Serdica
Mathematical Journal
Сердика
Математическо списание

Serdica Math. J. **43** (2017), 335–360

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

METHODS FOR CONSTRUCTING FACTORIZATIONS OF ABELIAN GROUPS WITH APPLICATIONS

Sándor Szabó

Communicated by V. Drensky

Abstract. The paper presents a number of methods for factoring finite abelian groups into a direct product of its subsets. Some are extension of existing techniques others are new.

1. Introduction. Let G be a finite abelian group written multiplicatively with identity element e. Let $A_1, \dots, A_n$ be subsets of G. The product $A_1 \cdots A_n$ is defined to be

$$\{a_1 \cdots a_n : \ a_1 \in A_1, \dots, a_n \in A_n\}.$$

We say that the product $A_1 \cdots A_n$ is a factorization of G if $G = A_1 \cdots A_n$ and each $a \in G$ can be represented uniquely in the form

$$a = a_1 \cdots a_n, \quad a_1 \in A_1, \dots, a_n \in A_n.$$

2010 *Mathematics Subject Classification:* Primary 20K01; Secondary 05B45, 52C22, 68R05

Key words: Factoring abelian groups into subsets, normalized subsets, periodic subsets, full-rank subsets.

A subset A of G is called normalized if $e \in A$. The factorization $G = A_1 \cdots A_n$ is called normalized if each A_i is normalized. The number of the elements of A is denoted by $|A|$. The smallest subgroup of G that contains A, that is, the span of A in G, is denoted by $\langle A \rangle$. For an integer k and a subset A of G the notation A^k stands for $\{a^k : a \in A\}$. Thus for example in this paper A^2 does not mean AA or A^k neither means the k-fold Descartes product $A \times \cdots \times A$. If G is a direct product of cyclic groups of orders $t_1, \ldots, t_n$, then we say that G is a $(t_1, \ldots, t_n)$ type group.

In section 4 we will describe two procedures to construct factorizations for finite abelian groups based on simultaneous factorizations. These generalize two methods given earlier by N. G. De Bruijn [2]. The constructions now can be applied in a more varied setting. In particular they can be used iteratively to generate large families of factorizations using chains of subgroups. In sections 5 and 6 factorizations are presented that are based on permutations and Latin squares. Section 7 shows how finite projective geometry can be used to construct factorizations.

The remaining part of the paper is about applications. Factorizations of cyclic groups in section 10 provide a source to enrich the collections of variable length codes. In section 9 we define the complementer factor problem. Then we point out that the graph theoretical equivalent of the problem suggests a family of new type of random graphs that computer scientists can use to test maximum clique algorithms.

The treatment of the factorization method is far from comprehensive. Important methods are not mentioned. For instance techniques based on error correcting codes are missing. This method first applied in [6] and later improved and extended in [3]. A similar construction in [19] with interesting geometric application is not covered either. Further we did not include the methods of [20] and [21].

2. Periodic subsets. By the fundamental theorem of finite abelian groups each finite abelian group can be decomposed into a direct product of cyclic subgroups. So most likely factoring a given group G into its subgroups comes into mind first when one looks for a factoring of G into its subsets. It is still quite natural to consider factorization $G = AB$, where one of the factors, say A, is equal to a subgroup H of G. The group G can be partitioned into right cosets modulo H. If the elements of B form a complete set of representatives modulo H, then plainly the product HB is direct and gives a factorization of G. For each element of B there are $|H|$ choices and consequently there are $|H|^{|B|}$ choices for B. In case we are looking for normalized factorizations, then there are $|H|^{|B|-1}$ choices for B. One can choose a subgroup K of H and construct a factorization $H = KC$ of H in a similar way. Combining the factorizations $H = KC$ and $G = HB$ we get a factorization $G = KCB$ of G.

In a more systematic manner let us consider an ascending chain of subgroups

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n \subseteq H_{n+1} = G$$

of G and the factorizations

$$H_{n+1} = H_n A_n,\ H_n = H_{n-1}A_{n-1}, \ldots, H_2 = H_1 A_1$$

of the subgroups $H_2, \ldots, H_{n+1}$ respectively. Combining these factorizations gives the factorization $G = H_1 A_1 \cdots A_n$. Of course we can rearrange the factors in any order we please and group factors together in various ways to get factorizations in the form $G = B_1 \cdots B_m$. What the above manipulations cannot make disappear is that a B_i factor is a direct product of the subgroup H_1 and certain other factors from $A_1, \ldots, A_n$.

For convenience we introduce the following terminology. A subset A of an abelian group G is called periodic if there is a $g \in G \setminus \{e\}$ such that $Ag = A$. The element g is termed a period of A. It turns out that all the periods of A together with the identity element e form a subgroup H of G. We refer to H as the subgroup of periods of A. There is a subset B of G such that the product HB is direct and is equal to A.

