TILING THE INTEGERS WITH TRANSLATES OF ONE FINITE SET

Ethan M. Coven and Aaron Meyerowitz

Abstract. A set *tiles the integers* if and only if the integers can be written as a disjoint union of translates of that set. We consider the problem of finding necessary and sufficient conditions for a finite set to tile the integers. For sets of prime power size, it was solved by D. Newman [J. Number Theory **9** (1977), 107–111]. We solve it for sets of size having at most two prime factors. The conditions are always sufficient, but it is unknown whether they are necessary for all finite sets.

Introduction

Let A be a finite set of integers. *A tiles the integers* if and only if the integers can be written as a disjoint union of translates of A, equivalently, there is a set C such that every integer can be expressed uniquely $a+c$ with $a \in A$ and $c \in C$. In symbols, $A \oplus C = \mathbb{Z}$. In this case A is called a *tile*, $A \oplus C = \mathbb{Z}$ a *tiling*, and C the *translation set*. For a survey of such tilings, see R. Tijdeman [Tij]. For connections with group theory and functional analysis, see [Haj] and [L-W].

We consider the problem of finding necessary and sufficient conditions for a finite set to tile the integers. For sets of prime power size (cardinality, denoted #), it was solved by D. Newman [New]. Newman remarked that "even for so simple a case as size six we do not know the answer." We find necessary and sufficient conditions for A to tile the integers when $\#A$ has at most two prime factors.

There is no loss of generality in restricting attention to translates of a finite set A of *nonnegative* integers. Then $A(x) = \sum_{a \in A} x^a$ is a polynomial such that $\#A = A(1)$. Let S_A be the set of prime powers s such that the s-th cyclotomic polynomial $\Phi_s(x)$ divides $A(x)$. Consider the following conditions on $A(x)$.

(T1) $A(1) = \prod_{s \in S_A} \Phi_s(1)$.

(T2) If $s_1, \ldots, s_m \in S_A$ are powers of distinct primes, then $\Phi_{s_1 \cdots s_m}(x)$ divides $A(x)$.

1991 *Mathematics Subject Classification.* Primary 05B45; Secondary 11B75, 20K01.

Part of this work was done while the first author was a member of the Mathematical Sciences Research Institute (MSRI), where research is supported in part by NSF grant DMS-9701755. The authors thank J. Propp for putting them in touch with each other. The first author thanks J. Jungman and M. Keane for helpful conversations.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Theorem A. *If $A(x)$ satisfies (T1) and (T2), then A tiles the integers.*

Theorem B1. *If A tiles the integers, then $A(x)$ satisfies (T1).*

Theorem B2. *If A tiles the integers and $\#A$ has at most two prime factors, then $A(x)$ satisfies (T2).*

Corollary. *If $\#A$ has at most two prime factors, then A tiles the integers if and only if $A(x)$ satisfies (T1) and (T2).*

It is unknown whether the sufficient conditions (T1) and (T2) are necessary for any finite set to tile the integers. (T1) is necessary but not sufficient (see the example after Theorem B1 in Section 2). However, if $\#A$ is a prime power, then (T2) follows from (T1), so in this case (T1) *is* necessary and sufficient. An examination of Newman's proof [New, Theorem 1] essentially yields this result.

Our proof of Theorem B2 provides a structure theory for finite sets A such that A tiles the integers and $\#A$ has at most two prime factors. We sketch this in Section 4.

If A is a finite set which tiles the integers, then $\bigcup_{a\in A}[a, a+\ 1)$ tiles the reals. J. Lagarias and Y. Wang [L-W] proved a structure theorem for closed subsets T of the reals with finite Lebesgue measure and boundary of measure zero such that the reals can be written as a countable union of measure-disjoint translates of T. It describes such sets in terms of finite sets which tile the integers.

1. Preliminaries

For A and B sets or multisets of integers, we denote the multiset $\{a+b : a \in\ A, b \in B\}$ by $A+B$. We write $A \oplus B$ when every element can be expressed uniquely $a+b$. For k an integer, we write kA for $\{ka : a \in A\}$, we call $\{k\} \oplus A$ a *translate* of A, and when k is a factor of every $a \in A$, we write A/k for $\{a/k : a \in A\}$.

For $s \geq 1$, the s-th *cyclotomic polynomial* $\Phi_s(x)$ is defined recursively by $x^s - 1 = \prod \Phi_t(x)$, where the product is taken over all factors t of s. The factors of s are positive and include both 1 and s.

Lemma 1.1. *Let p be prime. Then*

(1) *$\Phi_s(x)$ is the minimal polynomial of any primitive s-th root of unity.*
(2) *$1 + x + \cdots + x^{s-1} = \prod \Phi_t(x)$, where the product is taken over all factors $t > 1$ of s.*
(3) *$\Phi_p(x) = 1 + x + \cdots + x^{p-1}$ and $\Phi_{p^{\alpha+1}}(x) = \Phi_p(x^{p^\alpha})$.*
(4) $\Phi_s(1) = \begin{cases} 0 & \textit{if } s = 1 \\ q & \textit{if } s \textit{ is a power of a prime } q \\ 1 & \textit{otherwise.} \end{cases}$
(5) $\Phi_s(x^p) = \begin{cases} \Phi_{ps}(x) & \textit{if } p \textit{ is a factor of } s \\ \Phi_s(x)\Phi_{ps}(x) & \textit{if } p \textit{ is not a factor of } s. \end{cases}$
(6) *If s and t are relatively prime, then $\Phi_s(x^t) = \prod \Phi_{rs}(x)$, where the product is taken over all factors r of t.*

(7) *If $\bar{A}(x)$ is a polynomial and $A(x) = \bar{A}(x^p)$, then $\{t : \Phi_t(x)$ divides $A(x)\} = \{s' : \Phi_s(x)$ divides $\bar{A}(x)\} \cup \{ps : \Phi_s(x)$ divides $\bar{A}(x)\}$, where $s' = ps$ or s according as p is or is not a factor of s.*

