Quasiperiodic group factorizations

John P. Steinberger
Department of Mathematics, UC Davis
jpsteinb@math.ucdavis.edu
January 6, 2006

Abstract

The study of group factorizations originates with Hajós’s [4] famed solution to Minkowski’s cube tiling problem (whereby in any lattice cube tiling two cubes must share a face), see [14]. In the general setting, if \( \mathcal{R} \) is any ring or semi-ring (e.g. \( \mathbb{Z}_+ \)) and \( G \) is a finite abelian group, two elements \( a, b \) of the group (semi-)ring \( \mathcal{R}[G] \) are said to form a factorization of \( G \) if \( ab = r \sum_{g \in G} g \) for some \( r \in \mathcal{R} \). Hajós conjectured that all group factorizations with \( \mathcal{R} = \mathbb{Z}_+ \) and \( r = 1 \) are so-called “quasiperiodic”, meaning that there is some element \( g \in G \) of order \( m > 1 \) such that either \( a \) or \( b \)—say \( b \)—can be written as a sum \( b_0 + \ldots + b_{m-1} \) of \( m \) elements of \( \mathcal{R}[G] \) such that \( ab_h = g^h ab_0 \) for \( h = 0, \ldots, m - 1 \), but in 1974 Sands [12] found a counterexample for the group \( G = \mathbb{Z}_5 \times \mathbb{Z}_{25} \). Here we show that all factorizations of abelian groups are quasiperiodic when \( \mathcal{R} = \mathbb{Q} \) and that all factorizations of cyclic groups or of groups of the type \( \mathbb{Z}_p \times \mathbb{Z}_p \) are quasiperiodic when \( \mathcal{R} = \mathbb{Z} \) (in fact, we conjecture that all abelian group factorizations are quasiperiodic for \( \mathcal{R} = \mathbb{Z} \)). We also give some new examples of non-quasiperiodic factorizations with \( \mathcal{R} = \mathbb{Z}_+ \) for the groups \( G = \mathbb{Z}_5 \times \mathbb{Z}_5 \) and \( G = \mathbb{Z}_{35} \).

Introduction

Let \( \mathcal{R} \) be any ring (e.g. \( \mathbb{Z}, \mathbb{Q} \)) or semi-ring (e.g. \( \mathbb{Z}_+ = \{0, 1, 2, \ldots\} \)) and let \( G \) be a finite abelian group. Two elements \( a, b \) of the group (semi-)ring \( \mathcal{R}[G] \) are said to factorize \( G \) if \( ab = r \sum_{g \in G} g \) for some \( r \in \mathcal{R} \). We also say that the pair \( (a, b) \) forms a level \( r \) factorization of \( G \) (over \( \mathcal{R} \)).

When \( \mathcal{R} = \mathbb{Z}_+ \) and \( a, b \) are respectively of the form \( \sum_{g \in A} g, \sum_{g \in B} g \) for some subsets \( A, B \) of \( G \) then the pair \( (a, b) \) forms a level 1 factorization of \( G \) if and only if the sets \( \{gA : g \in B\} \) partition \( G \) (or vice-versa for the sets \( \{gB : g \in A\} \)). In this specific case, thus, one can interpret the set \( B \) as a set of positions for translates of the set \( A \) such that the union of all translates tiles \( G \) uniformly. Moreover if \( G = \mathbb{Z}_n \) is cyclic then \( (A, B + n\mathbb{Z}) \) factorizes \( \mathbb{Z} \), meaning that \( (A, B) \) encodes a tiling of the integers by translates of the set \( A \) (it also turns out that every tiling of the integers by translates of a finite set \( A \) reduces to a cyclic group factorization, because all tilings of the integers are periodic [5, 7]). Factorizations of this type have been rather extensively studied, see [2, 3, 14, 17, 18] for some additional references.

An element \( a \in \mathcal{R}[G] \) is called periodic if there is some nonzero element \( g \in G \) such that \( ga = a \). A factorization \( (a, b) \) of \( G \) is periodic if either \( a \) or \( b \) are periodic. For an example of a non-periodic level 1 factorization over \( \mathbb{Z}_+ \) take \( G = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \) with generators \( i, j, k \) and let
Figure 1: Translates of \((\mathbb{Z}_2)^3\) arranged in a non-periodic factorization of \((\mathbb{Z}_4)^3\). The two drawings represent the same arrangement of translates viewed from different angles. Certain translates wrap around from one side of \((\mathbb{Z}_4)^3\) to the other.

Figure 2: A partition into two sets of the translates of \((\mathbb{Z}_2)^3\) used in the Fig. 1 factorization of \((\mathbb{Z}_4)^3\) such that the unions of the translates in each set are translates of each other.

\[ a = (1+i)(1+j)(1+k), \quad b = 1 + ij^2 + i^2j^2 + jk^2 + j^2k^2 + i^2k^2 + i^2j^2k^2. \]  This factorization is pictured in Fig. 1. It is due to S. Szabó [15].

Even though the Fig. 1 factorization is non-periodic one can partition the eight translates of \(a\) into two groups of four that such that, upon taking the union of the translates in each group, we obtain two sets that are translates of each other (this operation is shown in Fig. 2). In other words, the non-periodic factorization \((a, b)\) of \(G\) is a “refinement” of the periodic factorization \((a', b')\) where \(a' = (1+i)(1+j)(1+k)(1+j^3k^2 + i^2k + i^2k^3)\), \(b' = 1 + j^2\). A factorization which is a refinement of a periodic factorization in the above sense is called \textit{quasiperiodic}. More formally, a factorization \((a, b)\) of a group \(G\) over \(\mathcal{R}\) is quasiperiodic if there is some element \(g \in G\) of order \(m > 1\) such that either \(a\) or \(b\)—say \(b\)—can be written as a sum \(b_0 + \ldots + b_{m-1}\) of \(m\) elements of \(\mathcal{R}[G]\) such that \(ab_h = g^h ab_0\) for \(h = 0, \ldots, n-1\) (the above example is thus shown to be quasiperiodic by taking \(g = j^2\), \(m = 2\), \(b_0 = 1 + j^3k^2 + i^2k + i^2k^3\), \(b_1 = jk^2 + ij^2 + i^3j^2 + i^2j^2k^2\)).

Hajós [4] conjectured that all level 1 factorizations over \(\mathbb{Z}_4\) are quasiperiodic but A.D. Sands [12] found a counterexample in the group \(G = \mathbb{Z}_3 \times \mathbb{Z}_{25}\) (Sands’ construction extends more generally to all groups of the type \(\mathbb{Z}_p \times \mathbb{Z}_{p^2}\) for \(p\) a prime \(\geq 5\)). See Fig. 3. On the other hand deBruijn [1] (nearly)
showed that all level 1 factorizations over \( \mathbb{Z} \) of cyclic groups of squarefree order are quasiperiodic (see Theorem 3). In this paper we continue deBruijn’s work by showing that all factorizations over \( \mathbb{Z} \) of cyclic groups and of groups of the type \( \mathbb{Z}_p \times \mathbb{Z}_p \) are quasiperiodic, as well as by showing that all factorizations over \( \mathbb{Q} \) of all abelian groups are quasiperiodic. We also give some new examples of non-quasiperiodic factorizations over \( \mathbb{Z}_+ \), including the first example of a non-quasiperiodic factorization of a cyclic group (our examples of non-quasiperiodic factorizations, however, have levels greater than 1, unlike Sands’ example).

Szabó [16] has recently found some new level 1 factorizations that are non-quasiperiodic over \( \mathbb{Z}_+ \) for groups of the type \( \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \) and \( \mathbb{Z}_p \times \mathbb{Z}_{p^3} \) (\( p \) an odd prime). In the same note, Szabó also shows that all level 1 factorizations over \( \mathbb{Z}_+ \) of groups of the type \( \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q, \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r \times \mathbb{Z}_s \times \mathbb{Z}_t \) (\( p, q, r, s, t \) distinct primes) as well as of the group \( \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \) are quasiperiodic.

The main open problem, at this point, seems to determine whether all abelian group factorizations are quasiperiodic over \( \mathbb{Z} \) (Sands’ example is quasiperiodic over \( \mathbb{Z} \) despite being non-quasiperiodic over \( \mathbb{Z}_+ \), as shown below). We conjecture this is the case, and that something even stronger is true (Conjecture 1). It also remains open whether all level 1 factorizations of cyclic groups over \( \mathbb{Z}_+ \) are quasiperiodic, which is the setting relevant to translational tilings of the integers.

