.3$. If $ord(x) = \infty$, then $\Phi_x(\Gamma) = \mathbb{T}$, so that $b.1$ follows from Lemma 4.2. If $ord(x) = m < \infty$, then $\Phi_x(\Gamma)$ is the set of m^{th} roots of 1, so that $b.2$ follows from Lemma 4.3.

To prove $b \Rightarrow a$: $b.3$ implies that $ord(x) = ord(\gamma(x))$ for every x. When $ord(x) = \infty$, $(*)$ holds by $b.1$ and Corollary 4.5 (applied with $k = 1$ and $z_n = \gamma(x)^{S(n)}$). When $0 < ord(x) = m < \infty$, $(*)$ holds by $b.2$. Thus, $(*)$ holds for all $x \neq 0$, so that γ is S-uniform by Lemma 4.4. $\square$

This theorem will be used in the proof of Lemma 5.2. The rest of the material in this section provides some further information on uniform distribution, but, with the exception of Definition 4.11, will not be used later.

Lemma 4.8 *The following are equivalent for any $\gamma \in \Gamma$:*

a. $(\gamma^{S(n)} : n \in \mathbb{N})$ *is uniformly distributed in* Γ *for some* $S : \mathbb{N} \to \mathbb{Z}$.

b. $\gamma \in \Omega_\Gamma$.

c. $(\gamma^n : n \in \mathbb{N})$ *is uniformly distributed in* Γ.

Proof. $(a) \to (b)$ is immediate from $(a) \to (b)$ of Theorm 4.7. $(b) \to (c)$ follows from $(b) \to (a)$ of Theorm 4.7, applied for $S(n) = n$, since then $(b.2)$ of 4.7 is trivial, and $(b.1)$ is just the observation that for this S, every element of $\mathbb{T}$ of infinite order is S-uniform in $\mathbb{T}$. $\square$

Note that unless $|\Gamma| = |G| = 1$, given any $\gamma \in \Gamma$, we can always find a 1-1 $S : \mathbb{N} \to \mathbb{Z}$ such that γ is not S-uniform. However, in many cases (Corollary 4.10 below), given any 1-1 $S : \mathbb{N} \to \mathbb{Z}$, it is true that γ is S-uniform for almost every γ. We first prove the following lemma, due to Weyl [22] in the case $G = \mathbb{Z}$:

Lemma 4.9 *Suppose that x_j, for $j \in \mathbb{N}$, are distinct elements of G. Then* $\lim_{N\to\infty} \frac{1}{N} \sum_{j<N} \gamma(x_j) = 0$ *holds for almost every $\gamma \in \Gamma$.*

Proof. Let $f_j(\gamma) = \gamma(x_j)$. Then $f_j \in L^2(\Gamma)$, each $|f_j(\gamma)| = 1$ for all γ, and the f_j form an orthonormal sequence in L^2 (since distinct characters are orthogonal).

Let $S_N(\gamma) = \frac{1}{N} \sum_{j<N} f_j(\gamma)$. We need to show that $S_N(\gamma) \to 0$ for almost every γ. Now, $\|S_N\|^2 = \frac{1}{N}$, so $\sum_{r=1}^{\infty} \|S_{r^2}\|^2 < \infty$, so the subsequence $S_{r^2}(\gamma) \to 0$ for almost every γ. Now, consider any $N > 0$ with $r^2 \leq N \leq (r+1)^2$. Then $|NS_N(\gamma) - r^2 S_{r^2}(\gamma)| \leq (r+1)^2 - r^2 \leq 3r$, so $|S_N(\gamma) - \frac{r^2}{N} S_{r^2}(\gamma)| \leq \frac{3}{r}$. Since

$\frac{r^2}{N} \to 1$ as $r \to \infty$, we have that $S_N(\gamma) \to 0$ for every γ such that $S_{r^2}(\gamma) \to 0$. $\square$

Corollary 4.10 *If G is countable and torsion-free, and $S : \mathbb{N} \to \mathbb{Z}$ is 1-1, then γ is S-uniform for almost every $\gamma \in \Gamma_G$.*

Proof. By Lemma 4.4, γ will be S-uniform iff

$$\lim_{N\to\infty} \frac{1}{N} \sum_{j<N} \gamma(S(j) \cdot x) = 0 \qquad (*)$$

holds for all $x \in G\backslash\{0\}$, since $\gamma^{S(j)}(x) = \gamma(S(j) \cdot x)$. For each fixed x, the elements $S(j) \cdot x$ are all distinct, since G is torsion-free; hence, Lemma 4.9 gives us a set E_x such that $(*)$ holds for all $\gamma \in E_x$ and $\lambda(E_x) = 1$. Let $E = \bigcap_{x\neq 0} E_x$. Then $\lambda(E) = 1$ because G is countable, and $(*)$ holds for every $\gamma \in E$ and every $x \in G\backslash\{0\}$. $\square$

When discussing uniform distribution in $\mathbb{T}$, it is often simpler to apply the exponential map and use the following terminology:

Definition 4.11 *A sequence $(y_n : n \in \mathbb{N})$ of real numbers is* uniformly distributed (mod 1) *iff $(e^{2\pi i y_n} : n \in \mathbb{N})$ is uniformly distributed in $\mathbb{T}$.*

This is the same as saying that $\{n \in \mathbb{N} : y_n (\mathrm{mod}\ 1) \in [a, b]\}$ has asymptotic density $b - a$ whenever $0 \leq a \leq b \leq 1$.

