## FULL RANK TILINGS OF FINITE ABELIAN GROUPS\*

## MICHAEL DINITZ†

Abstract. A tiling of a finite abelian group G is a pair (V,A) of subsets of G such that 0 is in both V and A and every  $g \in G$  can be uniquely written as g = v + a with  $v \in V$  and  $a \in A$ . Tilings are a special case of normed factorizations, a type of factorization by subsets that was introduced by Hajós [Casopsis Pěst Path. Rys., 74, (1949), pp. 157–162]. A tiling is said to be full rank if both V and A generate G. Cohen, Litsyn, Vardy, and Zémor [SIAM J. Discrete Math., 9 (1996), pp. 393–412] proved that any tiling of  $\mathbb{Z}_2^n$  can be decomposed into full rank and trivial tilings. We generalize this decomposition from  $\mathbb{Z}_2^n$  to all finite abelian groups. We also show how to generate larger full rank tilings from smaller ones, and give two sufficient conditions for a group to admit a full rank tiling, showing that many groups do admit them. In particular, we prove that if  $p \geq 5$  is a prime and  $n \geq 4$ , then  $\mathbb{Z}_p^n$  admits a full rank tiling. This bound on n is tight for  $1 \leq n \leq 1$ , and is conjectured to be tight for all primes  $n \leq n$ .

Key words. tiling, full rank, finite abelian group, factorization, direct sum, Hamming codes

AMS subject classifications. 05B45, 20K01

**DOI.** 10.1137/S0895480104445794

1. Introduction. Throughout this paper G is a finite abelian group. A factorization of G is a collection  $(A_1,\ldots,A_k)$  of subsets such that every  $g\in G$  can be uniquely represented as  $a_1 + \cdots + a_k$ , where  $a_i \in A_i$ . A factorization is normed if every subset in the factorization contains 0. A tiling is a special case of a normed factorization in which there are only two subsets (usually denoted V and A rather than  $A_1$  and  $A_2$ ). Any subset V for which there exists a subset A such that (V, A) is a tiling of G is called a tile of G. Cohen, Litsyn, Vardy, and Zémor first introduced this definition of a tiling in 1996 for the special case of tilings of  $\mathbb{Z}_2^n$  in [2], but it extends perfectly well to arbitrary finite abelian groups. Before then, there was no separate term for a normed factorization into two subsets, despite the fact that they had been studied by Hajós [7], Rédei [14], Sands [16], and others. The term "tiling" was a natural choice since all of [2] is phrased in terms of  $\mathbb{F}_2^n$  rather than  $\mathbb{Z}_2^n$  and a tiling of a vector space is a natural concept. In particular, tilings of the Euclidean space  $\mathbb{R}^n$  have been studied extensively (see [15, 18]). But since tilings do not depend on multiplicative structure,  $\mathbb{F}_2^n$  is identical to  $\mathbb{Z}_2^n$  with respect to tilings, and hence it suffices to look at finite abelian groups rather than vector spaces over finite fields.

The study of factorizations of finite abelian groups by subsets was introduced by Hajós in 1941 [6] as a tool to prove a conjecture on homogenous linear forms posed by Minkowski. Hajós then began to study a certain type of factorization which he called periodic (see [7]). A subset  $A \subseteq G$  is periodic if there is some nonidentity element  $g \in G$  such that g + A = A and a periodic factorization is a factorization in which one of the subsets is periodic. Hajós asked for which groups G any factorization into two subsets G = A + B necessarily has either A or B periodic. This question was eventually solved by Sands [16] after major contributions from de Bruijn [3] and Rédei [14].

<sup>\*</sup>Received by the editors August 26, 2004; accepted for publication (in revised form) September 1, 2005; published electronically March 3, 2006. This research was done at the University of Minnesota-Duluth and was supported by NSF grant DMS-0137611 and NSA grant H-98230-04-1-0050.

http://www.siam.org/journals/sidma/20-1/44579.html

<sup>&</sup>lt;sup>†</sup>Computer Science Department, Carnegie Mellon University, Pittsburgh, PA 15213 (mdinitz@cs. cmu.edu).

A group G possesses the  $R\acute{e}dei$  property if in every tiling (V,A) of G either V or A is contained in a proper subgroup of G. The question of which groups possess the Rédei property has been investigated since 1979, when Rédei [14] conjectured that  $\mathbb{Z}_p^3$  has the Rédei property for all primes p. If G does not possess the Rédei property then there is some tiling (V,A) of G in which  $\langle V \rangle = \langle A \rangle = G$ , where  $\langle S \rangle$  denotes the subgroup generated by S for any  $S \subseteq G$ . These tilings are said to be full rank [2]. Note that having the Rédei property is equivalent to not admitting a full rank tiling. Sands [17] asked whether every group has the Rédei property, which was shown not to be the case by Fraser and Gordon [5], who used results from coding theory to construct a full rank tiling of  $\mathbb{Z}_5^6$  as a counterexample.

Until recently the only motivation for studying full rank tilings was to find out which groups had the Rédei property. Then in 1996 Cohen, Litsyn, Vardy, and Zémor [2] found that any tiling of  $\mathbb{Z}_2^n$  can be decomposed into full rank tilings and trivial tilings (a tiling is trivial if one of V or A is  $\mathbb{Z}_2^n$  and the other is just the zero vector). This provided extra motivation for studying which elementary 2-groups (groups of the form  $\mathbb{Z}_2^n$ ) admit full rank tilings (or equivalently do not have the Rédei property). Cohen, Litsyn, Vardy, and Zémor [2] showed that there do not exist full rank tilings of  $\mathbb{Z}_2^n$  when  $n \leq 7$  and that there do exist full rank tilings of  $\mathbb{Z}_2^n$  when  $n \geq 112$ . Etzion and Vardy [4] then constructed full rank tilings for  $n \geq 14$  using techniques that, together with unpublished work of LeVan and Phelps, were used to construct full rank tilings when  $n \geq 10$ . Trachtenberg and Vardy then proved that  $\mathbb{Z}_2^8$  does not admit a full rank tiling [24], and the question of full rank tilings of  $\mathbb{Z}_2^n$  was resolved when Östergard and Vardy [9] showed that  $\mathbb{Z}_2^9$  does not admit a full rank tiling. All of the work done on full rank tilings of  $\mathbb{Z}_2^n$  was actually done in terms of  $\mathbb{F}_2^n$ , since the authors were approaching the problem from a coding theory perspective and were apparently not aware of much of the work done on the Rédei property or the connection of full rank tilings to it.