Proof. (1) is a standard fact. (2) and (3) follow from the definition, (4) from (2) and (3), and (5) from (1) because the roots of $\Phi_s(x^p)$ are $e^{2\pi ik/ps}$ for k relatively prime to s. Repeated application of (5) yields (6). For (7), let $\omega = e^{2\pi i/t}$. Then ω^p is a primitive s-th root of unity for some s and, from (5), $t \in \{s', ps\}$. $\Phi_t(x)$ divides $\bar{A}(x^p)$ if and only $\bar{A}(\omega^p) = 0$ if and only if $\Phi_s(x)$ divides $\bar{A}(x)$. $\square$

A set C of integers is *periodic* if and only if $C \oplus \{n\} = C$ for some $n \geq 1$. Then C is a union of congruence classes modulo n and $C = B \oplus n\mathbb{Z}$, where B is any set consisting of one representative from each class. If $A \oplus C = \mathbb{Z}$ is a tiling and C is periodic, the smallest such n is called the *period* of the tiling. Note that $n = (\#A)(\#B)$ and $A \oplus B$ is a complete set of residues modulo n. Conversely, if $A \oplus B$ is a complete set of residues modulo n, then $A \oplus (B \oplus n\mathbb{Z}) = \mathbb{Z}$ is a tiling of period n or less, as are $B \oplus (A \oplus n\mathbb{Z}) = \mathbb{Z}$ and $A' \oplus C = \mathbb{Z}$ for any $A' \equiv A \pmod{n}$.

The following basic result is due to G. Hajós [Haj] and N. deBruijn [deB-1], then C. Swenson [Swe], then Newman [New].

Lemma 1.2. *Every tiling by translates of a finite set is periodic, i.e., if A is finite and $A \oplus C = \mathbb{Z}$, then there is a finite set B such that $C = B \oplus n\mathbb{Z}$, where $n = (\#A)(\#B)$.* $\square$

Remark. Newman's proof shows that the period of any tiling by A is bounded by $2^{\max(A)-\min(A)}$. The tiling $\{j\} \oplus \mathbb{Z} = \mathbb{Z}$ has period 1. The tiling $A \oplus C = \mathbb{Z}$, where $A = \{j\} \oplus \{0, k\}$ and $C = \{0, 1, \ldots, k-1\} \oplus 2k\mathbb{Z}$, has period $2k$. We know of no other tilings whose period is as large as $2(\max(A) - \min(A))$. See the remarks following Lemma 2.1.

The collection of all finite multisets of nonnegative integers is in one-to-one correspondence with the set of all polynomials with nonnegative integer coefficients. The correspondence is

$$A \longleftrightarrow A(x) = \sum_{a \in A} m_a x^a,$$

where m_a is the multiplicity of a as an element of A. If B is another such multiset and $k \geq 1$, then the polynomial corresponding to $A + B$ is $A(x)B(x)$, to $A \cup B$ is $A(x) + B(x)$, and to kA is $A(x^k)$. Using this language we get

Lemma 1.3. *Let n be an integer and let A and B be finite multisets of nonnegative integers with corresponding polynomials $A(x)$ and $B(x)$. Then the following statements are equivalent. Each forces A and B to be sets such that $(\#A)(\#B) = A(1)B(1) = n$.*

(1) *$A \oplus (B \oplus n\mathbb{Z}) = \mathbb{Z}$ is a tiling.*
(2) *$A \oplus B$ is a complete set of residues modulo n.*
(3) *$A(x)B(x) \equiv 1 + x + \cdots + x^{n-1} \pmod{x^n - 1}$.*
(4) *$n = A(1)B(1)$ and for every factor $t > 1$ of n, the cyclotomic polynomial $\Phi_t(x)$ is a divisor of $A(x)$ or $B(x)$.* $\square$

There is no loss is restricting attention to conditions for a finite set of *nonnegative* integers to tile the integers. We can further restrict to finite sets whose minimal element is 0 and to translation sets which contain 0, although we will not always do so. For if A' and C' are translations of A and C, then $A \oplus C = \mathbb{Z}$ if and only if $A' \oplus C' = \mathbb{Z}$.

Recall that (T1) and (T2) concern the set S_A of prime powers s such that the cyclotomic polynomial $\Phi_s(x)$ divides $A(x)$. When A and a translate A' are finite sets of nonnegative integers, $A(x)$ and $A'(x)$ are divisible by the same cyclotomic polynomials, so

- A tiles the integers if and only if A' tiles the integers.
- $A(x)$ satisfies (T1) if and only if $A'(x)$ satisfies (T1).
- $A(x)$ satisfies (T2) if and only if $A'(x)$ satisfies (T2).

The next lemma allow us to further restrict attention to finite sets of integers with greatest common divisor 1.

Lemma 1.4. *Let $k > 1$ and let $A = k\bar{A}$ be a finite set of nonnegative integers.*

(1) *A tiles the integers if and only if $\bar{A}$ tiles the integers.*
(2) *If p is prime, then $S_{p\bar{A}} = \{p^{\alpha+1} : p^\alpha \in S_{\bar{A}}\} \cup \{q^\beta \in S_{\bar{A}} : q$ prime, $q \neq p\}$.*
(3) *$A(x)$ satisfies (T1) if and only if $\bar{A}(x)$ satisfies (T1).*
(4) *$A(x)$ satisfies (T2) if and only if $\bar{A}(x)$ satisfies (T2).*

Proof. For one direction of (1), let $\bar{A} \oplus C = \mathbb{Z}$. Then $k\bar{A} \oplus kC = k\mathbb{Z}$ and hence $A \oplus (\{0, 1, \ldots, k-1\} \oplus kC) = \mathbb{Z}$. For the other, let $k\bar{A} \oplus D = \mathbb{Z}$. Then $k\bar{A} \oplus D_0 = k\mathbb{Z}$, where $D_0 = \{d \in D : d \equiv 0 \pmod{k}\}$, and hence $\bar{A} \oplus D_0/k = \mathbb{Z}$. (2) follows from Lemma 1.1(7).

