To appear in
International Journal of Algebra and Computation
Vol. 18, No. 6 (2008)
© World Scientific Publishing Company

Small p-groups with full-rank factorization

HARRI HAANPÄÄ
Department of Information and Computer Science, Helsinki University of Technology, P.O. Box 5400, 02015 TKK, Finland
harri.haanpaa@tkk.fi

PATRIC R. J. ÖSTERGÅRD*
Department of Communications and Networking, Helsinki University of Technology, P.O. Box 3000, 02015 TKK, Finland
patric.ostergard@tkk.fi

SÁNDOR SZABÓ
Institute of Mathematics and Informatics, University of Pécs, Ifjúság u. 6, 7624 Pécs, Hungary
sszabo7@hotmail.com

The problem of determining which abelian groups admit a full-rank normalized factorization is settled for the orders $64 = 2^6$, $81 = 3^4$, and $128 = 2^7$. By a computer-aided approach, it is shown that such groups of these orders are exactly those of type $(2^2, 2^2, 2^2)$, $(2^2, 2^2, 2, 2)$, $(2^3, 2^2, 2^2)$, $(2^3, 2^2, 2, 2)$, $(2^2, 2^2, 2^2, 2)$, and $(2^2, 2^2, 2, 2, 2)$.

Mathematics Subject Classification (2000): Primary 20K01; Secondary 05B45, 52C22, 68R05

Keywords: factorization of finite abelian groups, periodic factorization, full-rank factorization.

1. Introduction

Let G be a finite abelian group. We use multiplicative notation, and denote the identity element of G by e. The order of an element $g \in G$ is denoted by $|g|$. Let A and B be subsets of G. The product AB is defined to be $\{ab \ : \ a \in A, b \in B\}$. The list of elements

$$ab, \quad a \in A, \quad b \in B \tag{1}$$

may contain equal elements in which case $|AB| \leq |A||B|$. If the elements in the list (1) are distinct, then we say that the product AB is direct. In this case $|AB| = |A||B|$. If the product AB is direct and is equal to G, then we say that the equation $G = AB$ is a factorization of G. Sometimes we say that the product AB is a factorization of G.

*Supported in part by the Academy of Finland under Grants No. 107493 and 110196.

If $e \in A$, then we say that the subset A is normalized. A factorization $G = AB$ is called normalized if both A and B are normalized subsets. Let $\langle A \rangle$ be the smallest subgroup of G that contains A. In other words, let $\langle A \rangle$ be the span of A in G. A normalized subset A of G is called a full-rank subset if $\langle A \rangle = G$. A normalized factorization $G = AB$ is defined to be a full-rank factorization if both A and B are full-rank subsets of G. If a finite abelian group G does not admit full-rank factorization, then we say that G has the Rédei property. It turns out that if a finite abelian group has the Rédei property then so does each of its nontrivial subgroups [14]. As a consequence, each factorization of a group having the Rédei property can be constructed from factorizations of its subgroups.

A subset A of G is called periodic if there is an element $g \in G \setminus \{e\}$ such that $Ag = A$. A factorization $G = AB$ is called periodic if either A or B is periodic. Periodicity is a useful property in the study of full rank tilings, since all groups that only admit periodic factorizations have the Rédei property [15, Lemma 1]. See also [4] for some more history and background.

Much of this work is motivated by connections between error-correcting codes and factorizations of abelian groups, cf. [1,2,4,5,8]. Investigation of factorizations of abelian groups has therefore led to a better understanding of, for example, the structure of perfect error-correcting codes. More specifically, regarding properties of abelian p-groups, the current work is concerned with the following transition phenomenon. Roughly speaking, abelian p-groups whose representation as a direct product of its cyclic subgroups has very few factors have the Rédei property, but with an increasing number of factors in the direct product, the groups admit full-rank factorizations from some point on. What is still not so well understood is the transition between these two phases. Computational studies, including the current one, aim at completing this picture by exploring the boundary.

We begin in Section 2 by looking at the computational problem of finding sets B of a factorization, given the set A. We call this the complementer factor problem. Two propositions regarding Corrádi subgroups are proved in Section 3, and some central characterization results for the Rédei property and full rank tilings are listed in Section 4. The (computational) results for the groups of order 81 are presented in Section 5 and those for groups of orders 64 and 128 in Section 6, respectively. It turns out that the abelian groups of these orders that admit a full-rank normalized factorization are exactly those of type $(2^2, 2^2, 2^2)$, $(2^2, 2^2, 2, 2)$, $(2^3, 2^2, 2^2)$, $(2^3, 2^2, 2, 2)$, $(2^2, 2^2, 2^2, 2)$, and $(2^2, 2^2, 2, 2, 2)$. The paper is concluded in Section 7.

2. The complementer factor problem

Suppose we are given a finite abelian group G and a subset A of G. The problem is to decide if there is a subset B of G such that $G = AB$ is a factorization of G. If $|A|$ does not divide $|G|$, then clearly there cannot be any factorization of G in the form $G = AB$. Thus we will assume that $|A|$ divides $|G|$.

The fact that $G = AB$ is a factorization of G is equivalent to the fact that the sets Ab, $b \in B$ form a partition of G. This suggests the following solution to the complementer factor problem. Form the family of the subsets Ag, $g \in G$, and search for members of this family that form a partition of G. The general problem of finding a partition of a set given a family of subsets of the set is known as the exact cover problem, so we here have instances of that problem and can apply known algorithms. In [8] and [7] the exact cover approach was used to study the Rédei property of elementary 2-groups and elementary 3-groups, respectively.

