Pacific Journal of Mathematics

PLANAR SIDONICITY AND QUASI-INDEPENDENCE FOR MULTIPLICATIVE SUBGROUPS OF THE ROOTS OF UNITY

L. THOMAS RAMSEY AND COLIN C. GRAHAM

Volume 225 No. 2 June 2006

PACIFIC JOURNAL OF MATHEMATICS
Vol. 225, No. 2, 2006

PLANAR SIDONICITY AND QUASI-INDEPENDENCE FOR MULTIPLICATIVE SUBGROUPS OF THE ROOTS OF UNITY

L. THOMAS RAMSEY AND COLIN C. GRAHAM

We study Sidon and quasi-independence properties (in the discrete complex plane $\mathscr{C}$) for subsets of the roots of unity. We obtain criteria for sets of roots of unity to be quasi-independent and to be Sidon in $\mathscr{C}$.

For any set of positive primes, P, let W be the be multiplicative subset of $\mathscr{Z}$ generated by P. Then $E = \{e^{i2\pi a/m} : a \in \mathscr{Z}$ and $m \in W\}$ is a finite union of independent sets (and therefore a Sidon subset) of the additive group of complex numbers if and only if $\sum_{p\in P} 1/p < \infty$.

More generally, $S \subset e^{2\pi i \mathbb{Q}}$ is a Sidon set if and only if its intersections with cosets of certain (multiplicative) subgroups, those with square-free order, satisfy a (quasi-independence related) criterion of Pisier.

Certain new aspects of the combinatorial geometry of the integer-coordinate points in n-dimensional Euclidean space are shown to be equivalent to quasi-independence for subsets of the roots of unity. These aspects are fully resolved in two-dimensional Euclidean space but lead to combinatorial explosion in three dimensions.

Overview

A subset B of a discrete abelian group G is a *Sidon set* set if and only if every bounded complex-valued function on B is the restriction to B of the Fourier–Stieltjes transform of a bounded Borel measure on the dual group of G. A subset B of a locally compact abelian group G is a Sidon set if and only if B is a Sidon set when G is given the discrete topology. A subset B of an (additively-written) abelian group G is said to be *quasi-independent* if, given $k \geq 1$ and $x_j \in B$, $\epsilon_j = 0, \pm 1$ for $1 \leq j \leq k$, we have

$$\sum_j \epsilon_j x_j = 0 \implies \epsilon_j = 0 \text{ for } 1 \leq j \leq k.$$

The set B is *independent* if the same implication holds for $\epsilon_j \in \mathbb{Z}$ for $1 \leq j \leq k$.

MSC2000: primary 42A16, 43A46; secondary 11A25, 11B99, 11Lxx.

Keywords: independent sets in discrete groups, Sidon sets, quasi-independent sets.

Some of this work was done while Graham was at Lakehead University. He was and is supported by NSERC grants.

For independence in divisible groups such as $\mathbb{C}$, it is equivalent to substitute "$\epsilon_j \in \mathbb{Q}$" for "$\epsilon_j \in \mathbb{Z}$".

The motivation of this paper is the question: *Which subsets of $e^{2\pi i \mathbb{Q}}$, the set of all roots of unity, are Sidon subsets of the complex plane $\mathbb{C}$ and which are quasi-independent?*

Varopoulos [1970] shows that for quasi-all differentiable functions $f : [0, 1] \to \mathbb{R}$, the graph of f in $\mathbb{R}^2$ is a Sidon set — in fact, a finite union of two independent sets. (This result was simplified and extended in [Stegeman 1971].) The quasi-all result of Varopoulos does not tell us if any particular function, such as $f(t) = (t, \sqrt{1-t^2})$, has as its image a finite union of independent sets, unless f is a polynomial, in which case the graph is not Sidon [Varopoulos 1970, Theorems 3 and 3′]. (These last results also suggest that the unit circle is not a Sidon subset of the discrete plane, but this case lies outside our scope here.)

Quasi-independent sets have been important in the study of Sidon sets since the work of Stečkin [1956] and Rider [1966]. Of particular importance is the *criterion of Pisier* [1983] (see also [Bourgain 1985]): a subset A of a discrete abelian group G is a Sidon set if and only if there is some positive integer k such that, for every finite subset $F \subset A$, there is some quasi-independent $E \subset F$ such that $\#E \geq \#F/k$. Hadamard sets are those sequences $\Lambda = \{\lambda_j : 1 \leq j\}$ in $\mathbb{R}$ with $\lambda_{j+1}/\lambda_j \geq \alpha > 1$; they are quasi-independent when $\alpha \geq 2$. We give new examples of quasi-independent sets in $\mathbb{C} = \mathbb{R}^2$.

One should not conclude from Pisier's result that A is a union of k quasi-independent sets: Grow and Whicher [1984] give an example that satisfies the Pisier condition for $k = 2$ but is not the union of two quasi-independent sets.

Throughout this paper n will denote a positive integer and T_n the set of n-th roots of unity. When we use the terms "quasi-independent" or "independent," we shall mean as subsets of the *additive group* $\mathbb{C}$ of complex numbers. We warn the reader that we shall be interested in the additive group $\mathbb{C}$ and the *multiplicative group* $\mathbb{T}$, the set of complex numbers of absolute value one and a closed sub*set* of $\mathbb{C}$. The interplay between those two multiplications is the source of the problems addressed here.

For consistency with the literature on finite abelian groups we shall often use additive notation for the finite subgroups of $\mathbb{T}$ which we study here! Thus, the group T_n of n-th roots of unity with multiplication is identified with $Z_n = \mathbb{Z}/n\mathbb{Z}$ with addition mod n. Hence, when we speak of a "coset" of the group T_n of n-th roots of unity, we mean a set of the form rT_n, where $r \in e^{2\pi i \mathbb{Q}}$.

A number of our results hold for both the class of independent sets and for the class of quasi-independent sets. We show this by writing *(quasi-)independent, (quasi-)independence*, and *(quasi)relation* (defined below) in the affected statements and proofs.

Statement of results. We prove Sidonicity for relatively small subsets of $e^{2\pi i\mathbb{Q}}$:

Theorem 1.4. *For any set of positive primes P, let W be the be multiplicative subset of $\mathbb{Z}$ generated by P. Then*

$$E = \{e^{i2\pi a/m} : a \in \mathbb{Z} \text{ and } m \in W\}$$

is a finite union of independent sets if and only if $\sum_{p\in P} 1/p < \infty$, in which case

$$M = \left\lceil \prod_{p\in P} \frac{p}{p-1} \right\rceil$$

independent sets will suffice (and no fewer) and E is Sidon in $\mathbb{C}$.

(For s real, $\lceil s\rceil$ denotes the smallest integer $k \geq s$.)

A maximal independent subset of T_n has cardinality equal to Euler's $\phi(n)$ (see Proposition 1.2), and this fact is essential to the proof of the theorem. Since $e^{2\pi i\mathbb{Q}}$ is not a finite union of independent sets (because $\sum_{p \text{ prime}} 1/p = \infty$; see for instance [Hardy and Wright 1960]), more than independent sets in $e^{2\pi i\mathbb{Q}}$ need to be studied and that leads to consideration of quasi-independent sets. We begin by showing that Pisier's criterion can be weakened as applied to sets of roots of unity by allowing one to test fewer finite sets for the proportionality property.

Theorem 3.1. *A subset A of $e^{2\pi i\mathbb{Q}}$ is Sidon in $\mathbb{C}$ if and only if there is an integer k such that, for every positive, square-free, integer $n > 1$, for every coset U of T_n in $e^{2\pi i\mathbb{Q}}$ (coset with respect to complex multiplication), and for every finite $F \subset (A \cap U)$, there is some quasi-independent set $E \subset F$ such that $\#E \geq \#F/k$.*

We then turn to the computation, for some integers n, of the size $\Psi(n)$ of a largest quasi-independent subset of T_n and to develop tools for that purpose.

First, using Proposition 1.2 and Corollary 2.2, we have $\phi(n) \leq \Psi(n) < n$. Now, $\inf_n \Psi(n)/n > 0$ suggests that $e^{2\pi i\mathbb{Q}}$ is Sidon, $\sup_n \Psi(n)/\phi(n) < \infty$ would prove that $e^{2\pi i\mathbb{Q}}$ is not Sidon, and we obtain some evidence pertinent to the second inequality: $\Psi(n) \geq \phi(n)+4$ if n has three (or more) distinct odd prime factors. (It is also the case that $\Psi(n) \geq \phi(n)+5$ if n has at least three distinct odd prime factors and 5 is not one of them; see [Ramsey and Graham 2006, Corollary 4.3.2(3)].)

The best exact information we have about Ψ is in the next three theorems.

Theorem 4.1. *Let $n \geq 2$ be an integer.*

(1) *If a prime p divides n, then $\Psi(pn) = p\Psi(n)$.*

(2) *If p is prime and $k \geq 1$, then $\Psi(p^k) = \phi(p^k) = p^{k-1}(p-1)$.*

(3) *If n is odd, then $\Psi(2n) = \Psi(n)$.*

(4) *Let p be a prime that does not divide n. Then $\Psi(pn) \geq (p-1)\Psi(n)$.*

Thus, Ψ is much like Euler's ϕ function, and calculations of $\Psi(n)$ reduce to the case of square-free, odd integers n.

The case where n has only two prime factors is simple, and that of $n = 15p$ only slightly more complex:

Theorem 6.3. *If the positive integer n has exactly two distinct, positive prime factors, then $\Psi(n) = \phi(n)$.*

Theorem 7.4. *If $n = 15p$, where $p \geq 7$ is a prime, then $\Psi(n) = \phi(n) + 4$.*

We know an example of a 52-element quasi-independent subset of T_{105} (Example 7.3). The upper bound for $\Psi(105)$ is established in Lemma 7.2; the example of a 52-element quasi-independent set was verified by computer calculation, after some technical simplifications, using in particular the permutation theorem of [Ramsey and Graham 2006]. This example is essential in establishing several inequalities that show $\Psi(n) > \phi(n)$ (with varying degrees of precision). The general question of the size of $\Psi(n)$ thus remains open (this is where the combinatorial explosion of the abstract occurs).

For many of our results, it is sufficient to consider the case of square-free n. Given an integer n, we denote by $\tilde{n}$ the product of the prime factors of n.

Theorem 2.12 (Square-free theorem). *A set $E \subset T_n$ is (quasi-)independent if and only if the intersection of E with each coset of $T_{\tilde{n}}$ is (quasi-)independent.*

As an immediate consequence:

Corollary. *A subset A of $e^{2\pi i \mathbb{Q}}$ is (quasi-)independent if and only if, for every positive square-free integer $n > 1$, the intersection of A with every coset of T_n in $e^{2\pi i \mathbb{Q}}$ is (quasi-)independent.*

A rephrasing of the square-free theorem is this: *Every relation for T_n is a sum of characteristic functions of cosets of nontrivial subgroups of $Z_{\tilde{n}}$, where $\tilde{n}$ is the square-free part of n.*

Permutations of sets of roots of unity that preserve the (quasi-)independent sets and "extensions" of (quasi-)independent sets by increasing the prime factors of n are studied in [Ramsey and Graham 2006], where some of the estimates here are given modest improvement.

Organization of this paper. Section 1 establishes notation and gives the computation of the maximal size of an independent subset of T_n, as well as the proof of Theorem 1.4.

In Section 2 we go over the construction of bases in the set of relations and the proof of Theorem 2.12.

The proof of Theorem 3.1 is given in Section 3, after some technical results needed for this theorem and later ones.

Section 4 is devoted to the arithmetic properties of $\Psi(n)$, and includes the proof of Theorem 4.1.

In Section 6 we consider products $n = pq$ of two distinct odd primes, and prove Theorem 6.3.

The case of Z_{105} is of particular interest. It is discussed in Section 7, along with related results. This section also contains the proof of Theorem 7.4. An Appendix discusses the computer-aided methods employed to investigate this and larger cases.

1. Preliminaries

Notation. The prime factorization of an integer $n \geq 2$ will be written

$$n = \prod_{j=1}^{K} p_j^{n_j}, \tag{1–1}$$

for K distinct, positive primes p_j, and integers $1 \leq n_j$. Let D denote $\{1, \dots, K\}$.

Let Z_n denote the cyclic group of order n, given by $\{0, \dots, n-1\}$ with addition mod n. Z_n is isomorphic to T_n under the mapping

$$\omega(k) = e^{2\pi ik/n}. \tag{1–2}$$

Z_n is also isomorphic to the product group,

$$\prod_{j \in D} Z_{p_j^n j} \tag{1–3}$$

We shall abuse notation and think of Z_n as if it were the product group (1–3) whenever convenient.

The isomorphism between Z_n and the product group is

$$\tau : \prod_{j \in D} Z_{p_j^n j} \to Z_n \quad \text{with } \tau(x_1, \dots, x_K) = \sum_{j \in D} x_j m_j, \tag{1–4}$$

where $m_j = n/(p_j^{n_j})$. Under this isomorphism, let h_j denote the j-th component of $h \in Z_n$:

$$h_j = P_j(\tau^{-1}(h)),$$

where P_j is the projection onto the j-th coordinate in (1–3).

We shall write

$$\tilde{n} = \prod_{j=1}^{K} p_j.$$

We shall say, abusing notation, that a subset $E \subset Z_n$ is *(quasi-)independent* if $\omega(E)$ is (quasi-)independent in $\mathbb{C}$. This is equivalent to E not supporting any nonzero function f in the kernel of ψ defined below (with the range of f a subset of $\{0, \pm 1\}$ for quasi-independence). We shall also abuse notation in using the same symbol H for both the factor subgroup H of $Z_n = H \times L$ and the subgroup $H \times \{0\}$. Here we have conflated, as we warned, the cyclic group with its product group representation (1–3).

