PERMUTATION AND EXTENSION FOR PLANAR QUASI-INDEPENDENT SUBSETS OF THE ROOTS OF UNITY

L. THOMAS RAMSEY AND COLIN C. GRAHAM

Abstract. Let $e^{2\pi iQ}$ denote the set of roots of unity. We consider subsets $E \subset e^{2\pi iQ}$ that are quasi-independent or algebraically independent (as subsets of the discrete plane). A bijective map on $e^{2\pi iQ}$ preserves the algebraically independent sets iff it preserves the quasi-independent sets, and those maps are characterized.

The effect on the size of (quasi-)independent sets in the $n^{th}$ roots of unity $\mathbb{Z}_n$ of increasing a prime factor of $n$ is studied.

March 29, 2022

1. Introduction and statement of results

1.1. Background. The motivation of this paper is the question: what are the properties of those subsets of $e^{2\pi iQ}$, the set of all roots of unity, that are quasi-independent? That is of interest for itself and because a theorem of Pisier [3] shows a set $E$ is a Sidon set iff there is a $\delta > 0$ such that each finite $F \subset E$ contains a quasi-independent set with $\# F \geq \delta \# E$. Hence, determining the properties of the quasi-independent subsets of subgroups of the roots of unity may help to resolve whether $e^{2\pi iQ}$ is Sidon.

The present paper is a continuation of [4], where we studied the size $\Psi(n)$ of the largest quasi-independent subset of the $n^{th}$ roots of unity and established some properties of $\Psi$ (some of those results are quoted in §2), and showed (among other things) that if a set of primes $P$ has $\sum_{q \in P} 1/q < \infty$, then the set $W$ of roots of unity generated by roots of the form $e^{2\pi i/(q_1^{n_1} \cdots q_k^{n_k})}$, where $q_j \in P$ and $1 \leq n_j$, $1 \leq j \leq k$, is a Sidon set in $\mathbb{C}$ when $\mathbb{C}$ is given the discrete topology.

We now define our terms.

Date: March 29, 2022.

2000 Mathematics Subject Classification. Primary: 42A16, 43A46. Secondary 11A25, 11B99, 11Lxx.

Key words and phrases. Independent sets in discrete groups, quasi-independent sets, Roots of unity, Sidon sets.

The second named author is partially supported by an NSERC grant.
A subset $B$ of an (additively-written) abelian group $G$ is quasi-independent if

$$k \geq 1, \ x_j \in B, \ \epsilon_j = 0, \pm 1 \text{ for } 1 \leq j \leq k \text{ and }$$

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

The set $B$ is independent if

$$k \geq 1, \ x_j \in B, \ \epsilon_j \in \mathbb{Z} \text{ for } 1 \leq j \leq k \text{ and }$$

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

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 set $E \subset \mathbb{C} \approx \mathbb{R}^2$ is a Sidon set if every bounded function on $E$ is the restriction of Fourier-Stieltjes transform of a bounded regular Borel measure on the Bohr compactification of $\mathbb{C}$. 

Throughout this paper $n$ will denote a positive integer and $T_n$ the $n$-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 are interested in interplay between the additive group $\mathbb{C}$ and the multiplicative group $\mathbb{T}$, the set of complex numbers of modulus one, which is a closed subset of $\mathbb{C}$. We shall ignore the topology of $\mathbb{C}$. 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, $T_n$ with multiplication is identified with the cyclic group $Z_n$ of order $n$ with addition mod $n$. We often abuse notation to abuse notation identify $T_n$ and $Z_n$ with the product of cyclic groups of prime order and do not distinguish between a factor of those groups and the isomorphic subgroup.

1.2. **Statement of results.** We characterize the permutations of $Z_n$ that preserve the quasi-independent and independent subsets of $e^{2\pi i \mathbb{Q}}$, and show that those classes of permutations are the same. The characterization is of interest in itself, as well as being helpful in machine assisted calculations. $E \subset \mathbb{C}$ is (quasi-)independent if and only if the product $\rho E$ of $E$ with a nonzero complex number $\rho$ is (quasi-)independent. Hence quasi-independence is invariant for $E \subset T_n$ under any rotation permutation of $T_n$, that is, (quasi-)independence is invariant under the group operation in $Z_n$.

From general algebraic principles, we would expect quasi-independence to be invariant under group automorphisms. However, there is
a much larger set of permutations of $T_n$ which preserve quasi-independence and independence. Here is a simplified version of our permutation result, with the full version being Theorem 3.1.2.

**Theorem 1.2.1.** Let $n$ be odd and square free, with prime factorization $n = \prod_{j=1}^{K} p_j$.

1. Let $\sigma_j$ be a permutation of $Z_{p_j}$, $1 \leq j \leq K$ and let $\sigma = \sigma_1 \times \cdots \times \sigma_K$ be the product permutation on $Z_n$. Then $\sigma$ preserves both the class of quasi-independent and the class of independent sets.

2. Let $\sigma$ be a permutation of $Z_n$ that preserves either the class of quasi-independent or the class of independent sets. Then $\sigma$ is a product of permutations as in (1).

The permutations of $e^{2\pi i Q}$ which preserve quasi-independent sets are identified in Corollary 3.1.4.

Our second main result shows that $\Psi$ is “monotone” in a certain sense:

**Theorem 1.2.2.** For primes $p_1 < p_2 < \ldots < p_K$, let $n = \prod_{j=1}^{K} p_j$. Let $s \in \{1, \ldots, K\}$. If $s = K$, let $q$ be any prime such that $q > p_K$. If $s < K$, let $q$ be any prime such that $p_s < q$ and $q \notin \{p_{s+1}, \ldots, p_K\}$. Let $m = n/p_s$, and $\Delta \geq 0$. Then the following hold.

1. $\Psi(qm) \geq \Psi(n) + (q - p_s)\Psi(m)$.
2. If $\Psi(n) \geq \phi(n) + \Delta$, then $\Psi(qm) \geq \phi(qm) + \Delta$.
3. If $\Psi(n) \geq (p_s - 1)\Psi(m) + \Delta$, then $\Psi(qm) \geq (q - 1)\Psi(m) + \Delta$.

The factors $p_s - 1$ and $q - 1$ are quite natural in this context, as $\Psi$ has properties quite similar to those of Euler’s $\phi$ [4, Thm. 4.1].

We give an application of Theorem 1.2.2 in §4.3.

1.3. **Organization of this paper.** Notation and the material needed from [4] are given in §2. We state and prove the general permutation theorem in §3. In §4 we show how $\Psi$ is monotonic and consider extensions of quasi-independent sets.