Proposition 4.12 *The following are equivalent for any $S : \mathbb{N} \to \mathbb{Z}$:*

a. S is uniformly distributed in $b\mathbb{Z}$.

b. Both of the following hold:

1. *αS is uniformly distributed* (mod 1) *for every irrational α.*
2. *The sequence $n \mapsto S(n)\,(\mathrm{mod}\ m)$ is uniformly distributed in $\mathbb{Z}_m$ for all $m > 1$.*

Proof. Note that (a) says that the element $1 \in \mathbb{Z}$ is S-uniform in $b\mathbb{Z}$. Also, 1, regarded as a character of $\mathbb{T}$, is the identity map on $\mathbb{T}$, and hence lies in $\Omega_{b\mathbb{Z}}$. So, we can apply Theorem 4.7, with $b\mathbb{Z}$ and 1 in place of Γ and γ. $\square$

5 Polynomial Sequences

Uniform distribution (mod 1) was studied in some detail by Weyl. In particular, the following is a special case of Theorem 9 of [22].

Theorem 5.1 (Weyl) *If $S(x)$ is a non-constant polynomial with integer coefficients, then $\{\alpha S(n) : n \in \mathbb{N}\}$ is uniformly distributed* (mod 1) *for every irrational α.*

We shall use Theorem 5.1 to compute the closure of the range of a polynomial in $\mathbb{Z}^\#$. First, a preliminary lemma:

Lemma 5.2 *Suppose that $E \subseteq \mathbb{Z}$ and for each $m \geq 1$, there is a sequence S of elements of $E \cap m\mathbb{Z}$ such that αS is uniformly distributed* (mod 1) *for every irrational α. Then 0 is a limit point of E in $\mathbb{Z}^\#$.*

Proof. We may assume that $0 \notin E$ (since uniform distribution does not change if we delete one element), so that we need only show that 0 is in the closure of E. Applying Lemma 3.12, fix a basic neighborhood of 0 of the form $m\mathbb{Z} \cap V(\epsilon; \theta_1, \ldots, \theta_n)$, where $m > 0$ and $1, \theta_1/\pi, \ldots, \theta_n/\pi$ are independent over the rationals. For this m, fix an S as hypothesized in the lemma. By Lemma 3.16, $(e^{i\theta_1}, \ldots, e^{i\theta_n})$ is in $\Omega_{\mathbb{T}^n}$, and is hence S-uniform in $\mathbb{T}^n$ by Theorem 4.7 applied with $G = \mathbb{Z}^n$. In particular, $\{(e^{iS(k)\theta_1}, \ldots, e^{iS(k)\theta_n}) : k \in \mathbb{N}\}$ is dense in $\mathbb{T}^n$, so we may fix a k such that $|e^{iS(k)\theta_\ell} - 1| < \epsilon$ for each $\ell = 1, \ldots, n$. Then $S(k) \in m\mathbb{Z} \cap V(\epsilon; \theta_1, \ldots, \theta_n)$. $\square$

Theorem 5.3 *Suppose that $f(x)$ is a non-constant polynomial with integer coefficients and r is an integer. Then the following are equivalent:*

a. r is a limit point of $f(\mathbb{N})$ in $\mathbb{Z}^\#$.
b. r is a limit point of $f(\mathbb{Z})$ in $\mathbb{Z}^\#$.
c. $f(\mathbb{Z}) \cap (m\mathbb{Z} + r) \neq \emptyset$ for each $m \geq 1$.

Proof. $a \Rightarrow b \Rightarrow c$ is trivial, so we assume c and prove a by showing that 0 is a limit point of $f(\mathbb{N}) - r$. For each m, we may fix a c such that $f(c) \in m\mathbb{Z} + r$. Then, let $S(j) = f(c + jm) - r$, and note that $S(j) \in m\mathbb{Z}$ for all j. The desired result is now immediate by Lemma 5.2 and Theorem 5.1. $\square$

Note that condition (c) just says that the equation $f(x) \equiv r \pmod{m}$ has a solution for each $m > 1$. This is trivial if $f(x) = r$ has a solution in $\mathbb{Z}$, so:

Theorem 5.4 *If $f(x)$ is a non-constant polynomial with integer coefficients, then every point of $f(\mathbb{Z})$ is a limit point of $f(\mathbb{N})$ in $\mathbb{Z}^\#$.*

For integers outside of $f(\mathbb{Z})$, the situation is more complicated because the solvability of $f(x) \equiv r \pmod{m}$ is more complicated; see, e.g., LeVeque [13]. We consider just two cases:

Theorem 5.5 *If $f(x) = x^k$, where k is a positive integer, then $f(\mathbb{Z})$ is closed in $\mathbb{Z}^\#$.*

Proof. It is sufficient to fix an $r \notin f(\mathbb{Z})$ and produce an m such that there are no solutions to $f(x) \equiv r \pmod{m}$. So, choose $m = 3r^2$, and suppose we could find an n such that $n^k \equiv r \pmod{3r^2}$. We may assume that $n > 0$ (by adding a multiple of $3r^2$), and choose t so that $n^k = r + 3r^2 t = r(1 + 3rt)$. Since r and $1 + 3rt$ are relatively prime, we may fix $y, z \geq 0$ such that either

1. $r, (1 + 3rt) > 0$ and $r = y^k$ and $1 + 3rt = z^k$, *or*
2. $r, (1 + 3rt) < 0$ and $r = -y^k$ and $1 + 3rt = -z^k$.