It is interesting to note that work on full rank tilings of  $\mathbb{F}_2^n$  and work on the Rédei property have proceeded almost independently. In the paper which started work on tilings of  $\mathbb{F}_2^n$ , Cohen, Litsyn, Vardy, and Zémor [2] reference the work of Hajós on periodic factorizations but do not reference any of the work done on the Rédei property, and neither do any of the papers mentioned above that extend the work of [2]. The only exception to this is a paper by Szabó and Ward [21] in which they reference work done on the Rédei property to prove the existence of full rank tilings of  $\mathbb{F}_2^n$  for  $n \geq 14$ .

We begin in section 2 by generalizing the decomposition of Cohen, Litsyn, Vardy, and Zémor [2, section 6] from  $\mathbb{Z}_2^n$  to arbitrary finite abelian groups. Then in section 3 we generalize a construction of Etzion and Vardy [4, section 5] and Szabó and Ward [21, Lemma 1] to create a full rank tiling of a group from a full rank tiling of one of its direct factors. Using this we devise two sufficient conditions for a group to admit a full rank tiling, showing that many groups admit them. The first condition states a group admits a full rank tiling if it contains as a direct factor a subgroup of the type  $\mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c$  with a, b, and c composite. This is based on work done by Szabó in [19]. Then in section 4 we extend the work done for  $\mathbb{Z}_2^n$  by showing that any group containing  $\mathbb{Z}_p^n$  with  $p \geq 5$  prime and n = 4 as a direct factor admits a full rank tiling. Thus, there exists a full rank tiling of  $\mathbb{Z}_p^n$  if  $p \geq 5$  is prime and  $n \geq 4$ . A conjecture of Rédei [14] implies that this is tight for all primes. This conjecture has been verified for primes less than or equal to 11 by Szabó and Ward [22], which completely solves the question of whether there exist full rank tilings of  $\mathbb{Z}_p^n$  when p is 5, 7, or 11. We conclude by discussing some remaining open problems on tilings.

**2. Decomposition of tilings.** In this section we study how tilings of arbitrary finite abelian groups can be recursively decomposed, generalizing some of the work done in [2] for  $\mathbb{Z}_2^n$ . We first develop a certain characterization of tilings which will prove particularly useful. The notation V - V denotes  $\{v_1 - v_2 : v_1, v_2 \in V\}$ .

PROPOSITION 1. Let  $V, A \subseteq G$  with  $0 \in V$  and  $0 \in A$ . Then (V, A) is a tiling of G if and only if  $(V - V) \cap (A - A) = \{0\}$  and |V||A| = |G|.

*Proof.* Suppose that  $(V - V) \cap (A - A) = \{0\}$  and |V||A| = |G|. Assume that  $v_1 + a_1 = v_2 + a_2$ . Then  $v_1 - v_2 = a_2 - a_1 = 0$ , so  $v_1 = v_2$  and  $a_1 = a_2$ , and thus the representation of each element of V + A is unique. Since |V||A| = |G|, we have that V + A = G and thus (V, A) is a tiling of G.

Now let (V, A) be a tiling of G, and suppose that  $(V - V) \cap (A - A) \neq \{0\}$ . Then there exist distinct elements  $v_1$  and  $v_2$  in V and  $a_1$  and  $a_2$  in A such that  $v_1 - v_2 = a_1 - a_2$ , and so  $v_1 + a_2 = v_2 + a_1$ . Thus (V, A) is not a tiling. If  $(V - V) \cap (A - A) = \{0\}$  and  $|V||A| \neq |G|$ , then clearly |V||A| < |G| so some element of G is not in V + A and thus (V, A) is not a tiling.  $\square$ 

Note that the |V||A| = |G| condition can be replaced with the condition V + A = G if needed. To motivate our discussion of full rank tilings, we give one reason why the subgroup generated by a tile is of interest.

PROPOSITION 2. A subset  $V \subseteq G$  is a tile of G if and only if it is a tile of  $\langle V \rangle$ .

*Proof.* Suppose that V is a tile of  $\langle V \rangle$ . Since  $\langle V \rangle$  is a subgroup of G it is clearly a tile of G. Let  $(\langle V \rangle, A_1)$  be a tiling of G and let  $(V, A_0)$  be a tiling of  $\langle V \rangle$ . Then clearly  $(V, A_0 + A_1)$  is a tiling of G.

Suppose that (V,A) is a tiling of G. Let  $A_0 = A \cap \langle V \rangle$ . Since  $A_0 \subseteq A$  and  $(V-V) \cap (A-A) = \{0\}$ , we have that  $(V-V) \cap (A_0-A_0) = \{0\}$ . Clearly  $V+A_0 \subseteq \langle V \rangle$ . Since  $\langle V \rangle \subseteq G = V+A$ , any  $w \in \langle V \rangle$  can be written as w=v+a with  $v \in V$  and  $a \in A$ . Then  $a=w-v \in \langle V \rangle$  since  $\langle V \rangle$  is a subgroup, and so  $a \in A_0$ . Hence  $\langle V \rangle \subseteq V+A_0$ , so  $V+A_0 = \langle V \rangle$  and thus  $(V,A_0)$  is a tiling of  $\langle V \rangle$ .  $\square$ 

Because of this proposition we are naturally interested in tilings (V, A) in which  $\langle V \rangle = G$ . Tilings with this property are called *proper tilings*, a term devised by Cohen, Litsyn, Vardy, and Zémor [2] that was originally used only for tilings of  $\mathbb{Z}_2^n$ . The following theorem is a generalization to arbitrary finite abelian groups of Theorem 6.2 in [2], the original decomposition showing that every tiling of  $\mathbb{Z}_2^n$  can be decomposed into proper tilings of its subgroups. This generalization shows that the classification of all tilings of G can be reduced to the study of all proper tilings of the subgroups of G.