$\mathbb{Q}[Z_n]$ denotes the vector space over $\mathbb{Q}$ which consists of functions $f : Z_n \to \mathbb{Q}$, under pointwise operations. Define $\psi : \mathbb{Q}[Z_n] \to \mathbb{C}$ by

$$\psi(f) = \sum_{j \in Z_n} f(j) e^{2\pi i j/n} = \sum_{j \in Z_n} f(j)\omega(j). \tag{1–5}$$

Note that ψ is a linear map whose range is the $\mathbb{Q}$-linear span of T_n in $\mathbb{C}$. The dimension of this range is $\phi(n)$ by Proposition 1.2 below. Thus the dimension of the kernel of ψ equals $n - \phi(n)$. Note that f in the kernel of ψ correspond one-to-one to relations (with coefficients in $\mathbb{Q}$) among the elements of T_n. A key technical step of this paper is the description of a basis for this kernel in Corollary 2.7.

Definition 1.1. An *N-relation* on Z_n is an integer-valued function $f \in \ker \psi$ with range in $[-N, N]$. A *relation* is an element of the union of the sets of N-relations, $1 \le N < \infty$.

We denote the set of N-relations supported on a set E by $R_N(E)$. The set of all relations supported on E is be denoted by $R_\infty(E)$. Let

$$\beta(E) = -1 + \inf\{N : R_N(E) \neq \{0\}\}. \tag{1–6}$$

Another way to say this: if f is a relation supported on E, and $\beta(E) = N$, then the range of f is not contained in $[-N, N]$. Thus, if $\beta(E) \ge 1$, then E is quasi-independent; if $\beta(E) \ge 2$, then E is dissociate (see [Graham and McGehee 1979, p.159ff]); and if $\beta(E) = \infty$, then E is independent. A *quasirelation* is a 1-relation. Thus, a set E is quasi-independent if and only if it does not support a nonzero quasirelation.

The size of a maximal independent subset in T_n is $\phi(n)$. This comes from classical algebra. For more details than we give here, see [Lang 1965].

Proposition 1.2. *The maximum size of a fully independent set in T_n (for any $n \ge 2$) is exactly Euler's $\phi(n)$. Furthermore, the set $\{e^{2\pi i k/n} : 0 \le k < \phi(n)\}$ is independent in $\mathbb{C}$.*

Proof. Let $\mathbb{Q}[Z_n]$ be the subset of the complex numbers that is generated by T_n as a vector space over $\mathbb{Q}$. The dimension of this subspace is $\phi(n)$, which is the same as the degree of the irreducible polynomial over $\mathbb{Q}$ for primitive n-th roots of unity. If $E \subset T_n$ has more than $\phi(n)$ elements, some nontrivial linear relation holds: $\sum_{x\in E} a_x x = 0$, with $a_x \in \mathbb{Q}$. Of course, we can rewrite this as $\sum_{x\in E} b_x x = 0$, with $b_x \in \mathbb{Z}$, which shows the nonindependence of E. The assertion about the set $\{e^{2\pi ik/n} : 0 \le k < \phi(n)\}$ is [Lang 1965, p. 204, Theorem 6]. □

Corollary 1.3. *The set of relations on Z_n has dimension $n - \phi(n)$.*

Proof. The dimension of the range of ψ is $\phi(n)$, so the dimension of the kernel is $n - \phi(n)$. Since $f \in \mathbb{Q}[Z_n]$ is a relation if and only if $\psi(f) = 0$, the conclusion follows. □

Theorem 1.4. *For any set of positive primes P, let W be the be multiplicative subset of $\mathbb{Z}$ generated by P. Then*

$$E = \{e^{i2\pi a/m} : a \in \mathbb{Z} \text{ and } m \in W\}$$

is a finite union of independent sets if and only if $\sum_{p\in P} 1/p < \infty$, in which case

$$M = \left\lceil \prod_{p\in P} \frac{p}{p-1} \right\rceil$$

independent sets will suffice (and no fewer) and E is Sidon in $\mathbb{C}$.

Proof. For $n \ge 2$ and $M(n) = \lceil n/\phi(n) \rceil$, let

$$(1\text{–}7)\qquad A_j(n) = \begin{cases} \{e^{2\pi im/n} : j\phi(n) \le m < (j+1)\phi(n)\} & \text{if } 1 \le j < M(n), \\ T_n \setminus \bigcup_{\ell=1}^{M(n)-1} A_\ell & \text{if } j = M(n). \end{cases}$$

Lemma 1.5. *T_n is the union of $M(n) = \lceil n/\phi(n) \rceil$ independent sets, for $n \ge 2$.*

Proof. Indeed if $F \subset \mathbb{T}$ is independent in $\mathbb{C}$ and $z \in \mathbb{T}$, then $z\,F$, the set of products of elements of F with z, is also independent. We apply that successively to see that $A_j(n) \subseteq e^{2\pi\phi(n)/n} A_{j-1}(n)$ is independent for $1 \le j \le M(n)$, using Proposition 1.2 to give the independence of $A_1(n)$. □

Remark 1.6. It is clear from the proof of Lemma 1.5 and Proposition 1.2 that fewer than $M(n)$ independent sets can not cover T_n.

Continuing with the proof of the theorem, set $P = \{p_1, \dots, p_n, \dots\}$ and $r_n = (p_1 \cdots p_n)^n$, where $1 \le n < \infty$.

Suppose $\sum_j 1/p_j < \infty$. Then

$$M = \left\lceil \prod_{j=1}^{\infty} \Bigl(1 + \frac{1}{p_j - 1}\Bigr) \right\rceil < \infty,$$

so $M(r_n) \le M$ for all n. Then for each $1 \le n$, T_{r_n} is the union of at most M independent sets, by the lemma above, while $E = \bigcup_n T_{r_n}$.

Let $x_1, \dots,$ be an enumeration of E. For n large enough, $x_1 \in T_{r_n}$. By Lemma 1.5, the $M(r_n)$ subsets $A_j(r_n)$ cover T_{r_n}. Thus $x_1 \in A_j(r_n)$ for some $j(1,n) \le M(r_n) \le M$. By passing to a subsequence $n_{(1,s)}$ we may assume that the sequence $s \mapsto j(1, n_{(1,s)})$ is constant. Inductively, for every integer $\ell > 1$, we choose a subsequence $n_{(\ell,s)}$ of $n_{(\ell-1,s)}$ so that $s \mapsto j(\ell, n_{(\ell,s)})$ is constant and

$$x_\ell \in A_{j(\ell,n_{(\ell,s)})}(r_{n_{(\ell,s)}}).$$

Then, for each ℓ the diagonal sequence $j(\ell, n_{(s,s)})$ is constant for $s \ge \ell$, and $x_\ell \in A_{j(\ell,n_{(s,s)})}(r_{n_{(s,s)}})$ for all sufficiently large s.

For each $1 \le j \le M$ let $A_j = \lim_{S\to\infty} \bigcap_{s=S}^{\infty} A_j(r_{n(s,s)})$. We claim that the A_j are nonempty, independent, pairwise disjoint, and cover E. Independence follows because each $A_j(r_{n(s,s)})$ is independent (the empty set is trivially "independent"). The pairwise disjointness follows because the $A_j(n)$ are pairwise disjoint. Let $x = x_\ell \in E$. Since $x_\ell \in A_{j(\ell,n_{(s,s)})}(r_{n_{(s,s)}})$ for all sufficiently large s, we have $x_\ell \in \bigcup A_j$ and the A_j cover E. Since fewer than M independent sets cannot cover E (by Remark 1.6), M independent sets are required, and all the A_j must be nonempty.

Since a union of M independent sets is Sidon, E is Sidon.

If $\sum_j 1/p_j = \infty$, then $r_n/\phi(r_n) = \prod_1^n p_j/(p_j - 1) \to \infty$, so the number of independent sets needed to cover T_{r_n} grows without bound. □

With more elaborate calculations, one can prove results such as this:

Proposition 1.7 [Ramsey and Graham 2006, Prop. 2.1.8]. *Suppose that $n \ge 2$ is any integer. Let p_1 be the smallest prime factor of n, and p_2 be the second smallest prime factor of n (if it exists).*

(1) *If $E \subset Z_n$ and $\#E < p_1$, then E is independent.*

(2) *If $E \subset Z_n$ has cardinality p_1, then E is (quasi-)independent if and only if E is a not coset of Z_{p_1}.*

(3) *If $E \subset Z_n$, n is odd and square-free, and $\#E < p_1 + p_2 - 2$, then E is (quasi-) independent if and only if E does not contain a coset.*

(4) $(Z_{p_1} \cup Z_{p_2})\backslash\{0\}$ *is not quasi-independent, and has cardinality $p_1 + p_2 - 2$.*

2. Bases, relations, and nonindependent sets

We describe bases for the relations that describe the non-(quasi-)independent sets. The underlying ideas are most easily understood if one keeps in mind the special cases of $n = 9$, $n = 3 \cdot 5$ and $n = 9 \cdot 5$. These bases are useful, because they provide a way to work with (quasi)relations without being directly concerned with the mapping ψ, and to move our discussion to the product group homomorph (1–3) for T_n.

Z_n itself will be used to index a basis for $\mathbb{Q}[Z_n]$, a subset of which will be a basis for the kernel of ψ. In fact, a basis $\mathcal{B}'$ of the kernel of ψ will be shown to consist of the characteristic functions of $Z_{\tilde{n}}$ and of all cosets (in Z_n) of nontrivial (i.e., not $\{0\}$) subgroups of $Z_{\tilde{n}}$. To establish that $\mathcal{B}'$ is indeed such a basis, we will need to find an enumeration of a basis of $\mathbb{Q}[Z_n]$.

First, some natural members of the kernel will be described.

Lemma 2.1. *Let G be a nonzero subgroup of Z_n. If U is a coset of G in Z_n (with respect to addition mod n), then χ_U is in the kernel of ψ.*

Proof. Because Z_n is a cyclic group, so is G. One has $G = \{km : 0 \le k < \#G\}$, where $m = n/\#G$. It follows that $\omega(m) = e^{2\pi i(n/\#G)/n} = e^{2\pi i/\#G}$ is a primitive $\#G$-th root of unity and that $\omega(G) = T_{\#G}$. Because $\#G > 1$, $\psi(\chi_G) = \sum_{g\in G}\omega(g) = \sum_{\nu\in T_{\#G}} \nu = 0$. Consider now $U = t + G$ for some $t \in Z_n$. Then

$$\begin{aligned}\psi(\chi_U) &= \sum_{v\in U}\omega(v) = \sum_{g\in G}\omega(t+g) = \sum_{g\in G}\omega(t)\omega(g)\\ &= \omega(t)\sum_{g\in G}\omega(g) = \omega(t)\cdot 0 = 0.\end{aligned}$$ □

Lemma 2.1 is an exhaustive description of the kernel of ψ because it describes the form of the functions in the promised basis.

Corollary 2.2. *If $n \ge 2$, then $\Psi(n) < n$. If $n \ge 2$ is prime, then $\Psi(n) = n-1$.*

Proof. Let $G = Z_n$ in Lemma 2.1; χ_G is in the kernel of ψ and the coefficients of $\psi(\chi_G)$ are all $+1$; hence Z_n is not quasi-independent and $\Psi(n) < n$. The second statement follows from Proposition 1.2. □

For the promised enumeration, some further notation is needed. For $j \in D$ and the previously specified prime factor p_j as in (1–1), let H_j denote the subgroup of Z_n of order p_j:

$$H_j = \{ks_j : 0 \le k < p_j\}, \tag{2–1}$$

where $s_j = n/p_j$. Note that $\tau^{-1}(H_j)$ equals $\{kp_j^{n_j-1} : 0 \le k < p_j\} \times \prod_{t\in(D\setminus\{j\})}\{0\}$. For any h in Z_n, let

$$S_h = \{j \in D : h_j \ge p_j^{n_j-1}\}, \text{ and } G_h = \sum_{t\in(D\setminus S_h)} H_t.$$

Because P_t is the projection onto the t-th factor in (1–3),

$$\tau^{-1}(G_h) = \Bigl(\prod_{t\in(D\setminus S_h)} P_t(\tau^{-1}(H_t))\Bigr) \times \Bigl(\prod_{t\in S_h}\{0\}\Bigr).$$

Finally, let $E_h = h + G_h$ and $r(h) = \#D - \#S_h$. One can think of $r(h)$ as the dimension of the subgroup G_h and, by translation, the dimension of E_h. We will show that

$$\mathcal{B} = \{\chi_{E_h} : h \in Z_n\} \tag{2–2}$$

is a basis for $\mathbb{Q}[Z_n]$ (Corollary 2.6) and that

$$\mathcal{B}' = \{\chi_{E_h} : h \in Z_n \text{ and } r(h) > 0\} \tag{2–3}$$

is a basis for the kernel of ψ (Corollary 2.7). That $\mathcal{B}'$ does indeed consist of the characteristic functions of the cosets claimed earlier is easily shown, since the sets E_h are cosets of nontrivial subgroups of $Z_{\tilde{n}}$. The indexing will be shown to ensure uniqueness, and the cosets $E_h \in \mathcal{B}\backslash\mathcal{B}'$, that is, those with $r(h) = 0$, are just singletons, with enough of them (as we shall show) to complete a basis of $\mathbb{Q}[Z_n]$.

Lemma 2.3. *If $r(h) \geq r(g)$ and $h \neq g$, then $h \in (E_h \backslash E_g)$.*

Proof. Because G_h is a subgroup of Z_n, it is trivially true that $h \in E_h$. What remains to be shown is that $h \notin E_g$. Since $r(h) \geq r(g)$, one has $\#S_g \geq \#S_h$. Suppose first that there is some $j \in (S_g \backslash S_h)$. By the definition of S_g, $g_j \geq p_j^{n_j-1}$. Since every element w of G_g has $w_j = 0$, we have $(g + w)_j \geq p_j^{n_j-1}$ for all $w \in G_g$. Because $E_g = g + G_g$, then every $v \in E_g$ has $v_j \geq p_j^{n_j-1}$. However, $h_j < p_j^{n_j-1}$ since $j \notin S_h$. Thus h cannot be in E_g.