But, since $r \notin f(\mathbb{Z})$, we must have (2) and k must be even. But then (2) yields $z^k \equiv -1 \pmod{3}$, which is impossible when k is even. $\square$

Also, $f(\mathbb{Z})$ is (trivially) closed in $\mathbb{Z}^\#$ whenever f is a linear polynomial, but this need not be true for quadratic polynomials, by the following theorem. As usual, (x, y) denotes the greatest common divisor of x, y, and "$x|y$" means that y is divisible by x.

Theorem 5.6 *Suppose that $f(x) = ax^2 + bx + c$, with $a \neq 0$ and $a, b, c \in \mathbb{Z}$. Let $e = (a, b)$. Then:*

1. *0 is a limit point of $f(\mathbb{Z})$ iff $e|c$ and $D = b^2 - 4ac$ is a square in $\mathbb{Z}$.*
2. *$f(\mathbb{Z})$ is closed in $\mathbb{Z}^\#$ iff a/e is not divisible by two distinct primes.*

Proof. For $\Rightarrow$ of (1): We have, by Theorem 5.3,

$$\forall m \geq 1 \; \exists x \; [ax^2 + bx + c \equiv 0 \pmod{m}] \qquad (*)$$

Taking $m = e$, and observing that $ax^2 + bx + c \equiv c \pmod{e}$ for all x, $(*)$ yields $e|c$. Taking m to be any prime, the solvability of $ax^2 + bx + c = 0$ in the field $\mathbb{Z}_m$ implies that the discriminant D is a perfect square (mod m). Since this is true for all primes, D must be a square in $\mathbb{Z}$ (see [13], Theorem 5-9).

For $\Leftarrow$ of (1): Now, we must establish $(*)$. Since $e|c$, the polynomial $f(x)/e$ has integer coefficients. Since D is a square, this polynomial has rational roots, so it factors over $\mathbb{Z}$. Thus, we can write

$$ax^2 + bx + c = e(\alpha_1 x + \beta_1)(\alpha_2 x + \beta_2) \quad ,$$

where $\alpha_\ell, \beta_\ell \in \mathbb{Z}$ for $\ell = 1, 2$. Since $e \cdot (\alpha_1, \alpha_2)$ divides both a and b, and hence e, we must have $(\alpha_1, \alpha_2) = 1$. Hence, any m may be factored as $m = m_1 m_2$, with $(\alpha_1, m_1) = (\alpha_2, m_2) = (m_1, m_2) = 1$. Now, to prove $(*)$, choose n_ℓ so that $(\alpha_\ell n_\ell + \beta_\ell) \equiv 0 \,(\mathrm{mod}\, m_\ell)$ for $\ell = 1, 2$; this is possible because α_ℓ is a unit in the ring $\mathbb{Z}_{m_\ell}$. Then apply the Chinese Remainder Theorem (as in [13], Chapter 3) to fix n such that $n \equiv n_\ell \,(\mathrm{mod}\, m_\ell)$ for $\ell = 1, 2$; then $(\alpha_1 n + \beta_1)(\alpha_2 n + \beta_2) \equiv 0 \,(\mathrm{mod}\, m)$.

For (2), we may first, by translation, assume that $c = 0$, so $f(x) = ax^2 + bx$. Then, we may assume that $e = 1$, since $f(\mathbb{Z})$ will be closed iff $\frac{1}{e} f(\mathbb{Z})$ is closed. Now, for any k, let $g_k(x) = ax^2 + bx + k$. Then $f(\mathbb{Z})$ will be closed iff for each k, if 0 is a limit point of $g_k(\mathbb{Z})$ then $0 \in g_k(\mathbb{Z})$. By part (1), 0 is a limit point of $g_k(\mathbb{Z})$ iff the discriminant $b^2 - 4ak$ is a square, say s^2, so $4ak = b^2 - s^2$. By the quadratic formula, $0 \in g_k(\mathbb{Z})$ iff at least one of $(-b \pm s)/2a$ is an integer. So, $f(\mathbb{Z})$ is closed iff

$$\forall s, k[4ak = b^2 - s^2 \implies 2a|(-b + s) \text{ or } 2a|(-b - s)]$$

Equivalently, letting $t = s - b$, so $t + 2b = s + b$,

$$\forall t[4a|t(t + 2b) \implies 2a|t \text{ or } 2a|(t + 2b)]$$

If $a = p^\ell$ for p a prime, this is true, since $(a, b) = 1$ (consider the cases $p = 2$, $p > 2$ separately). If a is not a prime power, this is false: Set $a = \mu\nu$, where $(\mu, \nu) = 1$ and $|\mu|, |\nu| > 1$, choose M, N so that $b = M\mu - N\nu$, and let $t = 2N\nu$, so that $t + 2b = 2M\mu$. Then $4a$ divides $t(t + 2b) = 4aMN$. If $2a = 2\mu\nu$ divides $t = 2N\nu$, then μ divides N, and hence b, contradicting $(a, b) = 1$. Likewise, $2a$ cannot divide $t + 2b$. $\square$

6 Haar Measure in bG

Computing the Haar probability measure of specific sets in bG seems a bit intractable, although some results on such questions were obtained by Blum, Eisenberg, and Hahn [2]. We add a few more results of this type here. We know of only two basic methods for computing measure, summarized in Lemmas 6.1 and 6.3.