It is well known that instances of exact cover where all candidate subsets have the same size (here, $|A|$) can be transformed into a clique problem. Namely, construct a graph with one vertex for each candidate subset and insert edges between vertices whose corresponding subsets are nonintersecting. In our case, the (maximum) cliques of size $|G|/|A|$ are the solutions to the complementer factor problem. The exact cover approach is more efficient than the clique approach, but there are two reasons why also the clique approach is useful here. First, only the clique approach is applicable if we want to find B given a partial A. Second, in the clique framework there are some additional possibilities for pruning, as we shall see next. In fact, computationally, the best approach is a combination of clique search and exact cover.

The fact that $G = AB$ is a factorization of G is equivalent to the fact that the product AB is direct and it has $|G|$ elements. Note that the product is direct if and only if

$$A^{-1}A \cap B^{-1}B = \{e\}. \tag{2}$$

Here A^t stands for the set $\{a^t \ : \ a \in A\}$, where t is an integer. In particular, note that A^t is *not* $AA \cdots A$ (t times). Let us introduce a graph Γ. The vertices of Γ are the elements of G. We insert an edge between the vertices g and h exactly when $gh^{-1} \notin A^{-1}A$. It is straightforward to see that the graph we obtain in this manner is isomorphic to the graph derived earlier from the exact cover formulation.

By Proposition 2 of [12], in the factorization $G = AB$ the factor A can be replaced by A^t to get the factorization $G = A^tB$ for each integer t provided t is relatively prime to $|A|$. This means that B is a complementer factor not only to A but to each A^t. One can define Γ_1 to use all this available information. Namely insert an edge between g and h exactly when

$$gh^{-1} \notin \bigcup_t A^{-t}A^t.$$

Clearly Γ_1 is constructed from Γ by deleting certain edges of Γ. Using Γ_1 instead of Γ speeds up the search.

Annihilators can also be useful in the search for full-rank factorizations as we shall now see. Let χ be a character of the finite abelian group G. For a subset A of G we define $\chi(A)$ to be the complex number

$$\sum_{a \in A} \chi(a).$$

Applying χ to the factorization $G = AB$ gives that $\chi(G) = \chi(A)\chi(B)$. If χ is the principal character of G then this reduces to $|G| = |A||B|$. If χ is not the principal character of G, then $\chi(G) = 0$ and from $0 = \chi(A)\chi(B)$ it follows that either $\chi(A) = 0$ or $\chi(B) = 0$. The set of all characters χ of G for which $\chi(A) = 0$ is called the annihilator set of A or simply the annihilator of A.

When $|A| = |B|$, one may assume that the annihilator of one of the sets is not smaller than the annihilator of the other; cf. [17]. Without loss of generality, one may therefore assume that the annihilator of one the sets, say A, contains at least $(|G| - 1)/2$ elements. In some cases, this is a very effective additional possibility of pruning the search.

The next section shows that sometimes with a little extra book keeping the characters can be used to recognize if a factor is periodic.

3. The Corrádi subgroup

If the finite abelian group G is a direct product of its cyclic subgroups of orders $t_1, \ldots, t_n$, then we say that G is of type $(t_1, \ldots, t_n)$. Let p be a prime and let G be a group of type $(p^{\alpha(1)}, \ldots, p^{\alpha(n)})$, where $\alpha(1) \geq \cdots \geq \alpha(n) \geq 1$. The p power $p^{\alpha(1)}$ is called the exponent of G. The order of each element of G divides the exponent. To a subset A of a finite abelian group G we assign

$$K = \bigcap_{\chi(A)=0} \mathrm{Ker}(\chi),$$

where the intersection is taken over all characters χ of G. Clearly K is a subgroup of G being the intersection of subgroups and it is called the Corrádi subgroup of A.

The following lemma is an extension of Lemma 2 of [7].

Lemma 1. *Let p be a prime and let G be a finite abelian p-group whose exponent is q. Let A be a normalized subset of G such that $|A|$ is a divisor of $|G|$ and $|A| > 2$. Set*

$$g = \Big[\prod_{a \in A} a\Big]^{q/p}.$$

Then g is an element of the Corrádi subgroup of A.

Proof. We would like to show that $\chi(g) = 1$ for each character χ of G. Let χ be a character of G for which

$$0 = \chi(A) = \sum_{a \in A} \chi(a).$$

There is a (p^{β})th primitive root of unity ρ such that each $\chi(a)$ is a power of ρ. Say $\chi(a) = \rho^{\gamma(a)}$ for each $a \in A$. Obviously, p^{β} is a divisor of q and consequently $\rho^q = 1$.

By the remark after Lemma 3.1.1 of [16],

$$\begin{aligned}\{\chi(a) \ : \ a \in A\} &= \bigcup_{i=1}^{t} \rho^{\delta(i)}\{1, \rho^{p^{\beta-1}}, \rho^{2p^{\beta-1}}, \ldots, \rho^{(p-1)p^{\beta-1}}\} \\ &= \{\rho^{\delta(i)}\rho^{jp^{\beta-1}} \ : \ 1 \le i \le t, \ 0 \le j \le p-1\}.\end{aligned}$$

Using this we compute $\chi(g)$. First we deal with the case when p is odd.

$$\begin{aligned}\chi(g) &= \prod_{i=1}^{t}\prod_{j=0}^{p-1}\left[\rho^{\delta(i)}\rho^{jp^{\beta-1}}\right]^{q/p} \\ &= \prod_{i=1}^{t}\left[\left(\rho^{\delta(i)}\right)^{(q/p)p}\prod_{j=0}^{p-1}\left(\rho^{jp^{\beta-1}}\right)^{q/p}\right] \\ &= \prod_{i=1}^{t}\left(\rho^{q}\right)^{\delta(i)}\left(\rho^{p^{\beta-1}(p-1)p/2}\right)^{q/p} \\ &= \prod_{i=1}^{t}\left(\rho^{q}\right)^{p^{\beta-1}(p-1)/2} \\ &= 1\end{aligned}$$

as required.