Theorem 3. Let V be a tile of G with  $\langle V \rangle \neq G$ . Let z = |G|/|V|, and let  $m = |G|/|\langle V \rangle|$ . The pair (V,A) is a tiling of G if and only if A has the following form:

- 1. For i = 0, 1, ..., m 1, let  $A_i \subset \langle V \rangle$  be such that  $(V, A_i)$  is a tiling of  $\langle V \rangle$ .
- 2. Let  $c_0 = 0, c_1, \dots, c_{m-1}$  be a set of coset representatives for  $G/\langle V \rangle$ . Then

(1) 
$$A = A_0 \cup (c_1 + A_1) \cup \cdots \cup (c_{m-1} + A_{m-1}).$$

*Proof.* Suppose that A is as in (1). Then  $|A_i| = z/m$  so |A| = z and |V||A| = |G|. So we just need to show that  $(V - V) \cap (A - A) = \{0\}$ . Note that any element of A - A has one of the following forms:

- 1.  $(c_i + a_i) (c_i + a_i) = 0$ ,
- 2.  $(c_i + a_{i1}) (c_i + a_{i2}) = a_{i1} a_{i2}$ , or
- 3.  $(c_i + a_i) (c_i + a_i)$ , for  $i \neq j$ ,

where  $a_i, a_{i1}, a_{i2}, a_j \in A$ . Let U denote the set of elements of type 2, and let W denote the set of elements of type 3. Clearly any element of U is also an element of some  $A_i - A_i$ , so since  $(V - V) \cap (A_i - A_i) = \{0\}$  for all i we have that  $(V - V) \cap U = \{0\}$ . Since  $c_i - c_j \notin \langle V \rangle$  for all  $i \neq j$  and  $A_i \subset \langle V \rangle$  for all i, it follows that  $\langle V \rangle$  and W are disjoint, so  $(V - V) \cap W = \emptyset$  and hence (V, A) is a tiling of G.

Now let (V,A) be a tiling of G. Pick a set of representatives  $c_0=0,c_1,\ldots,c_{m-1}$  of  $G/\langle V\rangle$  and let  $A_i=-c_i+(A\cap(c_i+\langle V\rangle))$ . We start by showing that we can always pick representatives of  $G/\langle V\rangle$  so that  $0\in A_i$  for all i. If  $0\not\in A_i$  for some i, then let  $a_i\in A_i$  and let  $c_i'=a_i+c_i$ . Note that  $c_i'$  represents the same coset of  $\langle V\rangle$  as  $c_i$  since  $a_i\in A_i\subset \langle V\rangle$ . If we let  $A_i'$  be the set we get by replacing  $c_i$  with  $c_i'$  in the definition of  $A_i$ , then we get that  $A_i'=-a_i-c_i+(A\cap(a_i+c_i+\langle V\rangle))=-a_i+A_i$ . Together with the fact that  $a_i\in A_i$ , this gives us that  $0\in A_i'$ , so we could have simply started with  $c_i'$  instead of  $c_i$ . Thus we can assume the  $0\in A_i$  for all i.

We have that  $c_i + A_i = A \cap (c_i + \langle V \rangle)$ , so

(2) 
$$\bigcup_{i=0}^{m-1} (c_i + A_i) = \bigcup_{i=0}^{m-1} (A \cap (c_i + \langle V \rangle)) = A.$$

Now we need to show that  $(V, A_i)$  is a tiling of  $\langle V \rangle$  for all i. Any element of  $A_i$  is of the form  $-c_i + a$ , so any element of  $A_i - A_i$  is of the form  $a_1 - a_2$ . So  $A_i - A_i \subseteq A - A$  and thus  $(A_i - A_i) \cap (V - V) = \{0\}$ . Note that  $A_i \subset \langle V \rangle$ , so  $V + A_i \subseteq \langle V \rangle$ . Thus to establish that  $(V, A_i)$  is a tiling of  $\langle V \rangle$ , it remains to show that  $|A_i| = z/m$ . Since  $(V - V) \cap (A_i - A_i) = \{0\}$  and  $V + A_i \subseteq \langle V \rangle$ , we obviously have that  $|A_i| \le z/m$ . However,  $z = |A| \le \sum_{i=0}^{m-1} |A_i|$  by (2), so  $|A_i| = z/m$  for all i.  $\square$ 

Theorem 3 implies that if all of the proper tilings of the subgroups of G are known, then we can construct all the tilings of G. However, proper tilings can be decomposed further by simply switching the roles of V and A. Suppose that (V, A) is a (proper) tiling of  $\langle V \rangle$ , and consider the tiling (A, V). Unless  $\langle A \rangle = \langle V \rangle$  this tiling is not proper, so by the above theorem

(3) 
$$V = V_0 \cup (c_1 + V_1) \cup \cdots \cup (c_{m-1} + V_{m-1}),$$

where  $(A, V_i)$  is a proper tiling of  $\langle A \rangle$  for all i and the elements  $0, c_1, \ldots, c_m$  are representatives of  $\langle V \rangle / \langle A \rangle$ . So by using (3), each of the tilings  $(V, A_i)$  of Theorem 3 can be decomposed into tilings of subgroups unless  $\langle V \rangle = \langle A_i \rangle$ . This process can be iterated until the remaining tilings are either trivial or of full rank. So any tiling can be decomposed into full rank and trivial tilings of its subgroups.

We can, however, decompose full rank tilings even further, into nonperiodic full rank tilings. For any subset  $A \subseteq G$ , let  $A_0 = \{g \in G : g + A = A\}$  denote the set of periodic points of A. By definition  $A_0 = \{0\}$  if and only if A is nonperiodic. In the literature  $A_0$  is sometimes referred to as the *kernel* of A (see [1, 10, 12]), particularly in regard to tilings derived from codes. Note that if  $0 \in A$ , then  $A_0 \subseteq A$ . The following proposition is rather obvious, first appearing in terms of codes over GF(2) [1], but can easily be generalized to finite abelian groups.

PROPOSITION 4. If  $0 \in A$ , then  $A_0$  is a subgroup of G contained in A and A is the union of disjoint cosets of  $A_0$ .