Lemma 6.1 *If X is any compact abelian group and $E \subseteq X$ is a Haar measurable set of positive measure, then $E - E$ contains a neighborhood of* 0.

Proof. Let $f(x) = \int \chi_E(y)\chi_E(x+y)d\lambda(y)$, where χ_E is the characteristic function of E. Then f is continuous and $f(0) = \lambda(E) > 0$, so f is positive in some neighborhood of 0, and $f(x) > 0$ implies $x \in E - E$. $\square$

Corollary 6.2 *If G is an infinite abelian group and $A \subseteq G$ is such that* 0 *is the only limit point of $A - A$ in $G^\#$, then $\overline{A}$ (the closure of A in bG) has Haar measure* 0.

Proof. Since G is infinite, every nonempty open subset of $G^\#$ is dense in itself. If $\overline{A-A}$ contained a neighborhood of 0 in $G^\#$, every point of that neighborhood would be a limit point of $A - A$, contradicting our hypothesis on A. Since $\overline{A} - \overline{A} \subseteq \overline{A-A}$, the result follows from Lemma 6.1. $\square$

In particular, if $A \subset \mathbb{Z}$ is a Hadamard set, then this corollary applies (by Theorem 2.3), so $\lambda(\overline{A}) = 0$. This generalizes a result in [2], which proved this for $A = \{a^n : n \in \mathbb{N}\}$ and $A = \{n! : n \in \mathbb{N}\}$.

The second method for computing $\lambda(\overline{A})$ is specific to $\mathbb{Z}$:

Lemma 6.3 *Suppose that $Q \subset \mathbb{N}$ is some set of primes and $A \subseteq \mathbb{Z}$. Suppose that for each $q \in Q$, there is a j_q such that $\{a \in A : a \equiv j_q \pmod{q}\}$ is finite. Then $\lambda(\overline{A}) \leq \prod_{q\in Q}(1 - 1/q)$. In particular, if $\sum_{q \in Q} 1/q = \infty$, then $\lambda(\overline{A}) = 0$.*

Proof. Fix a finite $F \subseteq Q$, let $m = \prod_{q\in F} q$, and define:

$$\begin{aligned} B_q &= \{a \in A : a \not\equiv j_q \pmod{q}\} \;; & B = \textstyle\bigcap_{q\in F} B_q \\ K_q &= \{k \in \{0, \ldots, m-1\} : k \not\equiv j_q \pmod{q}\} \;; & K = \textstyle\bigcap_{q\in F} K_q \end{aligned}$$

Then $A \backslash B$ is finite, $|K| = \prod_{q\in F}(q-1)$ by the Chinese Remainder Theorem, and $b \pmod{m} \in K$ for each $b \in B$. Therefore,

$$\lambda(\overline{A}) = \lambda(\overline{B}) \leq |K|/m = \prod_{q\in F}(1 - 1/q)$$

Since F was an arbitrary finite subset of Q, the lemma follows. $\square$

Something like this lemma was used in [2] to prove that $\lambda(\overline{A}) = 0$ in two cases: If A is the set of all primes, let $Q = A$ and let $j_q = 0$. If $A = \{x^k : x \in \mathbb{Z}\}$, where $k \geq 2$, let Q be the set of primes q such that $q \equiv 1 \pmod{k}$; an appropriate j_q can be found because for $q \in Q$, the map $x \mapsto x^k$ cannot be a bijection of the cyclic group of order $q-1$. The fact that $\sum_{q \in Q} 1/q = \infty$ follows from Dirichlet's Theorem (see [14], p. 217):

Theorem 6.4 *If m, n are two relatively prime positive integers, and Q is the set of all primes q such that $q \equiv m \pmod{n}$, then $\sum_{q \in Q} 1/q = \infty$.*

In view of the result for $A = \{x^k : x \in \mathbb{Z}\}$, it is tempting to conjecture that $\lambda(\overline{A}) = 0$ whenever $A = f(\mathbb{Z})$ for some polynomial f of degree at least 2. However, we are only able to prove the following cases of this:[1]

Theorem 6.5 *Let f be a polynomial with integer coefficients of degree at least 2, and let $A = f(\mathbb{Z})$. Then $\lambda(\overline{A}) < 1$. If f has degree either 2 or 3, then $\lambda(\overline{A}) = 0$.*

Proof. Let $g(x) = f(x+1) - f(x)$, and let Q be the set of primes q such that $g(x)$ has a root $(\bmod\, q)$. For $q \in Q$, the polynomial f, viewed as a function from $\mathbb{Z}_q$ to $\mathbb{Z}_q$, fails to be 1-1, so it fails to be onto, so Lemma 6.3 applies here.

To prove that $\lambda(\overline{A}) < 1$, it is sufficient to prove that $Q \neq \emptyset$. But if we fix any integer j with $|g(j)| \geq 2$, and let q be any prime divisor of $g(j)$, then $q \in Q$.