When our results are valid for both the class of independent sets and for the class of quasi-independent sets, we write (quasi-)independent, (quasi-)independence, and (quasi)relation (see below).
2. Preliminaries

2.1. Simple characterizations of (quasi-)independent sets. Given $n$, it will be convenient to have specified its prime factorization:

$$(2.1.1) \quad n = \prod_{j=1}^{K} p_j^{n_j},$$

for some $K$ and distinct, positive primes $p_j$, and the square-free versions:

$$(2.1.2) \quad \tilde{n} = \prod_{j=1}^{K} p_j \text{ and } Z_{\tilde{n}} = \left(\frac{n}{\tilde{n}}\right)Z_n.$$

**Theorem 2.1.1.** [4, Theorem 1.2.2] 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.

A set $E \subset \mathbb{Z}^{2\pi iQ}$ is independent (resp. quasi-independent) if $E$ supports no non-zero relation (resp. quasi-relation), that is a finitely supported function $f : E \rightarrow Q$ (resp. $E \rightarrow \{0, \pm 1\}$) such that $\sum_{z \in E} f(z)z = 0$. Switching to $Z_n$, we can describe the (quasi-)relations via a basis, since the set of relations is a vector space over $Q$.

**Lemma 2.1.2.** [?, Lemma 2.10] Let $2 \leq n$ be square-free with prime factorization $n = p_1 \cdots p_K$. Fix $1 \leq j \leq K$ and $0 \leq \ell < p_j$, and write $Z_n = Z_{p_j} \times H$. Then the set of relations on $Z_n$ has a basis consisting of

1. the characteristic functions of cosets of $Z_{p_j}$
2. relations each of which is supported on only one coset $H + k$, $0 \leq k < p_j$, and $k \neq \ell$.

Thus, each relation is a sum of (1) “spikes” (from cosets of $Z_{p_j}$) and (2) of relations supported on cosets of $H$, with one coset omitted.

**Corollary 2.1.3** (Empty Floor). [?, Cor. 2.11] Let $n, j, H$ be as above. Suppose that $E \subset Z_n$ is such that $E \cap (H + b) = \emptyset$ for some $b$. Then $E$ is (quasi-)independent if and only if $E \cap (H + a)$ is (quasi-)independent for all $a \in Z_{p_j}$.

**Corollary 2.1.4.** Let $n > 1$ be square-free and $q$ a positive prime that does not divide $n$. Then $\Psi(nq) \geq (q-1)\Psi(n)$.

**Proof.** Let $E \subset Z_n$ be quasi-independent such that $\#E = \Psi(n)$. Let $F = E \times \{1, \ldots, q-1\} \subset Z_{nq}$. Then $F$ is quasi-independent by Corollary 2.1.3, and $\#F = (q-1)\#E$. \qed
Remark 2.1.5. Spikes give us simple examples of independent sets: let $p$ be a prime factor of the square-free, odd integer $n$ and $m = n/p$. Suppose that $E \subset \mathbb{Z}_n = \mathbb{Z}_m \times \mathbb{Z}_p$ and $E$ meets each coset of $\mathbb{Z}_m$ in at most one point. Then $E$ is independent if either $\#E < p$ or $\#E = p$ but $E$ is not a coset of $\mathbb{Z}_p$.

We will need item (1) of the following theorem.

Theorem 2.1.6. [4, Thm. 4.1] For any integer $n \geq 2$, the following hold.

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 $\Psi(pn) \geq (p-1)\Psi(n)$.

Theorem 2.1.7. [4, Thm. 6.4] Let $p \neq q$ be odd primes. Then $E \subset \mathbb{Z}_{pq}$ is quasi-independent if and only if all of the following hold. For $t \in \mathbb{Z}_p$ and $v \in \mathbb{Z}_q$, let $E^{(t)} = E \cap (\mathbb{Z}_q + t)$ and $E^{(v)} = E \cap (\mathbb{Z}_p + v)$.

1. The intersection of $E$ with each coset of $\mathbb{Z}_p$ is quasi-independent.
2. The intersection of $E$ with each coset of $\mathbb{Z}_q$ is quasi-independent.
3. For every $t \in \mathbb{Z}_p$ and non-empty subset $F \subseteq E^{(t)}$, the spikes rising from $F$ are not shadowed by $E$.
4. For every $v \in \mathbb{Z}_q$ and non-empty 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.

Proposition 2.1.8. Suppose that $n \geq 2$ is any integer. Let $p_1$ be the smallest prime factor of $n$.

1. If $E \subset \mathbb{Z}_n$ and $\#E < p_1$, then $E$ is independent.
2. If $E \subset \mathbb{Z}_n$ has cardinality $p_1$, then $E$ is (quasi-)independent if and only if $E$ is a not coset of $\mathbb{Z}_{p_1}$.
3. If $E \subset \mathbb{Z}_n$, $n$ is odd, with at least two prime factors, 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. $(\mathbb{Z}_{p_1} \cup \mathbb{Z}_{p_2}) \setminus \{0\}$ is not quasi-independent, and has cardinality $p_1 + p_2 - 2$.

Proof. (1). This is trivial when $\#E \leq 1$ because a non-zero number in $\mathbb{C}$ is independent over $\mathbb{Q}$. So we may assume that $\#E \geq 2$. 

We argue by induction on \( K \), the number of prime factors of \( n \). Suppose \( K = 1 \). Then for each coset \( H \) of \( Z_n = Z_{p_1} \), \(#(H \cap E) < p_1\) so \( H \cap E \) is independent. By Theorem 2.1.1, \( E \) is (quasi-)independent.

So suppose \( K \geq 2 \), and that the conclusion holds for any \( Z_m \) when \( m \) has less than \( K \) prime factors. Suppose that \( n \) has \( K \) prime factors \( p_1 < \cdots < p_K \) and that \( E \subset Z_n \) has \(#E < p_1\). Again, \( E \) is independent if and only if \( E \cap U \) is independent for each coset \( U \) of \( Z_n \) where \( \tilde{n} = p_1 \cdot p_2 \cdots p_K \). Consider any \( E \cap U \). By translation we may assume \( E \subset Z_{\tilde{n}} \). We write \( Z_{\tilde{n}} = Z_{p_1} \times H \).