**Basics; factorizations over \( \mathbb{Q} \)**

We will exclude the trivial group from our discussions since the trivial group contains no elements of order \( > 1 \), so that no factorization of the trivial group can be either periodic or quasiperiodic. The term “abelian group” may thus be more accurately replaced by “nontrivial abelian group” and even more precisely by “finite nontrivial abelian group” wherever it appears.

To refine our terminology we say that a factorization \((a, b)\) over \( \mathcal{R} \) of \( G \) is \( g \)-right-quasiperiodic where \( g \in G \) is an element of order \( m > 1 \) if there exist \( b_0, \ldots, b_{m-1} \in \mathcal{R}[G] \) such that \( b_0 + \ldots +
$b_{m-1} = b$ and $ab_h = g^h ab_0$ for $0 \leq h \leq m - 1$; similarly we say that $(a, b)$ is $g$-left-quasiperiodic if there exist $a_0, \ldots, a_{m-1} \in \mathcal{R}[G]$ such that $a_0 + \ldots + a_{m-1} = a$ and $ba_h = g^h ba_0$ for $0 \leq h \leq m - 1$. We say that $(a, b)$ is “$g$-quasiperiodic” if it is either $g$-right-quasiperiodic or $g$-left-quasiperiodic, and we also say that $(a, b)$ is right-quasiperiodic (resp. left-quasiperiodic) if there is some $g \in G$ of order $> 1$ such that $(a, b)$ is $g$-right-quasiperiodic (resp. $g$-left-quasiperiodic). We finally say that a group ring element $a$ is $g$-periodic if $a = ga$. Obviously, if $b$ is $g$-periodic for some $g$ of order $> 1$ then $(a, b)$ is $g$-right-quasiperiodic.

We will frequently identify the group ring $\mathcal{R}[G]$ where $G = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ is any (nontrivial) finite abelian group with the polynomial ring $\mathcal{R}[x_1, \ldots, x_k]/\langle 1 - x_{1}^{n_1}, \ldots, 1 - x_{k}^{n_k} \rangle$. The exact representation of $G$ as a direct product of cyclic groups will not matter to us, as long as we can assume it remains fixed. Then the group ring elements $a$ and $b$ become polynomials $a(x_1, \ldots, x_k)$, $b(x_1, \ldots, x_k)$ in $\mathcal{R}[x_1, \ldots, x_k]/\langle 1 - x_{1}^{n_1}, \ldots, 1 - x_{k}^{n_k} \rangle$. We will switch without notice between considering $a$ and $b$ as group ring elements and as polynomials, which should not cause much confusion as the two structures are isomorphic anyway.

Multiplication between polynomials in $\mathcal{R}[x_1, \ldots, x_k]/\langle 1 - x_{1}^{n_1}, \ldots, 1 - x_{k}^{n_k} \rangle$ is automatically taken mod $(1 - x_{1}^{n_1}, \ldots, 1 - x_{k}^{n_k})$, which allows us to forgo the $\equiv$ sign in favor of the $=$ sign. Under these notational conventions, $a, b \in \mathcal{R}[G]$ form a level $r$ factorization of $G$ if and only if

$$a(x_1, \ldots, x_k)b(x_1, \ldots, x_k) = r \prod_{i=1}^{k} (1 + x_i + x_i^2 + \ldots + x_i^{n_i-1}). \quad (1)$$

Let $\mu_n$ denote the group of $n$-th roots of unity in the complex plane under multiplication (so $\mu_n \cong \mathbb{Z}_n$). If $\mathcal{R} \subseteq \mathbb{C}$ (as we will always assume) then (1) tells us that every tuple $(\theta_1, \ldots, \theta_k) \in \mu_{n_1} \times \ldots \times \mu_{n_k}$ except for the tuple $(1, \ldots, 1)$ is either a root of $a(x_1, \ldots, x_k)$ or $b(x_1, \ldots, x_k)$. This is a necessary condition for the pair $(a, b)$ to form a factorization of $G$. Its sufficiency will be established as a corollary of the following proposition:

**Proposition 1.** Let $F$ be a field and let $I = \langle f_1, \ldots, f_k \rangle$ be an ideal in $F[x_1, \ldots, x_k]$ generated by polynomials $f_1 \in F[x_1], \ldots, f_k \in F[x_k]$ such that each $f_i$ has deg$(f_i)$ distinct roots in the algebraic closure $\overline{F}$ of $F$. Then if $g \in F[x_1, \ldots, x_k]$ has the property that $g(\theta_1, \ldots, \theta_k) = 0$ whenever $\theta_1, \ldots, \theta_k$ are roots of $f_1, \ldots, f_k$ respectively we have $g \equiv 0 \mod I$.

**Proof.** We do the proof by induction on $k$. Clearly, unique factorization in $\overline{F}[x_1]$ implies the proposition for $k = 1$. Assume now that $k \geq 2$. Let $f_k$ be of degree $n$. Assuming that $g$ is reduced mod $\langle f_k(x_k) \rangle$ we can write

$$g(x_1, \ldots, x_k) = g_{n-1}(x_1, \ldots, x_{k-1})x_k^{n-1} + \ldots + g_1(x_1, \ldots, x_{k-1})x_k + g_0(x_1, \ldots, x_{k-1})$$

for some polynomials $g_{n-1}, \ldots, g_0 \in F[x_1, \ldots, x_{k-1}]$. If $\theta_1, \ldots, \theta_k$ are any roots of $f_1, \ldots, f_{k-1}$ respectively then the polynomial $g(\theta_1, \ldots, \theta_{k-1}, x_k) \in F[x_k]$ has degree $n - 1$ but has $n$ distinct roots (namely the $n$ roots of $f_k$) so must be the zero polynomial. Therefore $g_i(\theta_1, \ldots, \theta_{k-1}) = 0$ for all $0 \leq i \leq n - 1$ whenever $\theta_1, \ldots, \theta_{k-1}$ are roots of $f_1, \ldots, f_{k-1}$ respectively. It follows by induction that $g_i \equiv 0 \mod \langle f_1, \ldots, f_{k-1} \rangle$ for all $0 \leq i \leq n - 1$ and thus that $g \equiv 0 \mod \langle f_1, \ldots, f_k \rangle$. \hfill $\square$
**Corollary 1.** Let $\mathcal{R} \subseteq \mathbb{C}$ and let $a, b \in \mathcal{R}[G]$ where $G = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$. Then $a, b$ factorize $G$ if and only if every tuple $(\theta_1, \ldots, \theta_k) \in \mu_{n_1} \times \ldots \times \mu_{n_k}$ besides $(1, \ldots, 1)$ is either a root of $a(x_1, \ldots, x_k)$ or of $b(x_1, \ldots, x_k)$.

**Proof.** The necessity of the condition is established by (1). Now say that every $(\theta_1, \ldots, \theta_k) \in \mu_{n_1} \times \ldots \times \mu_{n_k}$ besides $(1, \ldots, 1)$ is either a root of $a(x_1, \ldots, x_k)$ or $b(x_1, \ldots, x_k)$. Then every tuple $(\theta_1, \ldots, \theta_k) \in \mu_{n_1} \times \ldots \times \mu_{n_k}$ is a root of the polynomial $(1-x_1)a(x_1, \ldots, x_k)b(x_1, \ldots, x_k)$ which implies by Proposition 1 that $(1-x_1)a(x_1, \ldots, x_k)b(x_1, \ldots, x_k) = 0$ for $i = 1, \ldots, k$ (multiplication taken in $\mathcal{R}[x_1, \ldots, x_k]/(1-x^{n_1}, \ldots, 1-x^{n_k})$, as wont). This shows that the coefficients of the monomials $x_1^{a_1} \cdots x_k^{a_k}$ and $x_1^{a_1+1} \cdots x_k^{a_k}$ in $a(x_1, \ldots, x_k)b(x_1, \ldots, x_k)$ are equal (where the exponent of $x_1$ is taken mod $n_1$) and symmetrically for other indices. Thus

\[ a(x_1, \ldots, x_k)b(x_1, \ldots, x_k) = r \prod_{i=1}^{k} (1 + x_i + x_i^2 + \ldots + x_i^{n_i-1}). \tag{2} \]

for some $r \in \mathcal{R}$, as desired. \(\square\)

Proposition 1 can also be used to give the following handy criterion for showing that a factorization is quasiperiodic; here we assume that $\mathcal{R}$ is a ring, not a semi-ring.