Using this terminology we can say that in the factorization $G = B_1 \cdots B_m$ we constructed from $G = H_1 A_1 \cdots A_n$ one factor B_i is periodic. When B_i is normalized and $|B_i|$ is a prime, then periodicity of B_i simply means that B_i is a subgroup of G. As a counterpart of our construction a celebrated theorem of L. Rédei [14] asserts that in a normalized factorization $G = A_1 \cdots A_n$ of a finite abelian group G, where each $|A_i|$ is a prime at least one of the factors necessarily is a subgroup of G.

G. Hajós [7] and A. D. Sands [16] pointed out that there is a nice organized way to construct factorizations $G = B_1 B_2$ from the factorization $G = H_1 A_1 \cdots A_n$. In fact the construction can be carried out easily by a computer.

Let G be a finite abelian group, let A, B be subsets of G and let $\varphi : B \to A$ be a function. We define $A \circ_\varphi B$ to be $\{\varphi(b)b : b \in B\}$. Let $D_1, \ldots, D_n$ be subsets of G such that D_i is a complete set of representatives for H_{i+1} modulo H_i. (For the sake of a uniform notation we introduce $D_0 = H_1$.) Then use the following recursion.

$$\begin{array}{lcllcl} U_n & = & D_n, & V_n & = & \{0\}, \\ U_{n-1} & = & D_{n-1}V_n, & V_{n-1} & = & D_{n-1} \circ U_n, \\ & \vdots & & & \vdots & \\ U_1 & = & D_1V_2, & V_1 & = & D_1 \circ U_2, \\ U_0 & = & D_0V_1, & V_0 & = & D_0 \circ U_1. \end{array}$$

Set $B_1 = V_0$, $B_2 = U_0$. The functions

$$\varphi_n : U_n \to D_{n-1}, \ldots, \varphi_1 : U_1 \to D_0$$

are suppressed in the formulas above. Then $G = B_1B_2$ is a factorization of G. Plainly B_1 is periodic as $B_1 = D_0V_1$ and $D_0 = H_1$.

3. Simultaneous factorizations. Let $F_1, \ldots, F_s$ be families of subsets of G. If

$$G = \prod_{A \in F_i} A, \quad 1 \leq i \leq s$$

are factorizations of G, then we have s simultaneous factorizations of G. Shortly we will talk about simultaneous factorizations of G.

Example 1. Let G be a group of type $(4, 4)$ with basis elements x, y. Consider the sets

$$\begin{array}{lcl} A_1 & = & \{e, x, x^2, x^3\}, \\ A_2 & = & \{e, y, y^2, y^3\}, \\ A_3 & = & \{e, xy, x^2y^3, x^3y^2\} \end{array}$$

of G and let

$$F_1 = \{A_1, A_2\}, \quad F_2 = \{A_2, A_3\}, \quad F_3 = \{A_1, A_3\}$$

be families of subsets of G. It is a routine computation to verify that

$$\begin{array}{lcl} G & = & \displaystyle\prod_{A \in F_1} A = A_1A_2, \\ G & = & \displaystyle\prod_{A \in F_2} A = A_2A_3, \end{array}$$

$$G = \prod_{A \in F_3} A = A_1 A_3$$

are factorizations of G and so we have three simultaneous factorizations of G.

Example 2. Let G be a group of type $(3,3)$ with basis elements x, y and let

$$A_1 = \{e, x, x^2\}, \quad A_2 = \{e, y, y^2\},$$
$$B_1 = \{e, xy, x^2y^2\}, \quad B_2 = \{e, x^2y, yx^2\}.$$

Set

$$F_1 = \{A_1, B_1\}, \quad F_2 = \{A_1, B_2\},$$
$$F_3 = \{A_2, B_1\}, \quad F_4 = \{A_2, B_2\}.$$

One can check that

$$G = \prod_{A \in F_1} A = A_1 B_1,$$
$$G = \prod_{A \in F_2} A = A_1 B_2,$$
$$G = \prod_{A \in F_3} A = A_2 B_1,$$
$$G = \prod_{A \in F_4} A = A_2 B_2$$

are factorizations of G and so we have four simultaneous factorizations of G.

In the special case when $|F_1| = \cdots = |F_s| = 2$ we can record the data conveniently by defining a graph Γ whose nodes are the elements of $F_1 \cup \cdots \cup F_s$ and the nodes A_i, A_j are adjacent if $G = A_i A_j$ is a factorization of G. We will refer to the graph Γ as the associated graph of the simultaneous factorizations.

The associated graph in Example 1 has three nodes A_1, A_2, A_3 and each of them are connected by an edge. In short the associated graph is K_3 the complete graph with three vertices. The associated graph of the simultaneous factorizations in Example 2 is the complete bipartite graph $K_{2,2}$. The nodes are A_1, A_2, B_1, B_2. The nodes are partitioned as $\{A_1, A_2\} \cup \{B_1, B_2\}$ and each A_i is connected with each B_j.