For \( 0 \leq t < p_1 \), \( E \cap (\{t\} \times H) \) is equivalent by translation to some \( S \subset H \). Since \(#(S) \leq #(E) < p_1 \) and \( p_1 \) is the smallest prime dividing the order of \( H \), the induction hypothesis implies that \( S \) and hence \( E \cap (\{t\} \times H) \) are (quasi-)independent. Since there are \( p_1 \) disjoint cosets of \( H \) in \( Z_{\tilde{n}} \) but \(#(E) < p_1 \), there is some coset of \( H \) having empty intersection with \( E \). By Corollary 2.1.3, \( E \) is independent. That proves (1).

(2). The “only if” direction is clear. For the converse, suppose that \( E \) is not a coset of \( Z_{p_1} \). If \( E \) has elements in different cosets of \( Z_{\tilde{n}} \), its intersection with each of those cosets would have fewer than \( p_1 \) elements. By (1) of this Proposition, each intersection \( E \cap U \) would be independent for each coset \( U \) of \( Z_{\tilde{n}} \). By Theorem 2.1.1 that would make \( E \) be independent. So we may assume that \( E \subset U \) for some coset \( U \) of \( Z_{\tilde{n}} \). By translating we may assume \( U = Z_{\tilde{n}} \). We again induct on the number \( K \) of prime factors of \( n \). If \( K = 1 \) and \(#(E \cap U) = p_1 \), \( E \) would have to be a coset of \( Z_{p_1} \). So we have \( K > 1 \).

Let \( H = Z_{p_1} \times \cdots \times Z_{p_{K-1}} \). Since \( p_K > p_1 \), there are more than \( p_1 \) cosets of \( H \) within \( Z_{\tilde{n}} \). Since \(#E = p_1 \), at least one coset of \( H \) has empty intersection with \( E \).

Suppose \( K = 2 \). Then \( H = Z_{p_1} \) and the intersection of \( E \) within each coset of \( H \) is a proper subset of that coset (otherwise, \( E \) having \( p_1 \) elements would make it equal that coset). By (1), translated to each coset of \( Z_{p_1} \), the intersection of \( E \) with each coset of \( Z_{p_1} \) is independent. By Corollary 2.1.3, \( E \) is independent.

Suppose that (2) holds for some \( K - 1 \geq 2 \). Let \( H \) be as in the previous paragraph. Again, since \( p_K > p_1 \), there is some coset of \( H \) with empty intersection with \( E \). For each coset \( W \) of \( H \), \( E \cap W \) has size at most \( p_1 \) and \( E \cap W \) is not a coset of \( Z_{p_1} \). If \(#(E \cap W) < p_1 \), by the translation of (1) to the coset \( W \), \( E \cap W \) is independent. If \(#(E \cap W) = p_1 \), the induction hypothesis implies that \( E \cap W \) is independent (if it were a coset of \( Z_{p_1} \), then \( E = E \cap W \) would be one also). By Corollary 2.1.3, \( E \) is independent.
Suppose that \( \#E < p_1 + p_2 - 2 \) and that \( E \) does not contain any cosets.

(i). Let \( H = Z_{p_1} \times \cdots \times Z_{p_{K-1}} \times \{0\} \). Suppose \( E \) has non-void intersection with every coset of \( H \). By counting, we see that there is a coset that meets \( E \) in at most one point.\(^1\) By translation (which preserves (quasi-)independent sets), we may assume that the zero coset has one point intersection with \( E \), and, by translation again, we may assume that the intersection of \( E \) with \( H \) is \( \{0\} \).

(ii). Consider any relation supported on \( E \), consisting of the combination of one spike \( f_0 \) rising from \( \{0\} \) and relations \( f_j \) on the non-zero cosets \( H + j, 1 \leq j < p_K \). The support of \( f_j \) is at most \( [E \cap (H + j)] \cup [Z_{p_K} \cap (H + j)] \). Therefore, each \( f_j = 0 \), unless \( E \cap (H + j) \) has cardinality at least \( p_1 - 1 \). (Throwing in \( Z_{p_K} \cap (H + j) \) will give the remaining point.) If \( f_j = 0 \) for all \( j > 0 \), then \( Z_{p_K} \subset E \), contradicting our assumption that \( E \) contains no cosets.

Hence, some \( f_j \neq 0 \). We now count. \( E \) meets every coset of \( H \): that’s \( p_K \) elements. Since some \( f_j \neq 0 \), that’s at least another \( p_1 - 2 \) elements. Hence, \( \#E \geq p_1 + p_K - 2 > p_1 + p_2 - 3 \). Hence, all \( f_j = 0 \). Another contradiction. That proves that \( E \) cannot meet all cosets of \( H \). We will repeat this argument as follows.

(iii). Let \( H + j \) be a coset of \( H \) that misses \( E \). By translation, we may assume that \( E \cap H = \emptyset \). Therefore, \( E \) is (quasi-)independent if and only if the intersection of \( E \) with each of the non-zero cosets of \( H \) is (quasi-)independent, by 2.1.3. Consider a non-zero coset of \( H \). By translation, we may assume that the coset is the zero coset. Hence, we have eliminated a factor of \( Z_n \), and \( E \subset Z_{p_1} \times \cdots \times Z_{p_{K-1}} \).

(iv). Repeating paragraphs (i)-(iii), we see that we may assume that \( K = 2 \), that is \( Z_n = Z_{p_1} \times Z_{p_2} \). If \( E \) meets all cosets of \( H = Z_{p_1} \), then by paragraphs (i)-(ii), \( E \) contains a coset. If \( E \) misses one coset of \( Z_{p_1} \), then we may assume that \( E \) is contained in some other coset of \( Z_{p_1} \), as above, and thus \( E \) is either independent, or \( E \) is (contains) that coset of \( Z_{p_1} \).

That proves (3).

(4). Let the quasirelation \( f \) be defined by \( f = \chi_{Z_{p_1}} - \chi_{Z_{p_2}} \). Then the support of \( f \) is \( (Z_{p_1} \cup Z_{p_2}) \setminus \{0\} \). That proves Proposition 2.1.8. \( \square \)

3. The permutation theorem

3.1. Preliminary remarks.

\(^1\)In fact, there at least five such cosets. Indeed, let \( b \) be the number of cosets with exactly one element. Then \( b + 2(p_K - b) \leq p_1 + p_2 - 3 \). Thus \( 2p_K - p_1 - p_2 + 3 \leq b \). But \( p_K \geq p_2 \). Thus \( p_K - p_1 + 3 \leq b \). Since \( n \) is odd, \( p_K \geq p_2 \geq p_1 + 2 \), so \( 5 \leq b \).
Notation 3.1.1. (i). Let \( n \geq 2 \) be an integer, with factorization (2.1.1). Let \( E \) be a full set of representations of the cosets in \( Z_n/Z_\tilde{n} \). Thus, \( Z_n = Z_\tilde{n} + E \).