*Proof.* Let  $a_1, a_2 \in A_0$ . Then  $(a_1 + a_2) + A = a_1 + (a_2 + A) = a_1 + A = A$ , so  $a_1 + a_2 \in A_0$ . Since every  $a \in A_0$  has some finite order this implies that  $-a \in A_0$  and thus  $A_0$  is a subgroup of G. Now let  $a \in A$ . Then  $a + A_0 \in A$  by the definition of

 $A_0$ , so A is the union of cosets of  $A_0$ . These cosets are clearly disjoint since  $A_0$  is a subgroup of G, proving the proposition.  $\square$ 

If  $A' \subseteq A$  is a set of representatives for  $A/A_0$ , then it follows from this proposition that  $A' + A_0 = A$ . Now we show how to reduce tilings by the kernel of one of the subsets.

THEOREM 5. Let (V, A) be a tiling of G, and let  $A_0$  be the kernel of A. Then  $(V/A_0, A/A_0)$  is a tiling of  $G/A_0$ .

*Proof.* Let  $\varphi: G \to G/A_0$  be the natural homomorphism. Suppose that the restriction of  $\varphi$  to V (which takes V to  $V/A_0$ ) is not one-to-one. Then there exist distinct elements  $v_1$  and  $v_2$  in V such that  $\varphi(v_1) = \varphi(v_2) = v' + A_0$ . So  $\varphi(v_1 - v_2) = \varphi(v_1) - \varphi(v_2) = (v' + A_0) - (v' + A_0) = A_0$ , which implies that  $v_1 - v_2 \in A_0$ . This is a contradiction since  $A_0 \subseteq A$  and  $(V - V) \cap (A - A) = \{0\}$ . Hence  $|V/A_0| = |V|$ , and thus  $|V/A_0| \cdot |A/A_0| = |G/A_0|$ .

Suppose that there exist distinct elements  $v_1'$  and  $v_2'$  in  $V/A_0$  and  $a_1'$  and  $a_2'$  in  $A/A_0$  such that  $v_1' - v_2' = a_1' - a_2'$ . Then there exist  $v_1, v_2 \in V, v_1 \neq v_2$  and  $a_1, a_2 \in A, a_1 \neq a_2$  such that  $(v_1 - v_2) + A_0 = (a_1 - a_2) + A_0$ . So there is some  $a_0 \in A_0$  such that  $v_1 - v_2 = a_1 - a_2 + a_0$ , and since  $a_0 \in A_0$  this implies that there is some  $a_3 \in A$  such that  $v_1 - v_2 = a_1 - a_3$ , which is a contradiction since  $(V - V) \cap (A - A) = \{0\}$ . Thus  $(V/A_0, A/A_0)$  is a tiling of  $G/A_0$ .

PROPOSITION 6. If (V, A) is a full rank tiling of G, then  $(V/A_0, A/A_0)$  is a full rank tiling of  $G/A_0$ .

*Proof.* We know from Theorem 5 that  $(V/A_0, A/A_0)$  is a tiling of  $G/A_0$ , so we just need to show that it is full rank. Let  $w + A_0 \in G/A_0$ . Since  $\langle V \rangle = G$ , there are  $v_1, \ldots, v_k \in V$ , not necessarily distinct, such that  $v_1 + \cdots + v_k = w$ . Then  $(v_1 + A_0) + \cdots + (v_k + A_0) = w + A_0$ . Hence  $\langle V/A_0 \rangle = G/A_0$ . By the same argument,  $\langle A/A_0 \rangle = G/A_0$ , so  $(V/A_0, A/A_0)$  is a full rank tiling of  $G/A_0$ .

The following propositions concern the periodicity of the tiling resulting from this decomposition.

Proposition 7.  $A/A_0$  is nonperiodic.

*Proof.* Let a be a periodic point of  $A/A_0$ , and let A' be a set of representatives for  $A/A_0$  including 0. Let  $c+A_0$  represent a, where  $c \in A'$ . Then clearly c is a periodic point of A and so is an element of  $A_0$ . However,  $A' \cap A_0 = \{0\}$ , and hence c = 0, so a = 0.

PROPOSITION 8.  $V/A_0$  is periodic if V is periodic.

*Proof.* Let  $v_0$  be a nonzero periodic point of V. Then since  $v_0 + v \in V$  for any  $v \in V$ , we have that  $\varphi(v_0) + \varphi(v) \in \varphi(V)$ , so  $\varphi(v_0)$  is a periodic point of  $V/A_0$ . From the proof of Theorem 5 we know that  $|V| = |V/A_0|$ , so  $\varphi(v_0) \neq 0$  and thus  $V/A_0$  is periodic.  $\square$ 

By Proposition 8, after an application of Theorem 5 we can switch  $V/A_0$  and  $A/A_0$  and apply it again. Since at each iteration one of the subsets loses all of its periodic points, this might seem to imply that this recursion never needs to be carried out more than twice, but it turns out that the other subset can acquire new periodic points. Cohen, Litsyn, Vardy, and Zémor [2, section 8] provide an example of this in  $\mathbb{Z}_2^7$ . The recursion will stop eventually, though, so we are interested not only in full rank tilings but especially in nonperiodic full rank tilings. Note that Proposition 6 also gives us a way to construct smaller full rank tilings from larger ones, which is helpful when trying to determine which groups admit full rank tilings.

3. Constructing full rank tilings of product groups. Etzion and Vardy [4, Construction C] developed a construction to build a full rank tiling of  $\mathbb{Z}_2^{n+1}$  from a

full rank tiling of  $\mathbb{Z}_2^n$ , and Szabó and Ward [21, Lemma 1] developed a similar but more general construction to allow the direct product with arbitrary cyclic groups rather than just  $\mathbb{Z}_2$ . We generalize both of these to a construction that gives a full rank tiling of any finite abelian group having some direct factor with a full rank tiling.

Theorem 9. If there is a full rank tiling (V, A) of G, then there is a full rank tiling of  $G \times H$ , where G is any nontrivial finite abelian group and H is any finite abelian group.