Second, suppose that $S_g \subset S_h$. Because $\#S_g \geq \#S_h$, one has $S_g = S_h$. It follows that $G_g = G_h$. Suppose $h \in E_g$. Then, for each $t \in S_h$, $g_t = h_t$ (since elements of G_h have zero in such coordinates). For each $t \in (D \backslash S_h)$, $h_t = g_t + w_t$ for some $w_t \in H_t$. However, both g_t and h_t are less that $p_t^{n_t-1}$. Recall that w_t is a multiple of $p_t^{n_t-1}$. It follows that $w_t = 0$. Thus $h_t = g_t$ for all $t \in D$, and hence $h = g$. This contradicts the hypotheses. □

Corollary 2.4. *The mapping $h \mapsto \chi_{E_h}$ is one-to-one.*

Proof. Clearly, for distinct members h and g of Z_n, $r(h) \geq r(g)$ or vice versa, and hence either $h \in (E_h \backslash E_g)$ or $g \in (E_g \backslash E_h)$. In either case, $\chi_{E_h} \neq \chi_{E_g}$. □

Lemma 2.5. *The elements of $\mathcal{B}$ are linearly independent over $\mathbb{Q}$.*

Proof. Consider any $\mathbb{Q}$-linear combination

$$f = \sum_{g \in Z_n} a_g \chi_{E_g}$$

of the elements of $\mathcal{B}$, and assume that $f = 0$. (Indexing $\mathcal{B}$ by $h \in Z_n$ is legal, because distinct h denote distinct elements of $\mathcal{B}$.) We claim that

$$f(h) = \sum_{\substack{g \in Z_n \\ r(g) > r(h)}} a_g \chi_{E_g(h)} + a_h. \tag{2–4}$$

Note that, for $h \in Z_n$,

$$\begin{aligned} f(h) = \sum_{g\in Z_n} a_g\chi_{E_g}(h) &= \sum_{\substack{g\in Z_n\\ r(g)>r(h)}} a_g\chi_{E_g}(h) + \sum_{\substack{g\in Z_n\\ r(g)\le r(h)}} a_g\chi_{E_g}(h) \\ &= \sum_{\substack{g\in Z_n\\ r(g)>r(h)}} a_g\chi_{E_g}(h) + \sum_{\substack{g\in Z_n\\ r(g)\le r(h)\\ g\neq h}} a_g\chi_{E_g}(h) + a_h\chi_{E_h}(h) \\ &= \sum_{\substack{g\in Z_n\\ r(g)>r(h)}} a_g\chi_{E_g}(h) + \sum_{\substack{g\in Z_n\\ r(g)\le r(h)\\ g\neq h}} a_g\cdot 0 + a_h\cdot 1 = \sum_{\substack{g\in Z_n\\ r(g)>r(h)}} a_g\chi_{E_g}(h) \;+\; a_h. \end{aligned}$$

When $r(h) = \#D$ (that is, the case when $S_h = \varnothing$), there is no g such that $r(g) > r(h)$ and (2–4) simplifies to the single term a_h as the value of $f(h)$. Since f is the 0 function, a_h vanishes in this case. Then we work by induction down from $\#D$. For an induction step, suppose there is an integer $k \in [0, \#D]$ such that $a_g = 0$ for g such that $r(g) \geq k$. This implies that

$$f = \sum_{\substack{g\in Z_n\\ r(g)<k}} a_g\chi_{E_g}.$$

Consider any h such that $r(h) = k - 1$. Then

$$f(h) = a_h + \sum_{\substack{g\in Z_n\\ r(g)>r(h)}} a_g\chi_{E_g}(h)$$

reduces to a single term a_h as the value of $f(h)$. Because $f(h) = 0$, we have $a_h = 0$ when $r(h) = k - 1$. This proves the induction step, and the principle of induction completes the proof. □

Corollary 2.6. *$\mathcal{B}$ is a basis for $\mathbb{Q}[Z_n]$.*

Proof. Because the mapping $h \mapsto \chi_{E_h}$ is one-to-one, $\#\mathcal{B} = \#Z_n = n$. Because n is the dimension of $\mathbb{Q}[Z_n]$, $\mathcal{B}$ is a basis for it. □

Corollary 2.7. *$\mathcal{B}'$ is a basis for the kernel of ψ.*

Proof. Since $\mathcal{B}'$ is linearly independent (as a subset of $\mathcal{B}$), we must check that $\mathcal{B}'$ is a subset of the kernel and that the cardinality of $\mathcal{B}'$ equals the dimension of the kernel. (This anticipates the rôle of $n - \phi(n)$, the dimension of the kernel of the mapping ψ.)

For the first point, note that $r(h) > 0$ implies that G_h is not the zero subgroup of Z_n. Since $E_h = h + G_h$ is a coset of G_h, Lemma 2.1 implies that χ_{E_h} is a element of the kernel of ψ.

For $\#\mathcal{B}'$, recall that χ_{E_h} is excluded from $\mathcal{B}'$ if and only if $r(h) = 0$. To have $r(h) = 0$, one must have $h_j \geq p_j^{n_j-1}$ in all coordinates j. The number of such h is $\prod_{j\in D}(p_j^{n_j} - p_j^{n_j-1}) = \prod_{j\in D} p^{n_j-1}(p_j - 1) = \phi(n)$. Therefore $\#\mathcal{B}' = n - \phi(n)$, exactly the dimension of the kernel of ψ. □

Lemma 2.8. *Let $n \geq 2$ have prime factorization $n = p_1^{n_1} \cdots p_K^{n_K}$. Fix $1 \leq j \leq K$ and $0 \leq \ell < p_j$. Let $m = n/p_j$. Then every relation supported on $Z_m + \ell$ is a linear combination of characteristic functions of cosets of nonzero subgroups of Z_m contained in $Z_m + \ell$.*

Proof. When $\ell = 0$, this is immediate from Corollary 2.7. For $\ell \neq 0$ this follows from the fact that translation in Z_n corresponds to a rotation in T_n, and that rotation preserves relations. □

Example 2.9. Let $p \neq q$ be odd primes and $n = pq$. The basis $\mathcal{B}'$ for the relations consists of the characteristic functions of the group Z_n and of the cosets $Z_p + (0, 1), \ldots, Z_p+(0, q-1)$, $Z_q+(1, 0), \ldots Z_q+(p-1, 0)$, where we have identified Z_p with $Z_p \times \{0\}$ and Z_q with $\{0\} \times Z_q$. Replacing the characteristic function of Z_n with that of Z_q yields another basis, one more useful in some situations. It consists of the characteristic functions of the following $p + q - 1$ sets:

(1) The p cosets of Z_q.

(2) The $(q - 1)$ nonzero cosets of Z_p.

Here is a more general version of the second basis of Example 2.9.

Lemma 2.10. *Let $n \geq 2$ have prime factorization $n = p_1^{n_1} \cdots p_K^{n_K}$. Suppose that $1 \leq s \leq K$ and that $n_s = 1$. Let $0 \leq \ell < p_s$, and write $Z_n = Z_{p_s} \times H$. Then the set of relations on Z_n has a basis consisting of*

(1) *the characteristic functions of cosets of Z_{p_s}, and*

(2) *characteristic functions of cosets of nonzero subgroups of H, each such coset being disjoint from $H + \ell$ and contained in $H + k$, $0 \leq k \neq \ell < p_s$.*

That is, each relation is a sum of "spikes", the characteristic functions of the cosets of Z_{p_s} and relations supported on cosets of H, with one coset of H being left out.

Proof. We induct on K, the number of prime factors of n. If $K = 1$, there is nothing to prove: the characteristic function of Z_{p_1} spans a space of dimension $1 = p_1 - \phi(p_1) = p_1 - (p_1 - 1)$.

Suppose the lemma is true when n has $1 \leq K$ prime factors. Let n have $K + 1$ distinct prime factors. By Lemma 2.8, for each coset $H + k$ in Z_n, $0 \leq k < p_s$, we can find a basis B_k for the relations supported on the coset and each such basis will have $m - \phi(m)$ elements, all supported on that coset of H. Consider any linear combination of characteristic functions of cosets of Z_{p_s} plus a linear combination of elements of $\bigcup_{k\neq\ell} B_k$. If that sum is zero, then it is zero on $H + \ell$.

That can happen only if the coefficients of all the spikes $\chi_{Z_{p_s}+h}$, $h \in H$, are zero. Because each B_k is supported on a distinct coset $H+k$, our sum is the 0 function on $H+k$ and expressible in terms of just B_k. By the independence of B_k, all the coefficients for that B_k part of our sum must be zero. Therefore, the union of the set of spikes with $\bigcup_{k \neq \ell} B_k$ is independent. Since $\#H + (p_s - 1)\#B_s = n/p_s + (p_s-1)((n/p_s) - \phi(n/p_s)) = n/p_s + n - n/p_s - \phi(n) = n - \phi(n)$, the union of the set of spikes with $\bigcup_{k \neq \ell} B_k$ is a basis. □

We can rephrase the conclusion of Lemma 2.10 as follows. Let n be given by (1–1), suppose $n_s = 1$, $1 \le s \le K$, $0 \le \ell < p_s$, and $m = n/p_s$. Then there is a basis for the kernel of ψ (for Z_n) that consists of

(2–5) the characteristic functions of all cosets of Z_{p_s}, and

(2–6) the characteristic functions of a set $\mathscr{L}$ of cosets of certain nonzero subgroups of $H = Z_m$ described below.

Each coset $L \in \mathscr{L}$ meets each coset of Z_{p_s} in at most one point, and, given any $0 \le t < p_s$, L is either contained in $t + H$ or is disjoint from it. Furthermore, each $L \in \mathscr{L}$ is disjoint from $H + \ell$.

The cosets of (2–5) meet each coset of $H = Z_m$ in at most one point.

Corollary 2.11 (Empty floor). *Let n, s, H be as in Lemma 2.10. Suppose that $E \subset Z_n$ is such that $E \cap H = \varnothing$. Then E is* (*quasi-*)*independent if and only if $E \cap (t + H)$ is* (*quasi-*)*independent for all* $1 \le t < p_s$.

Proof. One direction is easy: subsets of (quasi-)independent sets are always (quasi-) independent.

Let $m = n/p_s$ and let f be any (quasi)relation supported on E. We use the basis given in (2–5) and (2–6), with $\ell = 0$. Let $\mathscr{L}_j$ denote the cosets in $\mathscr{L}$ that are contained in $H + j$, $1 \le j < p_s$. Then for some rational numbers a_t and b_h,

$$f = \sum_{t \in Z_m} a_t \chi_{t+Z_{p_s}} + \sum_{\substack{1 \le j < p_s \\ L \in \mathscr{L}_j}} b_L \chi_L .$$

That follows from the properties of the basis.

Denote the value of f at $(t, w) \in H \times Z_{p_s} = Z_n$ by $f(t, w)$. Since $L \cap H = \varnothing$ for all $L \in \mathscr{L}_j$, $1 \le j < p_s$, $f(t, 0) = a_t$. But by the hypotheses $E \cap H = \varnothing$, $f(t, 0) = 0$ for all t: that is, $a_t = 0$ for all $t \in H$. Therefore

$$f = \sum_{\substack{1 \le j < p_s \\ L \in \mathscr{L}_j}} b_L \chi_L .$$

Fix $0 < u < p_s$. Because each $L \in \mathscr{L}_j$ meets only one coset of H, namely $j + H$,

$$\chi_{u+H}\, f = \sum_{\substack{1 \le j < p_s \\ L \in \mathscr{L}_j}} b_L \chi_{u+H}\, \chi_L = \sum_{L \in \mathscr{L}_u} b_L \chi_L,$$

is a (quasi)relation supported on $E \cap (u + H)$, which set is (quasi-)independent by the hypothesis. Therefore $\chi_{u+H} f = 0$ for $0 < u < p_s$; that is, $f = 0$. Hence E is (quasi-)independent. □

Theorem 2.12 (Square-free theorem). *A set $E \subset T_n$ is (quasi-)independent if and only if the intersection of E with each coset of $T_{\tilde{n}}$ is (quasi-)independent.*

Proof. If E is (quasi-)independent, so are all of its subsets, including the intersections of E with the cosets of $Z_{\tilde{n}}$.

On the other hand, suppose that all of the intersections of E with cosets of $Z_{\tilde{n}}$ are (quasi-)independent and that f is a (quasi-)relation supported on E. We must show that $f = 0$. We know that f is a sum of characteristic functions of cosets of nontrivial subgroups of $Z_{\tilde{n}}$, by Corollary 2.7. Let g be any such characteristic function. Let H be any coset of $Z_{\tilde{n}}$. Then either $\chi_H g = 0$ or $\chi_H g = g$. Thus, $\chi_H f$ is a sum of characteristic functions of cosets of nontrivial subgroups of $Z_{\tilde{n}}$ all of which are contained in H. Hence $\chi_H f$ is a (quasi-)relation supported on $E \cap H$. Since $E \cap H$ is assumed to be (quasi-)independent, $\chi_H f = 0$. Hence, $f = 0$. □

3. Characterization of Sidonicity

Theorem 3.1. *A subset A of $e^{2\pi i \mathbb{Q}}$ is Sidon in $\mathbb{C}$ if and only if there is an integer k such that, for every positive, square-free, integer $n > 1$, for every coset U of T_n in $e^{2\pi i \mathbb{Q}}$ (coset with respect to complex multiplication), and for every finite $F \subset (A \cap U)$, there is some quasi-independent set $E \subset F$ such that $\#E \ge \#F/k$.*

Lemma 3.2 (Quasi-independent sets partitioned by cosets). *Let p be a positive prime such that $p \mid n$. In Z_{np} let*

$$L_n = \{kp : 0 \le k < n\}.$$

The distinct cosets of L_n in Z_{np} are $t + L_n$, $0 \le t < p$. Suppose that $F_t \subset (t + L_n)$ is (quasi-)independent for $0 \le t < p$. Then $F = \bigcup_{t=0}^{p-1} F_t$ is (quasi-)independent.