(ii). By “\( Z_{p_a} \)” we remind the reader that we mean the subgroup of \( Z_n \) of order \( p_a \), so \( Z_{p_a} \cong p_a^{n_a-1}Z_{p_a^{n_a}} \).

Theorem 3.1.2. Under §3.1.1, the following hold.

1. Let \( 1 \leq a \leq K \) for some \( a \). Let \( \sigma' \) be any permutation of \( Z_{p_a^{n_a}} \) that maps each coset of \( Z_{p_a} \) into another (or the same) coset of \( Z_{p_a} \). Let \( \sigma \) be the permutation of \( Z_n \) that is the product of \( \sigma' \) with the identity permutations on the other \( K - 1 \) factors of \( Z_n \). Then \( \sigma \) preserves (quasi-)independent sets.

2. Suppose \( p_1 = 2 \). Let \( \sigma \) be any permutation of \( Z_n \) that maps each coset of \( Z_2 \) into itself. Then \( \sigma \) preserves (quasi-)independent sets.

3. Let \( \sigma' \) be any permutation of \( E \). Define a permutation \( \sigma \) on \( Z_n \) by \( \sigma(x + y) = x + \sigma'(y) \) \( x \in Z_\tilde{n}, y \in E \). Then \( \sigma \) preserves (quasi-)independent sets.

4. Let \( \sigma \) be any permutation of \( Z_\tilde{n} \). Extend \( \sigma \) to all of \( Z_n \) by letting \( \sigma \) be the identity on \( Z_n \setminus Z_\tilde{n} \). Then \( \sigma \) preserves the (quasi-)independent sets of \( Z_n \) iff it preserves the (quasi-)independent sets of \( Z_\tilde{n} \).

5. Any product of permutations of \( Z_n \) that preserve the (quasi-)independent sets preserves the (quasi-)independent sets.

6. Let \( \sigma \) be any group automorphism of \( Z_n \) or a translation of \( Z_n \). Then \( \sigma \) preserves (quasi-)independent sets.

7. Every permutation \( \sigma \) of \( Z_n \) that preserves (quasi-)independent sets is a product of permutations of the types of (1)-(4).

Remarks 3.1.3. (i.) The statement of the theorem is slightly redundant, since (3) implies part of (1). Part (1) is stated the way it is to assist the reader in understanding the more complicated (3).

(ii). It is easy to see that Theorem 1.2.1 follows immediately from Theorem 3.1.2.

For each prime \( p \), let \( Z_{p^\infty} \) denote the injective limit of \( Z_{p^j} \), and for a finite set of primes \( p_1 < \cdots < p_K \), let \( Z_{n,\infty} \) denote the product \( \prod_{j=1}^{K} Z_{p_j^\infty} \), where \( n = \prod_{j=1}^{K} p_j \).

Corollary 3.1.4. Let \( \sigma \) be a permutation of \( e^{2\pi i Q} \) with \( \sigma(1) = 1 \). For each \( n \geq 2 \), we identify \( T_n \) with \( Z_n \). Then \( \sigma \) preserves the quasi-independent sets iff \( \sigma \) preserves the independent sets iff for every \( n \geq 2 \) the following hold.
(1) $\sigma$ maps each coset of $Z_n$ in $Z_{\infty}$ to another (or the same) coset of $Z_{\infty}$. (The image coset need not be in $Z_{\infty}$.)

(2) If $\sigma(z_n + t) = z_n + u$, then there exists a product $\sigma_{n,t,u}$ of permutations as in Theorem 1.2.1 such that $\sigma(x) = \sigma_{n,t,u}(x - t) + u$ for all $x \in Z_n + t$.

Proof. Straightforward. □

We will use the following lemma.

Lemma 3.1.5. Let $\sigma$ be a permutation of $Z_n$ such that, for $1 \leq j \leq K$ and $x \in Z_n$, $\sigma(x + Z_{p_j})$ is a coset of $Z_{p_j}$. Then $\sigma$ preserves (quasi-)independence.

Proof. Because $\sigma$ is a permutation of $Z_n$, it sends disjoint cosets of $Z_{p_j}$ into disjoint cosets of $Z_{p_j}$. Thus, $\sigma$ induces a one-to-one mapping $\tau$ from $Z_n/Z_{p_j}$ into itself. Since $Z_n/Z_{p_j}$ is finite, $\tau$ is a permutation of $Z_n/Z_{p_j}$.

It follows that, for $1 \leq j \leq K$ and $x \in Z_n$, $\sigma^{-1}(x + Z_{p_j})$ is a coset of $Z_{p_j}$. To see this, observe that $x + Z_{p_j} = \tau(v + Z_{p_j}) = \sigma(v + Z_{p_j})$, for some $v \in Z_n$. Since $\sigma$ is a permutation of $Z_n$, $\sigma^{-1}(z + Z_{p_j}) = \sigma^{-1}[\sigma(v + Z_{p_j})] = v + Z_{p_j}$. Thus, the hypotheses of this Lemma apply equally to $\sigma$ and $\sigma^{-1}$.

Suppose that $E$ is (quasi-)independent. Consider any (quasi-)relation $f$ supported on $\sigma(E)$. Then, with a redundant (non-unique) choice of coefficients $c_{j,x}$ we have $f = \sum_{j=1}^{K} \sum_{x \in Z_n} c_{j,x} \chi_{x + Z_{p_j}}$. Then

$$f \circ \sigma = \sum_{j=1}^{K} \sum_{x \in Z_n} c_{j,x} \chi_{\sigma^{-1}(x + Z_{p_j})}.$$ 

Note that

(1) The mapping $g \mapsto g \circ \sigma$ is a linear algebra isomorphism on $Q(Z_n)$.

(2) $f \circ \sigma$ is supported on $E$. To see this, let $w \in Z_n \setminus E$. Then, since $\sigma$ is a permutation of $Z_n$, $\sigma(w) \not\in \sigma(E)$ and thus $f(\sigma(w)) = 0$.

(3) Similarly, $\chi_{x + Z_{p_j}} \circ \sigma = \chi_{\sigma^{-1}(x + Z_{p_j})}$.

(4) Since $\sigma^{-1}$ takes cosets of $Z_{p_j}$ to cosets of $Z_{p_j}$, we know that $f \circ \sigma$ is a relation.

(5) Since $\sigma$ is a permutation of the domain of $f$, the range of $f \circ \sigma$ is the same as the range of $f$. Thus, if $f$ is quasi-relation (a relation with its range a subset of $\{0, \pm 1\}$), then so is $f \circ \sigma$.