It suffices to prove (3) and (4) when k is prime, say $k = p$. (3) follows from (2) and Lemma 1.1(4) since $\#A = \#\bar{A}$. It remains to prove (4). Let $s' = ps$ or s according as p is or is not a factor of s. Let $s_1, \ldots, s_m$ be powers of distinct primes and $s = s_1 \cdots s_m$. Then $s'_1, \ldots, s'_m$ are powers of distinct primes and $s' = s'_1 \cdots s'_m$. From (2), every $s_i \in S_{\bar{A}}$ if and only if every $s'_i \in S_A = S_{p\bar{A}}$. From 1.1(7), $\Phi_s(x)$ divides $\bar{A}(x)$ if and only if $\Phi_{s'}(x)$ divides $A(x)$. Putting all this together yields (4). $\square$

Remark. It follows from (2) that B is not contained in $p\mathbb{Z}$ when $\Phi_p(x)$ divides $B(x)$.

Lemma 1.4 deals with $A \subset k\mathbb{Z}$. The related situation that $A \oplus C = \mathbb{Z}$ is a tiling with $C \subseteq k\mathbb{Z}$ leads to an important construction. We defer it to Lemma 2.5.

2. Tiling results

Theorem A. *Let A be a finite set of nonnegative integers with corresponding polynomial $A(x) = \sum_{a \in A} x^a$ and let S_A be the set of prime powers s such that the cyclotomic polynomial $\Phi_s(x)$ divides $A(x)$. If*

(T1) $A(1) = \prod_{s \in S_A} \Phi_s(1)$.
(T2) *If $s_1, \ldots, s_m \in S_A$ are powers of distinct primes, then $\Phi_{s_1 \cdots s_m}(x)$ divides $A(x)$,*

then A tiles the integers.

Proof. We construct a set B such that condition (4) of Lemma 1.3 is satisfied. Define $B(x) = \prod \Phi_s(x^{t(s)})$, where the product is taken over all prime power factors s of $\mathrm{lcm}(S_A)$ which are not in S_A and $t(s)$ is the largest factor of $\mathrm{lcm}(S_A)$ relatively prime to s. Since every such s is a prime power, $B(x)$ has nonnegative coefficients. Since 1.3(4) will be shown to hold, these coefficients are all 0 and 1.

Let $s > 1$ be a factor of $A(1)B(1)$ and write $s = s_1 \cdots s_m$ as a product of powers of distinct primes. If every $s_i \in S_A$, then by (T2), $\Phi_s(x)$ divides $A(x)$. Suppose then that some $s_i \notin S_A$. Then $\Phi_{s_i}(x^{t(s_i)})$ divides $B(x)$, $r = s/s_i$ is a factor of $t(s_i)$ and, by Lemma 1.1(6) (with $s = s_i$ and $t = t(s_i)$), $\Phi_{rs_i}(x)$ divides $\Phi_{s_i}(x^{t(s_i)})$. Thus $\Phi_s(x)$ divides $B(x)$ since $rs_i = s$. $\square$

Remarks. The set B constructed in the proof depends only on $S = S_A$ and not on A. Defining $C_S = B \oplus \mathrm{lcm}(S)\mathbb{Z}$, $A \oplus C_S = \mathbb{Z}$ for *all* A with $S_A = S$ which satisfy (T1) and (T2). Then $C_S \subseteq p\mathbb{Z}$ for every prime $p \in S$, since p is a factor of n and every divisor $\Phi_s(x^{t(s)})$ of $B(x)$ is a polynomial in x^p. For either $t(s)$ is a multiple of p, or $s = p^{\alpha+1}$ with $\alpha \geq 1$ and $\Phi_s(x^{t(s)}) = \Phi_p\left(x^{t(s)p^\alpha}\right)$, so every divisor $\Phi_s(x^{t(s)})$ of $B(x)$ is a polynomial in x^p.

Theorem B1. *Let A be a finite set of nonnegative integers with corresponding polynomial $A(x) = \sum_{a \in A} x^a$ and let S_A be the set of prime powers s such that the cyclotomic polynomial $\Phi_s(x)$ divides $A(x)$. If A tiles the integers, then*

(T1) $A(1) = \prod_{s \in S_A} \Phi_s(1)$.

Remark. (T1) is not sufficient for A to tile the integers. $A = \{0, 1, 2, 4, 5, 6\}$ does not tile the integers, but $A(x) = \Phi_3(x)\Phi_8(x)$ satisfies (T1).

Theorem B1 follows from Lemma 2.1(1) below.

Lemma 2.1. *Let $A(x)$ and $B(x)$ be polynomials with coefficients 0 and 1, $n = A(1)B(1)$, and R the set of prime power factors of n. If $\Phi_t(x)$ divides $A(x)$ or $B(x)$ for every factor $t > 1$ of n, then*

(1) *$A(1) = \prod_{s \in S_A} \Phi_s(1)$ and $B(1) = \prod_{s \in S_B} \Phi_s(1)$.*
(2) *S_A and S_B are disjoint sets whose union is R.*

Proof. For every factor $t > 1$ of n, $\Phi_t(x)$ divides $A(x)$ or $B(x)$, so $R \subseteq S_A \cup S_B$. Clearly $A(1) \geq \prod_{s \in S_A} \Phi_s(1)$ and $B(1) \geq \prod_{s \in S_B} \Phi_s(1)$. Thus

$$A(1)B(1) \geq \prod_{s \in S_A} \Phi_s(1) \prod_{s \in S_B} \Phi_s(1) \geq \prod_{t \in R} \Phi_t(1) = n,$$

the equality by Lemma 1.1(4). Hence all the inequalities and containments above are actually equalities, and S_A is disjoint from S_B. $\square$

Remarks. If a tiling $A \oplus C = \mathbb{Z}$ has period n and $C = B \oplus n\mathbb{Z}$, then $n = \mathrm{lcm}(S_A \cup S_B)$, so the period of any tiling by A is a multiple of $\mathrm{lcm}(S_A)$. A particular tiling by A

may have period larger than $\mathrm{lcm}(S_A)$, however when $A(x)$ satisfies (T1) and (T2), the tiling $A \oplus (B \oplus (\#A)(\#B)\mathbb{Z}) = \mathbb{Z}$ constructed in the proof of Theorem A has period $\mathrm{lcm}(S_A)$. In all cases known to the authors both $A(x)$ and $B(x)$ satisfy (T1) and (T2).