Let us turn to the $p = 2$ case. Note that now $\rho^{p^{\beta-1}} = -1$. Further note that as $2t = |A|$ divides $|G|$, it follows that $2t$ is a power of 2. As $2t > 2$, t must be even.

$$\begin{aligned}\chi(g) &= \prod_{i=1}^{t}\left[\rho^{\delta(i)}(+1)\rho^{\delta(i)}(-1)\right]^{q/2} \\ &= \prod_{i=1}^{t}\left(\rho^{2\delta(i)}\right)^{q/2}\prod_{i=1}^{t}(-1)^{q/2} \\ &= \prod_{i=1}^{t}\left(\rho^{q}\right)^{\delta(i)} \\ &= 1\end{aligned}$$

This completes the proof. □

Theorem 2. *Let p be a prime and let G be a finite abelian p-group whose exponent is q. Let $G = AB$ be a normalized factorization of G, where $|A| > 2$. Set*

$$d = \prod_{a \in A} a.$$

If $|d| = q$, then B is periodic.

Proof. Let $g = d^{q/p}$. As $|d| = q$, it follows that $g \neq e$. We claim that g is a period of B. It is enough to show that $\chi(Bg) = \chi(B)$ holds for each character χ of G.

If $\chi(g) = 1$ or $\chi(B) = 0$, then $\chi(Bg) = \chi(B)$ obviously holds. Thus we may assume that $\chi(g) \neq 1$ and $\chi(B) \neq 0$. From $\chi(g) \neq 1$ one can see that χ is not the principal character of G. Applying χ to the factorization $G = AB$ gives that $0 = \chi(G) = \chi(A)\chi(B)$. As $\chi(B) \neq 0$, it follows that $\chi(A) = 0$. Lemma 1 is applicable and gives the contradiction that $\chi(g) = 1$. □

We will use the following result several times later.

Lemma 3. *Let G be a finite abelian group such that each proper subgroup of G has the Rédei property. If $G = AB$ is a normalized full rank factorization of G, then neither A nor B is periodic.*

Proof. Assume on the contrary that one of the factors A and B is periodic. Say A is periodic. There is a subgroup H of G and a normalized subset C of A such that the product CH is direct and is equal to A. From the factorization $G = AB = CHB$ by considering the factor group G/H we get the factorization

$$G/H = [(CH)/H][(BH)/H].$$

Using the fact that G/H is isomorphic to a proper subgroup of G and that each proper subgroup of G has the Rédei property we can derive the contradiction that either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$. □

4. Previous work

For easier reference to central earlier results, we list these as theorems.

Theorem 4. (Szabó [14]) *Let G be a finite abelian group that has the Rédei property. If H is a nontrivial subgroup of G, then H also has the Rédei property.*

Corollary 5. *If H is a finite abelian group that admits a full-rank factorization, and H is a subgroup of a finite abelian group G, then G also admits a full-rank factorization.*

Theorem 6. (Sands [11]) *The groups of type (p^α) and type $(2^\alpha, 2)$ admit only periodic factorizations.*

Corollary 7. *The groups of type (p^α) and type $(2^\alpha, 2)$ have the Rédei property.*

Theorem 8. (Szabó and Ward [17]) *The groups of types $(3^2, 3^2)$, $(3, 3, 3, 3)$ and $(2^3, 2^3)$ have the Rédei property.*

Theorem 9. (Östergård and Vardy [8]) *An elementary 2-group of order 2^n has the Rédei property if and only if $n \leq 9$.*

Theorem 10. (M. Dinitz [4]) *The groups of type (a, b, c), where each of a, b, c is a composite number, admit a full-rank factorization.*

5. Groups of order 81

There are 5 partitions of the number 4 and so there are 5 nonisomorphic abelian groups of order $81 = 3^4$ as depicted in Table 1. In Table 1 as well as in the subsequent Tables 4 and 6, we indicate for each group whether it has the Rédei property (R) or a full-rank factorization (F). A reference (to a theorem or a corollary in this paper) is also given for each entry. For groups of order 81, all group types except $(3^2, 3, 3)$ and $(3^3, 3)$ are handled by earlier results.

Table 1. Abelian groups of order 81

Group type	Rédei/Full-rank?
(3^4)	R: Corollary 7
$(3^3, 3)$	R: Theorem 12
$(3^2, 3^2)$	R: Theorem 8
$(3^2, 3, 3)$	R: Theorem 11
$(3, 3, 3, 3)$	R: Theorem 9

Theorem 11. *The group of type* $(3^2, 3, 3)$ *has the Rédei property.*

Proof. Let G be a group of type $(3^2, 3, 3)$ with basis elements x, y, z, where $|x| = 3^2$, $|y| = |z| = 3$. Choose a normalized factorization $G = AB$ of G, and assume that this factorization is full-rank. Without loss of generality, we may assume that $|A| \leq |B|$. If $|A| = 3$, then as the two elements of $A \setminus \{e\}$ cannot span G the factorization $G = AB$ cannot be full-rank. Thus $|A| = |B| = 3^2$, and without loss of generality we assume that the annihilator of A is at least as large as the annihilator of B.