**Proposition 2.** Let $\mathcal{R} \subseteq \mathbb{C}$ be a ring and let $a, b \in \mathcal{R}[G]$ factorize $G = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$. If there exists an element $b' \in \mathcal{R}[G]$ such that $(a, b')$ is a right-quasiperiodic factorization $G$ and such that $b'(1, \ldots, 1) = b(1, \ldots, 1)$ then $(a, b)$ is right-quasiperiodic.

**Proof.** Since $(a, b')$ is right-quasiperiodic there is some $g \in G$ of order $m > 1$ and elements $b'_0, \ldots, b'_{m-1} \in \mathcal{R}[G]$ such that $ab'_h = g^h ab'_0$ for $0 \leq h \leq m-1$. Let $b_h = b'_h$ for $1 \leq h \leq m-1$ and put $b_0 = b'_0 + b - b'$. Then $b_0 + \cdots + b_{m-1} = b$ and every tuple $(\theta_1, \ldots, \theta_k) \in \mu_{n_1} \times \ldots \times \mu_{n_k}$ is a root of $a(b - b')$ because $(1, \ldots, 1)$ is a root of $b - b'$ and $(a, b)$, $(a, b')$ are factorizations of $G$. Therefore $a(b - b') = 0$, and for $1 \leq h \leq m-1$ we have $ab_h = ab'_h = g^h ab'_0 = g^h (ab'_0 + (b - b')) = g^h ab_0$, as desired. \(\square\)

As an example of an application of Proposition 2 we may show that Sands’ factorization of Fig. 3 is quasiperiodic over $\mathbb{Z}$. Indeed letting $i, j$ denote the generators of $\mathbb{Z}_5 \times \mathbb{Z}_{25}$ where $i^5 = j^{20} = 1$, then it suffices to choose $b' = 1 + ij^5 + i^2 j^{10} + i^3 j^{15} + i^4 j^{20}$. It is readily seen that $b'$ fulfills all the criteria of Proposition 2, so that the factorization $(a, b)$ of Fig. 3 is quasiperiodic over $\mathbb{Z}$. Another nearly immediate consequence of Proposition 2 is that all factorizations are quasiperiodic over $\mathbb{Q}$:

**Theorem 1.** All abelian group factorizations are quasiperiodic over $\mathbb{Q}$.

**Proof.** Let $a, b \in \mathbb{Q}[G]$ be a factorization of $G = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$. Put $b' = (b(1, \ldots, 1)/|G|) \sum_{g \in G} g$. Then $b'(1, \ldots, 1) = b(1, \ldots, 1)$ and $b'$ is $g$-periodic for any $g \in G$ so $(a, b)$ is quasiperiodic over $\mathbb{Q}$ by Propoosition 2. \(\square\)

Theorem 1 could equally well be stated with $\mathbb{R}$ instead of $\mathbb{Q}$ or, indeed, with any subfield of $\mathbb{C}$ instead of $\mathbb{Q}$. We need a field, though, since we appeal to division by $|G|$ in order to define $b'$. On the other hand if $b(1, \ldots, 1) = 0$ then the division by $|G|$ is superfluous, which gives us the following corollary:
Corollary 2. If \( (a, b) \) is a factorization of \( G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \) over any ring \( \mathcal{R} \subseteq \mathbb{C} \) and either \( a(1, \ldots, 1) = 0 \) or \( b(1, \ldots, 1) = 0 \) then \( (a, b) \) is quasiperiodic.

It also follows from the proof of Theorem 1 that all abelian group factorizations over \( \mathbb{Q} \) are in fact both \( g \)-left-quasiperiodic and \( g \)-right-quasiperiodic for any nonidentity element \( g \), since no assumptions are made about \( b \) that are not made about \( a \). The freedom in the choice of \( g \) and the interchangeability between \( a \) and \( b \) disappear for factorizations over \( \mathbb{Z} \), as discussed below. Nonetheless other very striking symmetries, which are as yet unexplained, do occur for factorizations over \( \mathbb{Z} \) (see Theorems 2, 4, Figs. 7, 8 and Conjecture 1).

**Factorizations over \( \mathbb{Z} \)**

All factorizations discussed in this section are over \( \mathbb{Z} \); we sometimes remind so and sometimes not. We start with the following simple observation:

**Proposition 3.** If \( a(1, \ldots, 1) \neq 0 \) and \( g \) has order \( m \) then \( (a, b) \) cannot be \( g \)-right-quasiperiodic over \( \mathbb{Z} \) unless \( m \mid b(1, \ldots, 1) \).

**Proof.** If \( g^h b_0 = ab_h \) for \( 0 \leq h \leq m - 1 \) then \( a(1, \ldots, 1) \neq 0 \) implies \( b_0(1, \ldots, 1) = b_h(1, \ldots, 1) \) so \( mb_0(1, \ldots, 1) = b(1, \ldots, 1) \).

For example the factorization \((a, b)\) of \( G = \mathbb{Z}_4 \) where \( a(x) = 1 + x^2 \), \( b(x) = 1 + x \) is not \( \mathbb{g} \)-quasiperiodic when \( g \) is an element of order 4 since \( 4 \mid 2 \). The same factorization is in fact not right-quasiperiodic at all. It is not hard to convince oneself of this by simply staring at the factorization, but we will give a careful proof in order to illustrate a technique that will recur later.

Say that \((a, b) = (1 + x^2, 1 + x) \) is a \( g \)-right-quasiperiodic factorization of \( \mathbb{Z}_4 \). Then \( g = x^2 \) is the unique element of order 2 in \( \mathbb{Z}_4 \) and \( b = b_0 + b_1 \) for some \( b_0, b_1 \in \mathbb{Z}[\mathbb{Z}_4] \) such that \( x^2b_0 = ab_1 \), i.e. \( ab_0 = ab_1 \) (since \( x^2a = a \)). Put \( b_0(x) = u_{0,0} + u_{0,1}x + u_{0,2}x^2 + u_{0,3}x^3 \), \( b_1(x) = u_{1,0} + u_{1,1}x + u_{1,2}x^2 + u_{1,3}x^3 \). The two constraints \( b = b_0 + b_1 \) and \( ab_0 = ab_1 \) are represented by the linear system

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 \\
0 & 1 & 0 & 1 & 0 & -1 & 0 & -1 \\
0 & 0 & 1 & 0 & -1 & 0 & -1 & 0 \\
0 & 1 & 0 & 1 & 0 & -1 & 0 & -1
\end{bmatrix}
\begin{bmatrix}
[u_{0,0}] \\
[u_{0,1}] \\
[u_{0,2}] \\
[u_{0,3}] \\
[u_{1,0}] \\
[u_{1,1}] \\
[u_{1,2}] \\
[u_{1,3}]
\end{bmatrix}
= \begin{bmatrix}
1 \\
0 \\
0 \\
0 \\
0 \\
0 \\
0 \\
0
\end{bmatrix}
\]

where the first four rows imply \( b = b_0 + b_1 \) and the last four rows imply \( ab_0 = ab_1 \). Put \( M \) for the \( 8 \times 8 \) matrix above, \( u \) for the column vector \((u_{0,0}, \ldots, u_{0,3}, u_{1,0}, \ldots, u_{1,3})^T\) of size 8 and \( v \) for the column vector \((1, 1, 0, 0, 0, 0, 0, 0)^T\), so that the above linear system becomes \( Mu = v \). The factorization is not right-quasiperiodic over \( \mathbb{Z} \) if \( Mu = v \) has no integral solution \( u \). To show \( Mu = v \) has no integral solution \( u \) it is sufficient to exhibit a row vector \( y \) of size 8 such that \( yM \) is integral but \( yv \) is non-integral. In this case the reader can verify that the vector \( y = (\frac{1}{2}, 0, \frac{1}{2}, 0, \frac{1}{2}, 0, 0, 0) \) fits
these requirements, since $yv = \frac{1}{2}$ and $yM = (1, 0, 1, 0, 0, 0)$. Thus the factorization $(a, b)$ is not right-quasiperiodic. It should be noted that the system $Mu = v$ does admit a rational solution, which we know without having to solve it by Theorem 1.

We now move to the more general case when $G = \mathbb{Z}_n$ is a cyclic group. If $(a, b)$ is a factorization of $\mathbb{Z}_n$ then we have already noted that every $n$-th of unity except for the root ‘1’ is either a root of $a(x)$ or of $b(x)$. Another way to say this (and this follows from the irreducibility of the cyclotomic polynomial) is that for every divisor $d \neq 1$ of $n$ either $\Phi_d(x)|a(x)$ or $\Phi_d(x)||b(x)$ where $\Phi_d(x)$ is the $d$-th cyclotomic polynomial.