We leave it to the interested reader to show that for any set A of nonnegative integers,

- $\mathrm{lcm}(S_A) \leq \frac{p}{p-1}(\max(A) - \min(A))$, where p is the smallest prime factor of $\#A$.
- The inequality is strict except when $A = \{j\} \oplus p^\alpha\{0, 1, \ldots, p-1\}$.

We show in Lemma 2.3 that there is always a tiling whose period is a product of powers of the prime factors of $\#A$.

Theorem B2. *Let A be a finite set of nonnegative integers with corresponding polynomial $A(x) = \sum_{a \in A} x^a$ such that $\#A$ has at most two prime factors and let S_A be the set of prime powers s such that the cyclotomic polynomial $\Phi_s(x)$ divides $A(x)$. If A tiles the integers, then*

(T2) *If $s_1, \ldots, s_m \in S_A$ are powers of distinct primes, then $\Phi_{s_1 \cdots s_m}(x)$ divides $A(x)$.*

The following result is crucial to our proof of Theorem B2. We give an alternate proof of it in Section 3.

Lemma 2.2. [Tij, Theorem 1] *Suppose that A is finite, $0 \in A \cap C$, and $A \oplus C = \mathbb{Z}$. If r and $\#A$ are relatively prime, then $rA \oplus C = \mathbb{Z}$.* $\square$

Remark. Translating A or C does not affect the conclusion. Thus the condition $0 \in A \cap C$ is not needed.

Lemma 2.3. *If a finite set A tiles the integers, then there is a tiling by A whose period is a product of powers of the prime factors of $\#A$.*

Proof. If $A \oplus C = \mathbb{Z}$ is a tiling of period n and $r > 1$ is a factor of n relatively prime to $\#A$, then by Lemma 2.2, $rA \oplus C = \mathbb{Z}$. Therefore $rA \oplus C_0 = r\mathbb{Z}$, where $C_0 = \{c \in C : c \equiv 0 \pmod{r}\}$, and hence $A \oplus C_0/r = \mathbb{Z}$ is a tiling of period n/r. $\square$

The following result is essentially Theorem 4 of [San]. We prove a more general result which implies it in Section 3.

Lemma 2.4. [San] *Let $A \oplus C = \mathbb{Z}$ be a tiling of period n such that A is finite, $0 \in A \cap C$, and n has one or two prime factors. Then there is a prime factor p of n such that either $A \subset p\mathbb{Z}$ or $C \subseteq p\mathbb{Z}$.* $\square$

Sands' result is stated in the terms of direct sum decompositions of finite cyclic groups, but it is easy to translate it into the terminology of this paper.

Lemma 2.5. *Suppose $A \oplus C = \mathbb{Z}$, where A is a finite set of nonnegative integers, $k > 1$, and $C \subseteq k\mathbb{Z}$. For $i = 0, 1, \ldots, k-1$, let $A_i = \{a \in A : a \equiv i \pmod{k}\}$, $a_i = \min(A_i)$, and $\bar{A}_i = \{a - a_i : a \in A_i\}/k$. Then*

(1) $A(x) = x^{a_0}\bar{A}_0(x^k) + x^{a_1}\bar{A}_1(x^k) + \cdots + x^{a_{k-1}}\bar{A}_{k-1}(x^k)$.

(2) *Every* $\bar{A}_i \oplus C/k = \mathbb{Z}$.
(3) *The elements of* A *are equally distributed modulo* k — *every* $\#\bar{A}_i = (\#A)/k$.
(4) $S_{\bar{A}_0} = S_{\bar{A}_1} = \cdots = S_{\bar{A}_{k-1}}$.
(5) *When* k *is prime,* $S_A = \{k\} \cup S_{k\bar{A}_0}$ *and if every* $\bar{A}_i(x)$ *satisfies (T2), then* $A(x)$ *satisfies (T2).*

Proof. (1) is clear. (2) follows from $A_i \oplus C = \{i\} \oplus k\mathbb{Z} = \{a_i\} \oplus k\mathbb{Z}$. To prove (3), note that the translation set C/k has some period n, so there is a set $\bar{B}$ such that $\bar{A}_i \oplus (\bar{B} \oplus n\mathbb{Z}) = \mathbb{Z}$ and every $\bar{A}_i \oplus \bar{B}$ is a complete set of residues modulo n. Thus the $\#\bar{A}_i$ are equal, so (3) holds. (4) also follows since by Lemma 2.1, every $S_{\bar{A}_i}$ is the complement of $S_{\bar{B}}$ in the set of prime power factors of n.

To prove (5), write p in place of k. From Lemma 1.4(2), $S_{p\bar{A}_i} = \{s' : s \in S_{\bar{A}_i}\}$, where $s' = ps$ or s according as p is or is not a factor of s. The polynomial corresponding to $p\bar{A}_i$ is $\bar{A}_i(x^p)$, so from (1) and (4), $S_{p\bar{A}_0} \supseteq S_A$. Also $p \in S_A$, since if $\Phi_p(\omega) = 0$, then $\omega^p = 1$, $\omega^{a_i} = \omega^i$, and $A(\omega) = \sum_{i=0}^{p-1} \omega^i \bar{A}_i(1) = (\#A/k) \sum_{i=0}^{p-1} \omega^i = 0$, the next-to-last equality by (3). We have thus shown that $S_A \supseteq \{p\} \cup S_{p\bar{A}_0}$. Since A_0 and A tile the integers, $A_0(x)$ and $A(x)$ satisfy (T1) and $S_A = \{p\} \cup S_{p\bar{A}_0}$.