If each element of A is of order 3, then $\langle A \rangle \subset \langle x^3, y, z \rangle$ and so A is not a full-rank factor. Thus we may assume that A contains an element of order 9. We can choose the basis x, y, z such that x is equal to this element of order 9. In other words we may assume that $x \in A$. As $|\langle x \rangle| = 9 < 81 = |G|$, there is an element in $A \setminus \langle x \rangle$. We can choose the basis x, y, z such that this element is of the form $x^\alpha y$. Continuing in this way there is an element in $A \setminus \langle x, x^\alpha y \rangle$. We can choose the basis x, y, z such that this element is of the form $x^\beta z$. Thus $e, x, x^\alpha y, x^\beta z$ are elements of A, that is,

$$A = \{e, x, x^\alpha y, x^\beta z, a_1, \ldots, a_5\} = A_1 \cup A_2,$$

where $0 \leq \alpha \leq \beta \leq 8$ and

$$A_1 = \{e, x, x^\alpha y, x^\beta z\}, \quad A_2 = \{a_1, \ldots, a_5\}.$$

In fact we may assume that $0 \leq \alpha \leq \beta \leq 2$. To see why let us divide α by 3 with remainder to get $\alpha = 3q + r$, $0 \leq r \leq 2$. Now $x^\alpha y = x^{3q+r} y = x^r (x^{3q} y)$ and we can denote $(x^{3q} y)$ by y.

There are

$$\binom{3+1}{2} = \binom{4}{2} = 6$$

choices for α and β and there are

$$\binom{81-4}{5} = \binom{77}{5} = 19\ 757\ 815$$

choices for $a_1, \ldots, a_5$.

When $\alpha = \beta = 1$ we computed the size of the annihilator of A in each of the 19 757 815 cases. In all except 3 cases, listed in Table 2, the size of the annihilator is at most 38. To settle this case, one can check that in the three exceptional cases A is periodic. Since each abelian group of order 27 has the Rédei property, by Lemma 3 we get a contradiction.

Table 2. The exceptional sets

000	000	000
100	100	100
110	110	110
101	101	101
002	010	012
102	020	021
111	111	112
112	120	121
001	121	122

We are still left with 5 choices of α and β. We do not sort out these cases rather we turn to a more efficient approach.

We combine the annihilator and clique methods. Let G be a normalized factorization, where $|A| = |B| = 9$. We may assume that $|\mathrm{Ann}(A)| \leq |\mathrm{Ann}(B)|$ since this is only a matter of swapping the factors A and B. Define the graph Γ_1 as described in Section 2. The vertices of Γ_1 are the elements of G. There is an edge between two vertices g and h in Γ_1 if

$$gh^{-1} \notin \bigcup_{t \in \{1,2,4,5,7,8\}} A^{-t}A^{t}.$$

Let us now define a new graph Γ_1^*. The nodes of Γ_1^* are the elements of G and the distinct nodes g and h are connected by an edge if

$$gh^{-1} \notin \bigcup_{t \in \{1,2,4,5,7,8\}} A_1^{-t}A_1^{t}.$$

In the definition of Γ_1^* only the elements of A_1 are appearing. Note that Γ_1 can be obtained from Γ_1^* by canceling certain edges. Therefore the cliques in Γ_1 of size k occur among the cliques in Γ_1^* of size k.

When $\alpha = \beta = 1$, then Γ_1^* has 14 767 (normalized) cliques of size 9. 8 172 of them are nonperiodic and full-rank. Each of these has annihilator of size at most 34. In the earlier approach we had to deal with 19 757 815 choices for the set A. Right now we have to handle only 14 767 possibilities.

We further reduce the number of possibilities for α and β. Suppose $\alpha = 2$, $\beta = 2$. Multiplying the elements

$$e,\ x,\ x^2y,\ x^2z$$

by $(x^2y)^{-1}$ we get

$$x^{-2}y^{-1},\ x^{-1}y^{-1},\ e,\ y^{-1}z. \tag{3}$$

Let $x_1 = x^{-1}y^{-1}$. Now $x_1^2 = x^{-2}y^{-2}$ and so $x_1^2y = x^{-2}y^{-1}$. Setting $y_1 = y^{-1}$, $z_1 = y^{-1}z$ the elements (3) are equal to

$$x_1^2y_1,\ x_1,\ e,\ z_1.$$

Note that x_1, y_1, z_1 is also a basis for G. In short the $\alpha = 2$, $\beta = 2$ case can be reduced to the $\alpha = 2$, $\beta = 0$ case.

Suppose $\alpha = 1$, $\beta = 1$. Multiplying the elements e, x, xy, xz by x^{-1} we get x^{-1}, e, y, z. Introducing the $x_1 = x^{-1}$, $y_1 = y$, $z_1 = z$ notations we can see that the $\alpha = 1$, $\beta = 1$ case reduces to the $\alpha = 0$, $\beta = 0$ case.