Proof. Without loss of generality, assume that $p = p_1$ in the prime factorization of n. To prove the lemma for quasi-independent sets, consider any $f \in \mathbb{Q}[Z_{np}]$ such that $f(j) = 0$ for $j \notin F$, $f(j) \in \{0, \pm 1\}$ for all $j \in Z_{pn}$, and that f is in the kernel of ψ (defined by (1–5), with np in the role of n). To prove the lemma for independent sets, simply drop the restriction of the range of f to $\{0, \pm 1\}$. Let

$\mathcal{W} = \{h \in Z_{np} : r(h) > 0\}$. Then, for some choice of rational coefficients f_h,

$$f = \sum_{h \in \mathcal{W}} f_h \chi_{E_h}. \tag{3–1}$$

It will be proved next that each E_h in (3–1) is a subset of exactly one coset of L_n. This will follow immediately from the fact that E_h is a coset of G_h, once one proves that G_h is a subgroup of L_n. Let τ be given by (1–4). Let $V = \prod_{t \in (D \setminus \{1\})} Z_{p_t^{n_t}}$. Then $L_n = \tau(\{kp : 0 \le k < p_1^{n_1}\} \times V)$. Thus, if $h_1 \ge p_1^{n_1}$, then G_h is a subgroup of $\tau(\{0\} \times V)$ and hence of L_n. Likewise, if $h_1 < p_1^{n_1}$, there is a subgroup V' of V such that $G_h = \tau(V_1 \times V')$, where $V_1 = \{kp_1^{n_1} : 0 \le k < p\}$. Clearly V_1 is a subgroup of the first factor of $\tau^{-1}(L_n)$ and thus G_h is a subgroup of L_n.

Let $U = t + L_n$ for any $0 \le t < p$. For $h \in \mathcal{W}$, either $E_h \subset U$ or $E_h \cap U = \varnothing$. Thus $\chi_{E_h} \cdot \chi_U = \chi_{E_h}$ in the former case, while $\chi_{E_h} \cdot \chi_U = 0$ in the latter. It follows that $f \cdot \chi_U$ is in the kernel of ψ, because

$$f \cdot \chi_U = \sum_{\substack{h \in \mathcal{W} \\ E_h \subset U}} f_h \chi_{E_h}.$$

If f is supported on F, $f \cdot \chi_U$ is supported on $F \cap U = F_t$. Also, because $f(j) \in \{0, \pm 1\}$ for all $j \in Z_{pn}$, the same is true for $f \cdot \chi_U$. For any $h \in \mathcal{W}$ such that $E_h \subset U$, if one has $f_h \neq 0$ then $f \cdot \chi_U \neq 0$ (because the χ_{E_h}'s are linearly independent). Thus, if any such $f_h \neq 0$, F_t would not be quasi-independent. This proves that $f_h = 0$ for all h such that $E_h \subset U$. As U ranges over the cosets of L_n, this includes all $h \in \mathcal{W}$. □

Proof of Theorem 3.1. Let $A \subset e^{2\pi i \mathbb{Q}}$ satisfy the hypotheses of the theorem. Let F be any finite subset of A. Then there is some n such that $F \subset T_n$. Let the distinct prime factors of n be listed as $p_1, \ldots, p_K$ and let $D = \{1, \ldots K\}$. By hypothesis, there is some k (independent of $r = \tilde{n}$ and therefore n) such that, for any coset U of T_r, there is some (quasi-)independent $E_U \subset (F \cap U)$ such that $\#E_U \ge \#(F \cap U)/k$. If $n = r$, we are done. Otherwise, proceed by induction. Suppose that we have $r|m$, $m|n$, $p_j|(n/m)$, and the fact that, for any coset U of T_m in $e^{i2\pi\mathbb{Q}}$, there is some (quasi-)independent $E_U \subset (F \cap U)$ such that $\#E_U \ge \#(F \cap U)/k$. Consider any coset V of T_{mp_j}. Any such coset consists of p_j disjoint cosets U_t of T_m, each of which contains a (quasi-)independent E_t of the desired size. By Lemma 3.2, $\bigcup_t E_t$ is (quasi-)independent. Also, $\#\bigl(\bigcup_t E_t\bigr) \ge (1/k) \sum_t \#(F \cap U_t) = \#(F \cap V)/k$. Thus Pisier's Sidon condition with the same k is satisfied for subsets of F which are also subsets of cosets of T_{mp_j}. This argument can be extended by induction on the exponents of the factors p_j of $\tilde{n}$ to include subsets of F which are subsets of T_n. That includes F itself. □

4. Arithmetic properties of Ψ

Theorem 4.1. *Let $n \geq 2$ be an integer.*

(1) *If a prime p divides n, then $\Psi(pn) = p\Psi(n)$.*

(2) *If p is prime and $k \geq 1$, then $\Psi(p^k) = \phi(p^k) = p^{k-1}(p-1)$.*

(3) *If n is odd, then $\Psi(2n) = \Psi(n)$.*

(4) *Let p be a prime that does not divide n. Then $\Psi(pn) \geq (p-1)\Psi(n)$.*

Lemma 4.2. *Let $\rho : Z_n \to Z_{mn}$ be defined by $\rho(k) = km$. Let R_n denote the range of ρ. For any $t \in Z_{mn}$, a set $E \subset (t + R_n)$ is (quasi-)independent in Z_{mn} if and only if $\rho^{-1}(E - t)$ is (quasi-)independent in Z_n.*

Proof. Note that ρ is an isomorphism from Z_n to R_n. Let $t \in Z_{mn}$ and $E \subset (t+R_n)$. Let $\lambda : \mathbb{Q}[Z_{mn}] \to \mathbb{C}$ be the mapping

$$\lambda(f) = \sum_{j=0}^{mn-1} f(j)e^{2\pi ij/(mn)},$$

while ψ continues to label the corresponding mapping for $\mathbb{Q}[Z_n]$. Suppose that f is in the kernel of λ, and that $f(j) = 0$ for $j \notin E$. Then, since $E \subset (t + R_n)$,

$$\begin{aligned}\lambda(f) &= \sum_{j=0}^{mn-1} f(j)e^{2\pi ij/(mn)} = \sum_{j\in(t+R_n)} f(j)e^{2\pi ij/(mn)}\\ &= \sum_{0\leq k<n} f(t+km)e^{2\pi i(t+km)/(mn)}\\ &= e^{2\pi it/(mn)} \sum_{0\leq k<n} f(t+km)e^{2\pi i(km)/(mn)}\\ &= e^{2\pi it/(mn)} \sum_{0\leq k<n} g(k)e^{2\pi ik/n} = e^{2\pi it/(mn)} \cdot \psi(g),\end{aligned}$$

where $g(k) = f(t+km)$. Since $e^{2\pi it/(mn)} \neq 0$, it is clear that $\lambda(f) = 0$ if and only if $\psi(g) = 0$. It is now clear that E is (quasi-)independent if and only if $\rho^{-1}(E-t)$ is. □

Lemma 4.3. $\Psi(n) \leq \Psi(mn) \leq m\Psi(n)$.

Proof. Let ρ and R_n be defined as in Lemma 4.2. The m distinct cosets of R_n are $t + R_n$, $0 \leq t < m$. Let F be an arbitrary quasi-independent subset of Z_{mn}. Then each subset of F is also quasi-independent, in particular the sets $F_t = F \cap (t+R_n)$.

By Lemma 4.2, $E \subset (t+R_n)$ is quasi-independent in Z_{mn} if and only if $\rho^{-1}(E-t)$ is quasi-independent in Z_n. Since the mapping $x \mapsto \rho^{-1}(x-t)$ is a one-to-one correspondence between $t+R_n$ and Z_n, $\#F_t = \#(\rho^{-1}(F_t-t))$. Because $\rho^{-1}(F_t-t)$

is quasi-independent in Z_n, we have $\#F_t \leq \Psi(n)$. Because $F = \bigcup_{t=0}^{m-1} F_t$, we also have $\#F \leq m\Psi(n)$.

To prove that $\Psi(n) \leq \Psi(mn)$, let S be a quasi-independent subset of Z_n of size $\Psi(n)$. By Lemma 4.2, $\rho(S)$ is quasi-independent in Z_{mn}. Since $\#S = \#\rho(S)$, we have $\Psi(mn) \geq \#\rho(S) = \Psi(n)$. □

Proof of Theorem 4.1. (1) Let $E \subset Z_n$ be a quasi-independent set of maximum size. Let

$$E' = \bigcup\nolimits_1^p E + x_j,$$

where $\{Z_n + x_j\}$ is a maximal set of disjoint cosets of Z_n in Z_{np}. Then $\#E' = p\#E$. Because $(np)\tilde{} = \tilde{n}$, $E' \cap (Z_{\tilde{n}} + y)$ is quasi-independent for all $y \in Z_{np}$, since those intersections are just translates of quasi-independent sets in Z_n. The conclusion now follows from the Square-free Theorem 2.12 and Lemma 4.3.

(2) The assertion is immediate by induction from Theorem 4.1(1).

(3) By Lemma 4.3, one has $\Psi(2n) \geq \Psi(n)$. To see the reverse inequality, let $\rho : Z_n \to Z_{2n}$ be defined by $\rho(k) = 2k$, with range R_n. Then

$$Z_{2n} = \{0, n\} \oplus R_n. \tag{4–1}$$

Let $F \subset Z_{2n}$. Suppose that k and $k + n$ were in F. Then

$$e^{2\pi i(k+n)/(2n)} = e^{2\pi ik/(2n)} \cdot e^{\pi i} = -e^{2\pi ik/(2n)}.$$

Thus, with $f(j) = 0$ for $j \notin \{k, k+n\}$ while $f(k) = f(n+k) = 1$, one has

$$\psi(f) = e^{2\pi ik/(2n)} + e^{2\pi i(k+n)/(2n)} = e^{2\pi ik/(2n)} - e^{2\pi ik/(2n)} = 0.$$

Thus F wouldn't be quasi-independent.

Suppose that $\#F > \Psi(n)$. It will be proved that F is not quasi-independent. By the previous paragraph, one may suppose that F does not contain any pair $\{k, k+n\}$. Thus the elements of F must have distinct R_n coordinates in (4–1) above. Let E be the set of these coordinates. Since $\#E > \Psi(n)$, there is a quasi-independent relation f supported on E (Lemma 4.2, and the fact that ρ is one-to-one). Let $g \in \mathbb{Q}[Z_{2n}]$ be defined as follows: for $k \in \{0, n\}$ and $j \in R_n$,

$$g(k+j) = \begin{cases} 0 & \text{if } k+j \notin F, \\ f(j) & \text{if } j \in F \text{ and } k = 0, \\ -f(j) & \text{if } n+j \in F \text{ and } k = n. \end{cases}$$

Then

$$\begin{aligned}\psi(g) &= \sum_{w\in Z_{2n}} g(w)e^{2\pi i w/(2n)} = \sum_{j\in R_n}\sum_{k\in\{0,n\}} g(k+j)e^{2\pi i(j+k)/(2n)}\\ &= \sum_{j\in(E\cap F)} f(j)e^{2\pi i j/(2n)} + \sum_{j\in(E\cap(F-n))} (-f(j))e^{2\pi i(j+n)/(2n)}\\ &= \sum_{j\in E} f(j)e^{2\pi i j/(2n)} = \psi(f) = 0.\end{aligned}$$

Thus F supports a quasi-independent relation g, as desired.

(4) Let $m = pn$ and let $Z_m = Z_n \times Z_p$. For each nonzero coset of $t + Z_n$, $0 < t < p$, in Z_n, we choose a quasi-independent set $E_t \subset t + Z_n$ with $\#E_t = \Psi(n)$. We let $E = \bigcup_{0<t<p} E_t$. We claim that E is quasi-independent (that $\#E = (p-1)\Psi(n)$ is obvious).

Let $p_s = p$ in the ordering of the prime factors $p_1, \dots, p_K$ of m. Then it is apparent that E satisfies the hypotheses of Corollary 2.11 (Empty Floor), and hence is quasi-independent. □

5. Spikes and shadows

The results of this section are included for their intrinsic interest and because some are needed in the next two sections.

Suppose that n is square-free, that it factors as $n = r_1 \cdot r_2$, and that $G = H_1 \times H_2$, where H_j has order $r_j > 1$, $j = 1, 2$. A "spike" is a coset of H_2. If a set $E \subset A$ contains any spike, E is not quasi-independent. More interestingly, E can effectively contain a spike without actually doing so, as we now show.

Theorem 5.1. *Suppose that n is square-free, that n factors as $n = r_1 \cdot r_2$, and that $E \subset G = H_1 \times H_2$, where H_j has order $r_j > 1$, $j = 1, 2$. Suppose that, for some (fixed) $a \in H_1$, for each coset $H_1 \times \{c\}$, $c \in H_2$, at least one of the following happens*:

(5–1) $(a, c) \in E$; *or*

(5–2) $\{(a, c)\} \cup \big(E \cap (H_1 \times \{c\})\big)$ *is not quasi-independent.*

Then E is not quasi-independent.

Proof. Let $S = \{a\} \times H_2$. If $S \subset E$, we are done. So, suppose that $(a, c) \notin E$ for some c. If $E \cap (H_1 \times \{c\})$ is not quasi-independent, we are also done (E supports a nontrivial quasirelation because a subset of E does). So, when $(a, c) \notin E$, we may assume that $E \cap (H_1 \times \{c\})$ is quasi-independent. However, (5–2) requires that $B_c = \{(a, c)\} \cup [E \cap (H_1 \times \{c\})]$ would fail to be quasi-independent. Hence B_c is the support of a nontrivial quasirelation, f_c. If $f_c(a, c) = 0$, then f_c would be supported on just $E \cap (H_1 \times \{c\})$], which we have ruled out. So $f_c(a, c) = \pm 1$. By replacing f_c with $-f_c$, if necessary, we may assume that $f_c(a, c) = -1$.