Hence, if $E$ is quasi-independent and $f$ is a quasi-relation on $\sigma(E)$, we would have $f \circ \sigma$ being a quasi-relation on $E$ and hence $f \circ \sigma = 0$. That
makes \( f = 0 \) and hence \( \sigma(E) \) is quasi-independent as well. Likewise, if \( E \) is independent and \( f \) is a relation on \( \sigma(E) \), that would make \( f \circ \sigma \) be a relation on \( E \) and again \( f \circ \sigma = 0 \). That makes \( f = 0 \) and \( \sigma(E) \) independent.

The previous paragraph applies with \( \sigma^{-1} \) in the role of \( \sigma \). Thus, if \( E \) is (quasi-)independent, so is \( \sigma^{-1}(E) \). Thus, if \( \sigma(E) \) is (quasi-)independent, so is \( E = \sigma^{-1}(\sigma(E)) \).

\[ \square \]

3.2. Proof of Theorem 3.1.2.

\textbf{Proof of Theorem 3.1.2 (1).} Let \( x \in \mathbb{Z}_n \) and \( 1 \leq j \leq K \). In the direct sum

\[ Z_n = \prod_{j=1}^{K} Z_{p_j}^{n_j}, \]

let \( x_i \) be the \( i \)-th coordinate of \( x \).

Suppose first that \( j = a \). Consider any \( w \in x + Z_{pa} \). We have \( w_i = x_i \) for \( i \neq a \) and \( w_a \in x_a + Z_{pa} \), where \( x_a + Z_{pa} \) is a coset of \( Z_{pa} \) inside \( Z_{p_a} \). Then \( \sigma(w)_i = x_i \) for \( i \neq a \) and \( \sigma(w)_a = \sigma'(x_a + Z_{pa}) \).

By hypothesis, \( \sigma'(x_a + Z_{pa}) = v_a + Z_{pa} \) for some \( v_a \in Z_{p_a} \). Thus we have

\[ \sigma(x + Z_{pa}) \subseteq \lambda + Z_{pa}, \]

a coset of \( Z_{pa} \) inside \( Z_n \), where \( \lambda_i = x_i \) for \( i \neq a \) and \( \lambda_a = v_a \). However, since \( x + Z_{pa} \) and \( \lambda + Z_{pa} \) are finite sets of equal size, and \( \sigma \) is a permutation of \( \mathbb{Z}_n \), we have \( \sigma(x + Z_{pa}) = \lambda + Z_{pa} \).

Next, suppose that \( j \neq a \). Consider any \( w \in x + Z_{pj} \). Then \( \sigma(w)_i = w_i \) for \( i \neq a \) and \( \sigma(w)_a = \sigma'(w_a) \). Let \( \lambda_i = x_i \) for \( i \neq a \) and \( \lambda_a = \sigma'(w_a) \). Then \( \sigma(w) \in \lambda + Z_{pj} \). Thus, \( \sigma(x + Z_{pj}) \subseteq \lambda + Z_{pj} \). Since these are cosets of equal size and \( \sigma \) is permutation, we have \( \sigma(x + Z_{pj}) = \lambda + Z_{pj} \). By Lemma 3.1.5, \( \sigma \) preserves (quasi-)independence.

\[ \square \]

\textbf{Proof of Theorem 3.1.2 (2).} Let \( F \subset \mathbb{Z}_n \). We shall prove that if \( F \) is not (quasi-)independent, then \( \sigma(F) \) is not. This will suffice to show that \( F \) is (quasi-)independent if and only if \( \sigma(F) \) is (quasi-)independent, because \( \sigma^{-1} \) satisfies the same hypotheses as does \( \sigma \).

Suppose first that \( F \) contains a full coset of \( \mathbb{Z}_2 \). Then of course, since \( \sigma \) preserves the cosets of \( \mathbb{Z}_2 \), \( \sigma(F) \) contains the same coset of \( \mathbb{Z}_2 \) and hence is not quasi-independent (and hence not independent).

So we may assume that \( F \) intersects each coset of \( \mathbb{Z}_2 \) in at most one point. Let \( f \) be a nontrivial relation that is supported on \( F \) with the
appropriate range. Let \( h \) be defined as follows:
\[
h = f - \sum_{x \in F, \sigma(x) \neq x} f(x)g_x
\]
where \( g_x \) is the characteristic function of \( x + Z_2 \). By Corollary 1.2.2, each \( g_x \) is a relation. Since \( f \) is a relation, so is \( h \).

We shall prove that \( h \) is supported on \( \sigma(F) \) and has the appropriate range. To do that, let \( t \in Z_n \). Suppose first that \( t + Z_2 \) does not intersect \( F \). Then \( t \) and \( \sigma(t) \) are not in \( F \). So \( f(t) = 0 \) and \( g_x(t) = 0 \) for \( x \) in the sum above. So \( h(t) = 0 \).

Next suppose that \( t + Z_2 \) does intersect \( F \) and that \( t \in F \). If \( \sigma(t) = t \), then each \( g_x \) in the sum above is 0 at \( t \) (distinct \( x \) in \( F \) have disjoint cosets of \( Z_2 \), since \( F \) meets each coset at most once). Then \( h(t) = f(t) \) with \( \sigma(t) = t \). So \( t \in \sigma(F) \), and \( h(t) \) has a value from the range of \( f \). If \( \sigma(t) \neq t \), then \( h(t) = f(t) - f(t)g_t(t) = 0 \).

Finally, suppose that \( t + Z_2 \) does intersect \( F \) but \( t \notin F \). Then \( f(t) = 0 \). Let \( w \in t + Z_2 \) with \( w \neq t \). We have \( w \in F \). If \( \sigma(w) = w \), then \( g_x(t) = 0 \) for each \( g_x \) in the sum above (distinct \( x \) in \( F \) have non-overlapping cosets of \( Z_2 \)). Hence \( h(t) = 0 \). If \( \sigma(w) \neq w \), then \( \sigma(w) = t \) and \( t \in \sigma(F) \). Then
\[
h(t) = f(t) - f(w)g_w(t) = 0 - f(w) \cdot 1 = -f(w).
\]
Thus \( t \in \sigma(F) \) and the value of \( h(t) \) is in \( \{0, \pm 1\} \) if \( f \) is a quasi-relation, and in \( \mathbb{Q} \) generally.