Now assume that every $\bar{A}_i(x)$ satisfies (T2). Condition (T2) for $A(x)$ is: if $s_1, \ldots, s_m \in S_{\bar{A}_0}$ are powers of distinct primes, then $\Phi_{s_1' \cdots s_m'}(x)$ divides $A(x)$ and $\Phi_{ps_1 \cdots s_m}(x)$ divides $A(x)$. By (T2), $\Phi_{s_1 \cdots s_m}(x)$ divides every $\bar{A}_i(x)$. Hence by Lemma 1.1(7), $\Phi_{s_1' \cdots s_m'}(x)$ and $\Phi_{ps_1 \cdots s_m}(x)$ divide all the $\bar{A}_i(x^p)$, so they divide $A(x)$ as well. □

Corollary. *If* A *is a finite set of integers and* $C \subseteq k\mathbb{Z}$, *then* $A \oplus C = \mathbb{Z}$ *if and only if* $A = \bigcup_{i=0}^{k-1} \left(\{a_i\} \oplus k\bar{A}_i\right)$ *for some complete set* $\{a_0, a_1, \ldots, a_{k-1}\}$ *of residues modulo* k, *and* k *sets* $\bar{A}_i$, *each of which satisfies* $\min(A_i) = 0$ *and tiles the integers with translation set* C/k. □

The decomposition is unique. We can have $\gcd(A) = 1$ although this may not be true for the $\bar{A}_i$. If the $\bar{A}_i$ are equal, then the union is a direct sum, $A = \{a_0, a_1 \ldots, a_{k-1}\} \oplus k\bar{A}_0$. For some simple choices of translation set C, every tile has this form.

Proof of Theorem B2. From Lemma 1.4 and the comments before it there is no loss of generality in assuming that $\gcd(A) = 1$ and $0 \in A$.

By Lemma 2.3 there is a tiling $A \oplus C = \mathbb{Z}$ whose period n is a product of powers of the prime factors of $\#A$. We complete the proof by induction on n. If $n = 1$, then $A = \{0\}$ and $A(x) \equiv 1$ satisfies (T2) vaccuously. If $n > 1$, then by Lemma 2.4, there is a prime factor p of n such that $C \subseteq p\mathbb{Z}$. Then by Lemma 2.5, $A(x) = x^{a_0}\bar{A}_0(x^p) + x^{a_1}\bar{A}_1(x^p) + \cdots + x^{a_{p-1}}\bar{A}_{p-1}(x^p)$ and every $\bar{A}_i \oplus C/p = \mathbb{Z}$ is a tiling of period n/p. By the inductive hypothesis, every $\bar{A}_i(x)$ satisfies (T2), so by Lemma 2.5(5), $A(x)$ satisfies (T2). □

Every set known to the authors, regardless of size, which tiles the integers satisfies the tiling conditions (T1) and (T2). However, our proof of Theorem B2 cannot be extended to sets whose size has more than two prime factors because Lemma 2.4 need not hold. For m a positive integer with more than two prime factors, a very general construction due to S. Szabó [Sza] gives sets A such that $\#A = m$, $\min(A) = 0$, $\gcd(A) = 1$, and A tiles the integers, yet the members of A are *not* equally distributed modulo k for any $k > 1$. Hence, from Lemma 2.5(3), every set C such that $0 \in C$ and $A \oplus C = \mathbb{Z}$ satisfies $\gcd(C) = 1$. All these sets A satisfy (T1) and (T2).

These examples also show that both Tijdeman's conjecture [Tij, p. 266] — if $A \oplus C = \mathbb{Z}$, $0 \in A \cap C$, and $\gcd(A) = 1$, then $C \subseteq p\mathbb{Z}$ for some prime factor of $\#A$ — and the weaker conjecture — if A tiles the integers, $\min(A) = 0$ and $\gcd(A) = 1$, then there is *some* translation set of the desired type — are false without further conditions. Tijdeman's conjecture would have implied an inductive characterization of all tilings $A \oplus C = \mathbb{Z}$. The weaker conjecture would have implied an inductive characterization of the finite sets which tile the integers. We established the weaker conjecture in Lemma 2.4 for those A such that $\#A$ has one or two prime factors. We show how to use it in Section 4. Tijdeman [Tij, Theorem 3] proved his conjecture when $\#A$ is a prime power. We do not know whether it holds when $\#A$ has exactly two prime factors.

3. Alternate proofs of Tijdeman's and Sands' Theorems

Tijdeman's Theorem (Lemma 2.2) follows from Lemma 1.3 and

Lemma 3.1. *Let A and B be finite sets of nonnegative integers with corresponding polynomials $A(x)$ and $B(x)$ and let $n = A(1)B(1)$. If*

$$A(x)B(x) \equiv 1 + x + \cdots + x^{n-1} \pmod{x^n - 1}$$

and p is a prime which is not a factor of $A(1)$, then

$$A(x^p)B(x) \equiv 1 + x + \cdots + x^{n-1} \pmod{x^n - 1}.$$

Proof. Since p is prime, $A(x^p) \equiv (A(x))^p \pmod{p}$, i.e., when the coefficients are reduced modulo p. Let $G_n(x) = 1 + x + \cdots + x^{n-1}$. Then

$$A(x^p)B(x) = (A(x))^{p-1} A(x)B(x) \equiv (A(x))^{p-1} G_n(x),$$

where $\equiv$ means the exponents are reduced modulo n and then the coefficients are reduced modulo p. Every $x^i G_n(x) \equiv G_n(x) \pmod{x^n - 1}$, so

$$(A(x))^{p-1} G_n(x) \equiv (A(1))^{p-1} G_n(x) \pmod{x^n - 1}.$$

By Fermat's Little Theorem, $(A(1))^{p-1} \equiv 1 \pmod{p}$. Therefore $A(x^p)B(x) \equiv G_n(x)$, where the exponents are reduced modulo n and then the coefficients are reduced modulo p. Both $A(x^p)B(x)$ and $G_n(x)$ have nonnegative coefficients whose sum is n since $A(1)B(1) = G_n(1) = n$. Consider the following reductions.