Consider

$$h = \chi_S + \sum_{\substack{0 \le c < r_2 \\ (a,c) \notin E}} f_c. \tag{5–3}$$

Each term of h is a quasirelation and hence the sum is in the kernel of ψ (as defined for T_n).

We claim that h is a nontrivial quasirelation supported on E. Thus h is nonzero at some point of each coset of the form $H_1 \times \{c\}$. To see these things, let $0 \le c < r_2$. If $(a, c) \in E$, only χ_S among the terms defining h is nonzero on the coset $H_1 \times \{c\}$, and there χ_S is nonzero only at (a, c) and has the value 1. If, contrariwise, $(a, c) \notin E$, we have $\chi_S(a, c) = 1$ and $\chi_S = 0$ elsewhere in $H_1 \times \{c\}$, while f_c is supported on $\{(a, c)\} \cup [E \cap (H_1 \times \{c\})]$ and is -1 at (a, c). All other terms of h are 0 on this coset. So

$$h|_{H_1 \times \{c\}} = (\chi_S + f_c)|_{H_1 \times \{c\}}.$$

Note that $\chi_S + f_c$ vanishes at (a, c) and hence (within this coset) is supported on $E \cap (H_1 \times \{c\})$. Also, since a single point such as (a, c) cannot be the sole support of a nontrivial quasirelation, f_c is nonzero for at least one member of $E \cap (H_1 \times \{c\})$. Finally, since χ_S is nonzero only at (a, c) in this coset, adding χ_S to f_c changes f_c only at (a, c) (making the value of the sum there 0). Thus h on this coset continues to have range values among $\{0, \pm 1\}$, and has at least one nonzero value there. Hence, h is a nontrivial quasirelation supported on E. □

In the situation above, we shall say that E *shadows* the spike, $S = \{a\} \times H_2$. Theorem 5.1 has two generalizations, as follows.

Corollary 5.2. *Let $E \subset H_1 \times H_2$, and let S be any non-quasi-independent set that meets each coset of H_1 in exactly one point (a_c, c). Suppose that, for each coset $H_1 \times \{c\}$, $c \in H_2$, at least one of* (5–1) *and* (5–2) *holds with (a_c, c) in the rôle of (a, c). Then E is not quasi-independent.*

Sketch of proof. We adapt the proof of Theorem 5.1 as follows. The function χ_S is replaced by a quasirelation supported on S, and a weighted sum replaces (5–3), the weights being 0, ±1. □

Corollary 5.3. *Let $E \subset H_1 \times H_2$, and let the set S be any non-independent set that meets each coset of H_1 in exactly one point (a_c, c). Suppose that, for each coset $H_1 \times \{c\}$, $c \in H_2$, either* (5–1) *holds with (a_c, c) in the rôle of (a, c) or*

$$\{(a_c, c)\} \cup [E \cap (H_1 \times \{c\})] \textit{ is not independent} \tag{5–4}$$

holds. Then E is not independent.

Sketch of proof. We replace "quasi-independent" with "independent" in the proof of Theorem 5.1. The function χ_S in that proof is replaced by a relation R_F supported on S, and a weighted sum replaces (5–3). In this case, the weight for R_S is the least common multiple k of the (integer) values $|f_c(a_c, c)|$, and the weight for each f_c is given by $-k/f_c(a_c, c)$. □

Here is another application of Theorem 5.1: the sets constructed using Corollary 2.11 are maximal quasi-independent sets.

Corollary 5.4. *Let E, n, s, H be as in Corollary 2.11, but with $E \cap (t + H)$ maximally quasi-independent as a subset of $t + H$, for each $0 < t < p_s$. If $E \subsetneq F \subset Z_n$, then F is not quasi-independent.*

Proof. Suppose $0 < t < p_s$. If $F \cap (t + H) \neq E \cap (t + H)$, then $F \cap (t + H)$ is not quasi-independent, so F is not quasi-independent. Hence, we may assume that $F \cap H \neq \varnothing$. Let $x \in F \cap H \neq \varnothing$. Then it is easy to see that F shadows the spike $\{x\} \times Z_{p_s}$, so F is not quasi-independent by Theorem 5.1. □

We now develop more elaborate criteria for a set to be quasi-independent.

The general situation is that of Lemma 2.10: we suppose that $K \geq 2$ and $j \in \{1, \dots, K\}$. We let $m = n/p_j$.

We recall the notation $R_N(E)$ and $\beta(E)$ (see (1–6) and the paragraph preceding). We use $S_N(E)$ to denote the set of functions f on Z_n with support contained in E and integer range $[-N, N]$. Hence, $R_N(E) \subset S_N(E)$.

Theorem 5.5. *Suppose that $K \geq 2$, $j \in [1, \dots, K]$, and $n_j = 1$. Let $m = n/p_j$. For $s \in [0, \dots, p_j - 1]$, let J_s be the characteristic function of $Z_m + s$ (the s-th layer). Let $E \subset Z_n$. For $s \in \{0, \dots, p_j - 1\}$ let $E^{(s)} = E \cap (Z_m + s)$ and set $M = \inf\{\beta(E^{(s)}) : 1 \leq s \leq p_j - 1\}$. Then*

(1) $\beta(E) \leq M$.

Moreover, the following are equivalent:

(2) $\beta(E) < N \leq M$.

(3) *There is some nonzero $f : E^{(0)} \to [-N, \dots, N]$ such that*

$$(J_s g + R_\infty(Z_m + s)) \cap S_N(E^{(s)}) \neq \varnothing \quad \textit{for each } 1 \leq s \leq p_j - 1,$$

where

$$g = \sum_{y \in E^{(0)}} f(y) \chi_{Z_{p_j} + y}.$$

Remarks 5.6. (i) The relations in (3) provide the recipe for construction of a nontrivial N-relation on E. This is essentially linear algebra.

(ii) It is not always possible to replace S_N with R_N above: the $E^{(s)}$ can be independent, without E being even quasi-independent.

(iii) We can rephrase the theorem: $\beta(E) < N \leq M$ if and only if there is some nonzero $f : E^{(0)} \to [-N, \dots, N]$ which specifies a "set of spikes" parallel to the j-th direction (namely, g in the theorem) such that every $E^{(s)}$ with $s \neq 0$ "shadows" the set of spikes. By "shadowing" we mean that, using a relation supported on the s-th level, we can additively modify $J_s g$ to obtain a function on that level with the proper range and support, so that the overall effect is to produce a function with values in $[-N, \dots, N]$ that's supported only on E.

(iv) Equivalently, $\beta(E) \geq N$ for some $N \leq M$ if and only if, for every nonzero $f : E^{(0)} \to [-N, \dots, N]$, there is some $s \neq 0$ such that $E^{(s)}$ "blocks" the set of spikes (g in the theorem) determined by f. That is, $J_s g + R_\infty(Z_m + s)$ and $S_N(E^{(s)})$ are disjoint. Hence there is no relation supported on $Z_m + s$ such that we can additively modify $J_s g$ to be supported only on $E^{(s)}$ and have range in $[-N, \dots, N]$.

(v) The previous paragraph contains the method used by our computer programs to search for E with a specified $\beta(E)$. Each choice of a candidate $E^{(0)}$ determines a supply of nonzero functions $f : E^{(0)} \to [-N, \dots, N]$. Each such f specifies a set of spikes as a challenge to be "blocked". One attempts to find $E^{(s)}$ for $s \neq 0$ so that, hopefully, each of these sets of spikes is blocked.

Proof of Theorem 5.5. (1) is obvious.

(2) $\Rightarrow$ (3). We shall use the basis provided by Lemma 2.10. We are assuming there is some nonzero $q \in R_N(E)$. Lemma 2.10 shows there are coefficients a_y in $\mathbb{Q}$ and $h_s \in R_\infty(E^{(s)})$ such that

$$q = \sum_{y \in Z_m} a_y \chi_{Z_{p_j}+y} + \sum_{s \in Z_{p_j},\, s \neq 0} h_s. \tag{5–5}$$

Multiplying by J_0, we have $J_0 q$ supported on $E^{(0)}$, $J_0 \chi_{Z_{p_j}+y} = \delta_y$ for $y \in Z_m$, and $J_0 h_s = 0$ for $s \in Z_{p_j}$ such that $s > 0$. Therefore $J_0 q = \sum_{y \in Z_m} a_y \delta_y$. Thus, for $y \in Z_m$, $a_y = (J_0 q)(y) = q(y)$. Let f be the restriction of $J_0 q$ to $E^{(0)} = E \cap Z_m$. Then, for all $y \in E^{(0)}$, $a_y = q(y) = f(y)$. We first assume that $f \neq 0$.

Since q is supported on E, we have $a_y = 0$ for $y \in Z_m \backslash E^{(0)}$. Since the range of q is a subset of $[-N, \dots, N]$, the same holds for f. Let

$$g = \sum_{y \in E^{(0)}} f(y) \chi_{Z_{p_j}+y} = \sum_{y \in E^{(0)}} a_y \chi_{Z_{p_j}+y}. \tag{5–6}$$

Then, from (5–5) and the fact that $a_y = 0$ for $y \notin E^{(0)}$,

$$q = g + \sum_{s \in Z_{p_j},\, s \neq 0} h_s. \tag{5–7}$$

Consider any $s \in \{1, \dots, p_j - 1\}$. Then $J_s q \in S_N(E^{(s)})$. Therefore,

$$J_s q = J_s g + J_s \sum_{1 \le t \le p_j - 1} h_t = J_s g + h_s \in S_N(E^{(s)}).$$

Thus, the relations in (3) hold.

Only one task remains: to show $f \neq 0$. Suppose that $f = 0$. Because f is the restriction to Z_m of $J_0 q$, $J_0 q = 0$. From (5–6), we also have $g = 0$. Therefore, q is an N-relation supported on the nonzero cosets of Z_m. By Lemma 2.10, $J_s q \in R_N(E^{(s)})$. (That is stronger than $J_s q \in S_N(E^{(s)})$). Since $N \le M \le \beta(E^{(s)})$ for $s \neq 0$, $R_N(E^{(s)}) = \{0\}$. Therefore $J_s q = 0$. This holds for all $s \neq 0$. Thus $q = \sum_{s=0}^{n_j - 1} J_s q = 0$. But $q \neq 0$. So $f \neq 0$. That completes the proof of implication (2) $\Rightarrow$ (3) of Theorem 5.5.

(3) $\Rightarrow$ (2). Assume (3) to be true. For $s \in [1, \dots, p_j - 1]$, let

$$q_s \in (J_s g + R_N(E^{(s)})) \cap S_N(E^{(s)}).$$

Note that q_s is supported on $E^{(s)}$. Let

$$q = g + \sum_{s=1}^{n_j - 1} (q_s - J_s g). \tag{5–8}$$

We claim that $q \in R_N(E)$. First, note that $q_s - J_s g \in R_N(E^{(s)})$ by our choice of q_s when $s \neq 0$. Thus, (5–8) is just an expansion using spikes and layers, so $q \in R_\infty(Z_n)$.

We check that the support of q is E and the range is in $[-N, \dots, N]$, one layer at a time.

For $s = 0$, since $J_0 q_s = 0$ and $J_0 J_s g = 0$ for $s \neq 0$,

$$J_0 q = J_0 g = \sum_{y \in E^{(0)}} f(y) J_0 \chi_{Z_{p_j} + y} = \sum_{y \in E^{(0)}} f(y) \delta_y.$$

Thus, on the 0-th level, which is Z_m, q is supported on $E^{(0)} \subset E$ and the range of q is a subset of the union of $\{0\}$ and the range of f. Since $0 \in [-N \dots N]$ and range$(f) \subset [-N \dots N]$, q on Z_m has values in $[-N \dots N]$. Note that f is the restriction of q to $E^{(0)}$. Since f is nonzero, q is nonzero.

For $s \in [1, \dots, p_j - 1]$ and $p \notin \{0, s\}$, we have $J_s(q_p - J_p g) = 0$. Therefore

$$J_s q = J_s g + J_s(q_s - J_s g) = J_s g + (q_s - J_s g) = q_s \in S_N(E^{(s)}).$$

Thus the restriction of q to $Z_m + s$ is supported on $E^{(s)}$ and the range on the s-th level is a subset of $[-N, N]$. Since this holds for all $s \in [0, \dots, p_j - 1]$, and

$Z_n = \bigcup_{s=0}^{p_j-1} Z_m + s$, q is supported on E and its range is a subset of $[-N \dots N]$. Since q is nonzero and in $R_N(E)$, we have $\beta(E) < N$. □

6. When $n = pq$ and $n = 15p$

Assume $n = pq$ for distinct, positive primes p and q. Then $Z_n = H_1 \oplus H_2$, where

$$H_i = \{kp_j : 0 \le k < p_i\}, \quad \text{with } p_j \ne p_i. \tag{6–1}$$

We now describe the subsets of Z_n which support a nontrivial quasi-independent relation. We give characterizations of (quasi-)independent sets of Z_{pq} in Theorem 6.4, where we also show that every quasi-independent set in Z_{pq} is independent ($p \ne q$ being odd primes).

Lemma 6.1 (The Tartan Lemma). *A subset $E \subset Z_n$ equals the support of a quasi-independent relation if and only if there are sets $E_1 \subset H_1$ and $E_2 \subset H_2$ such that*

$$E = (E_1 + E_2) \cup \big((H_1 \backslash E_1) + (H_2 \backslash E_2)\big). \tag{6–2}$$

(Here $E = \varnothing$ is allowed as the support of the trivial relation $f \equiv 0$.)