To prove that $\lambda(\overline{A}) = 0$, it is sufficient to prove that $\sum_{q \in Q} 1/q = \infty$. If f is quadratic, then g is linear; say $g(x) = rx + s$, and Q contains all primes larger than $|r|$. If f is cubic, then g is quadratic; say $g(x) = rx^2 + sx + t$. Let $D = s^2 - 4rt$ be the discriminant. Let $p_1, \ldots, p_\ell$ be the odd prime divisors of D, and let $M = 8p_1 \ldots p_\ell$. We shall show that D is a square in $\mathbb{Z}_q$ whenever q is a prime and $q \equiv 1 \pmod{M}$. If we do so, then Q will contain all primes $q > |r|$ such that $q \equiv 1 \pmod{M}$, so that $\sum_{q \in Q} 1/q = \infty$ by Dirichlet's Theorem.

To simplify notation, we use the Legendre symbol $(a \,|\, q)$, defined whenever $a \in \mathbb{Z}$ and q is an odd prime: if $(a, q) = 1$, then $(a \,|\, q)$ is 1 if a is a quadratic residue $(\bmod\, q)$ and -1 otherwise; $(a \,|\, q) = 0$ whenever $q | a$. Now, we assume that $q \equiv 1 \pmod{M}$ and we must show that $(D \,|\, q) = 1$. Since $(ab \,|\, q) = (a \,|\, q)(b \,|\, q)$ (see [13], Theorem 5-3), it is sufficient to prove that $(p \,|\, q) = 1$ for

[1] David W. Boyd has pointed out that the Čebotarev Density Theorem (*Math. Ann.* 95 (1925-1926) 191-229) can be used to establish this result for all f of degree at least 2.

each prime divisor p of D. If $p = 2$, use the fact that $(2\,|\,q) = 1$ whenever $q \equiv 1 \pmod 8$ (see [13], p. 68). If p is odd, use the quadratic reciprocity law: $(p\,|\,q)(q\,|\,p) = (-1)^{(p-1)(q-1)/4}$ (see [13], Theorem 5-7). Since $q \equiv 1 \pmod 8$ here, this reduces to $(p\,|\,q) = (q\,|\,p)$. Since also $q \equiv 1 \pmod p$, we have $(p\,|\,q) = (q\,|\,p) = (1\,|\,p) = 1$. $\square$

7 Sidon Sets and $\Lambda(p)$ Sets

Since the sets we study in this section are built from sets of the form $A - A$, we begin by using some graph theory to describe the topology on $A - A$.

If X is an abelian group and $A \subseteq X$, an (undirected) *A-graph* is a collection Π of *unordered* pairs $\{a, b\}$ (called "edges"), where $a, b \in A$ and $a \neq b$. The points a and b are called the *end-nodes* of $\{a, b\}$. The *chromatic number*, $\chi(\Pi)$, is the least κ such that A can be partitioned into κ sets (colors), C_i (for $i < \kappa$), such that no edge of Π has both end-nodes in the same C_i.

Definition 7.1 *If Π is an A-graph, then $\delta(\Pi) = \{a - b : \{a, b\} \in \Pi\}$. If $0 \notin E \subseteq A - A$, then* Π spans E *iff $E \cup (-E) = \delta(\Pi)$. Π is a* minimal spanning A-graph *for E iff Π spans E and, for every $e \in E$ there is exactly one $\{a, b\} \in \Pi$ such that $a - b = \pm e$.*

Note that $\delta(\Pi) = -\delta(\Pi)$, since $\{a, b\} = \{b, a\}$. An element $x \in E$ may have more than one representation of the form $a - b$, so that there may be more than one Π which spans E, and more than one minimal spanning graph.

Lemma 7.2 *If X is a compact abelian group, $A \subseteq X$, and $0 \notin E \subseteq A - A$, then (1) $\Rightarrow$ (2) $\Rightarrow$ (3), and (3) $\Rightarrow$ (1) in the case that A is discrete in its relative topology and C^*-embedded in X.*

1. *$\chi(\Pi) \geq \aleph_0$ for every Π which spans E.*
2. *$\chi(\Pi) \geq \aleph_0$ for some Π which spans E.*
3. *$0 \in \overline{E}$*

Proof. (1) $\Rightarrow$ (2) is obvious. For (2) $\Rightarrow$ (3), if $0 \notin \overline{E}$, let U be a neighborhood of 0 which is disjoint from $E \cup (-E)$, and then let V be a neighborhood of 0 with $V - V \subseteq U$. By compactness, let $\bigcup_{i<\kappa}(V + x_i) = X$, where κ is finite, and let $C_i = A \cap (V + x_i)$. If $a, b \in C_i$, then $a - b$ and $b - a$ are in U, and hence not in $E \cup (-E)$, so $\{a, b\} \notin \Pi$. Hence, $\chi(\Pi) \leq \kappa < \aleph_0$. Note that the sets C_i defined here need not be disjoint, but they can always be reduced to disjoint sets.

For (3) $\Rightarrow$ (1), assume Π spans E and $\chi(\Pi) < \aleph_0$. Let $A = \bigcup_{i<\kappa} C_i$, where κ is finite, the C_i are disjoint, and no edge in Π has both end-nodes in the same C_i. Since A is C^*-embedded, the $\overline{C_i}$ are also disjoint, so $0 \notin \overline{C_i} - \overline{C_j}$ whenever $i \neq j$. Now, $\overline{E} \subseteq \bigcup\{\overline{C_i} - \overline{C_j} : i, j < \kappa$ and $i \neq j\}$, since this union is closed and contains E. So, $0 \notin \overline{E}$. $\square$

In the case that $A \subseteq \mathbb{Z}$, $X = b\mathbb{Z}$, and A is a Hadamard set, this lemma will be useful for studying $\Lambda(p)$ subsets of $A - A$. As usual, if $f \in L^1(\mathbb{T})$, then $\hat{f}(n)$ denotes its n^{th} Fourier coefficient. If $E \subseteq \mathbb{Z}$, then f is *E-spectral* iff $\hat{f}(n) = 0$ whenever $n \notin E$.