(R1) $A(x^p)B(x)$ is reduced modulo $x^n - 1$, yielding a polynomial $G^*(x)$.
(R2) The coefficients of $G^*(x)$ are reduced modulo p, yielding $G_n(x)$.

(R1) preserves the sum of the coefficients, but (R2) reduces the sum by some nonnegative multiple of p. Because the sum of the coefficients of both $G^*(x)$ and $G_n(x)$ is n, that multiple is 0. Therefore $G^*(x) = G_n(x)$. □

We use the following result to prove Sands' Theorem (Lemma 2.4). Let $A - A$ be the difference set $\{a_1 - a_2 : a_1, a_2 \in A\}$.

Lemma 3.2. *Let A and B be finite, $A, B \neq \{0\}$, and $A \oplus B$ a complete set of residues modulo $(\#A)(\#B)$. Then at least one of the following is true.*

(1) *No member of $A - A$ is relatively prime to $\#B$.*
(2) *No member of $B - B$ is relatively prime to $\#A$.*

Proof. Let $n = (\#A)(\#B)$. By Lemma 1.3,

$$A(x)B(x) \equiv 1 + x + \cdots + x^{n-1} \pmod{x^n - 1}.$$

Suppose $0 < a_1 - a_2 = \delta'$ is relatively prime to $\#B$ and $0 < b_1 - b_2 = \delta''$ is relatively prime to $\#A$. Lemma 2.2 shows that

$$A(x^{\delta''})B(x^{\delta'}) \equiv 1 + x + \cdots + x^{n-1} \pmod{x^n - 1},$$

so by Lemma 1.3 again, $\delta'' A \oplus \delta' B$ is a complete set of residues modulo n. But

$$(b_1 - b_2)a_1 + (a_1 - a_2)b_2 = (b_1 - b_2)a_2 + (a_1 - a_2)b_1.$$

Thus the same number can be expressed $\delta'' a + \delta' b$ in two ways, which is impossible. □

Lemma 2.4. [San] *Let $A \oplus C = \mathbb{Z}$ be a tiling of period n such that A is finite, $0 \in A \cap C$, and n has one or two prime factors. Then there is a prime factor p of n such that either $A \subset p\mathbb{Z}$ or $C \subseteq p\mathbb{Z}$.*

Proof. Let $C = B \oplus n\mathbb{Z}$ and the prime factors of n be p and possibly q. Then at least one of 3.2(1) and 3.2(2) holds.

If 3.2(1) holds, then $A \subseteq A - A \subset p\mathbb{Z} \cup q\mathbb{Z}$, the first containment because $0 \in A$. If neither $p\mathbb{Z}$ nor $q\mathbb{Z}$ contains A, then there exist $a_1, a_2 \in A$ such that $a_1 \in p\mathbb{Z} \setminus q\mathbb{Z}$ and $a_2 \in q\mathbb{Z} \setminus p\mathbb{Z}$. But then $a_1 - a_2$ is relatively prime to $\#B$.

If 3.2(2) holds, the same argument shows that $B \subseteq p\mathbb{Z}$ or $B \subseteq q\mathbb{Z}$. Then the same is true for $C = B \oplus n\mathbb{Z}$. □

Lemma 3.3. *Suppose A is finite, $0 \in A$, A tiles the integers with period n, and n has two prime factors, p and q. If neither $\Phi_p(x)$ nor $\Phi_q(x)$ is a divisor of $A(x)$, then $A \subset p\mathbb{Z}$ or $A \subset q\mathbb{Z}$.*

Proof. Let $A \oplus (B \oplus n\mathbb{Z}) = \mathbb{Z}$ be a tiling of period n. By Lemma 1.3(4), $\Phi_p(x)$ and $\Phi_q(x)$ are divisors of $B(x)$. From the remark after Lemma 1.4, neither $p\mathbb{Z}$ nor $q\mathbb{Z}$ contains B. Then the conclusion follows by Lemma 2.4. □

4. A structure theory

In this section we describe the structure of those finite sets A such that A tiles the integers and $\#A$ has at most two prime factors. Equivalently, such that the set S_A of prime powers s such that the cyclotomic polynomial $\Phi_s(x)$ divides $A(x)$ consists of powers of at most two primes. For S such a set of prime powers, let $\mathcal{T}_S$ be the collection of all subsets A of $\{0, 1, \dots, \mathrm{lcm}(S)-1\}$ which tile the integers and satisfy $\min(A) = 0$ and $S_A = S$. Note that $\mathcal{T}_\varnothing = \{0\}$ because $\mathrm{lcm}(\varnothing) = 1$, and that $\mathcal{T}_{\{p^{\alpha+1}\}}$ is the set whose only member is $p^\alpha\{0, 1, \dots, p-1\}$. We have seen that there is no loss in requiring $\min(A) = 0$. We claim that a finite set A' with $\min(A') = 0$ and $S_{A'} = S$ tiles the integers if and only if A' is congruent modulo $\mathrm{lcm}(S)$ to a member of $\mathcal{T}_S$. For if $A' \equiv A \pmod{\mathrm{lcm}(S)}$, then $S_{A'} = S_A = S$, and as noted after the proof of Lemma 1.1, $A' \oplus C_S = \mathbb{Z}$ if and only if $A \oplus C_S = \mathbb{Z}$. Recall that C_S is the universal translation set corresponding to S: $A \oplus C_S = \mathbb{Z}$ for every A such that A tiles the integers and $S_A = S$.