Proof. Sufficiency will be proved first, because it is easier. Let E satisfy (6–2). Consider $f : Z_n \to \mathbb{Q}$ defined by

$$f(j) = \begin{cases} 1 & \text{if } j \in (E_1 + E_2), \\ -1 & \text{if } j \in (((H_1 \backslash E_1) + (H_2 \backslash E_2)), \\ 0 & \text{elsewhere.} \end{cases}$$

Recall from the proof of Lemma 2.1 that, for any coset U of H_1 or H_2,

$$\sum_{v \in U} \omega(v) = 0.$$

Thus, for any $t \in Z_n$, $\sum_{v \in (H_2 \backslash E_2)} \omega(t+v) = -\sum_{v \in E_2} \omega(t+v)$, and therefore

$$\begin{aligned} \psi(f) &= \sum_{x \in E} f(x)\omega(x) = \sum_{x \in (E_1+E_2)} (+1)\omega(x) + \sum_{x \in ((H_1 \backslash E_1) + (H_2 \backslash E_2))} (-1)\omega(x) \\ &= \sum_{x \in (E_1+E_2)} \omega(x) - \sum_{t \in (H_1 \backslash E_1)} \sum_{v \in (H_2 \backslash E_2)} \omega(t+v) \\ &= \sum_{t \in E_1} \sum_{v \in E_2} \omega(t+v) - \sum_{t \in (H_1 \backslash E_1)} \Big(- \sum_{v \in E_2} \omega(t+v) \Big) \\ &= \sum_{v \in E_2} \sum_{t \in H_1} \omega(t+v) = \sum_{v \in E_2} 0 = 0. \end{aligned}$$

(An empty sum of 0's is considered equal to 0.) That proves sufficiency.

For the proof of necessity, let f be in the kernel of ψ such that f is supported on E and the range of f is a subset of $\{0, \pm 1\}$. Let $S = \{1\}$. We use the basis of relations given in Example 2.9. Then for some set of rational coefficients a_t and b_w, one has

$$f = \sum_{t=0}^{p_1-1} a_t \chi_{tp_2+H_2} + \sum_{w=1}^{p_2-1} b_w \chi_{wp_1+H_1}, \tag{6–3}$$

(using the fact that $Z_n = H_1 \oplus H_2$). Because every point of Z_n has the form $tp_2 + wp_1$ for some $0 \le t < p_1$ and $0 \le w < p_2$, and the pair (t, w) is unique, each point of Z_n is the member of each of a unique pair of cosets $tp_2 + H_2$ and $wp_1 + H_1$, with $0 \le t < p_1$ and $0 \le w < p_2$. We set $b_0 = 0$ (to formally allow the zero coset of H_2). This means that

$$f(tp_2 + wp_1) = a_t + b_w, \text{ for all } 0 \le t < p_1,\ 0 \le w < p_2. \tag{6–4}$$

Since the range of f is contained in $\{0, \pm 1\}$,

$$f(tp_2 + wp_1) = a_t + b_w \in \{0, \pm 1\}, \text{ for all } 0 \le t < p_1,\ 0 \le w < p_2. \tag{6–5}$$

Thus, for $w = 0$ we have $f(tp_2) = a_t + b_0 = a_t$ for $0 \le t < p_1$, and the a_t's are in $\{0, \pm 1\}$.

Case I: there are t and t' such that $a_t = 1$ while $a_{t'} = -1$. By (6–5),

$$a_t + b_w = 1 + b_w \in \{0, \pm 1\} \text{ and } a_{t'} + b_w = -1 + b_w \in \{0, \pm 1\},$$

so

$$b_w \in \{-2, -1, 0\}, \quad \text{while} \quad b_w \in \{0, 1, 2\}, \text{ for all } w.$$

Thus $b_w = 0$ for all w. Therefore the support of f consists only of cosets of H_2. In this case, the support has the form

$$(E_1 + H_2) \cup ((H_1 \backslash E_1) + \varnothing)),$$

which proves the lemma in this case.

Case II: $a_t = 0$ for all t. Then the support of f consists only of cosets of H_1, and has the form

$$(H_1 + E_2) \cup (\varnothing + (H_2 \backslash E_2)), \tag{6–6}$$

which proves the lemma in this case.

Case III: $a_t = 1$ for all t. Then $f(tp_2 + wp_1) = 1 + b_w$ for all points in Z_n. Then the support of f again has the form of has the same form as in Case II, with E_2 equal to the set of wp_1 such that $b_w \in \{-2, 0\}$.

Case IV: some $a_t = 0$ and some $a_{t'} = 1$. By (6–5), we have $a_t + b_w = 0 + b_w \in \{0, \pm 1\}$ and $a_{t'} + b_w = -1 + b_w \in \{0, \pm 1\}$, so

$$b_w \in \{1, -1, 0\}, \quad \text{while} \quad b_w \in \{0, -1, -2\}, \text{ for all } w,$$

that is $b_w \in \{-1, 0\}$. Let E_1 be the set of tp_2 where $a_t = 1$ and E_2 the set of wp_1 where $b_w = 0$. On $E_1 + E_2$, $f(tp_2 + wp_1) = 1 + 0 = 1$. On $(H_1 \backslash E_1) + (H_2 \backslash E_2)$, $f(tp_2 + wp_1) = 0 - 1 = -1$. On $E_1 + (H_2 \backslash E_2)$, $f(tp_2 + wp_1) = 1 - 1 = 0$. Likewise, on $(H_1 \backslash E_1) + E_2$, $f(tp_2 + wp_1) = 0 + 0 = 0$. Therefore, the support of f has the desired form.

Case V: $a_t \in \{0, -1\}$ for all t. Note that $-f$ is also in the kernel of ψ, and can be expanded in terms of the basis with a_t replaced by $-a_t$ and b_w by $-b_w$. Also, the range of $-f$ is still a subset of $\{0, \pm 1\}$. We apply the previous four cases to $-f$ to conclude that the support of $-f$ has the correct form. Since the support of $-f$ is the same as the support of f, that completes the proof. □

The lemma says that for $F \subset Z_n$ to be quasi-independent, it is necessary and sufficient for $F \not\supseteq E$ for any nonempty E as in (6–2). This means that F can contain a full coset of neither H_1 nor H_2 (a fact also easily seen from Lemma 2.1). Subject to that modest condition, one can now give many examples of quasi-independent sets.

Lemma 6.2. *Let $S_1 \subset H_1$ and $S_2 \subset H_2$ such that $|\#S_1 - \#S_2| = 2$. Let a denote the smaller of $\#S_1$ and $\#S_2$. If $S \subset (S_1 + S_2)$ such that $\#S \geq a^2$ and $a > 0$, then there is a nonempty set $E \subset S$ of the form*

$$E = (E_1 + E_2) \cup (F_1 + F_2),$$

with E_i and F_i a disjoint partition of S_i, $i = 1$ and $i = 2$.

Proof. This will be proved by induction on a. Let $a = 1$. Without loss of generality assume that $\#S_1 = a$. Since $\#S \neq 0$, there is some $t \in S_1$ and $w \in S_2$ such that $t + w \in S$. So, with $E_1 = S_1$, $F_1 = \varnothing$, $E_2 = \{w\}$, and $F_2 = S_2 \backslash \{w\}$, one has $S \supset \{t + w\} = (E_1 + E_2) \cup (F_1 + F_2)$. Next, let $a = 2$. Again, assume without loss of generality that $\#S_1 = a$. Then $\#S_2 = 4$ and $\#S \geq 4$. Consider the two cases: either there is some $w \in S_2$ such that $(S_1 + w) \cap S = \varnothing$, or there is no such w. If such w exist, there is at least one $v \in S_2$ such that $S \supset (S_1 + v)$ (otherwise, S contains at most one element of the three sets $S_1 + v$, $v \in S_2$, $v \neq w$, so $\#S \leq \#S_2 - 1 = 3$). Thus, $S \supset E = (S_1 + \{v\}) \cup (\varnothing + (S_2 \backslash \{v\}))$. It is clear that $E \neq \varnothing$. Now consider the case of no such w. Then for all $v \in S_2$, $(S_1 + v) \cap S \neq \varnothing$. Let $S_1 = \{t_1, t_2\}$. Set $E_1 = \{t_1\}$ and $F_1 = \{t_2\}$. Let E_2 consist of all $w \in S_2$ such that $t_1 + w \in S$. Then $S \supset E = (E_1 + E_2) \cup (F_1 + (S_2 \backslash E_2))$. Here $E_2 \neq \varnothing$ or $(S_2 \backslash E_2) \neq \varnothing$. In either case, $E \neq \varnothing$.

For an induction hypothesis, assume that Lemma 6.2 is true for all $a' < a$, $a \geq 3$. Again, without losing generality, assume $\#S_1 = a$ and $\#S_2 = a + 2$. There will be two cases to the argument: there is some $w \in S_2$ such that $S_1 + w \subset S$, or there is no such w. In the former case, $S \supset E = (S_1 + \{w\}) \cup (\varnothing + (S_2 \backslash \{w\})$. Clearly $E \neq \varnothing$. In the latter case, we estimate the number

$$b = \#\big(\{w \in S_2 : \#((S_1 + w) \cap S) = a - 1\}\big).$$

Then, because no "sections" of S_1 have a elements in S, b sections have exactly $a{-}1$, and the rest $(a{+}2{-}b)$ have at most $a - 2$, we have

$$a^2 \leq \#S \leq b(a - 1) + (a + 2 - b)(a - 2).$$

Thus, $a^2 \leq b + (a{+}2)(a{-}2) = b{+}a^2{-}4$, and hence $b \geq 4$. So there is a subset T of S_2 such that $\#T = 4$ and, for $w \in T$, $\#\big((S_1 + w) \cap S\big) = a - 1$. Let $S_2' = S_2 \backslash T$. Then

$$\#\big(S \cap (S_1 + S_2')\big) \geq a^2 - 4(a - 1) = (a - 2)^2.$$

Note that $\#S_2' = a - 2 \geq 3 - 2 = 1$. By induction, there is a disjoint partition E_1 and F_1 of S_1, and E_2' and F_2' of $S_2 \backslash T$, such that $S \cap (S_1 + S_2') \supset E' = (E_1 + E_2') \cup (F_1 + F_2')$, with $E' \neq \varnothing$. Now let $E_2 = E_2' \cup \{w \in T : E_1 + w \subset S\}$ and $F_2 = F_2' \cup \{w \in T : F_1 + w \subset S\}$. Since E_1 and F_1 are a disjoint partition of S_1, and each $w \in T$ has $(S_1 + w) \cap S = a - 1 = \#S_1 - 1$, each $w \in T$ is in E_2 or F_2 but not both. Thus E_2 and F_2 disjointly partition S_2. Clearly, $S \supset E = (E_1 + E_2) \cup (F_1 + F_2)$. Because $E \supset E' \neq \varnothing$, the induction argument is complete. □

Theorem 6.3. *If the positive integer n has exactly two distinct, positive prime factors, then $\Psi(n) = \phi(n)$.*

Proof. The case of even n is handled by Theorem 4.1(3).

So assume that n is odd (and hence $p_i \geq 3$). Without loss of generality, $p_1 < p_2$. Let $S \subset Z_n$ such that $\#S > \phi(n)$. It will be shown that S contains a nonempty set E of the form given by (6–2), and so E is not quasi-independent, by Lemma 6.1. There are two cases: for some $w \in H_2$, $(H_1 + w) \subset S$, or there is no such w. In the former case, let $E_1 = H_1$, and $E_2 = \{w\}$. Then

$$\begin{aligned} E &= (E_1 + E_2) \cup ((H_1 \backslash E_1) + (H_2 \backslash E_2)) \\ &= (H_1 + w) \cup (\varnothing + (H_2 \backslash \{w\})) = H_1 + w \subset S, \end{aligned}$$

and clearly $E \neq \varnothing$. That disposes of the first case. (Alternatively, one notes that if $(H_1 + w) \subset S$, then S contains a nontrivial coset, so cannot be quasi-independent.)

In the second case, let x denote the number of $w \in H_2$ such that $H_1 + w$ has exactly $p_1 - 1$ elements of S. Then

$$(p_1 - 1)(p_2 - 1) + 1 \leq \#S \leq x(p_1 - 1) + (p_2 - x)(p_1 - 2).$$

This implies that $x \geq p_2 - (p_1 - 2)$. Let T consist of $p_2 - (p_1 - 2)$ elements w of H_2 such that $H_1 + w$ has exactly $p_1 - 1$ elements of S. Let $S_1 = H_1$ and $S_2 = H_2 \backslash T$. Then, with $S' = S \cap (S_1 + S_2)$, one has

$$\#S' \geq (p_1 - 1)(p_2 - 1) + 1 - [p_2 - (p_1 - 2)](p_1 - 1) = (p_1 - 2)^2.$$

Note that $\#S_2 = p_1 - 2$, while $\#S_1 = \#H_1 = p_1$. Because p_1 is an odd, positive prime, $p_1 - 2 > 0$. So, by Lemma 6.2, there is a nonempty set $E' \subset S_1 + S_2$ of the form $E' = (E_1 + E_2') \cup (F_1 + F_2')$, where E_1 and F_1 partition H_1 and E_2' and F_2' partition S_2. For each $w \in T$, $S \supset (E_1 + w)$ or $S \supset (F_1 + w)$ but not both. In the former case, adjoin such w's to E_2' to form E_2. In the latter case, adjoin them to F_2' to form F_2. Then $F_2 = H_2 \backslash E_2$, $F_1 = H_1 \backslash E_1$ and $S \supset E = (E_1 + E_2) \cup ((H_1 \backslash E_1) + (H_2 \backslash E_2)$, with $E \supset E' \neq \varnothing$. □

Quasi-independent sets in Z_{pq}. To discuss the case Z_{pq}, we need a generalization of shadowing, as follows. Suppose $E \subset Z_n$, and that $Z_n = H \times L$. Let $h \in H$, and let $F \subset (\{h\} \times L)$. We say that E *shadows the spikes rising from* F if, for every $k \in H$, $k \neq h$,

$$\text{(6–7)} \quad \text{either } (F + (k - h, 0)) \subset E \cap (\{k\} \times L) \\ \text{or } (F + (k - h, 0)) \cup (E \cap (\{k\} \times L)) = \{k\} \times L.$$

Theorem 6.4. *Let $p \neq q$ be odd primes. Then $E \subset Z_{pq}$ is quasi-independent if and only if all of the following hold. For $t \in Z_p$ and $v \in Z_q$, let $E^{(t)} = E \cap (Z_q + t)$ and $E_{(v)} = E \cap (Z_p + v)$.*

(1) *The intersection of E with each coset of Z_p is quasi-independent.*

(2) *The intersection of E with each coset of Z_q is quasi-independent.*

(3) *For every $t \in Z_p$ and nonempty subset $F \subseteq E^{(t)}$, the spikes rising from F are not shadowed by E.*

(4) *For every $v \in Z_q$ and nonempty subset $F \subseteq E_{(v)}$, the spikes rising from F are not shadowed by E.*

Furthermore, E is independent if and only if E is quasi-independent.