Definition 7.3 *If $p \in (2, \infty)$ and $C < \infty$, then C is a $\Lambda(p)$* constant *for $E \subseteq \mathbb{Z}$ iff $\|f\|_p \leq C\|f\|_2$ for all E-spectral trigonometric polynomials. E is a $\Lambda(p)$* set *iff E has some finite $\Lambda(p)$ constant.*

It is immediate from the definition that each finite set is $\Lambda(p)$, and every subset of a $\Lambda(p)$ set is $\Lambda(p)$. Every finite union of $\Lambda(p)$ sets is also $\Lambda(p)$ by:

Lemma 7.4 *If C is a $\Lambda(p)$ constant for E_1 and for E_2, then $C\sqrt{2}$ is a $\Lambda(p)$ constant for $E_1 \cup E_2$.*

Proof. We may assume that E_1, E_2 are disjoint. Any $(E_1 \cup E_2)$-spectral trigonometric polynomial is of the form $f_1 + f_2$, where each f_ℓ is E_ℓ spectral. Then

$$\|f_1 + f_2\|_p \leq \|f_1\|_p + \|f_2\|_p \leq C(\|f_1\|_2 + \|f_2\|_2) \leq C\sqrt{2}\,\|f_1 + f_2\|_2 \ .$$

The last "$\leq$" is by orthogonality of f_1, f_2. $\square$

For more on these notions, see Rudin [19] and Edwards and Gaudry [3]. To construct non-trivial examples of $\Lambda(p)$ sets, one can piece together finite sets by applying the following:

Definition 7.5 *A* Hadamard decomposition *of $\mathbb{Z}$ is a sequence of finite sets $(\Delta_j : j \in \mathbb{Z})$ such that for some Hadamard set (see Definition 2.2) $A = \{a_n : n \in \mathbb{N}\}$: Δ_j is $[a_{j-1}, a_j)$ when $j > 0$, $(a_{|j|}, a_{|j|-1}]$ when $j < 0$, and $(-a_0, a_0)$ when $j = 0$.*

Theorem 7.6 *If $E \subset \mathbb{Z}$, $(\Delta_j : j \in \mathbb{Z})$ is a Hadamard decomposition, and C is a $\Lambda(p)$ constant for each $E \cap \Delta_j$, then E is a $\Lambda(p)$ set.*

This follows immediately from the Littlewood-Paley Theorem ([3], Theorem 8.2.8), which asserts that Hadamard decompositions have the LP property, plus the fact ([3], Theorem 9.1.4) that every decomposition with the LP property satisfies Theorem 7.6. Applying this theorem once, and noting that 1 is a $\Lambda(p)$ constant for every singleton, we generate the classical result that all Hadamard sets are $\Lambda(p)$ for all $p \in (2, \infty)$. Applying the theorem again, we see:

Theorem 7.7 *If $A = \{a_n : n \in \mathbb{N}\}$ is a Hadamard set, then $A - A$ is a $\Lambda(p)$ set for all $p \in (2, \infty)$.*

Proof. Assume that A satisfies the Hadamard condition with ratio $M > 1$. Applying Lemma 7.4, it is sufficient to prove that $E = \{a_n - a_m : m < n\}$ is $\Lambda(p)$. Fix r such that $(M-1)M^r > 1$. Then the only elements of E in the interval $[a_{n-1}, a_n]$ are of the form $a_{n+j} - a_m$ for $j \le r$ and $m < n + j$, since if $j > r$, then $a_{n+j} - a_m \ge a_{n+j} - a_{n+j-1} \ge (M-1)a_{n+j-1} \ge (M-1)M^r a_n > a_n$. Thus, if $(\Delta_j : j \in \mathbb{Z})$ is the associated Hadamard decomposition, then each $E \cap \Delta_j$ is covered by $r+1$ translates of $-A$. Since A, $-A$, and all its translates have the same $\Lambda(p)$ constant, we may apply Lemma 7.4 and fix a C which is a $\Lambda(p)$ constant for each $E \cap \Delta_j$, and then apply Theorem 7.6. $\square$

In the case that $M = 2$, this result is Theorem 9.2.1 of [3]. Modifying this construction, we may construct a dense $\Lambda(p)$ set:

Theorem 7.8 *There is an $E \subseteq \mathbb{N}$ such that E is a $\Lambda(p)$ set for all $p \in (2, \infty)$ and E is dense in $\mathbb{Z}^\#$.*

Proof. For $m \ge 1$, let a_m, b_m, c_m be positive integers such that

α. $a_{m+1} \ge 2a_m$.

β. $b_1 = 1$, $b_m < b_{m+1}$, and $b_{m+1} - b_m \nearrow \infty$ as $m \nearrow \infty$.

γ. $c_m \le b_m$, and $\{m : c_m = q\}$ is infinite for every positive integer q.