Suppose $\alpha = 1$, $\beta = 2$ and consider the elements e, x, xy, x^2z. Let $x_1 = x^2z$. Now $x_1^5 = (x^2z)^5 = x^{10}z^5 = xz^2$ and so $x_1^5z = x$. Therefore $xy = x_1^5(yz) = x_1^2(x_1^3yz)$. Setting $y_1 = x_1^3z$, $z_1 = x_1^3yz$ we get that the elements e, x, xy, x^2z are equal to the elements e, $x_1^2y_1$, $x_1^2z_1$, x_1. Thus the $\alpha = 1$, $\beta = 2$ case can be reduced to the $\alpha = 2$, $\beta = 2$ case.

In summary we should consider only the cases when (α, β) is equal to one of the $(0, 0)$, $(0, 1)$, $(0, 2)$.

In the $\alpha = \beta = 0$ case there are 75 399 cliques of size 9 in Γ_1^* containing e. 55 692 of these are nonperiodic and full-rank. These are the possible choices for B. We compute the size of the annihilator of B in each case. In each case the size of the annihilator is at most 20.

In the $\alpha = 0$, $\beta = 1$ case Γ_1^* contains 35 969 (normalized) cliques of size 9. 22 752 of them are nonperiodic and full-rank. Each of these has annihilator of size at most 20.

When $\alpha = 0$, $\beta = 2$, then Γ_1^* has 14 767 (normalized) cliques of size 9. 8 172 of them are nonperiodic and full-rank. Each of these has annihilator of size at most 34. □

Theorem 12. *The group of type* $(3^3, 3)$ *has the Rédei property.*

Proof. Let G be a group of type $(3^3, 3)$ with basis elements x, y, where $|x| = 3^3$, $|y| = 3$. Choose a normalized factorization $G = AB$ of G, and assume that this factorization is full-rank. We assume that $|A| \leq |B|$. If $|A| = 3$, then by Lemma 3

Table 3. Summary of computations for Theorem 11

$\lvert\mathrm{Ann}(B)\rvert$	$(\alpha,\beta)=(0,0)$	$(\alpha,\beta)=(0,1)$	$(\alpha,\beta)=(0,2)$
0	14 094	8 100	3 240
2	25 272	7 560	2 484
4	5 508	3 672	216
6	2 916	1 944	
8	5 346	468	432
10	972		
12	72		540
14	810	360	
20	702	648	1 152
34			108
Total	55 692	22 752	8 172

of [10], the factorization is periodic. Thus we may assume that $|A| = |B| = 3^2$, and that the annihilator of B is at least as large as the annihilator of A.

If each element of A is of order at most 9, then $\langle A\rangle \subset \langle x^3, y\rangle$ and so $\langle A\rangle \neq G$. Thus we may assume that A contains an element of order 27. We can choose the basis x, y such that $|x| = 27$.

As $|\langle x\rangle| = 27 < 81 = |G|$, there is an element in $A \setminus \langle x\rangle$. We can choose the basis x, y such that this element is of the form $x^\alpha y$. Thus

$$A = \{e, x, x^\alpha y, a_1, \ldots, a_6\} = A_1 \cup A_2,$$

where $0 \leq \alpha \leq 26$ and

$$A_1 = \{e, x, x^\alpha y\}, \quad A_2 = \{a_1, \ldots, a_6\}.$$

Let us divide α by 9 with remainder to get $\alpha = 9q + r$, $0 \leq r \leq 8$. Now $x^\alpha y = x^{9q+r} y = x^r(x^{9q}y)$ and we can denote $(x^{9q}y)$ by y. Thus we may assume that $0 \leq \alpha \leq 8$.

We further reduce the number of choices for α. Suppose $\alpha = 8$. Multiplying the elements e, x, $x^8 y$ by x^{-1} we get x^{-1}, e, $x^7 y$. Let $x_1 = x^{-1}$. Note that $x^7 = (x^{-1})^{20}$ and so $x^7 y = x_1^{20} y = x_1^2(x_1^{18} y)$. Setting $y_1 = x_1^{18} y$ we can see that the elements e, x, $x^8 y$ are equal to x_1, e, $x_1^2 y_1$. Thus the $\alpha = 8$ case can be reduced to the $\alpha = 2$ case. A similar argument gives that the $\alpha = 7$ case can be reduced to the $\alpha = 3$ and the $\alpha = 6$ case can be reduced to the $\alpha = 4$ case.

Suppose $\alpha = 5$. Raising the elements e, x, $x^5 y$ to the power 2 we get e, x^2, $x^{10} y^2 = x(x^9 y^2)$. Let $x_1 = x(x^9 y^2)$. Now $x_1^2 = x^2(x^{18} y)$ and so $x_1^2(x^9 y^2) = x^2$. Setting $y_1 = x^9 y^2$ one can see that the elements e, x, $x^5 y$ are equal to e, $x_1^2 y_1$, x_1. Therefore the $\alpha = 5$ case can be reduced to the $\alpha = 2$ case. A similar argument gives that the $\alpha = 4$ case can be reduced to the $\alpha = 7$ case. In summary we should consider only the $\alpha = 0, 1, 2, 3$ possibilities.

In the $\alpha = 0, 1, 2, 3$ cases the number of the (normalized) cliques of size 9 in the graph Γ_1^* was

$$1\ 568\ 836, \quad 1\ 568\ 836, \quad 1\ 562\ 276, \quad 1\ 562\ 284$$

respectively. These cliques correspond to the factors B. As it turned out each of them was either periodic or not full-rank.

It is worth pointing out that the number of the choices for A_2 is

$$\binom{81-3}{6} = \binom{78}{6} = 256\ 851\ 595$$

and so trying to find the complementer factors to A first extending A_1 to A would lead to a large number of instances of the exact cover problem. □

We now summarize the situation for order 81.