Proof. Suppose E does not satisfy the conditions. We shall construct a quasirelation supported on E. If either the first or second condition fails, then there is automatically a quasirelation supported on the intersection concerned, and we are done.

The fourth condition is dealt with just as we do for the third. So suppose that the third condition fails. Let $t \in Z_p$ and let the nonempty subset $F \subseteq E^{(t)}$ have spikes rising from F shadowed by E. We define a quasirelation:

$$f = \sum_{\ell \in F} \chi_{Z_p + \ell} - \sum_{\substack{m \in Z_p,\ m \neq t, \\ (F+m-t) \cup E^{(m)} = Z_q + m}} \chi_{Z_q + m}.$$

Then f is supported in E for the following reasons. On $F \subseteq E \cap (Z_q + t)$, we have exactly the sum of characteristic functions of some of the cosets of Z_p that meet that intersection, so $f = 1$ on F. Likewise, if $(F + m - t) \cup E^{(m)} \neq Z_q + m$ and $m \neq t$, then f is 1 on $F + m - t$ and 0 otherwise in $Z_q + m$. By (6–7), $F + m - t \subset E$ and thus f is supported on E (and has values 0 and 1 there).

Finally, suppose $(F + m - t) \cup E^{(m)} = Z_{q+m}$ for some $m \neq t$. Consider an element x of such a coset $Z_q + m$. If $x \notin F + m - t$, then $x \in E$ (because E shadows the spikes rising from F). Also, $f(x) = -1$.

If $x \in F + m - t$ then $f(x) = 0$, since $f(x)$ is a difference of the characteristic functions of the two cosets that meet at x. Thus, f is supported on E. Hence, E is not quasi-independent.

Now suppose that E does satisfy the four conditions. We must show that E supports no nonzero relations. We suppose the contrary.

Consider the set of relations f supported on E. Let $N(f)$ be the minimal *nonzero* cardinality of the intersections of the support of f with cosets of Z_p, assuming that there are f's with nonempty intersections. Choose f with minimal $N(f)$. By replacing f and E with translates, we may assume that the support of f has smallest intersection with Z_p:

$$F = \{x \in E \cap Z_p : f(x) \neq 0\}.$$

We are assuming that $\#F \neq 0$. We write

$$f = \sum_{s \in Z_p \cap E} b_s \chi_{Z_q + s} + \sum_{\substack{u \in Z_q \\ u \neq 0}} c_u \chi_{Z_p + u}.$$

It will be enough to show that F does not have minimal cardinality. To show that it will be enough to delete one element from F. Since E does not shadow the spikes rising from F, there exists $u \in Z_q$ such that neither $F + u \subset E_{(u)}$ nor $(F + u) \cup E_{(u)} = Z_p + u$. Let $w \in Z_p$ be such that $w + u \notin (F + u) \cup E_{(u)}$ and let $s \in F$ be such that $s + u \notin E^{(u)}$. Then

$$c_u + b_w = f(u + w) = 0 = f(u + s) = c_u + b_s.$$

Now, since $w + u \notin (F + u) \cup E^{(u)}$, $b_w = 0$. Hence both $b_s = 0$ and $c_u = 0$, which contradicts the definition of F. Therefore E supports only the zero relation and is independent.

We see that we have shown that if the four conditions fail, then E is not quasi-independent, and that if the four conditions hold, then E supports no nonzero relation. Since independence implies quasi-independence, it now follows that E is quasi-independent if and only if E is independent. □

By similar methods one can prove the following results.

Theorem 6.5. *Let $E \subset Z_{pq}$. Then the only relations supported on E are sums of quasirelations each of which is supported on E.*

Theorem 6.5 does not say that there are no relations on E. If we specify that a relation must have a certain value (e.g., 1) at an element of E, then it may be the case that there are no quasirelations supported on E with that property; blocking is concerned with this phenomenon.

Let $E \subset Z_{pq}$ be the support of a relation f. We write

$$f = \sum_{t \in Z_q \cap E} b_t \chi_{Z_p + t} + \sum_{\substack{v \in Z_p \\ v > 0}} c_v \chi_{Z_q + v}. \tag{6–8}$$

Theorem 6.6. *Let f be a relation on Z_{pq}.*

(1) *We have $f = \sum_{k \in \mathbb{Q}} f_k$, where*

$$f_k = \sum_{\substack{t \in Z_q \cap E \\ |b_t| = k}} b_t \chi_{Z_p + t} + \sum_{\substack{v \in Z_p \\ t > 0,\ |c_v| = k}} c_v \chi_{Z_q + v},$$

and each f_k has support contained in the support of f.

(2) *If the support of f is minimal among the relations supported on E, then the nonzero coefficients in* (6–8) *have equal absolute values.*

Remark 6.7. We can draw several conclusions:

(i) If all the coefficients of f have the same sign, then the support of f includes a coset of a subgroup, and so E contains a coset.

(ii) If, in (6–8), all of the $b_t = 1$ and all of the $c_v = -1$ then $|f| \le 1$, and f is a quasirelation. If the coefficients in (6–8) are integers with some nonzero b_t and some nonzero c_v of the same sign, then $\sup |f| \ge 2$. We can see this by noting that the cosets of Z_p run "perpendicular" to the cosets of Z_q.

(iii) In (6–8), suppose that: E does not contain any coset of Z_p; E does not contain coset of Z_q; and that f is a quasirelation.

Note that (6–8) forces $b_t = f(t) \in \{\pm 1\}$ (in (6–8), E is the support of the relation). If all the c_v are zero, then E is a nonempty, finite union of cosets of Z_p. So, at least one $c_v \ne 0$. We have $b_t + c_v \in \{0, \pm 1\}$ for all b_t. If some $b_t = 1$, then $c_v \in \{-2, -1, 0\}$; if some $b_t = -1$, then $c_v \in \{0, 1, 2\}$. Thus having some b_t's of different sign forces $c_v = 0$. So, all the b_t's are equal. Finally, since Z_q is not a subset of E, there is some $x \in Z_q \backslash E$ and $f(x+w) = c_w \in \{0, \pm 1\}$ for all $w > 0$ in Z_p. So each c_w is an integer. By (ii), each nonzero c_w has sign opposite to that of any b_t.

Thus, given that E is the support of a quasirelation but E does not contain any coset of Z_p or of Z_q, then all the b_t equal 1, with every $c_w \in \{0, -1\}$ and at least one $c_v \neq 0$; or all the b_t equal -1, with every $c_w \in \{0, 1\}$ and at least one $c_v \neq 0$.

7. $\Psi(105)$

Simple estimates. We estimate $\Psi(105)$ in a number of related, and improving, ways, eventually obtaining $\Psi(105) = 52$.

Let $p < q < r$ be distinct odd primes and let $n = pqr$, Then

$$\Psi(n) \leq r(p-1)(q-1). \tag{7–1}$$

In particular, $\Psi(105) \leq 56$.

This is easy: let $E \subset T_{pqr}$ be quasi-independent. A coset of ωT_{pq}, where $\omega = e^{2\pi ik/r}$, can contain at most $(p-1)(q-1)$ elements of E, by Theorem 6.3 and Lemma 4.2. There are r such cosets, so $\#E \leq r(p-1)(q-1)$.

We can improve the estimate (7–1) slightly to show that

$$\Psi(pqr) < (p-1)(q-1)r - 1, \tag{7–2}$$

for distinct odd primes p, q, r. In particular, $\Psi(105) < 55$.

Here is the argument. Suppose that $E \subset T_{pqr}$ had $(p-1)(q-1)r - 1$ elements. Let a denote the number of cosets of T_{pq} that have $(p-1)(q-1)$ elements of E. Then $a = r - 1$. Let F be the coset with the smallest number of elements of E. Then $\#(E \cap F) = (p-1)(q-1) - 1$. We let $w \in F \cap E$. Then $w \in F$, so (5–1) holds for wT_{pq}. At all the other cosets of T_{pq} the intersection of E with the coset has $(p-1)(q-1)$ elements, so either (5–1) holds, or (5–2) holds: we cannot add an element without getting a non-quasi-independent set. Hence, E shadows wT_r, so E cannot be quasi-independent.

We now give an extension lemma, a simple version of [Ramsey and Graham 2006, Theorem 1.2.2].

Lemma 7.1. *When* $2 < p < q < r < s$ *are prime*, $\Psi(pqr) + (s-r)\Psi(pq) \leq \Psi(pqs)$.

Proof. We will construct a quasi-independent subset of Z_{pqs} whose cardinality is $\Psi(pqr) + (s-r)\Psi(pq)$.

Let $E \subset Z_{pqr}$ be a quasi-independent set such that $\#E = \Psi(pqr)$ and $F \subset Z_{pq}$ a quasi-independent set such that $\#F = \Psi(pq)$.

Let a mapping of sets

$$j : Z_{pqr} \cup (Z_{pq} \times [r, \dots, s)) \to Z_{pqs}$$

be given by $j(a, b, c) = (a, b, c)$ for $0 \le a < p$, $0 \le b < q$ and $0 \le c < s$, where we identify Z_{pqr} with $[0, p) \times [0, q) \times [0, r)$ and Z_{pqs} with $[0, p) \times [0, q) \times [0, s)$. Let $E' = j(E \cup (F \times [r, s))$. Then $\#E' = \Psi(pqr) + (s - r)\Psi(pq)$. We claim that E' is quasi-independent. Suppose that f is a quasirelation on Z_{pqs} supported on E'. We write f using the basis of (2–5) and (2–6), so for some rational numbers a_t and b_h,

$$f = \sum_{t \in Z_{pq}} a_t \chi_{t+Z_s} + \sum_{\substack{1 \le j < s \\ L \in \mathscr{L}_j}} b_L \chi_L,$$

where $\mathscr{L}_j$ denotes the cosets in $\mathscr{L}$ that are contained in $Z_{pq} + j$, $1 \le j < s$. Let g be the characteristic function of $Z_{pq} \times [0, r) \subset Z_{pqs}$. Then

$$(gf) \circ j = \sum_{t \in Z_{pq}} a_t \chi_{t+Z_r} + \sum_{\substack{1 \le j < r \\ L \in \mathscr{L}_j}} b_L \chi_L$$

is a quasirelation on Z_{pqr}. Of course, the support of $(gf) \circ j$ is E, so $(gf) \circ j = 0$. In particular, $a_t = 0$ for all t and $b_L = 0$ for all $L \in \mathscr{L}_j$, $1 \le j < r$. Hence, the support of our original f excludes $Z_{pq} \times [0, r)$, that is, $\operatorname{Supp} f \subset j(F \times [r, s))$. Then Corollary 2.11 (Empty Floor) implies that $j(F \times [r, s))$ is quasi-independent and thus $f = 0$. Hence E' is quasi-independent. □

Lemma 7.2. *Let $p \ge 7$ be any prime. Then $\Psi(15p) \le \phi(15p) + 4$. In particular, $\Psi(105) \le 52$.*

Proof. We view T_{15p} as $Z_3 \times Z_5 \times Z_p$. Let $E \subset T_{15p}$ have $\phi(15p)+5 = 8(p-1)+5 = 8p - 3$ elements. We will show that E is not quasi-independent.

If, for any coset wT_{15}, $E_w = E \cap (wT_{15})$ is not quasi-independent, we are done (E is not quasi-independent because a subset is not quasi-independent). So we may assume that E_w is quasi-independent for all w. In particular, if $\#E_w > 8$ for any w, E_w cannot be quasi-independent. So, $\#E_w \le 8$ for all w. Let a be the number of distinct cosets wT_{15} in T_{15p} such that $\#E_w = 8$. Then $8p - 3 \le a(8) + (p - a)(7) = a + 7p$, so $a \ge p - 3$. Let $t_i T_{15}$, for $1 \le i \le p$, enumerate the distinct cosets of T_{15} in T_{15p} so that (with E_{t_i} shortened to E_i) $\#E_i = 8$ for integers $i \in [4, p]$. Then $F = E_1 \cup E_2 \cup E_3$ satisfies $\#F = \#(E_1 \cup E_2 \cup E_3) = (8p - 3) - 8(p - 3) = 21$. Among the 5 cosets of T_{3p} in T_{15p}, at least one has at least 5 elements of F. Let such a coset be labeled L. Note that $L \cap t_i T_{15}$ is a coset of T_3; label it R_i. Thus $5 \le \#(F \cap L) = \#\big(\bigcup_{i=1}^{3}(E \cap R_i)\big)$. Suppose that some $E \cap R_i$ has three elements. Then E contains a full coset of Z_3 and hence is not quasi-independent. So assume that each $E \cap R_i$ has at most two elements. Together, R_1, R_2 and R_3 have at least

5 elements of E; so at least two of them have exactly two elements of E and the third has at least one. By relabeling the cosets t_1T_{15}, t_2T_{15} and t_3T_{15}, we may assume that R_1 and R_2 have exactly two elements of E and R_3 at least one — say $w \in E \cap R_3$. (It is important that only one of the sets $R_1, \dots, R_3$ have only one element of F.)