Let $D_n = \{d : d \neq 1, d|n\}$. If $A \subseteq D_n$ then we write $A|a$ if $d \in A \implies \Phi_d(x)|a(x)$. By the above remarks, if $(a, b)$ is any factorization of $\mathbb{Z}_n$ we can find a partition $(A, B)$ of $D_n$ such that $A|a$, $B|b$. It seems natural that we should focus on the underlying partition $(A, B)$ of $D_n$ instead of on the actual polynomials $a(x), b(x)$. In this vein we will say that a partition $(A, B)$ of $D_n$ is “quasiperiodic” if every factorization $(a, b)$ of $\mathbb{Z}_n$ such that $A|a$, $B|b$ is quasiperiodic. By extension, we say that a partition $(A, B)$ of $D_n$ is “right-quasiperiodic” if all factorizations $(a, b)$ of $\mathbb{Z}_n$ such that $A|a$, $B|b$ are right-quasiperiodic, and so forth for left-quasiperiodic, $g$-left-quasiperiodic and $g$-right-quasiperiodic factorizations.

Our results on factorizations of cyclic groups over $\mathbb{Z}$ are summarized by the following theorem:

**Theorem 2.** Let $G$ be a cyclic group of order $n$ and let $g \in G$ be an element of prime order $p$. Then a partition $(A, B)$ of $D_n$ is $g$-right-quasiperiodic over $\mathbb{Z}$ if and only if $p^\alpha \in B$, where $p^\alpha$ is the largest power of $p$ dividing $n$.

For example the factorization $(1 + x^2, 1 + x)$ of $\mathbb{Z}_4$ is not $g$-right-quasiperiodic for $g$ an element of order 2 (as already shown) since $\Phi_4(x) = 1 + x^2 \not| 1 + x$.

It follows from Theorem 2 that for every $g \in G = \mathbb{Z}_n$ of prime order and every partition $(A, B)$ of $D_n$ either $(A, B)$ or $(B, A)$ is $g$-right-quasiperiodic, but not both. In particular, every partition $(A, B)$ is quasiperiodic and every factorization $(a, b)$ of $G$ is quasiperiodic. DeBruijn [1] proved a weaker version of the “backward” direction of Theorem 2:

**Theorem 3.** (deBruijn [1]) If $(a, b)$ is a level 1 factorization of a cyclic group $G$ of squarefree order $n$ such that $\Phi_n(x)|b(x)$ and $b(1) > 1$, then there is a prime $p$ dividing $n$ such that $(a, b)$ is $g$-right-quasiperiodic over $\mathbb{Z}$ for $g$ an element of order $p$.

Our proof of the backward direction of Theorem 2 is more or less deBruijn’s own proof, simplified by removing some extraneous steps.

**Proof of Theorem 2.** First assume that $(A, B)$ is a partition of $D_n$ such that $p^\alpha \in B$ and let $(a, b)$ be a factorization of $G$ such that $A|a$, $B|b$ (this is the “backward” direction). Since $p^\alpha \in B$ we have $\Phi_{p^\alpha}(x)|b(x)$. As $\Phi_{p^\alpha} = 1 + x^{p^\alpha-1} + x^{2p^\alpha-1} + \cdots + x^{(p-1)p^\alpha-1}$ is a monic polynomial we can divide $b(x)$ by $\Phi_{p^\alpha}(x)$ in $\mathbb{Z}[x]$ to get

$$b(x) = \Phi_{p^\alpha}(x)q(x)$$

for some $q(x) \in \mathbb{Z}[x]$. Note that the set $\{0, n/p, 2n/p, \ldots, (p-1)n/p\}$ forms a complete set of representatives of multiples of $p^{\alpha-1}$ mod $p^\alpha$, so there is a bijection $f : \{0, 1, \ldots, p-1\} \rightarrow \{0, 1, \ldots, p-1\}$
such that \( f(h) p^{a-1} \equiv h n / p \mod p^a \) for \( 0 \leq h \leq p - 1 \). Note that \( x^{f(h) p^{a-1}} - x^{h n / p} = (1 - x^{p^a}) q_h(x) \) for some \( q_h(x) \in \mathbb{Z}[x] \). Put \( b_h(x) = x^{f(h) p^{a-1}} q(x) \) for \( 0 \leq h \leq p - 1 \). Then
\[
b_0(x) + b_1(x) + \ldots + b_{p-1}(x) = b(x)
\]
and (since \( f(0) = 0 \)),
\[
a(x) b_h(x) - x^{h n / p} a(x) b_h(x) = a(x) q(x) \left( x^{f(h) p^{a-1}} - x^{h n / p} \right)
= a(x) q(x) (1 - x^{p^a}) Q_h(x)
= a(x) q(x) (1 - x^{p^a}) Q_h(x)
= a(x) b(x) (1 - x^{p^a}) Q_h(x)
= 0
\]
where the last equality (which holds mod \( 1 - x^n \), as convention) follows because every \( n \)-th root of unity is a root of \( a(x) b(x) (1 - x^{p^a}) \). Therefore \( a(x) b_h(x) = x^{h n / p} a(x) b_h(x) \), as desired.

For the other direction of the theorem it will be convenient to adopt the convention that if \( w = (w_0, \ldots, w_{n-1}) \) or \( w = (w_0, \ldots, w_{n-1})^T \) is any vector of size \( n \), then \( w(x) \) stands for the polynomial \( w_0 + w_1 x + \ldots + w_{n-1} x^{n-1} \). Also \( w(x^{-1}) \) stands for the same polynomial obtained by substituting \( x^{-1} \) for \( x \) and then reducing mod \( 1 - x^n \) in the natural way, namely \( w(x^{-1}) = w_0 + w_{n-1} x + \ldots + w_1 x^{n-1} \).

Note that if \( u, w \) are two \( n \)-vectors then the constant term of \( u(x^{-1}) w(x) \) is equal to \( uw \). Also if \( A \) is a circulant matrix whose first column is \( w \) then
\[
(Au)(x) = w(x) u(x)
\]
and (if \( u \) is a row vector)
\[
(uA)(x) = u(x) w(x^{-1}).
\]

So assume now that \( p^a \notin \mathcal{B} \). We need to find some polynomials \( a(x), b(x) \in \mathbb{Z}[x] / (1 - x^n) \) such that \( \mathcal{A} | a, \mathcal{B} | b \) and such that \( (a, b) \) is not a \( g \)-right-quasiperiodic factorization of \( G \). We simply take \( a(x) = \prod_{d \in \mathcal{A}} \Phi_d(x), b(x) = \prod_{d \in \mathcal{B}} \Phi_d(x) \). Note that \( a(x) b(x) = 1 + x + \ldots + x^{n-1} \).

We need to show there do not exist \( b_0(x), \ldots, b_{p-1}(x) \in \mathbb{Z}[x] / (1 - x^n) \) such that \( b_0 + \ldots + b_{p-1} = b \) and such that \( a(x) b_h(x) = x^{h n / p} a(x) b_0(x) \) for \( 1 \leq h \leq p - 1 \). The method that we use is the same that we used to show the factorization \( (1 + x^2, 1 + x) \) is not right-quasiperiodic. Namely, we show that a certain set of linear equations has no solutions over the integers.

The linear system has \( np \) unknown variables, one for each coefficient of the polynomials \( b_0, \ldots, b_{p-1} \). The first \( n \) equations of the system encode the constraint \( b_0 + \ldots + b_{p-1} = b \), with one equation for each power of \( x \) between 0 and \( n - 1 \). There are \( (p - 1)n \) more equations for the constraints \( a(x) b_h(x) = x^{h n / p} a(x) b_0(x) \), \( 1 \leq h \leq p - 1 \). Altogether, the matrix for the system looks like Fig. 4 where \( [I] \) stands for an \( n \times n \) identity matrix, \( [0] \) for an \( n \times n \) null matrix, and \( [A_0], \ldots, [A_{p-1}] \) are \( n \times n \) circulant matrices specified below.

The vector of unknowns \( u \) is the concatenation of \( p \) vectors \( u_0, \ldots, u_{p-1} \) of size \( n \) defined by \( u_h(x) = b_h(x) \). The right-hand side vector \( v \) for the system has its first \( n \) entries reading off the coefficients of \( b(x) \) (from smallest to largest power, top to bottom) and its last \( p(n - 1) \) entries

8
equal to 0. Obviously, the first $n$ equations of the linear system $Mu = v$ are satisfied if and only if $b_0 + \cdots + b_{p-1} = b$.