Define

$$E_m = \{a_s + c_m - a_r : b_m < r < s \le b_{m+1}\} \quad ; \quad E = \bigcup_{m=1}^{\infty} E_m \quad .$$

To prove that E is $\Lambda(p)$, we apply Theorem 7.6 with the Hadamard decomposition associated with $A = \{a_m : m \ge 1\}$. Fix $k > 1$, and let n be the integer for which $b_n < k \le b_{n+1}$. We claim that

$$E \cap [a_{k-1}, a_k) \subseteq (a_k + c_n) - A \qquad (*)$$

Assuming $(*)$, each $E \cap [a_{k-1}, a_k)$ is a subset of a translate of $-A$, and hence has uniformly the same $\Lambda(p)$ constant as does A, so Theorem 7.6 applies. To prove $(*)$, fix $x \in E \cap [a_{k-1}, a_k)$, let m be any integer for which $x \in E_m$, and fix r, s so that

$$x = a_s + c_m - a_r \quad \text{and} \quad b_m < r < s \le b_{m+1} \quad .$$

Since $c_m \le b_m < r \le a_r$ we have $x < a_s$, whereas $r < s$ and (α) imply $a_{s-1} \le a_s - a_r < x$. Thus, $x \in (a_{s-1}, a_s) \cap [a_{k-1}, a_k)$, which forces $s = k$, and hence $s \in (b_m, b_{m+1}] \cap (b_n, b_{n+1}]$, so that $m = n$, and $(*)$ is proved.

To prove that E is dense in $\mathbb{Z}^\#$, it is sufficient to show that $\overline{E}$ contains all positive integers. So, we fix a positive $q \notin E$ and prove that $q \in \overline{E}$; or, equivalently, that $0 \in \overline{E - q}$.

For those m for which $c_m = q$, let

$$F_m = E_m - q \;\; ; \;\; F = \bigcup \{F_m : c_m = q\} \quad ,$$

and note that $F \subseteq (E - q) \cap (A - A)$. Let

$$\Pi_m = \{\{a_r, a_s\} : b_m < r < s \le b_{m+1}\} \;\; ; \;\; \Pi = \bigcup \{\Pi_m : c_m = q\} \quad .$$

Then Π_m is a complete N-graph (with $N = b_{m+1} - b_m$), so that $\chi(\Pi_m) = b_{m+1} - b_m$. Hence, by (β), $\chi(\Pi) = \aleph_0$. Since Π spans F, Lemma 7.2, applied in $b\mathbb{Z}$, shows that $0 \in \overline{F} \subseteq \overline{E - q}$. $\square$

We next consider Sidon sets. One definition is:

Definition 7.9 *A* Sidon set *is an $E \subseteq \mathbb{Z}$ such that the Fourier series of every E-spectral function in $C(\mathbb{T})$ converges absolutely.*

Every I_0 set is Sidon and every Sidon set is $\Lambda(p)$ for each $p \in (2, \infty)$. For proofs of this, and for many equivalents to the notion of "Sidon", see [3] [11] [15] [19] [20]. It is unknown whether there is a Sidon set with a limit point in $\mathbb{Z}^\#$, although Ramsey [18] showed that if there is such a set, then there is another Sidon set which is dense in $\mathbb{Z}^\#$.

Theorem 7.15 below indicates that one cannot construct a Sidon set with a limit point by using the method of Theorems 7.7 and 7.8. To prove this, we use, as did Ramsey, the following combinatorial characterization of Sidon sets.

Definition 7.10 *A set $P \subseteq \mathbb{Z}$ is* quasi-independent *iff $\sum_{j=i}^{n} k_j x_j \ne 0$ whenever $n \ge 1$, the x_j are distinct elements of P, and all the $k_j \in \{-1, 1\}$.*

Theorem 7.11 (Pisier [16]) *A set $E \subseteq \mathbb{Z}$ is Sidon iff there is a positive $C \in \mathbb{N}$ such that every finite $P \subseteq E$ contains a quasi-independent subset Q with $|Q| \geq |P|/C$.*

Now, if we consider Sidon subsets of $A - A$, we can relate Pisier's characterization to properties of the associated graph. A *cycle* in a graph Π is a sequence of distinct nodes, $(a_0, \ldots, a_{n-1})$, such that $n \geq 3$ and all the edges $\{a_0, a_1\}, \ldots \{a_{n-2}, a_{n-1}\}, \{a_{n-1}, a_0\}$ are in Π. The next two lemmas show that cycles in the associated graph destroy quasi-independence, whereas graphs with large chromatic number contain cycles.

Lemma 7.12 *If $A \subseteq \mathbb{Z}$, Q is a quasi-independent subset of $A - A$, and Π is a minimal spanning A-graph for Q, then Π contains no cycles.*

Proof. Suppose that $(a_0, \ldots, a_{n-1})$ were a cycle in Π. Let $e_j = a_j - a_{j+1}$ for $0 \leq j \leq n-1$, where we set $a_n = a_0$. Note that $e_j \neq \pm e_k$ when $j \neq k$, since $a_j - a_{j+1} = \pm(a_k - a_{k+1})$ would contradict minimality of Π. But then $e_0 + \cdots + e_{n-1} = 0$ and each e_j or $-e_j$ is in Q, contradicting quasi-independence of Q. □

Definition 7.13 *If Π is an A-graph, and $B \subseteq A$, then Π_B is the set of edges of Π which have both their end-nodes in B.*