Proof. Szabó and Ward [21, Lemma 1] proved this for the case when  $H = \langle k \rangle$  is cyclic and there is an element  $a \in A \setminus \{0\}$  such that  $\langle A \setminus \{a\} \rangle = G$ . They did this by letting  $V' = \{(v,h) : v \in V, h \in H\}$  and  $A' = \{(a',0) : a' \in (A \setminus \{a\})\} \cup \{(a,k)\}$  and proving that (V',A') is a full rank tiling of  $G \times H$ . Note that the element (0,k) is not necessary for  $\langle V' \rangle$  to equal  $G \times H$  since (v,k) and (v,k+k) are both elements of V' and (v,k+k) - (v,k) = (0,k). So we can switch the roles of V' and V' are both elements of V' and V' and V' and V' and V' and V' are both elements of V' and V' and V' and V' are both elements of V' and V' and V' and V' and V' are both elements of V' and V' and V' and V' are both elements of V' and V' and V' and V' are both elements of V' and V' and V' and V' are both elements of V' and V' and V' and V' are both elements of V' and V' and V' are both elements of V' and V' and V' are both elements of V' and V' and V' are both elements of V' and V' are both

The only case when there is not such an a is when both  $A \setminus \{0\}$  and  $V \setminus \{0\}$  are minimal generating sets of G. Let m equal the sum of the multiplicities of the prime divisors of |G|. We first show that any minimal generating set of G has at most m elements. Let  $A = \{a_1, \ldots, a_k\}$  be a minimal generating set of G. Let  $G_i = \langle a_1, \ldots, a_i \rangle$ , where  $G_0 = \{0\}$ . Note that  $\prod_{i=0}^{k-1} |G_{i+1}|/|G_i| = |G|$ . We know that  $G_i$  is a proper subgroup of  $G_{i+1}$  since A is a minimal generating set, which means that  $|G_{i+1}|/|G_i| > 1$  for all i. Hence  $k \leq m$ . So if (V,A) is a full rank tiling and  $V \setminus \{0\}$  and  $A \setminus \{0\}$  are both minimal generating sets, then  $(m+1)^2 \geq |G|$ . Clearly  $m \leq \lfloor \log_2 |G| \rfloor$ , so  $(\lfloor \log_2 |G| \rfloor + 1)^2 \geq |G|$ . This is true only if  $1 \leq |G| \leq 36$ . Since |G| = |V||A|, it is only possible for both V and A to have at most m+1 elements when |G| is 2, 4, 6, 8, 9, 12, or 16, so we consider the finite abelian groups of those orders. Clearly any tiling of  $\mathbb{Z}_2$  is trivial. Rédei [13] proved that if both V and A have prime order, then one of them is a subgroup of G, which implies that there are no full rank tilings of  $\mathbb{Z}_2 \times \mathbb{Z}_2$ ,  $\mathbb{Z}_6$ ,  $\mathbb{Z}_3 \times \mathbb{Z}_3$ ,  $\mathbb{Z}_4$ , or  $\mathbb{Z}_9$ .

For the |G| = 8, |G| = 12, and |G| = 16 cases we need a few results on the Hajós property. We say that a finite abelian group G has the Hajós property if in any tiling (V, A) of G at least one of V and A is periodic. Groups with the Hajós property have been completely classified [16]. In particular, all finite abelian groups of order 8, 12, or 16 have the Hajós property. Szabó [20, Lemma 1] has shown that if a finite abelian group has the Hajós property, then it has no full rank tilings.  $\Box$ 

Szabó [19, section 4] has proven that there exists a full rank tiling of the direct product of at least three cyclic groups of composite orders other than 4 or 6. We remove the restriction that the orders not be 4 or 6 and combine it with Theorem 9 to get the following theorem.

THEOREM 10. If G has  $\mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c$  as a direct factor, where a, b, c are composite, then G has a full rank tiling.

*Proof.* Let G be the direct product of cyclic groups of orders  $m_1, m_2, m_3$  (all composite) and generators  $g_1, g_2, g_3$  respectively. Let  $v_i = m_i/u_i$ , where  $u_i$  is the smallest prime divisor of  $m_i$ . Also let  $[g]_m$  denote the set  $\{0, g, 2g, \ldots, (m-1)g\}$ . If  $V = \{(a, b, c) : a \in [g_1]_{u_1}, b \in [g_2]_{u_2}, c \in [g_3]_{u_3}\}$  and  $A = \{(a, b, c) : a \in [u_1g_1]_{v_1}, b \in [u_2g_2]_{v_2}, c \in [u_3g_3]_{v_3}\}$ , then it is not hard to see that (V, A) is a tiling of G. Let  $\pi$  be some cyclic permutation of  $\{1, 2, 3\}$ , and define the following two sets:

$$\begin{split} X &= \bigcup_{i=1}^{3} \{(a_1,a_2,a_3): a_i \in [u_ig_i]_{v_i} \text{ and } a_{\pi(i)} = u_{\pi(i)}g_{\pi(i)} \text{ and } a_{\pi^{-1}(i)} = 0\} \\ Y &= \bigcup_{i=1}^{3} \{(a_1,a_2,a_3): a_i \in [u_ig_i]_{v_i} + g_i \text{ and } a_{\pi(i)} = u_{\pi(i)}g_{\pi(i)} \text{ and } a_{\pi^{-1}(i)} = 0\}. \end{split}$$

Note that  $X \subset A$ . Szabó [19, section 2] proved that if  $A' = A \cup Y \setminus X$  then (V, A') is a tiling of G, and the tiling is full rank if  $v_i$  is at least 4 for all i. Note that if  $j = \pi(i)$  and  $v_j = 3$  then  $0, u_j g_j + g_i, 2u_j g_j \in A'$ , so  $2u_j g_j + (u_j g_j + g_i) = g_i \in \langle A' \rangle$ . If  $v_j > 3$  then  $3u_j g_j \in A'$ , so  $3u_j g_j - 2u_j g_j = u_j g_j \in \langle A' \rangle$  and thus  $u_j g_j + g_i - u_j g_j = g_i \in \langle A' \rangle$ . So if every  $v_i$  is at least 3 then (V, A') is a full rank tiling of G.