We now define the matrices $[A_0]$ through $[A_{p-1}]$. The matrix $A_0$ is an $n \times n$ circulant matrix whose first column reads off the coefficients of $a(x)$ from $x^0$ to $x^{n-1}$, top to bottom. The matrix $A_h$ for $1 \leq h \leq p - 1$ is an $n \times n$ circulant matrix whose first column reads off minus the coefficients of $x^{-hn/p}a(x)$, also from $x^0$ to $x^{n-1}$ and from top to bottom. By (9) $(A_0u_0)(x) = a(x)b_0(x)$ and $(A_hu_h)(x) = -x^{-hn/p}a(x)b_h(x)$. Therefore $A_0u_0 + A_hu_h = 0$ if and only if $a(x)b_0(x) - x^{-hn/p}a(x)b_h(x) = 0$, so the last $n(p - 1)$ equations of the linear system $Mu = v$ are satisfied if and only if $a(x)b_h(x) = x^{hn/p}a(x)b_0(x)$ for $1 \leq h \leq p - 1$.

To show $Mu = v$ has no integral solution $u$ it is sufficient to find a row vector $y$ such that $yM$ is integral but $yv$ is fractional. Let $P(x) = 1 + x^p + \cdots + x^{n-p}$. We define $y$ as the concatenation of $p$ vectors $y_0, \ldots, y_{n-1}$ of size $n$ where

$$y_0(x) = \frac{1}{p} P(x)a(x^{-1})$$

and

$$y_h(x) = \frac{1}{p} P(x)$$

for all $h \geq 1$. Since the last $n(p-1)$ entries of $v$ are 0 we have that $yv$ is equal to the constant term of $y_0(x^{-1})b(x) = \frac{1}{p} P(x)a(x)b(x) = \frac{1}{p} (n/p^n)(1 + x + \cdots + x^{n-1})$, which is fractional since $p^{a+1} \nmid n$.

Note that $P(x^{-1}) = P(x)$ and that $x^j P(x)a(x) = P(x)a(x)$ for any $j \equiv 0 \pmod{p^{a+1}}$ since $\Phi_{p^{a+1}}(x)a(x) \implies (1 + x^{p^{a+1}} + \cdots + x^{n-p^{a+1}})P(x)a(x)$, so $x^{hn/p}P(x)a(x^{-1}) = x^{hn/p}P(x^{-1})a(x^{-1}) = P(x)a(x^{-1})$ for any $1 \leq h \leq p - 1$. Because $y_1 = \ldots = y_{p-1}$, $yM$ is integral if and only if $y_0 + (p-1)y_1 A_0$ is integral and $y_0 + y_h A_h$ is integral for $1 \leq h \leq p - 1$. Using (10),

$$(y_1 A_0)(x) = \frac{1}{p} P(x)a(x^{-1}) = y_0(x), \text{ so } y_0 + (p-1)y_1 A_0 = py_0 \text{ is integral. On the other hand if } h \geq 1 \text{ then } (y_h A_h)(x) = -\frac{1}{p} P(x)a(x^{-1}) = -\frac{1}{p} P(x)a(x^{-1}) = -y_0(x) \text{ so } y_0 + y_h A_h = 0 \text{ is integral for } 1 \leq h \leq p - 1. \text{ Thus } yM \text{ is integral, which concludes the proof. } \Box$

We now turn to the case of non-cyclic groups, for which our main result is an analog of Theorem 2 for groups of the type $\mathbb{Z}_p \times \mathbb{Z}_p$. The following key proposition, however, applies to all abelian groups:

**Proposition 4.** If $(a,b)$ is a level $r$ factorization of $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ such that $a = ga$ where $g$ has order $m > 1$ not dividing $r$ then $(a,b)$ is not $g$-right-quasiperiodic.
Proof. For the proof we establish a lexicographic order on the elements of $G$, whereby $(i_1, \ldots, i_k) < (j_1, \ldots, j_k)$ if there is some $t \leq k$ such that $i_c = j_c$ for $c < t$ and such that $i_t < j_t$. Monomials in the variables $x_1, \ldots, x_k$ are likewise ordered lexicographically, so that $x_1^{i_1} \cdots x_k^{i_k} < x_1^{j_1} \cdots x_k^{j_k}$ if and only if $(i_1, \ldots, i_k) < (j_1, \ldots, j_k)$. To any vector $u$ of size $|G|$ we associate a polynomial $u(x_1, \ldots, x_k)$ where the coefficient of the $j$-th monomial in lexicographic order is the $j$-th entry of $u$. Also the polynomial $u(x_1^{-1}, \ldots, x_k^{-1})$ is obtained by substituting $x_i^{-1}$ for $x_i$ in $u(x_1, \ldots, x_k)$ and then reducing the exponent of $x_i$ mod $n_i$. It should be noted that if $u$, $w$ are two vectors of size $|G|$ then $uw$ is the constant term of $u(x_1^{-1}, \ldots, x_k^{-1})w(x_1, \ldots, x_k)$.

We need to show there do not exist $b_0, \ldots, b_{m-1}$ such that $b_0 + \cdots + b_{m-1} = b$ and $ab_0 = ab_h$ for $h \geq 1$ (since $ga = a$). We will again operate by showing that a certain set of linear equations has no solution over the integers. This time however the linear system will not encode all the constraints on the variables, but only a certain subset. More precisely, the linear system will encode the constraint $b_0 + \cdots + b_{m-1} = b$ (which takes $|G|$ equations) and the constraints $(ab_0)(0, \ldots, 0) = (ab_h)(0, \ldots, 0)$ for $1 \leq h \leq m-1$ (namely, the fact that the constant terms of $(ab_0)(x_1, \ldots, x_k)$ and $(ab_h)(x_1, \ldots, x_k)$ must agree for $h \geq 1$).

$$M = \begin{bmatrix} [I] & [I] & [I] & \cdots & [I] \\ 0 & 0 & 0 & \cdots & 0 \\ w & -w & 0 & \cdots & 0 \\ w & 0 & -w & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ w & 0 & 0 & \cdots & -w \end{bmatrix}$$

Figure 5

The matrix $M$ for the system looks like Fig. 5 where $[I]$ stands for a $|G| \times |G|$ identity matrix, $w$ is a vector of size $|G|$ defined by $w(x_1^{-1}, \ldots, x_k^{-1}) = a(x_1, \ldots, x_k)$ and 0 stands for a 0-vector of size $|G|$ (we leave a row of zeroes in the middle of the matrix to simplify the indexing scheme). The vector $u$ of unknowns is the concatenation of $m$ vectors $u_0, \ldots, u_{m-1}$ of size $|G|$ given by $u_h(x_1, \ldots, x_k) = b_h(x_1, \ldots, x_k)$. The right-hand side vector $v$ is the vector whose first $|G|$ entries read off the coefficients of $b(x_1, \ldots, x_k)$ in lexicographic order and whose last $m$ entries are 0. The first $|G|$ equations of the linear system $Mu = v$ are then obviously satisfied only if $b_0 + \cdots + b_{m-1} = b$. Of the remaining $m$ equations, the $h$-th is satisfied only if $wu_0 - wu_h = 0$, which is to say if the constant term of $a(x_1, \ldots, x_k)b_0(x_1, \ldots, x_k)$ is equal to the constant term of $a(x_1, \ldots, x_k)b_h(x_1, \ldots, x_k)$.

To show the system $Mu = v$ has no integral solution we need to exhibit a vector $y$ such that $yM$ is integral and $yw$ is fractional. We define $y$ as the vector $\frac{1}{m}w$ followed by $m$ entries equal to
\( \frac{1}{m} \) (so \( y \) has size \( |G| + m \), as desired). Then \( yw \) is the constant term of \( \frac{1}{m}a(x_1, \ldots, x_k)b(x_1, \ldots, x_k) \) which is \( \frac{1}{m}r \) which is fractional. On the other hand \( yM \) is integral since \( \frac{1}{m}w + (m - 1) \frac{1}{m}w \) and \( \frac{1}{m}w - \frac{1}{m}w \) are both integral vectors. This concludes the proof. \( \square \)

In preparation for our results on factorizations groups of the type \( \mathbb{Z}_p \times \mathbb{Z}_p \) we need to make some more general remarks. We let \( \zeta_n = e^{2\pi i/n} \).