Theorem 13. *All abelian groups of order* $81 = 3^4$ *have the Rédei property.*

To conclude the section on groups of order 81, only the status of the group of type $(3^3, 3)$ was open. By a computer search tailored for this purpose, we found that it, too, has the Rédei property.

Among abelian groups of order 64 and 128, there are a larger number of open cases. It would be a tedious and error-prone process to tailor arguments to each case separately. Therefore, in the following section we design a method that is applicable to all p-groups, in principle only limited by the available computation resources. While this algorithm is not as efficient as an algorithm tailored for a specific group might be, we are able to obtain results for groups of order 64 and 128.

6. Groups of orders 64 and 128

In order to test the abelian groups of orders 64 and 128 for the Rédei property, we designed an algorithm that enumerates, up to isomorphism, all possible ways of factoring an abelian p-group. The algorithm does not make use of properties of specific individual groups.

In principle, to test for a group G whether a full-rank factorization $G = AB$ with $|A| = k$ exists, the algorithm first constructs all k-element subsets A of G and tests for each of them whether $\langle A \rangle = G$. In the positive case, the question is then whether there exist sets B such that $G = AB$. The approach outlined in Section 2 is then used to find all such B. Then it only remains to test whether $\langle B \rangle = G$.

In practice, however, abelian groups have a considerable amount of symmetry, and we need not consider all k-element subsets A. We consider two k-subsets A and A' equivalent, if one can be obtained from the other by applying an automorphism of the underlying abelian group and a translation. These operations form a group of equivalence operations that partitions the k-subsets into orbits; it suffices to examine one k-subset from each equivalence class.

To construct all k-subsets of G up to equivalence, we use an orderly algorithm in the style of Faradžev [6] and Read [9]. We order the elements of G in the lexicographical order of their list representations, and we order the k-subsets of G lexicographically. We have a group of equivalence operations that partitions the k-subsets into orbits; from each orbit we choose the lexicographical minimum element as the canonical representative of the orbit. Under these assumptions, it can be shown that every canonical k-subset can be constructed from a canonical $(k-1)$-subset by adding an element that comes after all the elements previously in the $(k-1)$-subset; consequently we may eliminate noncanonical subsets encountered during the search from consideration. In the problem at hand, two k-subsets of G are equivalent, if one can be mapped onto the other by an automorphism of G, by translation, or by a combination of these operations.

Testing canonicity of a k-subset of an abelian group is not entirely straightforward. Shoda [13] found that when the elements of a primary abelian group G whose order is a power of prime p are expressed as row vectors x, the automorphisms of G may be described as $\alpha(x) = xM$, where M is a matrix of the form

$$M_p = \begin{pmatrix} h_{11} & h_{12} & h_{13} & & h_{1k} \\ p^{e_1-e_2}h_{21} & h_{22} & h_{23} & \cdots & h_{2k} \\ p^{e_1-e_3}h_{31} & p^{e_2-e_3}h_{32} & h_{33} & & h_{3k} \\ & \vdots & & \ddots & \vdots \\ p^{e_1-e_k}h_{k1} & p^{e_2-e_k}h_{k2} & p^{e_3-e_k}h_{k3} & \cdots & h_{kk} \end{pmatrix} \qquad (4)$$

with $\det M \not\equiv 0 \pmod p$, where h_{ij} are integers in the range $0 \leq h_{ij} < p^{e_\mu}$ with $\mu = \max(i,j)$. To save us the trouble of matrix manipulation during the search, we precompute a lookup table for the canonical forms of t-subsets of G for as large t as we have computer memory for. Using the table, we can look up the canonical form of a t-subset. To save space, we only consider t-subsets that contain e.

We use a union-find method for constructing the table. Initially all t-subsets that contain e are assumed to be in different equivalence classes, and then classes are joined as we find that their elements are in fact equivalent. Our union-find is structured so that we can always easily find the lexicographic minimum t-subset in a class. First we consider all translations: if a translation maps a t-subset in some equivalence class onto a t-subset in a different equivalence class, those classes are joined. Then, we let a number of random automorphisms of G act on the lexicographic minimum t-subset of each class, and if the automorphism would map the t-subset onto a t-subset in a different class, those classes are then joined. After a sufficient number of random automorphisms of G join the classes together, our lookup table gives the canonical representative of each t-subset with high probability. To see this, suppose that at some point our algorithm has two classes of t-subsets that are actually equivalent and let a random automorphism act on the lexicographic minimum t-subset in the smaller class. By the orbit-stabilizer theorem, there is then at least a $1/2$ probability that the t-subset is mapped onto a t-subset in the other class and our algorithm will join the classes. In our computations, we generate random automorphisms of the abelian group until no classes have been joined by ten consecutive automorphisms. Our algorithm also works correctly in the unlikely event that the lookup table returns a noncanonical orbit member for some t-subset, but that may result in missing an opportunity for pruning the search.

We may use the lookup table for the canonical representatives of t-subsets for testing the canonicity of a k-subset S with $t \leq k$ by taking advantage of the properties of lexicographical ordering of subsets. Namely, we know that S cannot be canonical if $\min_t S > c(T)$ for some t-element $T \subseteq S$, where $\min_t S$ denotes the t least elements in S and $c(T)$ is the canonical representative in the same orbit with T.