If  $v_i = 2$  for all i then  $u_i = 2$ , and G is the group  $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$ . It is easy to check by hand that Szabó's construction results in a full rank tiling. In the final case, there is some  $v_j > 2$ . Let  $i = \pi^{-1}(j)$ . Then by the above argument  $g_i \in \langle A' \rangle$ . Let  $k = \pi(j)$ . Since  $\pi$  is cyclic,  $k = \pi^{-1}(i)$ . By definition  $u_i g_i + g_k \in A'$ , so since  $g_i \in \langle A' \rangle$  we have that  $g_k \in \langle A' \rangle$ . Also,  $u_k g_k + g_j \in A'$ , so  $g_j \in \langle A' \rangle$ . Thus  $\langle A' \rangle = G$ , so (V, A') is a full rank tiling of G. Now by Theorem 9 any group containing G as a direct factor has a full rank tiling, which proves the theorem.  $\square$ 

4. Constructions using codes. In this section we get another sufficient condition for G to admit a full rank tiling by using codes. We will work in vector spaces over finite fields in this section since we will on occasion use properties of the vector space. However, as noted in the introduction a tiling of a vector space is also a tiling of the additive group associated with that space, so at the end of the section we translate our main result back to groups. Throughout this section p is a prime. The Hamming distance of two n-tuples is the number of coordinates in which they differ. A perfect code is a subset  $C \subset \mathbb{F}_q^n$  such that  $(C, S_R(0))$  is a tiling of  $\mathbb{F}_q^n$ , where  $S_R(0)$  is the Hamming ball of radius R centered on 0 [8]. Since a Hamming ball clearly generates the entire space, this gives a full rank tiling if the code itself generates the entire space. An important special case of perfect codes are the Hamming codes, which are the linear perfect codes for R = 1 (see [8]). A Hamming code forms a proper subspace of  $\mathbb{F}_q^n$ , and so does not immediately result in a full rank tiling. However, we will see how to slightly modify a Hamming code to get a full rank tiling.

Sands posed the question of whether every group has the Rédei property in [17]. Answering this question in the negative, Fraser and Gordon [5] constructed a full rank tiling of  $\mathbb{F}_5^6$  by applying permutations of GF(5) to a Hamming code. They state that their construction generalizes to provide an infinite number of counterexamples, but they omit the details. We begin by generalizing their argument to show that there exist full rank tilings of  $\mathbb{F}_p^{p+1}$ , where  $p \geq 5$  is prime. We do this by starting out with the same code they do, a Hamming code on  $\mathbb{F}_p^{p+1}$ , and then permute the values in the first two coordinates of the vectors in the code. Permuting only the first two coordinates is a property that will prove important when computing the kernel. Let  $p \geq 7$  be prime and let H be the following  $2 \times (p+1)$  matrix:

$$H = \left(\begin{array}{ccccc} 0 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & 2 & \cdots & p-1 \end{array}\right).$$

Let  $C = \{u \in \mathbb{F}_p^{p+1} : Hu^T = 0\}$ . It is easy to show that C is a Hamming code, which implies that  $(C, S_1(0))$  is a tiling of  $\mathbb{F}_p^{p+1}$ . It is not a full rank tiling since C is a proper subspace of  $\mathbb{F}_p^{p+1}$  of dimension p-1. Let  $u_i = (p-i, p-1, 0, \dots, 0, 1, 0, \dots, 0)$ , where the 1 is in the (i+2)nd coordinate. Note that  $\{u_1, u_2, \dots, u_{p-1}\}$  is a basis for C.

Now let  $\pi_i$ , for i = 1, ..., p + 1, be permutations of the elements of GF(p). Then the map

$$\pi: (x_1, \dots, x_{p+1}) \mapsto (\pi_1(x_1), \dots, \pi_{p+1}(x_{p+1}))$$

from  $\mathbb{F}_p^{p+1}$  to itself clearly preserves the Hamming distance. Hence  $\pi(C)$  is still a perfect code with R=1 for any choice of the  $\pi_i$ 's. We will use this fact to construct full rank tilings from C.

PROPOSITION 11. There exists a full rank tiling of  $\mathbb{F}_p^{p+1}$  if  $p \geq 5$ .

Proof. Let  $\pi_1 = ((p-3)(p-4))$  be the transposition interchanging p-3 and p-4, let  $\pi_2 = ((p-2)(p-3))$  be the transposition interchanging p-2 and p-3, and let every other  $\pi_i$  be the identity permutation. We claim that  $(\pi(C), S_1(0))$  is a full rank tiling of  $\mathbb{F}_p^{p+1}$  for  $p \geq 7$ . The basis we constructed of  $\mathbb{F}_p^{p+1}$  gets mapped to p-1 linearly independent vectors since only the first two coordinates get permuted. Also,  $\pi(u_1+u_2)=(p-4,p-3,1,1,0,\ldots,0)$  is another linearly independent vector, since otherwise the 1's in the third and fourth coordinates would force it to equal  $\pi(u_1) + \pi(u_2)$ , which it does not since  $\pi(u_1) + \pi(u_2) = (p-3,p-2,1,1,0,\ldots,0)$ .

Now consider the vector  $\pi(u_5 + u_{p-1}) = (p-3, p-3, 0, \dots, 0, 1, 0, \dots, 0, 1)$ , where the 1's are in the seventh and the p+1st coordinates. Assume that this is a linear combination of the previous p vectors. Because of the placement of the 1's it is clear that  $\pi(u_5)$  and  $\pi(u_{p-1})$  each have a coefficient of 1 in this linear combination, so the remaining parts of the linear combination must sum to  $\pi(u_5 + u_{p-1}) - \pi(u_5) - \pi(u_{p-1}) = (1, p-1, 0, \dots, 0)$ . Clearly the remaining  $\pi(u_i)$ 's other than  $\pi(u_1)$  and  $\pi(u_2)$  do not appear in the linear combination. The only way  $\pi(u_1)$  and  $\pi(u_2)$  can contribute is if each has the negative coefficient of  $\pi(u_1 + u_2)$ . If x is the coefficient of  $\pi(u_1 + u_2)$ , then we get the following two equations from the first and second coordinate, respectively:

$$(p-1)(-x) + (p-2)(-x) + (p-4)x = 1$$

$$(p-1)(-x) + (p-1)(-x) + (p-3)x = p-1$$

The left-hand side of each equation simplifies to (p-1)x, which is a contradiction since (p-1)x cannot equal both 1 and p-1. Thus the coefficients of  $\pi(u_1)$ ,  $\pi(u_2)$ , and  $\pi(u_1+u_2)$  are zero, so  $\pi(u_5+u_{p-1})=\pi(u_5)+\pi(u_{p-1})$ . However, this is a contradiction since  $\pi(u_5)+\pi(u_{p-1})=(p-4,p-2,\ldots)$ . Hence  $\{\pi(u_i):1\leq i\leq p-1\}\cup \{\pi(u_1+u_2)\}\cup \{\pi(u_5+u_{p-1})\}$  is a linearly independent set of size p+1, and therefore forms a basis of  $\mathbb{F}_p^{p+1}$ . Thus  $\langle \pi(C)\rangle=\mathbb{F}_p^{p+1}$ , so  $(\pi(C),S_1(0))$  is a full rank tiling of  $\mathbb{F}_p^6$  given by Fraser and Gordon starts with the same basis as our construction  $(\{u_1,u_2,\ldots,u_{p-1}\})$  and just uses different permutations (still only changing the elements in the first two coordinates).  $\square$ 

To get even smaller full rank tilings we find the kernel of  $\pi(C)$  and use Proposition 6.

PROPOSITION 12. There exist full rank tilings of  $\mathbb{F}_p^4$  when  $p \geq 5$ .

Proof. Since C is a Hamming code, it is a subgroup of  $\mathbb{F}_p^{p+1}$ , and so every element of C is a periodic point. The map  $\pi$  used in Proposition 11 only changes the first two coordinates of a vector, so any element of C that has 0's in the first and second coordinates is still a periodic point of  $\pi(C)$ . We claim that these vectors form a subspace of dimension at least p-3. To see this, let  $u_i = (0,0,\ldots,0,1,0,\ldots,0,i-1,p-i)$ , where the 1 is in the *i*th coordinate, for  $3 \le i \le p-1$ . Note that 1+(i-1)

1) + (p-i) = 0 and i-2+(i-1)(p-2)+(p-i)(p-1) = 0, so  $Hu_i^T = 0$  for all i, and thus each of these p-3 vectors is a periodic point of  $\pi(C)$ . They are linearly independent, which shows that the periodic points form a subspace of dimension at least p-3. Thus by Proposition 6 there is a full rank tiling of  $\mathbb{F}_p^4$ .  $\square$ 

Now we use Proposition 12 to obtain another sufficient condition for a finite abelian group to admit a full rank tiling.

THEOREM 13. If G has  $\mathbb{Z}_p^4$  with  $p \geq 5$  as a direct factor, then G admits a full rank tiling.

*Proof.* Proposition 12 proves that there exists a full rank tiling of  $\mathbb{F}_p^4$ . Since tilings depend only on the additive group structure, this is the same thing as saying that there is a full rank tiling of  $\mathbb{Z}_p^4$ . Combining this with Theorem 9 we get that any group containing  $\mathbb{Z}_p^4$  as a direct factor has a full rank tiling.  $\square$ 

Rédei [14] conjectured that there do not exist full rank tilings of  $\mathbb{Z}_p^3$  for any p. This conjecture is still open, but it has been verified for  $p \leq 11$  (see [22]), so when p is 5, 7, or 11 we know exactly for which values of n there is a full rank tiling of  $\mathbb{Z}_n^n$ .

Unfortunately we could not get as strong a bound for the case when p=3. The construction that we have been using does not work when p=3, so we need to use something else. Phelps, Rifa, and Villanueva [11] have recently found full rank perfect codes of  $\mathbb{F}_p^n$  when  $n=(p^m-1)/(p-1)$ , where  $m\geq 4$ , with a kernel of dimension  $(p-1)^{m-1}$ . So when p=3 this gives the existence of full rank tilings for  $\mathbb{Z}_3^n$  for all  $n\geq ((p^4-1)/(p-1))-(p-1)^3=4p^2-2p+2=32$ . Thus there exists a full rank tiling of  $\mathbb{Z}_3^n$  if  $n\geq 32$ . This is not nearly as good a bound as we have for either p=2 or  $p\geq 5$ , so it can almost definitely be improved. The only lower bound in the literature says that there do not exist full rank tilings of  $\mathbb{Z}_3^n$  when  $n\leq 4$  [23], so it is not known whether  $\mathbb{Z}_3^n$  admits a full rank tiling for  $1\leq n\leq 3$ .

**5. Open problems.** Probably the most tractable open problem remaining is the one mentioned at the end of the last section, the existence of full rank tilings of  $\mathbb{Z}_3^n$  for  $5 \le n \le 31$ . Since p = 3 allows more freedom in the construction than p = 2 but less than p = 5, we conjecture that there is some k with  $4 < k \le 10$  for which  $\mathbb{Z}_3^n$  has a full rank tiling if and only if  $n \ge k$ . As with other cases of  $\mathbb{Z}_p^n$ , we suspect that coding theory approaches will prove valuable, in particular finding full rank perfect ternary codes.

A more difficult open question is what conditions on G are necessary for G to admit a full rank tiling. We know that neither of our two sufficient conditions is necessary on its own, and we suspect that it is not necessary for either of them to be satisfied for G to have a full rank tiling. We have shown that many groups admit full rank tilings, so our conditions are close to necessary, but there is no reason to think that we have characterized all groups admitting full rank tilings. An easier subproblem of this is Rédei's conjecture, mentioned previously, that  $\mathbb{Z}_p^3$  does not admit a full rank tiling for any prime p. This conjecture is still wide open, with the only progress being a computer check for  $p \leq 11$  by Szabó and Ward [22]. This conjecture immediately implies that our bound of  $n \geq 4$  for the existence of full rank tilings of  $\mathbb{Z}_p^n$  with  $p \geq 5$  is tight and so if proved would give a complete characterization of which elementary p-groups  $(p \geq 5)$  admit full rank tilings.