For purposes of comparison we recall the simpler structure of *all* finite sets which tile the nonnegative integers $\mathbb{N}_0 = \{0, 1, \dots\}$, due to deBruijn [deB-3]. Note that every such set has a unique translation set, so the unique associated tiling has a period. One such set is $A = \{0, 1, 2, 3, 4\} \oplus \{0, 10, 20, 30\} \oplus \{0, 120, 240\}$, which tiles $\mathbb{N}_0$ with period 360. A can be written $A = \tilde{A} \oplus 120\{0, 1, 2\}$, where $\tilde{A}$ tiles $\mathbb{N}_0$ with period 60, and it can be written $A = \{0, 1, 2, 3, 4\} \oplus 5\bar{A}$, where $\bar{A}$ tiles $\mathbb{N}_0$ with period $72 = 360/5$. If $A \neq \{0\}$ is any finite set which tiles $\mathbb{N}_0$, then there are always these two types of direct sum decompostions, $A = \tilde{A} \oplus (n/p)\{0, 1, \dots, p-1\}$ and $A = k\{0, 1, \dots, q-1\} \oplus q\bar{A}$, where p and q are prime factors of the period n of the tiling, $k = \gcd(A)$, and $\tilde{A}$ and $\bar{A}$ are shorter tiles. Iterating either decomposition, every tile is a direct sum, in one or more ways, of tiles of the form $m\{0, 1, \dots, p-1\}$. If the order is as above, then $\tilde{A}$ is the direct sum of all but the last of the summands and $q\bar{A}$ is the direct sum of all but the first. $A(x)$ is thus a product of terms $(x^{mp}-1)/(x^m-1) = \Phi_p(x^m)$ and can easily be shown to satisfy (T1) and (T2).

We return to $\mathcal{T}_S$ for the case that S consists of the powers of at most two primes. Both decompositions above generalize, the second more usefully than the first.

Corresponding to the first decomposition, we will see that every member of $\mathcal{T}_S$ is a disjoint union of translates of $(n/p)\{0, 1, \dots, p-1\}$ and $(n/q)\{0, 1, \dots, q-1\}$, where $n = \mathrm{lcm}(S)$. The simplest case where both must be used is $S = \{p, p^3, q^2\}$. An important example of this with $\mathrm{lcm}(S) = 72$ is given below. More usefully, we will show that when $S \neq \varnothing$, every tile $A \in \mathcal{T}_S$ is, as in Lemma 2.5, a union of translates of multiples of p or q smaller tiles: $A = m\bigcup_{i=0}^{p-1}\left(\{a_i\} \oplus p\bar{A}_i\right)$, where $m = \gcd(A)$, $a_0 = 0$, $\{a_0, a_1, \dots, a_{p-1}\}$ is a complete set of residues modulo p, every $\{a_i\} \oplus p\bar{A}_i \subset \{0, 1, \dots, \mathrm{lcm}(S)-1\}$, and for some smaller set $\bar{S}$, every $\bar{A}_i \in \mathcal{T}_{\bar{S}}$. We need not get a direct sum, as the $\bar{A}_i$ need not be equal. Every $\bar{A}_i$ in turn is a union of p or q translates of multiples of even shorter tiles. Iterating the procedure until $S = \varnothing$ gives the disjoint union referred to above.

Suppose that S contains powers of only p, so that $\mathrm{lcm}(S)$ is a power of p. If $A \in \mathcal{T}_S$, then $A \oplus C_S = \mathbb{Z}$ and either $p \in S$ and $C_S \subseteq p\mathbb{Z}$, or $p \notin S$ and $A \subset p\mathbb{Z}$.

Let $\bar{S} = \{p^\alpha : p^{\alpha+1} \in S\}$. If $p \notin S$, then $\#\bar{S} = \#S$ and, as in Lemma 1.4, $\mathcal{T}_S = \{p\bar{A} : \bar{A} \in \mathcal{T}_{\bar{S}}\}$. If $p \in S$, then by the Corollary to Lemma 2.5, the members of $\mathcal{T}_S$ can be constructed by taking all unions $\bigcup_{i=0}^{p-1} \left(\{a_i\} \oplus p\bar{A}_i\right)$ with $\bar{A}_i \in \mathcal{T}_{\bar{S}}$, $a_0 = 0$, $\{a_0, a_1, \dots, a_{p-1}\}$ a complete set of residues modulo p, and every $\{a_i\} \oplus p\bar{A}_i \subset \{0, 1, \dots, \mathrm{lcm}(S) - 1\}$. This procedure gives all of $\mathcal{T}_S$ and nothing else.

Suppose now that S contains powers of both p and q and let

$$\bar{S} = \{p^\alpha : p^{\alpha+1} \in S\} \cup \{q^\beta : q^\beta \in S\}, \quad \bar{S}' = \{p^\alpha : p^\alpha \in S\} \cup \{q^\beta : q^{\beta+1} \in S\}.$$

We consider the three cases: $p \in S$, $q \in S$, and $p, q \notin S$. If $p \in S$, then $C_S \subseteq p\mathbb{Z}$ and $\mathcal{T}_S$ can be constructed as above by taking all unions $\bigcup_{i=0}^{p-1} \left(\{a_i\} \oplus p\bar{A}_i\right)$ with $\bar{A}_i \in \mathcal{T}_{\bar{S}}$, $a_0 = 0$, $\{a_0, a_1, \dots, a_{p-1}\}$ a complete set of residues modulo p, and every $\{a_i\} \oplus p\bar{A}_i \subset \{0, 1, \dots, \mathrm{lcm}(S) - 1\}$. If $q \in S$, then the analogous procedure, with the roles of $p, \bar{S}$ and $q, \bar{S}'$ interchanged, gives $\mathcal{T}_S$. If both p and q are in S, then $C_S \subseteq pq\mathbb{Z}$ and either procedure gives $\mathcal{T}_S$. If neither p nor q is in S, then by Lemma 3.3, every member of $\mathcal{T}_S$ is contained in $p\mathbb{Z}$ or $q\mathbb{Z}$. Then $\#S = \#\bar{S} = \#\bar{S}'$, and $\{A \in \mathcal{T}_S : A \subset p\mathbb{Z}\} = \{p\bar{A} : \bar{A} \in \mathcal{T}_{\bar{S}}\}$, while $\{A \in \mathcal{T}_S : A \subset q\mathbb{Z}\} = \{q\bar{A} : \bar{A} \in \mathcal{T}_{\bar{S}'}\}$. In all three cases, this procedure gives all of $\mathcal{T}_S$ and nothing else.