By applying a group translation to Z_{15p}, we may assume that $w = t_3 = 0$, since composition with a group translation clearly preserves basis elements of the relations and group translations map quasi-independent sets into quasi-independent sets. (See [Ramsey and Graham 2006, Theorem 3.1.2] for a characterization of those permutations of Z_n that preserve (quasi-)independent sets.)

We claim that T_p is a (vertical) spike shadowed by the set E. Note that $t_3 \in R_3 \subset L$. The intersection $T_p \cap t_i T_{15}$ contains but a single point z_i for each $1 \le i \le p$, and that point is a member of R_i.

We now check the conditions (5–1) and (5–2) of Theorem 5.1. For $i \in [4, p]$, $E \cap t_i T_{15}$ has 8 elements and hence is maximally quasi-independent within that coset. If $z_i \notin E$, then $\{z_i\} \cup (E \cap t_i T_{15})$ has 9 elements and thus is not quasi-independent. For $i = 1$ and $i = 2$, if $z_i \notin E$, then $\{z_i\} \cup (E \cap R_i) = R_i$ is a full coset of T_3 and hence not quasi-independent. Note that $E \cap R_i \subset E \cap t_i T_{15}$. For $i = 3$, $z_i = 0 \in E$. Thus E shadows a coset of T_p, and hence is not quasi-independent. □

Example 7.3 ($\Psi(105) \ge 52$). Here is a 52-element quasi-independent subset of Z_{105}, given by the 7 layers:

Layer 0: $\{1, 2, 3, 6, 9, 12, 15\}$
Layer 1: $\{2, 3, 4, 6, 8, 9, 15\}$
Layer 2: $\{1, 3, 4, 6, 7, 8, 15\}$
Layer 3: $\{1, 2, 4, 7, 9, 10, 13\}$
Layer 4: $\{2, 3, 4, 5, 6, 12, 13, 14\}$
Layer 5: $\{1, 3, 4, 5, 8, 10, 12, 14\}$
Layer 6: $\{1, 2, 3, 4, 10, 11, 12, 14\}$

We have identified the elements on each layer lexicographically, not group theoretically (this makes the computer programming easier). The properties of this 52-element set have been verified by two very different computer programs, one based on a linear programming principles and the other a direct search for efficient blocking of sets of spikes. We believe that $\Psi(105)$ is at least 52 because a logically complex, months-long computer search told us so. (See the Appendix for details on the computer program used for $n = 165$ and 195, which is an adaptation of the one used for $n = 105$.)

Theorem 7.4. *If $n = 15p$, where $p \ge 7$ is a prime, then $\Psi(n) = \phi(n) + 4$.*

Proof. By Lemma 7.1, Example 7.3 and computation, we see that $p \ge 7$ implies $\Psi(15p) \ge \Psi(105) + (p - 7)\Psi(15) = 4 + \phi(15p)$. By Lemma 7.2, $\Psi(15p) \le 4 + \phi(15p)$. □

Only 2 or 3 independent sets are needed for $n = pqr$. When n is the product of 3 distinct, odd (positive) prime numbers, T_n is the union of 3 independent sets. With the exceptions of $p_1 = 3$, $p_2 = 5$ and $7 \le p_3 \le 13$, this can be reduced to two independent sets:

Proposition 7.5. *Let $n = p_1 p_2 p_3$ with each p_i a positive prime number and $p_3 > p_2 > p_1 \ge 3$.*

(1) *If $p_1 \ge 5$, or $p_1 = 3$ and $p_2 \ge 7$, or $p_1 = 3$, $p_2 = 5$ and $p_3 \ge 17$, then Z_n is the union of two independent sets.*

(2) *If $p_1 = 3$, $p_2 = 5$ and $p_3 = 11$ or $p_3 = 13$, then Z_n is the union of three independent sets, but not of two independent sets.*

(3) *If $p_1 = 3$, $p_2 = 5$ and $p_3 = 11$ or $p_3 = 13$, then Z_n is the union of two quasi-independent sets.*

(4) *If $p_1 = 3$, $P_2 = 5$ and $P_3 = 7$, then Z_n is the union of* 3 *independent sets and not the union of two quasi-independent sets.*

The integers n are 165 and 195 in cases (2)–(3): and 105 in case (4).

Proof. We use Proposition 1.2 without comment here.

(1) We need only show that $\phi(n)/n \ge \frac{1}{2}$. When $p_1 \ge 5$,

$$\frac{\phi(n)}{n} = \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdot \frac{p_3 - 1}{p_3} \ge \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} > 0.62 > \frac{1}{2}.$$

When $p_1 = 3$ and $p_2 \ge 7$,

$$\frac{\phi(n)}{n} \ge \frac{2 \cdot 6 \cdot 10}{3 \cdot 7 \cdot 11} > .519 > \frac{1}{2}.$$

When $p_1 = 3$ and $p_2 = 5$ and $p_3 \ge 17$,

$$\frac{\phi(n)}{n} \ge \frac{2 \cdot 4 \cdot 16}{3 \cdot 5 \cdot 17} > 0.501 > \frac{1}{2}.$$

(2) As long as $p_3 > p_2 > p_1 \ge 3$:

$$\frac{\phi(n)}{n} \ge \frac{2 \cdot 4 \cdot 6}{3 \cdot 5 \cdot 7} > 0.45 > \frac{1}{3}.$$

When $p_1 = 3$, $p_2 = 5$ and $p_3 \le 13$, we have $\phi(n)/n < 0.493$, so three independent sets are needed.

(3) For both $n = 165$ and $n = 195$ a computer search (see the Appendix) produced a pair of quasi-independent sets with union the entire group.

(4) $n = 105$, $3\phi(105) = 3 \cdot 48 > 105$, and $\frac{105}{2} > 52 = \phi(105) + 4$. □

The first n for which Z_n is not a union of 3 independent sets is 111546435, the product of the first 8 odd primes. To show by our methods that there are three quasi-independent sets covering Z_n seems impossible.

Appendix

We list here the elements of two quasi-independent sets whose union gives us the 165th roots of unity, and briefly discuss the computing method used to find these set. Further details are available on request.

We view the 165th roots of unity as $Z_5 \times Z_3 \times Z_{11}$ and list the elements in lexicographic order; each line corresponds to a horizontal layer (coset of $Z_5 \times Z_3$).

layer	Elements of 1st set	Elements of 2nd set
0	$\{1, 2, 3, 4, 6, 10, 12\}$	$\{5, 7, 8, 9, 11, 13, 14, 15\}$
1	$\{2, 3, 4, 6, 7, 13, 15\}$	$\{1, 5, 8, 9, 10, 11, 12, 14\}$
2	$\{1, 3, 4, 6, 7, 13, 15\}$	$\{2, 5, 8, 9, 10, 11, 12, 14\}$
3	$\{1, 2, 4, 6, 8, 14, 15\}$	$\{3, 5, 7, 9, 10, 11, 12, 13\}$
4	$\{1, 2, 3, 7, 10, 13, 14\}$	$\{4, 5, 6, 8, 9, 11, 12, 15\}$
5	$\{3, 4, 5, 6, 8, 9, 11, 12\}$	$\{1, 2, 7, 10, 13, 14, 15\}$
6	$\{1, 2, 5, 6, 8, 9, 12, 14\}$	$\{3, 4, 7, 10, 11, 13, 15\}$
7	$\{1, 2, 3, 7, 9, 13, 14, 15\}$	$\{4, 5, 6, 8, 10, 11, 12\}$
8	$\{2, 3, 5, 6, 9, 10, 11, 12\}$	$\{1, 4, 7, 8, 13, 14, 15\}$
9	$\{2, 3, 4, 7, 10, 11, 13, 15\}$	$\{1, 5, 6, 8, 9, 12, 14\}$
10	repeat any layer	

The same example works for 195th roots of unity: the first 10 layers are the same, layers labeled from 0 through 9, and the last three layers can be a repeat of any earlier layer. When repeating a layer, keep both the part in the first set and the part in the second set.

These examples have been verified by two independent computer programs:

- With one program, one picks a layer and generates all the nonzero sets of vertical spikes that are supported within that layer. Then, successively through the layers, one finds which sets of vertical spikes are still shadowed by each layer. By the 10th layer, one finds that none are left. Hence all these sets of spikes are blocked; also, the subset within each layer is quasi-independent. It follows that the entire set is quasi-independent.

- A program based upon linear programming principles finds, directly, that no nontrivial quasi-independent relation is supported on the set.

Although we stopped after generating one example, we believe there are many because the search process succeeded too easily. The search was often "greedy", sometimes optimizing locally when a choice had to be made. At other times, a random choice was made to reduce the search possibilities to manageable proportions. Usually, in this subject, greediness and randomness do not produce the best results but they were good enough in this application. Several things helped this search substantially:

• A necessary condition is that the intersection of each set with a layer must be quasi-independent, which limits the size to eight within any layer. If the set's complement is to enjoy the same property, its size can be at most 8 as well. Thus, within each layer, the set can have 7 or 8 elements. By an exhaustive search, there are exactly 1440 subsets of $Z_5 \times Z_3$ that are quasi-independent, have size 7, and have a quasi-independent complement with respect to $Z_5 \times Z_3$. This bounds the search to 1440^{11} or 1440^{13}, approximately $5.5 \cdot 10^{34}$ or $1.1 \cdot 10^{41}$.

• Modulo permutations of the rows and columns of $Z_5 \times Z_3$, there are only 4 quasi-independent subsets of size 7 whose complements are also quasi-independent. This gives a further reduction. We can assume that the 0-layer of the 1st set is one of these 4. That reduces the search by a factor that is approximately 0.0028. The example given above was found working with the first of these 4 possibilities.

• We generated the 1093, unique modulo multiplication by -1, nonzero sets of vertical spikes that were supported within the 0-layer by the size-7 set we chose there for the first set. It is a fact that some sets of vertical spikes are shadowed by every quasi-independent set of size 8. This is even more true, if we restrict the size-8 sets to have complements that are quasi-independent sets. Here there were 29 sets of spikes that were shadowed by every candidate size-8 set. We then searched for the minimum number of candidate size-7 sets that would block these 29. We found that we needed to use four 7-sets in addition to the 7-set in the 0-layer. Here there were many choices; we worked with the first one that we found, giving us the 2nd through the 5th layers of the first set. At the this point, using these first five layers, only 4 sets of vertical spikes survived.

• We then generated the 3280 unique (modulo multiplication by -1) nonzero sets of vertical spikes that were supported within the 0-layer by the complement of what the first set had in that layer. We then determined which of these were shadowed by the complements of what the first set had in layers 2 through 4. There were 316 of these.

• We then proceeded with a greedy algorithm: for layers 6 through 10, a 7-set was chosen to block the most sets of spikes that survive all layers before it. Given more than one 7-set that fits this role, then a 7-set was chosen whose complement blocks the most of the (at most 4) heretofore surviving spikes of the first set.

Acknowledgments

We thank the referee for suggesting an argument we use in the more difficult direction of the proof of Theorem 1.4, and that we combine what was two papers into the present one.

References

[Bourgain 1985] J. Bourgain, "Sidon sets and Riesz products", *Ann. Inst. Fourier* (*Grenoble*) **35**:1 (1985), 137–148. MR 86h:43009 Zbl 0578.43008

[Graham and McGehee 1979] C. C. Graham and O. C. McGehee, *Essays in commutative harmonic analysis*, Grundlehren der Mathematischen Wissenschaften **238**, Springer, New York, 1979. MR 81d:43001 Zbl 0439.43001

[Grow and Whicher 1984] D. Grow and W. C. Whicher, "Finite unions of quasi-independent sets", *Canad. Math. Bull.* **27**:4 (1984), 490–493. MR 86d:43007 Zbl 0554.43004

[Hardy and Wright 1960] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., The Clarendon Press, Oxford, 1960. MR 81i:10002 Zbl 0086.25803

[Lang 1965] S. Lang, *Algebra*, Addison-Wesley, Reading, 1965. MR 33 #5416 Zbl 0193.34701

[Pisier 1983] G. Pisier, "Arithmetic characterizations of Sidon sets", *Bull. Amer. Math. Soc.* (*N.S.*) **8**:1 (1983), 87–89. MR 84h:43015 Zbl 0505.43002

[Ramsey and Graham 2006] L. T. Ramsey and C. C. Graham, "Permutation and extension for planar quasi-independent subsets of the roots of unity", preprint, 2006. math.FA/0606546

[Rider 1966] D. Rider, "Gap series on groups and spheres", *Canad. J. Math.* **18** (1966), 389–398. MR 32 #8047 Zbl 0141.12602

[Stečkin 1956] S. B. Stečkin, "On absolute convergence of Fourier series", *Izv. Akad. Nauk SSSR. Ser. Mat.* **20** (1956), 385–412. In Russian. MR 18,126f Zbl 0074.29104

[Stegeman 1971] J. D. Stegeman, *Studies in Fourier and tensor algebras*, Rijksuniv. Utrecht, 1971. Doctoral dissertation. MR 42 #8308

[Varopoulos 1970] N. T. Varopoulos, "Sidon sets in R^n", *Math. Scand.* **27** (1970), 39–49. MR 42 #8184 Zbl 0214.13302

Received December 4, 2004.

L. Thomas Ramsey
Department of Mathematics
University of Hawaii
Keller Hall
2565 The Mall
Honolulu, HA 96822
United States
ramseyl001@hawaii.rr.com

Colin C. Graham
1115 Lenora Road
Bowen Island BC V0N 1G0
Canada
ccgraham@alum.mit.edu