Lemma 7.14 *Suppose that Π is an A-graph, C is a positive integer, and $\chi(\Pi) \geq 2C + 1$. Then there is a finite set $B \subseteq A$ such that every subgraph $\Psi \subseteq \Pi_B$ with $|\Psi| \geq |\Pi_B|/C$ contains a cycle.*

Proof. Among the finite $B \subseteq A$ with $\chi(\Pi_B) \geq 2C+1$, fix one that is minimal – that is, $\chi(\Pi_{B\setminus\{b\}}) \leq 2C$ for each $b \in B$. It follows that each $b \in B$ lies on at least $2C$ edges in Π_B (otherwise, one could color B with $2C$ colors by first coloring $B\setminus\{b\}$). Counting edges and nodes then yields $2|\Pi_B| \geq 2C \cdot |B|$. Thus, if Ψ is as in the statement of the lemma, $|\Psi| \geq |B|$. Thus, Ψ has at least as many edges as nodes, whereas finite acyclic graphs have more nodes than edges. □

Combining these two lemmas:

Theorem 7.15 *If $A \subseteq \mathbb{N}$ is a Hadamard set and $E \subseteq A - A$ is a Sidon set, then E has no limit points in $\mathbb{Z}^\#$.*

Proof. The only possible limit point of E is 0 by Theorem 2.3.2. Assume that 0 is a limit point and that E is Sidon. We may assume that $0 \neq E$.

Choose a minimal spanning A-graph Π for E, and fix C as in Pisier's Theorem 7.11. Since A is Hadamard, it is C^*-embedded in $b\mathbb{Z}$ by Theorem 2.3, so we may apply Lemma 7.2 to conclude that $\chi(\Pi) = \aleph_0 > 2C + 1$. Now, fix a finite $B \subset A$ satisfying the conclusion to Lemma 7.14.

For each $\{a, b\} \in \Pi_B$, choose $e_{\{a,b\}} \in E$ so that $e_{\{a,b\}}$ is either $a - b$ or $b - a$. Let $P = \{e_{\{a,b\}} : \{a, b\} \in \Pi_B\}$. Then $|P| = |\Pi_B|$. Applying Pisier's criterion, fix $Q \subseteq P$ such that $|Q| \geq |P|/C$ and Q is quasi-independent. Let Ψ be the subgraph of Π_B such that $Q = \{e_{\{a,b\}} : \{a, b\} \in \Psi\}$. Then Ψ is a minimal spanning graph for Q, so that Ψ contains no cycles by Lemma 7.12. On the other hand, $|\Psi| = |Q| \geq |P|/C = |\Pi_B|/C$, so that Ψ contains a cycle by Lemma 7.14. This contradiction proves the theorem. $\square$

References

[1] A. V. Arkhangel'skii, *Topological Function Spaces* (Mathematics and its applications (Soviet Series) ; v. 78), Kluwer, 1992.

[2] J. R. Blum, B. Eisenberg, and L. S. Hahn, Ergodic theory and the measure of sets in the Bohr group, *Acta Sci. Math. (Szeged)* 34 (1973) 17-24.

[3] R. E. Edwards and G. I. Gaudry, *Littlewood-Paley and Multiplier Theory* (Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 90) Springer-Verlag, 1977.

[4] G. B. Folland, *A Course in Abstract Harmonic Analysis*, CRC Press, 1995.

[5] L. Gillman and M. Jerison, *Rings of Continuous Functions*, Springer-Verlag, 1976.

[6] P. R. Halmos, *Measure Theory*, D. Van Nostrand Company, 1950.

[7] J. E. Hart and K. Kunen, Bohr topologies of discrete structures, *to appear.*

[8] K. P. Hart and J. van Mill, Discrete sets and the maximal totally bounded group topology, *J. Pure Appl. Alg.* 70 (1991) 73-80.

[9] S. Hartman and C. Ryll-Nardzewski, Almost periodic extensions of functions I, *Colloq. Math.* 12 (1964) 23-29.

[10] E. Hewitt and K. A. Ross, *Abstract Harmonic Analysis*, Volume I, Springer-Verlag, 1963.

[11] J.-P. Kahane, *Séries de Fourier absolument convergentes*, Springer-Verlag, 1970.

[12] I. Kaplansky, *Infinite Abelian Groups*, University of Michigan Press, 1969.

[13] W. J. LeVeque, *Topics in Number Theory*, Volume I, Addison-Wesley, 1956.

[14] W. J. LeVeque, *Topics in Number Theory*, Volume II, Addison-Wesley, 1956.

[15] J. M. Lopez and K. A. Ross, *Sidon Sets*, M. Dekker, 1975.

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

[17] L. T. Ramsey, A theorem of C. Ryll-Nardzewski and metrizable L.C.A. groups, *Proc. Amer. Math. Soc.* 78 (1980) 221-224.

[18] L. T. Ramsey, Bohr cluster points of Sidon sets, *Colloq. Math.* 68 (1995) 285-290.

[19] W. Rudin, Trigonometric series with gaps, *J. Mathematics and Mechanics* 9 (1960) 203-227.

[20] W. Rudin, *Fourier Analysis on Groups*, Interscience Publishers, 1962.

[21] C. Ryll-Nardzewski, Concerning almost periodic extensions of functions, *Colloq. Math.* 12 (1964) 235-237.

[22] H. Weyl, Über die Gleichverteilung von Zahlen mod. Eins, *Math. Annalen* 77 (1916) 313-352.