Finally, we need to observe that \( h \) is nontrivial. Since \( f \) is nontrivial, there is some \( x \in F \) such that \( f(x) \neq 0 \). If \( \sigma(x) = x \), then \( x \in \sigma(F) \) and (as noted above) \( h(x) = f(x) \neq 0 \). Suppose instead that \( \sigma(x) \neq x \). Let \( t = \sigma(x) \). Then \( \sigma(t) = x \) and \( t \notin F \). As noted above, \( h(t) = -f(x) \neq 0 \).

Proof of Theorem 3.1.2. (3)-(6). (3) is immediate from Theorem 2.1.1.
(4) is immediate from (1) and Theorem 2.1.1.
(5) is immediate. Also, (6) follows immediately from (1) and (5).

Proof of Theorem 3.1.2. (7), \( n \) square-free. If \( K = 1 \), there is nothing to prove, by Theorem 3.1.2 (1). So assume \( K \geq 2 \). We will have four steps. For all of them, we may assume (by composing \( \sigma \) with a translation) that \( \sigma(0) = 0 \).

(i) Reduction to \( n \) is odd. Let \( H_1 = \{0\} \times Z_{p_2} \times \cdots \times Z_{p_n} \). Suppose that \( p_1 = 2 \). We define a permutation \( \tau \) of \( Z_n \) as follows. Consider a coset \( C = \{0, 1\} \times \{a\} \) of \( Z_2 \) with \( a \in H_1 \). Then \( \sigma(C) = Z_2 \times \{b\} \).
for some $b \in H$. Otherwise $\sigma$ would map the two element non-quasi-independent coset to an independent two element set. If $\sigma(0,a) = (0,b)$, we define $\tau(0,b) = (0,b)$ and $\tau(1,b) = (1,b)$. Otherwise we define $\tau(0,b) = (1,b)$ and $\tau(1,b) = (0,b)$. Proceeding in this way, we define $\tau$. It’s clear that $\tau$ maps cosets of $Z_2$ to themselves, and that $\tau \circ \sigma$ is the product of the identity function on $Z_2$ and some permutation on $H_1$. It’s also clear that $\tau \circ \sigma$ preserves (quasi-)independent sets, by Theorem 3.1.2 (2) applied to $\tau$. We thus may assume that $\sigma$ maps $H_1$ into itself. We have reduced to the case that $\sigma$ does not change the $Z_2$–coordinate of elements of $Z_n$: that is, we have reduced to the case of $H_1$, and we have begun our induction (reducing $K$ by 1) in this case (that $p_1 = 2$). We have also reduced to the case of odd $n$ (still assumed to be square-free).

For the remaining steps, we define $H = Z_{p_1} \times \cdots \times Z_{p_K-1}$.

(ii) $\sigma$ maps each coset of $H$ into another (or the same) coset of $H$. We begin with consideration of $Z_{p_1}$. Since $\sigma(0) = 0$, Proposition 2.1.8 (2) tells us that $\sigma(Z_{p_1}) = Z_{p_1}$ because $\sigma(Z_{p_1})$ is a coset of $Z_{p_1}$ containing 0. Hence, $\sigma$ maps $Z_{p_1}$ (which is contained in $H$) into $H$. Let $1 \leq j < K$ and consider any coset $F$ of $Z_{p_j}$. Then $F$ is entirely contained in a coset of $H$. Suppose that $E = \sigma(F)$ meets two different cosets of $H$. Since $H$ has $p_K > p_j$ cosets, $E$ must miss at least one coset of $H$. Therefore, for $E$ to non (quasi-)independent (which it is, since $\sigma$ preserves the non (quasi-)independent sets), the intersection of $E$ with a coset of $H$ must be non (quasi-)independent by Corollary 2.1.3. Since $E$ is presumed to meet at least 2 cosets of $H$, there is a proper subset $E'$ which is not (quasi-)independent. Hence $\sigma^{-1}(E')$ is a proper subset of $F$ which is not (quasi-)independent. But $F$ is a coset of $Z_{p_j}$, so every proper subset of $F$ is independent. This contradiction shows that $\sigma(F)$ is entirely contained in one coset of $H$.

Now let $m \in Z_{p_K}$ and $a, b \in H \times \{m\}$. Then there exists a “path” from $a$ to $b$ via cosets of the $Z_{p_j}, 1 \leq j < K$. That is, there exists a finite set of cosets $F_1, \ldots, F_s$ such that $a \in F_1, b \in F_s, F_i \cap F_{i+1} \neq \emptyset, 1 \leq i < s$ and each $F_i$ is a coset of one of $Z_{p_j}, 1 \leq j < K$. By the preceding paragraph, there exists $\ell$ such that $\sigma(F_j) \subset H \times \{\ell\}$ for all $j$. Therefore, $\sigma(H \times \{m\}) \subset H \times \{\ell\}$. By cardinality, the last containment is an equality.

In the case of $H$ itself, because $\sigma(0) = 0$, we see that $\sigma(H) = H$. By composing $\sigma$ with a permutation of $Z_{p_K}$ that leaves 0 fixed, we may assume that

$$\sigma(H \times \{\ell\}) = H \times \{\ell\}$$

for all $\ell$. 

(iii) \( \sigma \) maps each coset of \( Z_{pK} \) to another coset (or the same) of \( Z_{pK} \). Let \( F \) be a coset of \( Z_{pK} \). Suppose that \( E = \sigma(F) \) is not a coset of \( Z_{pK} \). There are two ways this might occur. First, that \( E \) does not meet all cosets of \( H \). Or, secondly, that \( E \) meets all cosets of \( H \), but nevertheless, \( E \) is not a coset of \( Z_{pK} \). Now, if \( E \) did not meet all cosets of \( H \), then two elements of \( F \) would be mapped into the same coset of \( H \). Since different elements of \( F \) belong to different cosets of \( H \), that’s impossible, by Step (ii). Therefore, \( E \) meets every coset of \( H \). Since \( F \) is not independent, \( E = \sigma(F) \) is not independent. By Remark 2.1.5, \( E \) is a coset of \( Z_{pK} \).

(iv). \( \sigma \) factors. We have already shown that \( \sigma \) maps cosets of \( Z_{pK} \) onto cosets of \( Z_{pK} \).

It now follows that \( \sigma \) is (reduced to) a product of a permutation on \( H \) with the identity permutation of \( Z_{pK} \). That shows that \( \sigma \) is (now) determined by what it does on \( H \): that is, we have eliminated the factor \( Z_{pK} \). In other words, we have reduced \( K \) by one. By induction, we may assume that \( K = 1 \), which case has been taken care of.