6.1. *Groups of order* 64

There are 11 ways of expressing 6 as a sum of positive integers, and thereby 11 nonisomorphic abelian groups of order $64 = 2^6$. The results regarding these groups are depicted in Table 4. The group types that are not handled by earlier results are $(2^2, 2^2, 2, 2)$, $(2^4, 2^2)$, $(2^3, 2^2, 2)$, $(2^3, 2, 2, 2)$, and $(2^2, 2, 2, 2, 2)$.

Table 4. Abelian groups of order 64

Group type	Rédei/Full-rank?
(2^6)	R: Corollary 7
$(2^5, 2)$	R: Corollary 7
$(2^4, 2^2)$	R: Theorem 15
$(2^4, 2, 2)$	R: Theorem 15
$(2^3, 2^3)$	R: Theorem 8
$(2^3, 2^2, 2)$	R: Theorem 15
$(2^3, 2, 2, 2)$	R: Theorem 15
$(2^2, 2^2, 2^2)$	F: Theorem 10
$(2^2, 2^2, 2, 2)$	F: Theorem 14
$(2^2, 2, 2, 2, 2)$	R: Theorem 15
$(2, 2, 2, 2, 2, 2)$	R: Theorem 9

Theorem 14. *The group G of type $(2^2, 2^2, 2, 2)$ admits a full-rank factorization.*

Proof. Choose

$$\begin{aligned} A = \{&(0,0,0,0),(0,0,0,1),(0,1,0,0),(0,3,0,1),\\ &(1,0,0,0),(1,1,1,0),(3,0,0,1),(3,3,1,1)\} \text{ and}\\ B = \{&(0,0,0,0),(0,0,1,0),(1,2,0,0),(1,3,1,1),\\ &(2,1,1,0),(2,3,0,0),(3,1,0,1),(3,2,1,0)\}. \end{aligned} \tag{5}$$

Now AB is a full-rank factorization of G. □

Theorem 15. *Groups of type* $(2^4, 2^2)$, $(2^4, 2, 2)$, $(2^3, 2^2, 2)$, $(2^3, 2, 2, 2)$, *and* $(2^2, 2, 2, 2, 2)$ *have the Rédei property.*

Proof. For these groups, no full-rank factorization was found in an exhaustive search. The computation details are summarized in Table 5. Without loss of generality we assume that $|A| \leq |B|$, and as A must contain the identity element and generate G, it follows that $|A|$ must exceed the number of direct factors of G. Thus for the first two groups we must search for A with $|A| = 4$ or 8, while for the remaining two $|A| = 8$. In Table 5 we give for each combination of G and $|A|$ the number of $|A|$-subsets examined by the program, how many of those indeed generate G as required, and the total number of B obtained that satisfy $G = AB$ for some full-rank A considered. In each case none of these B generated G. We also give the computation time required. For the computations with $|A| = 8$ we constructed lookup tables for the canonical form of the $\binom{63}{6}$ subsets with 7 elements one of which is 0.

Table 5. Summary of computations for groups of Theorem 15

Group type	$\lvert A\rvert$	$\#A$	Full-rank A	$\#B$	Time
$(2^4, 2^2)$	4	201	48	218	0.1 s
$(2^4, 2^2)$	8	329 414	309 079	44 345	348 s
$(2^4, 2, 2)$	4	145	13	159	0.1 s
$(2^4, 2, 2)$	8	142 954	124 806	38 237	347 s
$(2^3, 2^2, 2)$	4	127	6	28	0.1 s
$(2^3, 2^2, 2)$	8	69 205	56 888	23 587	318 s
$(2^3, 2, 2, 2)$	8	9 482	6 597	5 851	315 s
$(2^2, 2, 2, 2, 2)$	8	899	479	1 108	316 s

□

The characterization of the abelian groups of order 64 with respect to the Rédei property is then as follows.

Theorem 16. *The only abelian groups of order* $2^6 = 64$ *that admit a full-rank factorization are those of type* $(2^2, 2^2, 2^2)$ *and* $(2^2, 2^2, 2, 2)$.

6.2. *Groups of order* 128

The 15 nonisomorphic abelian groups of order 2^7 correspond to the 15 ways of expressing 7 as a sum of positive integers. The details are depicted in Table 6. Theorem 17 settles the cases that were previously open.

Theorem 17. *Groups of type* $(2^5, 2^2)$, $(2^5, 2, 2)$, $(2^4, 2^3)$, $(2^4, 2^2, 2)$, $(2^4, 2, 2, 2)$, $(2^3, 2^3, 2)$, $(2^3, 2, 2, 2, 2)$, *and* $(2^2, 2, 2, 2, 2, 2)$ *have the Rédei property.*

Table 6. Abelian groups of order 128

Group type	Rédei/Full-rank?
(2^7)	R: Corollary 7
$(2^6, 2)$	R: Corollary 7
$(2^5, 2^2)$	R: Theorem 17
$(2^5, 2, 2)$	R: Theorem 17
$(2^4, 2^3)$	R: Theorem 17
$(2^4, 2^2, 2)$	R: Theorem 17
$(2^4, 2, 2, 2)$	R: Theorem 17
$(2^3, 2^3, 2)$	R: Theorem 17
$(2^3, 2^2, 2^2)$	F: Theorem 10
$(2^3, 2^2, 2, 2)$	F: Corollary 5, Theorem 14
$(2^3, 2, 2, 2, 2)$	R: Theorem 17
$(2^2, 2^2, 2^2, 2)$	F: Corollary 5, Theorem 10
$(2^2, 2^2, 2, 2, 2)$	F: Corollary 5, Theorem 14
$(2^2, 2, 2, 2, 2, 2)$	R: Theorem 17
$(2, 2, 2, 2, 2, 2, 2)$	R: Theorem 9