Say \( G = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k} \) is any finite abelian group. Put \( n = \text{lcm}(n_1, \ldots, n_k) \) and let \( \mathbb{Z}_n^* \) denote the group of integers mod \( n \) relatively prime to \( n \) under multiplication. Then \( \mathbb{Z}^*_n \) acts on \( \mu_{n_1} \times \ldots \times \mu_{n_k} \) by exponentiation, namely each \( u \) in \( \mathbb{Z}^*_n \) induces a permutation of \( \mu_{n_1} \times \ldots \times \mu_{n_k} \) given by \( (\theta_1, \ldots, \theta_k) \mapsto (\theta_1^u, \ldots, \theta_k^u) \). If \( (\theta_1, \ldots, \theta_k), (\theta'_1, \ldots, \theta'_k) \) are in the same orbit of \( \mu_1 \times \ldots \times \mu_k \) under the action of \( \mathbb{Z}^*_n \) then \( a(\theta_1, \ldots, \theta_k) = 0 \iff a(\theta'_1, \ldots, \theta'_k) = 0 \) for any \( a(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k] \). To see why, take \( u \in \mathbb{Z}^*_n \) such that \( (\theta_1^u, \ldots, \theta_k^u) = (\theta'_1, \ldots, \theta'_k) \). Choose powers \( l_1, \ldots, l_k \) such that \( (\theta_1, \ldots, \theta_k) = (\zeta_1^{l_1}, \ldots, \zeta_k^{l_k}) \) and put \( g(z) = a(z^{l_1}, \ldots, z^{l_k}) \). Since \( a(\theta_1, \ldots, \theta_k) = 0 \) we have \( g(\zeta_n) = 0 \) so all primitive \( n \)-th roots of unity are roots of \( g \) and therefore, since \( \gcd(u, n) = 1 \), we have \( 0 = g(\zeta_n^u) = a(\zeta_1^{ul_1}, \ldots, \zeta_k^{ul_k}) = a(\theta'_1, \ldots, \theta'_k) \). This shows \( a(\theta_1, \ldots, \theta_k) = 0 \implies a(\theta'_1, \ldots, \theta'_k) = 0 \) and the other direction is symmetric.

We write \( \mathcal{O}_{n_1, \ldots, n_k} \) for the set of orbits of \( \mu_{n_1} \times \ldots \times \mu_{n_k} \) under the action of \( \mathbb{Z}^*_n \) but with the trivial orbit \( \{(1, \ldots, 1)\} \) removed (the set \( \mathcal{O}_{n_1, \ldots, n_k} \) is the analogue of the set \( \mathcal{D}_n \) for cyclic groups; we apologize for the slight shift in paradigm, as \( \mathcal{D}_n \) is a set of numbers whereas \( \mathcal{O}_{n_1, \ldots, n_k} \) is a set of sets of \( k \)-tuples of complex numbers). If \( \mathcal{A} \subseteq \mathcal{O}_{n_1, \ldots, n_k} \) and \( a = a(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k] \) then we write \( \mathcal{A}[a] \) if \( a(\theta_1, \ldots, \theta_k) = 0 \) for all \( (\theta_1, \ldots, \theta_k) \) in the orbits of \( \mathcal{A} \). By the above remarks and those following Eq. (1), if \( (a, b) \) is any factorization of \( G = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k} \) then there is a partition \( (\mathcal{A}, \mathcal{B}) \) of \( \mathcal{O}_{n_1, \ldots, n_k} \) such that \( \mathcal{A}[a], \mathcal{B}[b] \). Our philosophy here, too, will be to focus on the partition \( (\mathcal{A}, \mathcal{B}) \) rather than on the polynomials \( a, b \). We adopt the same terminology as for cyclic groups by saying that a partition \( (\mathcal{A}, \mathcal{B}) \) of \( \mathcal{O}_{n_1, \ldots, n_k} \) is “\( g \)-right-quasiperiodic” if every factorization \( (a, b) \) of \( G \) such that \( \mathcal{A}[a], \mathcal{B}[b] \) is \( g \)-right-quasiperiodic, and so on for \( g \)-left-quasiperiodic, etc.

Our main theorem for non-cyclic groups concerns groups of the type \( G = \mathbb{Z}_p \times \mathbb{Z}_p \) where \( p \) is a prime. Since the action of \( \mathbb{Z}^*_p \) on \( \mu_p \times \mu_p \) is torsion-free \( \mathcal{O}_{p,p} \) consists of \( p+1 \) orbits of size \( p-1 \) each (for comparison, see Fig. 6 showing the orbits in \( \mathcal{O}_{4,4} \)). If \( \beta \) is an orbit \( \mathcal{O}_{p,p} \) then we write \( F_\beta \) for the polynomial \( 1 + \sum_{(c_1, c_2) \in \beta} x^{c_1}y^{c_2} \in \mathbb{Z}[x,y] \). Note that \( F_\beta = \sum_{u=0}^{p-1} (x^uy^u)^a \) where \( (r,s) \) is any pair such that \( (\zeta_p^r, \zeta_p^s) \in \beta \) and where the equality is taken mod \( (1-x_p, 1-y_p) \) (as per our convention).

\( \mathcal{O}_{p,p} \) has the somewhat special property that for any orbit \( \beta \in \mathcal{O}_{p,p} \) there exists a unique “orthogonal orbit” \( \beta^\perp \in \mathcal{O}_{p,p} \) such that \( (\zeta_p^r, \zeta_p^s) \in \beta \iff F_\beta(\zeta_p^r, \zeta_p^s) \neq 0 \), which is to say there exists a unique orbit \( \beta^\perp \) such that \( (\zeta_p^r, \zeta_p^s) \in \beta, (\zeta_p^r, \zeta_p^s) \in \beta^\perp \implies rr^* + ss^* \equiv 0 \mod p \). To see the existence and uniqueness of \( \beta^\perp \), first assume that \( r = 0 \). Then \( s \neq 0 \) since the orbit \( \{(1,1)\} \) is excluded from \( \mathcal{O}_{p,p} \), so the equation \( rr^* + ss^* \equiv 0 \mod p \) forces \( s^* = 0 \) and leaves \( r^* \) arbitrary; \( \beta^\perp \) is therefore the orbit \( \{(c_2, 0), (c_2, 0), \ldots, (c_2, 0)\} \). The case when \( s = 0 \) is handled similarly. We can therefore assume that \( r, s \neq 0 \). But if \( r, s \neq 0 \) then the congruence \( rr^* + ss^* \equiv 0 \mod p \) has exactly one solution \( s' \in \mathbb{Z}_p \) for each value of \( r' \in \mathbb{Z}_p \) so has exactly \( p \) solution pairs \((r', s')\) in all, and moreover if \((r', s')\) is a solution then \((r'u, s'u)\) is a solution for any \( u \in \mathbb{Z}_p^* \), the pairs \((\zeta_p^r, \zeta_p^s) \neq (1,1) \) such that \((r', s') \in \mathbb{Z}_p \times \mathbb{Z}_p \) are solutions of the congruence \( rr^* + ss^* \equiv 0 \mod p \) therefore form an orbit in \( \mathcal{O}_{p,p} \).

Obviously \( (\beta^\perp)^\perp = \beta \) so \( F_\beta(\zeta_p^r, \zeta_p^s) \neq 0 \) only if \( (\zeta_p^r, \zeta_p^s) \in \beta \) or \( (\zeta_p^r, \zeta_p^s) = (1,1) \). Thus the
elements of $\beta$ are all the “non-roots” of $F_{\beta^\perp}$ not equal to $(1,1)$. Note that $\beta$ and $\beta^\perp$ can coincide, such as for example when $\beta = \{(-1,-1)\}$ in $\mu_2 \times \mu_2$ or $\beta = \{ (\zeta_5, \zeta_5^2), (\zeta_3, \zeta_3^2), (\zeta_3^4, \zeta_3^5), (\zeta_3^3, \zeta_3^5) \}$ in $\mathbb{Z}_5 \times \mathbb{Z}_5$.

The following theorem, which consists of our main result on groups of the type $\mathbb{Z}_p \times \mathbb{Z}_p$, should be compared with Theorem 2 for cyclic groups:

**Theorem 4.** Let $G = (\mathbb{Z}_p)^2$, let $g = (r,s) \neq (0,0)$ be an element of $G$ and let $\beta$ be the orbit in $O_{p,p}$ containing the element $(\zeta_p^t, \zeta_p^s)$. Then a partition $(A,B)$ of $O_{p,p}$ is $g$-right-quasiperiodic if and only if $B = O_{p,p}$ or $\beta^\perp \notin B$ and $B \neq \emptyset$.