That completes the proof of Theorem 3.1.2 (7) in the case that \( n \) is square free. \( \square \)

Proof of Theorem 3.1.2 (7): General case. By applying a translation, we see that we may assume that \( \sigma(0) = 0 \), as in the square free case. We claim that \( \sigma \) maps each coset of \( Z_{\tilde{n}} \) onto another (or the same) coset of \( Z_{\tilde{n}} \). Indeed, suppose first that \( F \) is a coset of some \( Z_{p_j} \), \( 1 \leq j \leq K \), and that \( E = \sigma(F) \). If \( E \) is not entirely contained in one coset of \( Z_{\tilde{n}} \), then one of the intersections of \( E \) with a coset of \( Z_{\tilde{n}} \) would not be (quasi-)independent, by Theorem 2.1.1. But that intersection has cardinality less than \( p_j \), so is independent, since \( \sigma \) preserves (quasi-)independence. By using the path argument of the square-free case, we see that \( \sigma \) maps cosets of \( Z_{\tilde{n}} \) onto cosets of \( Z_{\tilde{n}} \). By applying Theorem 3.1.2 (3), we may assume that \( \sigma \) maps each coset of \( Z_{\tilde{n}} \) onto itself.

Now the proof for the case of square free \( n \), applied to each coset of \( Z_{\tilde{n}} \), shows that \( \sigma \) has the required form on each coset of \( Z_{\tilde{n}} \), and thus completes the proof of Theorem 3.1.2 (7). \( \square \)

4. QUASI-INDEPENDENT SET EXTENSION & \( \Psi \)'S MONOTONICITY

4.1. An extension theorem. Before proving Theorem 1.2.2, we need an extension theorem. It shows one way to construct new quasi-independent sets from old ones, leading to estimates for \( \Psi(n) \).

Theorem 4.1.1. Let \( n > 1 \) be square-free, with prime factors \( p_1 < p_2 < \ldots < p_K \). Let \( s \in \{1, \ldots, K\} \). If \( s = K \), let \( q \) be any prime
such that \( q > p_K \). If \( s < K \), let \( q \) be any prime such that \( p_s < q \) and \( q \notin \{ p_{s+1}, \ldots, p_K \} \). Let \( m = n/p_s \) and identify \( Z_n \) with \( Z_{p_s} \times Z_m \); also, identify \( Z_{q m} \) with \( Z_q \times Z_m \). Let \( \lambda \) be the identity embedding of \( Z_n \) into \( Z_{q m} \) under the identifications \( \lambda(k, w) = (k, w) \) for \( 0 \leq k < p_s < q \) and \( w \in Z_m \). Let \( m = n/p_s \) and identify \( Z_n \) with \( Z_{p_s} \times Z_m \); also, identify \( Z_{q m} \) with \( Z_q \times Z_m \). Let \( \lambda \) be the identity embedding of \( Z_n \) into \( Z_{q m} \) under the identifications \( \lambda(k, w) = (k, w) \) for \( 0 \leq k < p_s < q \) and \( w \in Z_m \). Let \( E \) be quasi-independent in \( Z_n \). Choose \( F \subseteq Z_{q m} \) so that

1. \( F \cap (k + Z_m) = \emptyset \) for \( k \in Z_{p_s} \).
2. For \( k \geq p_s \) in \( Z_q \), \( F \cap (k + Z_m) \) is a quasi-independent set of maximum size \( \Psi(m) \).

Then \( \lambda(E) \cup F \) (or, more simply, just \( E \cup F \)) is quasi-independent in \( Z_{q m} \).

Proof. In \( \mathbb{Q}[Z_{q m}] \), we use the following basis for the kernel of \( \psi \):

1. All characteristic functions of cosets of \( Z_q \).
2. Any fixed set \( B_0 = \{ E_j \} \) of cosets of subgroups of \( Z_m \) such that \( \{ \chi_{E_j} \} \) spans \( \ker \psi|_{Z_m} \).

Then \( \bigcup_{1 \leq h < q} B_0 + h \) (together with the cosets of \( Z_q \)) will span the kernel of \( \psi \). That is possible by Lemma 2.1.2.

Suppose that \( f \) were a quasirelation supported on \( R = \lambda(E) \cup F \). Then for some rational numbers \( a_t \) and \( b_{h,j} \), \( f = \sum_{t \in Z_{p_s}} a_t \chi_{t + Z_{p_s}} + \sum_{0 < h < q} b_{h,j} \chi_{E_j + h} \). Let \( g = \sum_{t \in Z_{p_s}} a_t \chi_{t + Z_{p_s}} + \sum_{0 < h < p} b_{h,j} \chi_{E_j + h} \in \mathbb{Q}[Z_n] \).

Note that \( f \) restricted to \( Z_n \) is \( g \), so \( g \) is a quasirelation supported on \( R \cap Z_n = E \): that is, \( g = 0 \). In particular, \( a_t = 0 \) for all \( t \in Z_{p_s} \). Therefore \( f = \sum_{0 < h < q} b_{h,j} \chi_{E_j + h} \). Fix \( h \in Z_q, h > 0 \). Then the restriction of \( f \) to the coset \( h + Z_m \) of \( Z_m \) is a quasirelation supported on the quasi-independent set \( R \cap (h + Z_m) \). Therefore, \( \sum_{j} b_{h,j} \chi_{E_j + h} = 0 \) and so \( f = 0 \). Therefore \( R \) is quasi-independent.

4.2. Proof of Theorem 1.2.2.

Proof of (1). The special case of the assertion for \( s = K = 3 \) appears as [4, Lemma 7.1]. The proof there generalizes without difficulty to the general case here.

Proof of (2). Let \( E \) be a quasi-independent set such that \( \#(E) = \phi(n) + \Delta \).
We induce an imbedding of $\mathbb{Z}_n$ into $\mathbb{Z}_{qn/p}$ from the following “lattice” imbedding: let $\lambda$ be the mapping of $\mathbb{Z}_p^s \times \prod_{j \in D \setminus \{s\}} \mathbb{Z}_{p_j}$ into $\mathbb{Z}_q \times \prod_{j \in D \setminus \{s\}} \mathbb{Z}_{p_j}$ literally (let it be the identity mapping at the level of the coordinates of vectors). Let $E^* = \lambda(E) \cup F$ where $F$ is an arbitrary choice in the cosets $w + T_m$, for $p_s \leq w < q$ and $w \in \mathbb{Z}_q$, of a quasi-independent set of size $\phi(m)$. (The idea of [4, 1.7.1] suggests this approach.)