There are many generalizations of this problem that could also prove to be interesting. Tilings can easily be defined for groups that are not finite or abelian, so removing those constraints gives many questions. We could also extend the work done for  $\mathbb{F}_2^n$  in a different direction by considering not more general groups but more general transformations. We have pointed out that vector spaces are equivalent to groups

with respect to tilings, but that is not true if we allow linear or affine transformations other than translation. Define an affine factorization of  $\mathbb{F}_q^n$  to be a pair  $(V, \Phi)$  with V a subset of  $\mathbb{F}_q^n$  and  $\Phi = \{\phi_i\}$  a set of affine transformations satisfying  $\mathbb{F}_q^n = \bigcup_i \phi_i(V)$  and  $\phi_i(V) \cap \phi_j(V) = \emptyset$  for all  $i \neq j$ . Any tiling (V, A) of  $\mathbb{F}_q^n$  automatically gives an affine factorization  $(V', \Phi)$  by letting V' = V and  $\phi_i \in \Phi$  be translation by the ith element of A. However, tilings only give a small subset of affine factorizations. Allowing arbitrary affine transformations seems to make the problem very difficult, but perhaps adding some extra restrictions would make it tractable. In particular, requiring that  $|\phi_i(V)| = |V|$  for all i might be helpful.

**6. Conclusions.** We have generalized the notions of tilings and full rank tilings from  $\mathbb{F}_2^n$  to general finite abelian groups and have generalized many existing theorems to this new setting. We then combined and extended these results to prove that a group admits a full rank tiling if any of its direct factors do, allowing us to take any sufficient condition for a group to admit a full rank tiling and extend it by simply requiring a group to have a direct factor for which the condition holds. This method results in two such sufficient conditions: a group G admits a full rank tiling if it has a direct factor of the form  $\mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c$  with a, b, and c composite, or if it has a direct factor of the form  $\mathbb{Z}_p^4$  with  $p \geq 5$  prime. Since any finite abelian group can be decomposed into the direct product of finite abelian groups of prime power order, these are obviously quite strong conditions when the size of the group is large, showing that many groups admit a full rank tiling. We have also suggested some open problems in the area that we feel are tractable and could lead to some interesting results.

**Acknowledgments.** We would like to thank Joe Gallian for his encouragement and support, and Philip Matchett and Melanie Wood for many helpful discussions. We would also like to thank Reid Barton and Geir Helleloid for their insightful comments.

## REFERENCES

- H. BAUER, B. GANTER, AND F. HERGERT, Algebraic techniques for nonlinear codes, Combinatorica, 3 (1983), pp. 21–33.
- [2] G. COHEN, S. LITSYN, A. VARDY, AND G. ZEMOR, Tilings of binary spaces, SIAM J. Discrete Math., 9 (1996), pp. 393–412.
- [3] N. DE BRUIJN, On the factorization of finite abelian groups, Indag. Math. (N.S.), 15 (1953), pp. 258–264.
- [4] T. ETZION AND A. VARDY, On perfect codes and tilings: Problems and solutions, SIAM J. Discrete Math., 11 (1998), pp. 205–223.
- [5] O. Fraser and B. Gordon, Solution to a problem of A.D. Sands, Glasg. Math. J., 20 (1977), pp. 115–117.
- [6] G. Hajós, Uber einfache und mehrfache bedeckung des n-dimensionalen raumes mit einem wurfelgitter, Mathematische Zeitschrift, 47 (1941), pp. 427–467.
- [7] G. HAJÓS, Sur la factorisation des groupes abéliens, Casopis Pest Path. Rys., 74 (1949), pp. 157–162.
- [8] F. MacWilliams and N. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
- [9] P. R. J. OSTERGARD AND A. VARDY, Resolving the existence of full-rank tilings of binary hamming spaces. SIAM J. Discrete Math., 18 (2004), pp. 382–387.
- [10] K. Phelps, Kernels of nonlinear Hamming codes, Des. Codes Cryptogr., 6 (1995), pp. 247–257.
- [11] K. Phelps, J. Rifa, and M. Villanueva, Kernels and p-kernels of  $p^r$ -ary 1-perfect codes. Des. Codes Cryptogr., 37 (2005), pp. 243–261.
- [12] K. Phelps and M. Villanueva, Ranks of q-ary 1-perfect codes, Des. Codes Cryptogr., 27 (2002), pp. 139–144.
- [13] L. Rédei, Die neue theorie der endlichen abelschen gruppen und verallgemeinerung des hauptsatzes von Hajós, Acta. Math. Acad. Sci. Hungar., 16 (1965), pp. 329–373.
- [14] L. RÉDEI, Lacunary Polynomials Over Finite Fields, American Elsevier, New York, 1973.

- [15] C. Rogers, Packing and Covering, Cambridge University Press, London, 1964.
- [16] A. SANDS, On the factorization of finite abelian groups II, Acta. Math. Acad. Sci. Hungar., 13 (1962), pp. 153-169.
- [17] A. SANDS, On a conjecture of G. Hajós, Glasg. Math. J., 15 (1974), pp. 88–89.
- [18] S. Stein, Tiling space by congruent polyhedra, Bull. Amer. Math. Soc., 80 (1974), pp. 819–820.
- [19] S. SZABÓ, A type of factorization of finite abelian groups, Discrete Math., 54 (1985), pp. 121-
- $[20]\,$  S. Szabó, Groups with the Rédei property, Matematiche, 52 (1997), pp. 357–364.
- [21] S. SZABÓ AND C. WARD, Factoring abelian groups and tiling binary spaces, Pure Math. Appl., 8 (1997), pp. 111-115.
- [22] S. Szabó and C. Ward, Factoring elementary groups of prime cube order into subsets, Math. Comp., 67 (1998), pp. 1199-1206.
- [23] S. SZABÓ AND C. WARD, Factoring groups having periodic maximal subgroups, Bol. Soc. Mat.
- Mexicana (3), 5 (1999), pp. 327–333. [24] A. Trachtenberg and A. Vardy, Full-rank tilings of  $\mathbb{F}_2^8$  do not exist, SIAM J. Discrete Math., 16 (2003), pp. 390-392.