**Proof.** First we show that if $B = O_{p,p}$ or $\beta^\perp \notin B$, $B \neq \emptyset$ then any factorization $(a,b)$ of $(\mathbb{Z}_p)^2$ such that $A[a,B]b$ is $g$-right-quasiperiodic. If $B = O_{p,p}$ and $B|b$ then $b$ is an integer multiple of the polynomial $(1+x+\ldots+x^{p-1})(1+y+\ldots+y^{p-1})$ so $b$ is $g$-periodic and $(a,b)$ is $g$-right-quasiperiodic. Otherwise say that $\beta^\perp \notin B$, $B \neq \emptyset$. Recall that the only pairs $(\zeta_p^t, \zeta_p^s) \neq (1,1)$ that are not roots of $F_{\beta}(x,y)$ are the pairs in $\beta^\perp$. Therefore, since $\beta^\perp \notin B$, every pair $(\zeta_p^t, \zeta_p^s)$ in an orbit of $B$ is a root of $F_{\beta}(x,y)$. Thus $(a,F_{\beta})$ is a factorization of $\mathbb{Z}_p \times \mathbb{Z}_p$. Hence $B \neq \emptyset$ we have that $b(\zeta_p^t, \zeta_p^s) = 0$ for some $(l,m) \in \mathbb{Z}_p \times \mathbb{Z}_p$, $(l,m) \neq (0,0)$, so $\Phi_p(z)|b(z^l, z^m)$ and therefore $p|b(1,1)$. Let $k = b(1,1)/p \in \mathbb{Z}$. Then $kF_{\beta} \in \mathbb{Z}[x,y]$ and $kF_{\beta}(1,1) = b(1,1)$ since $F_{\beta}(1,1) = p$. Since $F_{\beta}$ is $g$-periodic it follows by Proposition 2 applied with $b' = kF_{\beta}$ that $(a,b)$ is $g$-right-quasiperiodic.

For the converse, note first that $-(B = O_{p,p} \wedge (\beta^\perp \notin B \wedge B \neq \emptyset)) = -(B = O_{p,p}) \wedge -(\beta^\perp \notin B \wedge B \neq \emptyset) = (A \neq \emptyset) \wedge (\beta^\perp \in B \wedge B = \emptyset) = (A \neq \emptyset \wedge \beta^\perp \in B) \wedge (B = \emptyset)$. So we must show that if $B = \emptyset$ or $A \neq \emptyset$ and $\beta^\perp \notin B$ then there is some factorization $(a,b)$ of $(\mathbb{Z}_p)^2$ such that $A[a,B]b$ and that is not $g$-right-quasiperiodic. Say first that $B = \emptyset$. Then we can take $b = 1$, $a = (1 + x + \ldots + x^{p-1})(1 + y + \ldots + y^{p-1})$ and since $p \nmid b(1,1)$, $a(1,1) \neq 0$ it follows from Proposition 3 that $(a,b)$ is not $g$-right-quasiperiodic.

Having taken care of the case $B = \emptyset$, assume now that $A \neq \emptyset, \beta^\perp \in B$. Then $\beta^\perp \notin A$ so every pair $(\zeta_p^t, \zeta_p^s)$ in an orbit of $A$ is a root of $F_{\beta}(x,y)$. We can therefore take $a = F_{\beta}$. Moreover since $A$ is nonempty there is some $\alpha \in A$; since $\alpha \notin B$ every pair $(\zeta_p^t, \zeta_p^s)$ in the orbits of $B$ is a root of $F_{\alpha^\perp}(x,y)$, so we can take $b = F_{\alpha^\perp}$. But now $a = ga$ and $(a,b)$ is a factorization of level 1 which is not divisible by $p$ (the order of $g$), so it follows from Proposition 4 that $(a,b)$ is not $g$-right-quasiperiodic.

Theorem 4 can be re-summarized like so:

$(A,B)$ is $g$-right-quasiperiodic if $(B = O_{p,p}) \wedge (\beta^\perp \notin B \wedge B \neq \emptyset)$

$(A,B)$ is not $g$-right-quasiperiodic if $(A = O_{p,p}) \wedge (\beta^\perp \notin A \wedge A \neq \emptyset)$

As the second characterization is obtained from the first by interchanging $A$ and $B$, we obtain the following corollaries:

**Corollary 3.** A partition $(A,B)$ of $O_{p,p}$ is $g$-right-quasiperiodic if and only if $(B,A)$ is not $g$-right-quasiperiodic, for all $g \in (\mathbb{Z}_p)^2, g \neq (0,0)$.

**Corollary 4.** Every partition $(A,B)$ of $O_{p,p}$ is $g$-quasiperiodic for all $g \in (\mathbb{Z}_p)^2, g \neq (0,0)$.

**Corollary 5.** Every factorization $(a,b)$ over $\mathbb{Z}$ of a group of the type $(\mathbb{Z}_p)^2$ is quasiperiodic.

12
In light of Theorem 2 and Corollary 3 we propose the following conjecture:

**Conjecture 1.** Let \( G = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k} \) be a finite abelian group and let \( g \in G \) be an element of prime order. Then a partition \((\mathcal{A}, \mathcal{B})\) of \( \mathcal{O}_{n_1, \ldots, n_k} \) is \(g\)-right-quasiperiodic if and only if \((\mathcal{B}, \mathcal{A})\) is not \(g\)-right-quasiperiodic.

The assumption that \( g \) be an element of prime order is necessary, cf. the factorization \((1 + x, 1 + x^2)\) of \(\mathbb{Z}_4\).

We verified Conjecture 1 by computer for the group \(\mathbb{Z}_4 \times \mathbb{Z}_4\). Some results of this computation are shown in Figs. 7 and 8, where we show which orbit partitions \((\mathcal{A}, \mathcal{B})\) are \((2, 2)\)-right-quasiperiodic (the legend for this figure is given in Fig. 6). We find that a partition \((\mathcal{A}, \mathcal{B})\) appears in the list if and only if \((\mathcal{B}, \mathcal{A})\) does not appear, in accordance with Conjecture 1 (in other words, if we take a \(4 \times 4\) square in the list and switch the white and shaded parts then we always obtain a square which is not in the list). As the reader may tell, the list does not otherwise have any salient patterns or regularity (nonetheless, there must a “good reason” why exactly half of the orbit partitions appear in the list, and none together with their complement!).

We will finish this section by sketching the methods used to generate the data for Figs. 7-8. The question is how to determine, given a partition \((\mathcal{A}, \mathcal{B})\) of \(\mathcal{O}_{4,4}\), whether every factorization \((a, b)\) of \((\mathbb{Z}_4)^2\) such that \(\mathcal{A}|a, \mathcal{B}|b\) is \((2, 2)\)-right-quasiperiodic over \(\mathbb{Z}\). For continuity with the previous material we will use “\(\zeta_4\)” to denote \(e^{2\pi i/4}\), though in this particular case we could of course use the more standard notation “\(i\)” instead of \(\zeta_4\) (already used to define \(\zeta_n\), for that matter).

Our first step is to find integral bases \(A\) and \(B\) in \(\mathbb{Z}[x, y]/(1 - x^4, 1 - y^4)\) for those functions vanishing on the orbits in \(\mathcal{A}\) and in \(\mathcal{B}\) respectively (by “integral basis” we mean that any function in \(\mathbb{Z}[x, y]/(1 - x^4, 1 - y^4)\) vanishing on the orbits in \(\mathcal{A}\) (resp. \(B\)) can be obtained as an integer linear combination of functions in \(A\) (resp. \(B\))). To do so, consider first the question of finding out which functions \(a(x, y)\) vanish on a single orbit \(\alpha \in \mathcal{A}\). Let \((\zeta_4^1, \zeta_4^2) \in \alpha\). Then we need \(a(\zeta_4^1, \zeta_4^2) = 0\), meaning that \(z = \zeta\) is a root of the polynomial \(a(z^*, z^*) \in \mathbb{Z}[z]\), i.e. that \(\Phi_4(z)|a(z^*, z^*)\). Effecting the division and setting the remainder equal to 0 yields linear relations between the coefficients of \(a\); the relationship is if-and-only-if, so that \(a\) vanishes on \(\alpha\) if and only if its coefficients obey

<table>
<thead>
<tr>
<th>(1, −i)</th>
<th>(i, −i)</th>
<th>(−1, −i)</th>
<th>(−i, −i)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1, −1)</td>
<td>(i, −1)</td>
<td>(−1, −1)</td>
<td>(−i, −1)</td>
</tr>
<tr>
<td>(1, i)</td>
<td>(i, i)</td>
<td>(−1, i)</td>
<td>(−i, i)</td>
</tr>
<tr>
<td>(1, 1)</td>
<td>(i, 1)</td>
<td>(−1, 1)</td>
<td>(−i, 1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B</th>
<th>G</th>
<th>I</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>F</td>
<td>J</td>
<td>F</td>
</tr>
<tr>
<td>B</td>
<td>E</td>
<td>I</td>
<td>G</td>
</tr>
<tr>
<td>A</td>
<td>D</td>
<td>H</td>
<td>D</td>
</tr>
</tbody>
</table>