We claim that $E^*$ has the correct cardinality, and is quasi-independent. For the cardinality, we compute:

$$\#(E^*) = \#(E) + (q - p_s)\phi(m) = \phi(mp^s) + \Delta + (q - p_s)\phi(m)$$

$$= (p_s - 1)\phi(m) + (q - p_s)\phi(m) + \Delta = \phi(qm) + \Delta$$

$$= \phi(nq/p^s) + \Delta.$$

To see that $E^*$ is quasi-independent, apply Theorem 4.1.1. □

4.3. Beyond 105 and 15p. In [4, Thm. 7.4] it was shown that $\Psi(105) = \phi(105) + 4 = 52$ and that $\Psi(15p) = \phi(15p) + 4$ for all primes $7 \leq p$.

We can extend those results to larger prime factors.

**Proposition 4.3.1.** Let $n > 1$ be odd with at least three odd prime factors. Then $\Psi(n) \geq \phi(n) + 4$.

**Proof.** For $n = 15p$ ($p \geq 7$), $\Psi(n) = \phi(n) + 4$ by [?, Thm. 4.4]. Now apply Theorem 1.2.2 (1) to obtain $\Psi(n) \geq \phi(n) + 4$ for all $n$ the product of three distinct, odd, prime factors. For square free $n$, we apply Corollary 2.1.4, noting that $\phi(nq) = (q - 1)\phi(n)$ holds under the hypotheses of Corollary 2.1.4. Now an application of Theorem 2.1.6 (1) completes the proof. □
Corollary 4.3.2. (1) For all odd primes $p < q < r$, $\Psi(pqr) \geq \phi(pqr) + 4$.
(2) For all odd primes $p < q < r$ with $5 < q$, $\Psi(pqr) \geq \phi(pqr) + 5$.

Proof. We begin with the equality $\phi(15p) + 4 = \Psi(15p)$ [?, Thm. 7.4]. Then (1) follows from that and Theorem 1.2.2.
(2) follows from Proposition 4.3.3 and Theorem 1.2.2. □

The time and space complexity of the computation of $\Psi$ grows super exponentially with $n$. However, to get lower bounds, there is a somewhat simpler approach.

Let $n_1, \ldots, n_k \geq 2$ be integers. Consider the finite abelian group $G = Z_{n_1} \times \cdots \times Z_{n_k}$. We identify $Z_{n_i}$ with its image $\{0\} \times \cdots \times \{0\} \times Z_{n_i} \times \{0\} \cdots$ in $G$. A relation on $G$ is a sum, with integer coefficients, of characteristic functions of certain cosets of $Z_{n_i}$. Note that if $Z_{n_i}$ contains a subgroup isomorphic to $Z_{n_j}$, we do not include characteristic function of that subgroup. The cosets we do include are all and only those of the form $x_1 \times \cdots \times x_{j-1} \times Z_{n_j} \times x_{j+1} \cdots$. That is, we move layers (the $Z_{n_i}$) around, but we do not do pick up a coset inside a layer. A quasi-relation is a relation that takes on only the values $\pm 1$ and 0. A subset of $G$ is (quasi-)independent iff it does not support a (quasi-)relation.

It is then not hard to see that Theorem 3.1.2 (1)-(4) extend to this context, as does Theorem 1.2.2.

Proposition 4.3.3. $\Psi(231) \geq \phi(231) + 5$.

Proof. First, $231 = 3 \cdot 7 \cdot 11$. Then the proof is immediate from the extended monotonicity theorem which tells us that $\Psi(231) \geq \phi(231) + 5$ follows from $\Psi(3 \cdot 6 \cdot 9) \geq (3-1)(6-1)(9-1) + 5$, and that inequality is the assertion of the next example. □

An Example of $\Psi - \phi = 5$ in the $3 \times 6 \times 9$ lattice: the following example has been verified by two independent computer programs. It is organized by horizontal layers (9 of them), of sizes 9, 9, 9, 9, 10, 10, 10 and 10. This totals to 85 elements, 5 more than $2(5)(8)$. By layers we have

\[
\begin{align*}
\{1, 2, 3, 4, 7, 8, 9, 11, 18\} & \quad \{1, 3, 8, 10, 12, 13, 14, 15, 17, 18\} + 18 \\
\{3, 4, 5, 6, 8, 9, 10, 11, 13\} + 36 & \quad \{2, 3, 8, 9, 10, 11, 12, 13, 16, 17\} + 54 \\
\{1, 3, 4, 6, 9, 10, 11, 12, 14\} + 72 & \quad \{1, 2, 3, 4, 5, 7, 8, 12, 15, 17\} + 90 \\
\{1, 3, 5, 6, 7, 8, 11, 12, 16\} + 108 & \quad \{2, 3, 4, 5, 6, 7, 9, 11, 14, 1\} + 126 \\
\{1, 2, 4, 5, 7, 8, 9, 10, 18\} + 144 &
\end{align*}
\]
Whether \(\Psi(n) - \phi(n)\) is unbounded we do not know (even for \(n\) the product of 3 primes), much less whether \(\Psi(n)/\phi(n)\) is unbounded.

When \(p = 11\), \(4 + \phi(3 \cdot 5 \cdot 11) = 84 > 165/2\). Likewise, when \(p = 13\) \(4 + \phi(3 \cdot 5 \cdot 13) = 100 > 195/2\). So, it is possible that \(Z_{165}\) and \(Z_{195}\) are the unions of two quasi-independent sets. Whether this is so seems to require (nearly) maximal quasi-independent sets that are nearly disjoint. See [4, Prop. 7.5] for a related result.

**References**

[1] Jean Bourgain, *Sidon sets and Riesz products.*, Ann. Inst. Fourier (Grenoble), 35 (1985, no. 1) 137-148.

[2] Colin C. Graham and O. Carruth McGehee, *Essays in Commutative Harmonic Analysis*, Springer-Verlag, New York, (1979).

[3] Gilles Pisier, *Arithmetic Characterizations of Sidon Sets*, Bull. Amer. Math. Soc., 8 (1983), 87-89.

[4] L. Thomas Ramsey and Colin C. Graham, *Planar Sidonicity and quasi-independent for multiplicative subgroups of the roots of unity*, Pacific J. Math., (2006), to appear.

[5] Walter Rudin, *Fourier Analysis on Groups*, Wiley Interscience, New York, (1962).

Department of Mathematics, University of Hawaii, Keller Hall, 2565 The Mall, Honolulu, Hawaii, 96822, email: ramseymath.hawaii.edu

University of British Columbia. Mailing address: RR#1–H-46, Bowen Island, BC, V0N 1G0 Canada. email: ccgraham@alum.mit.edu