We examine a few cases in more detail, including the important example of deBruijn [deB-2].

When S contains only powers of p, every member of $\mathcal{T}_S$ is a union of translates of $p^\alpha\{0, 1, \dots, p-1\}$, where $p^{\alpha+1}$ is the largest member of S. Hence every member of $\mathcal{T}_S$ is a direct sum of this set and a set $\tilde{A}$ which also tiles the integers. Then $S_{\tilde{A}} = S \setminus \{p^{\alpha+1}\}$, but $\tilde{A}$ need not be a direct sum. An example with $S = \{2, 4, 32\}$ is $16\{0, 1\} \oplus \{0, 1, 2, 11\}$.

It is easy to show that if $S = \{p^\alpha, q^\beta\}$, then every member of $\mathcal{T}_S$ is

$$p^{\alpha-1}\left(\tilde{A} \oplus pq^{\beta-1}\{0, 1, \dots, q-1\}\right)$$

for $\tilde{A} \subseteq \{0, \dots, pq^{\beta-1} - 1\}$ a complete set of residues modulo p containing 0, or an analogous set with the roles of p and q interchanged. Thus $\{k : \Phi_k(x) \text{ divides } A(x)\}$ contains $\{p^\alpha\} \cup \{q^\beta, pq^\beta, p^2q^\beta, \dots, p^\alpha q^\beta\}$ or $\{q^\beta\} \cup \{p^\alpha, p^\alpha q, p^\alpha q^2, \dots, p^\alpha q^\beta\}$. If $\alpha > 1$ and $\beta > 1$, there are cyclotomic polynomial divisors of $A(x)$ in addition to the three required by (T2).

The situation when S has at least three elements is different. In this case $\mathcal{T}_S$ has members whose corresponding polynomial has only the cyclotomic polynomial divisors required by (T2). We illustrate this with the promised example. Among the members of $\mathcal{T}_{\{4,9\}}$ are $\bar{A}_0 = \{0, 3, 6, 18, 21, 24\}$ and $\bar{A}_1 = \{0, 2, 12, 14, 24, 26\}$. Each is a direct sum. Consider

$$\begin{aligned} A &= \left(\{0\} \oplus 2\bar{A}_0\right) \cup \left(\{1\} \oplus 2\bar{A}_1\right) \\ &= \{0, 1, 5, 6, 12, 25, 29, 36, 42, 48, 49, 53\} \in \mathcal{T}_{\{2,8,9\}}. \end{aligned}$$

The cyclotomic polynomial divisors of $A(x) = \bar{A}_0(x^2) + x\bar{A}_1(x^2)$ are $\Phi_2(x)$ and those $\Phi_k(x)$ which divide both $\bar{A}_0(x^2)$ and $\bar{A}_1(x^2)$, i.e.,

$$\begin{aligned}\{k : \Phi_k(x) \text{ divides } A(x)\} &= \{2\} \cup (\{8, 9, 18, 36, 72\} \cap \{8, 9, 18, 24, 72\}) \\ &= \{2, 8, 9, 18, 72\},\end{aligned}$$

exactly the set required by (T2). Then as in Theorem A, $A \oplus (B \oplus 72\mathbb{Z}) = \mathbb{Z}$ for $B = \{0, 8, 16, 18, 26, 34\}$. deBruijn's example was actually $\big(\{12\} \oplus 2\bar{A}_0\big) \cup \big(\{17\} \oplus 2\bar{A}_1\big)$. It was the first example where $A \oplus B$ is a complete set of residues modulo n but neither A nor B is periodic modulo n. Equivalently, neither A nor B is a disjoint union of translates of $(n/p)\{0, 1, \ldots, p-1\}$ for a single prime factor p of n.

References

[deB-1] deBruijn, N. G., *On bases for the set of integers*, Publ. Math. Debrecen **1** (1950), 232–242.
[deB-2] ———, *On the factorization of cyclic groups*, Indag. Math. **17** (1955), 370–377.
[deB-3] ———, *On number systems*, Nieuw Arch. Wisk. (3) **4** (1956), 15–17.
[Haj] Hajós, G., *Sur la factorisation des groupes abéliens*, Časopis Pěst. Mat. Fys. (3) **4** (1950), 157–162. (French)
[L-W] Lagarias, J. and Wang, Y., *Tiling the line with translates of one tile*, Invent. Math. **124** (1996), 341–365.
[New] Newman, D. J., *Tesselation of integers*, J. Number Theory **9** (1977), 107–111.
[San] Sands, A. D., *On Keller's conjecture for certain cyclic groups*, Proc. Edinburgh Math. Soc. (2) **22** (1977), 17–21.
[Swe] Swenson, C., *Direct sum subset decompositions of Z*, Pacific J. Math. **53** (1974), 629–633.
[Sza] Szabó, S., *A type of factorization of finite abelian groups*, Discrete Math. **54** (1985), 121–124.
[Tij] Tijdeman, R., *Decomposition of the integers as a direct sum of two subsets*, Number theory (Paris, 1992–1993), London Math. Soc. Lecture Note Ser., vol. 215, Cambridge Univ. Press, Cambridge, 1995, pp. 261–276.

Ethan M. Coven, Deparment of Mathematics, Wesleyan University, Middletown, CT 06459-0128
E-mail address: `ecoven@wesleyan.edu`

Aaron Meyerowitz, Deparment of Mathematics, Florida Atlantic University, Boca Raton, FL 33431-0991
E-mail address: `meyerowi@fau.edu`