**Figure 6:** The orbits of \(\mu_4 \times \mu_4\) when acted on by \(\mathbb{Z}_4^*\); on the left, the group \(\mu_4 \times \mu_4\); on the right, elements in the same orbit as each other are marked with a common letter.
Figure 7: The first 130 (2, 2)-right-quasiperiodic partitions \((A, B)\) of \(O_{4,4}\); shaded squares correspond to pairs of roots \((c_{4}^{1}, c_{4}^{m})\) in orbits of the partition \(B\) under the coordinatization of Fig. 6 (thus certain pairs of squares always appear either both shaded or both blank). The bottom left square corresponding to the orbit \(((1, 1))\) is excluded since we never consider orbit partitions containing \(((1, 1))\).
Figure 8: The last 126 $(2,2)$-right-quasiperiodic partitions $(A,B)$ of $\mathcal{O}_{4,4}$. 
these relations. We gather all these relations for the various orbits in $\mathcal{A}$ into a single linear system, so that $a$ vanishes on all the orbits of $\mathcal{A}$ if and only if its coefficients $u_{t,m}$ satisfy a certain linear system $Mu = 0$. Our problem is thus reduced to finding an integral basis for the lattice of vectors $u$ satisfying some linear system $Mu = 0$ where $M$ is a rational (in fact integral) matrix. This can be done using the Hermite normal form of the matrix (cf. [13] section 4.1).

We do this for $\mathcal{A}$ and $\mathcal{B}$ both, so that we have integral bases $A$ and $B$ for those polynomials vanishing respectively on all orbits in $\mathcal{A}$ and all orbits in $\mathcal{B}$. Now for any factorization $(a,b)$ with root orbits $(\mathcal{A},\mathcal{B})$ we have that $a$ is an integer linear combination of polynomials in $A$ and that $b$ is an integer linear combination of polynomials in $B$. We find a polynomial $b'$ in the integer span of $B$ such that $b'(1,1) = \text{gcd}(b(1,1) : b \in B)$. Then for any other polynomial $b$ in the integer span of $B$ there is some $k \in \mathbb{Z}$ such that $b(1,1) = kb'(1,1)$, so by Proposition 2 it is necessary and sufficient that $(a,b')$ be $(2,2)$-right-quasiperiodic in order for all factorizations $(a,b)$ to be $(2,2)$-right-quasiperiodic.

Let $a^1, \ldots, a^k$ list the elements of $A$. To verify that a factorization $(a,b')$ is $(2,2)$-right-quasiperiodic for any $a$ of the form $n_1a^1 + \cdots + n_ka^k$ it suffices to find $b_0, b_1$ such that $b_0 + b_1 = b'$ and such that $a^jb'_j = x^jy^ja^j b_0'$ for each $1 \leq j \leq k$. We can do this using a system of linear equations as in Theorems 2 or 4 (but with more rows because we are considering different $a$'s for the same $b$). If the system of linear equations has a solution over the integers, which we can again determine using the Hermite normal form, then we have shown that every factorization $(a,b)$ such that $A|a, B|b$ is $(2,2)$-right-quasiperiodic.

In the other event, if the linear system does not have a solution over the integers, it does not automatically follow that we have found a factorization which is not $(2,2)$-right-quasiperiodic since the linear system in question is matching $b'$ up against against several different $a$'s at once. In this case we throw out in turn all but one element of $A$, redoing the check for each element of $A$ individually and hoping to find some $a^i \in A$ for which the factorization $(a^i,b')$ is not $(2,2)$-right-quasiperiodic. In the event that no such $a^i$ can be found (which happened 17 times in all, though this number will depend on the particular implementation of the algorithm) we reverted to working by hand in order to find an $a$ in the integer span of $A$ for which $(a^i,b')$ failed to be $(2,2)$-right-quasiperiodic, which always turned out to be possible.

**Factorizations over $\mathbb{Z}_+$**

Sands [12] already showed that not all factorizations over $\mathbb{Z}_+$ are quasiperiodic by an example involving the group $\mathbb{Z}_5 \times \mathbb{Z}_{25}$, cf. Fig. 3. His counterexample is complemented by more recent ones of Szabó [16]. The counterexamples of Sands and Szabó are particularly nice because they are level 1 factorizations, that is factorizations of the form $ab = \sum_{g \in G} g$. Here we give two more examples of factorizations that are not quasiperiodic over $\mathbb{Z}_+$ involving the relatively simpler groups $\mathbb{Z}_5 \times \mathbb{Z}_5$ and $\mathbb{Z}_5 \times \mathbb{Z}_7 = \mathbb{Z}_{35}$, but which are factorizations of much higher levels. We thus exhibit the first example of a non-quasiperiodic factorization of a cyclic group over $\mathbb{Z}_+$, though it seems that we are still missing an example of a level 1 non-quasiperiodic cyclic group factorization over $\mathbb{Z}_+$.

Our counterexamples are shown in Figs. 9 and 10. We verified these factorizations are not quasiperiodic over $\mathbb{Z}_+$ by a brute force computer search, trying first all possible decompositions for $b$ and then all possible decompositions for $a$, for all possible periods $g$. The factorization of Fig. 9
$a =$ 
\[
\begin{array}{ccc}
2 & 1 & 2 \\
1 & 5 & 4 \\
2 & 5 & 1 \\
1 & 4 & 1 \\
1 & 4 & 1 \\
\end{array}
\]

$b =$ 
\[
\begin{array}{ccc}
1 & 2 & 1 \\
1 & 2 & 1 \\
1 & 2 & 1 \\
1 & 2 & 1 \\
1 & 2 & 1 \\
1 & 2 & 1 \\
\end{array}
\]

Figure 9: A factorization of $\mathbb{Z}_5 \times \mathbb{Z}_7$ which is non-quasiperiodic over $\mathbb{Z}_+$. Blank entries denote 0’s. Note the row sums of the array on the left are all equal to 7 and the column sums are all equal to 5, whereas the array on the right is a linear combination of rows and columns; hence the pair $(a,b)$ forms a factorization of $\mathbb{Z}_5 \times \mathbb{Z}_7$.

$a =$ 
\[
\begin{array}{ccc}
3 & 1 & 1 \\
1 & 4 & 1 \\
1 & 4 & 1 \\
1 & 4 & 1 \\
1 & 4 & 1 \\
\end{array}
\]

$b =$ 
\[
\begin{array}{ccc}
1 & 2 & 2 \\
2 & 2 & 2 \\
2 & 2 & 2 \\
1 & 2 & 1 \\
1 & 2 & 1 \\
\end{array}
\]

Figure 10: A factorization of $\mathbb{Z}_5 \times \mathbb{Z}_5$ which is non-quasiperiodic over $\mathbb{Z}_+$. Blank entries denote 0’s. Note the column sums, row sums and north-east diagonal sums of the array on the left are all equal to 5, whereas the array on the right can be obtained as a linear combination of columns, rows and north-east diagonals; hence the pair $(a,b)$ forms a factorization of $\mathbb{Z}_5 \times \mathbb{Z}_5$. 
is a little special in this regard since the entry sum of $b$ is neither a multiple of 5 or 7, discarding entirely the possibility that the factorization is right-quasiperiodic. The reader should not scrutinize these factorizations too closely for structural clues as to why they are not quasiperiodic over $\mathbb{Z}_+$; while the Fig. 9 factorization was found “by hand” and then verified by computer, the “$a$” term of the Fig. 10 factorization, for example, is simply chosen at random among $5 \times 5$ arrays with constant column, row, and northeast diagonal sum equal to 5 and such as to have “enough zeroes” (though not too many that we start encountering structure again, e.g. the array whose northwest diagonal consists of 5’s and has 0’s elsewhere). We believe that non-quasiperiodic factorizations of high level over $\mathbb{Z}_+$ are in fact quite abundant, and that one mainly needs to be lucky enough to find a small enough example that a computer can verify it in a reasonable amount time.

References


[16] Sandor Szabó, “Quasi-periodic factorizations”, personal communication


[18] J.P. Steinberger, Tilings of the integers can have superpolynomial periods, preprint