Proof. For these groups, no full-rank tiling was found in an exhaustive computer search. As before, in Table 7 we give for each combination of G and $|A|$ the number of $|A|$-subsets examined by the program, how many of those indeed generate G as required, and the total number of B obtained that satisfy $G = AB$ for some full-rank A considered. In each case none of these B generated G. We also give the computation time required. For computations with $|A| = 8$ we constructed lookup tables for the $\binom{127}{5}$ subsets with 6 elements one of which is 0. □

Theorem 18. *The only abelian groups of order* $128 = 2^7$ *that admit a full-rank factorization are those of type* $(2^3, 2^2, 2^2)$, $(2^3, 2^2, 2, 2)$, $(2^2, 2^2, 2^2, 2)$, *and* $(2^2, 2^2, 2, 2, 2)$.

7. Conclusions

As a consequence of the current work, the categorization of all abelian groups up to order 128 with respect to the Rédei property is now complete. A proof that a certain group has the Rédei property is a essentially a nonexistence proof—one proves that the group does *not* admit a full-rank factorization—and therefore gives less structural information about objects than full-rank tilings obtained. Most of the instances settled here are of the former type, but Theorem 14 indeed gives a new full-rank tiling.

Although the main focus of the current work is on the specific results obtained with respect to the Rédei property, we anticipate that the presented algorithm be applicable in other related studies as well.

Table 7. Summary of computations for groups of Theorem 17

Group type	$\|A\|$	$\#A$	Full-rank A	$\#B$	Time
$(2^5, 2^2)$	4	692	155	33 631	1.3 s
$(2^5, 2^2)$	8	26 005 809	24 084 142	1 107 435 343	13 246 s
$(2^5, 2, 2)$	4	488	33	33 087	1.3 s
$(2^5, 2, 2)$	8	11 721 754	9 985 183	1 113 171 844	14 067 s
$(2^4, 2^3)$	4	300	49	404	1.0 s
$(2^4, 2^3)$	8	7 008 942	6 423 798	12 902 941	2 805 s
$(2^4, 2^2, 2)$	4	456	18	328	1.1 s
$(2^4, 2^2, 2)$	8	5 496 620	4 420 448	35 654 757	2 495 s
$(2^4, 2, 2, 2)$	8	906 733	636 710	23 452 320	1 554 s
$(2^3, 2^3, 2)$	4	138	5	38	1.1 s
$(2^3, 2^3, 2)$	8	1 567 312	1 269 575	15 317 390	1 625 s
$(2^3, 2, 2, 2, 2)$	8	120 932	72 318	1 273 302	1 309 s
$(2^2, 2, 2, 2, 2, 2)$	8	38 655	16 320	218 112	1 301 s

References

[1] J. Berstel and D. Perrin, *Theory of codes*, Academic Press, New York, 1985

[2] G. Cohen, S. Litsyn, A. Vardy and G. Zémor, Tilings of binary spaces, *SIAM J. Discrete Math.* **9** (1996), 393–412.

[3] K. Corrádi and S. Szabó, Factoring a finite abelian group by prime complexes, *Math. Pann.* **16** (2005), 79–94.

[4] M. Dinitz, Full rank tilings of finite abelian groups, *SIAM J. Discrete Math.* **20** (2006), 160–170.

[5] T. Etzion and A. Vardy, On perfect codes and tilings: Problems and solutions, *SIAM J. Discrete Math.* **11** (1998), 205–223.

[6] I. A. Faradžev, Constructive enumeration of combinatorial objects, in *Problèmes Combinatoires et Théorie des Graphes*, (Université d'Orsay, July 9–13, 1977), CNRS, Paris, 1978, pp. 131–135.

[7] P. R. J. Östergård and S. Szabó, Elementary p-groups with the Rédei property, *Internat. J. Algebra Comput.* **17** (2007), 171–178.

[8] P. R. J. Östergård and A. Vardy, Resolving the existence of full-rank tilings of binary Hamming spaces, *SIAM J. Discrete Math.* **18** (2004), 382–387.

[9] R. C. Read, Every one a winner; or, How to avoid isomorphism search when cataloguing combinatorial configurations, *Ann. Discrete Math.* **2** (1978), 107–120.

[10] A. D. Sands, On the factorisation of finite abelian groups, *Acta Math. Acad. Sci. Hungar.* **8** (1957), 65–86.

[11] A. D. Sands, On the factorisation of finite abelian groups. II, *Acta Math. Acad. Sci. Hungar.* **13** (1962), 153–169.

[12] A. D. Sands, Replacement of factors by subgroups in the factorization of abelian groups, *Bull. London Math. Soc.* **32** (2000), 294–304.

[13] K. Shoda, Über die Automorphismen einer endlichen Abelschen Gruppe, *Math. Ann.* **100** (1928), 674–686.

[14] S. Szabó, Factoring finite abelian groups by subsets with maximal span, *SIAM J. Discrete Math.* **20** (2006), 920–931.

[15] S. Szabó, Groups with the Rédei property, *Matematiche (Catania)* **52** (1997), 357–364.

[16] S. Szabó, *Topics in Factorization of Abelian Groups*, Birkhäuser Verlag, Basel, 2004.

[17] S. Szabó and C. Ward, Factoring groups having periodic maximal subgroups, *Bol. Soc. Mat. Mexicana (3)* **5** (1999), 327–333.