4. Not full-rank factorizations. Let G be a finite abelian group and let H be a subgroup of G. In this section we will show how simultaneous factorizations of H give rise factorizations of G. The constructions we present generalize constructions due to N. G. De Bruijn [2].

Suppose $B = \{b_1, \dots, b_r\}$ is a complete set of representatives in G modulo H with $r \geq 2$ and $b_1 = e$. Suppose H admits simultaneous normalized factorizations such that the associated graph has a node with degree $s \geq 2$. In other words, there are subsets $A_1, \dots, A_{s+1}$ of H such that $H = A_i A_{s+1}$ is a normalized factorization of H for each i, $1 \leq i \leq s$. Set

$$\begin{aligned} C &= A_{s+1}, \\ D &= b_1 D_1 \cup \cdots \cup b_r D_r, \end{aligned}$$

where $D_i \in \{A_1, \dots, A_s\}$.

Lemma 1. *$G = DC$ is a factorization of G.*

Proof. We will show that the product DC is equal to G and that $|D||C|$ is equal to $|G|$, that is the product DC is direct. The next computation verifies that $G = DC$.

$$\begin{aligned} DC &= (b_1 D_1 \cup \cdots \cup b_r D_r) C \\ &= (D_1 b_1 \cup \cdots \cup D_r b_r) A_{s+1} \\ &= (D_1 A_{s+1}) b_1 \cup \cdots \cup (D_r A_{s+1}) b_r \\ &= H b_1 \cup \cdots \cup H b_r \\ &= H\{b_1, \dots, b_r\} \\ &= HB \\ &= G \end{aligned}$$

From the factorizations $H = A_i A_{s+1}$ it follows that $|A_1| = \cdots = |A_s|$. Let this common value be t. From the previous computation we can read off that $b_i D_i$ is contained by the coset $b_i H$ for each i, $1 \leq i \leq s$. Therefore $b_1 D_1, \dots, b_s D_s$ are disjoint subsets. From $|b_1 D_1| = \cdots = |b_s D_s| = t$ it follows that $|D| = st$. Finally we have

$$\begin{aligned} |D||C| &= st|A_{s+1}| \\ &= |B||A_1||A_{s+1}| \\ &= |B||H| \end{aligned}$$

$$= \quad |G|$$

as required. □

Let

$$B = \{b_1, \ldots, b_r\}, \quad C = \{c_1, \ldots, c_s\}$$

be normalized subsets of G such that the product BC is direct and form a complete set of representatives in G modulo H. The index of H in G is equal to rs. If $r \geq 2$, $s \geq 2$, then this index is a composite number. Suppose H admits uv simultaneous factorizations such that the associated graph is the complete bipartite graph $K_{u,v}$ with $u \geq 2$, $v \geq 2$. In other words there are subsets $A_1, \ldots, A_u$, $B_1, \ldots, B_v$ of H such that $H = A_i B_j$ is a normalized factorization of H for each i, j, $1 \leq i \leq u$, $1 \leq j \leq v$. Set

$$D = b_1 D_1 \cup \cdots \cup b_r D_r,$$

where $D_i \in \{A_1, \ldots, A_u\}$ and set

$$E = c_1 E_1 \cup \cdots \cup c_s E_s,$$

where $E_i \in \{B_1, \ldots, B_v\}$.

Lemma 2. *$G = DE$ is a factorization of G.*

Proof. We will show that the product DE is equal to G and that $|D||E| = |G|$.

The following straightforward computation shows that $G = DE$.

$$\begin{aligned} DE &= (b_1 D_1 \cup \cdots \cup b_r D_r)(c_1 E_1 \cup \cdots \cup c_s E_s) \\ &= b_1 c_1 D_1 E_1 \cup \cdots \cup b_r c_s D_r E_s \\ &= b_1 c_1 H \cup \cdots \cup b_r c_s H \\ &= \{b_1 c_1, \ldots, b_r c_s\} H \\ &= (BC)H \\ &= G \end{aligned}$$

From the factorizations $H = A_i B_1$ it follows that $|A_1| = \cdots = |A_u| = t$ and from the factorizations $H = A_1 B_j$ it follows that $|B_1| = \cdots = |B_v| = w$. From the computation above we can see that the coset $b_i H$ contains $b_i D_i$. Consequently, $b_1 D_1, \ldots, b_r D_r$ are disjoint subsets. Therefore $|D| = rt$. Similarly, the coset c_jH contains c_jE_j and so $c_1E_1, \ldots, c_sE_s$ are disjoint subsets. Hence $|E| = sw$. Now

$$\begin{aligned} |D||E| &= (rt)(sw) \\ &= r|A_1|s|B_1| \\ &= rs|A_1||B_1| \\ &= rs|H| \\ &= |B||C||H| \\ &= |G| \end{aligned}$$

as required. $\square$

5. Latin squares. An n by n array is called a Latin square if each of its n^2 entries is filled with one of the symbols $0, 1, \ldots, n-1$ such that no symbol appears twice in a row and no symbol appears twice in a column. Latin squares are well-known and well-studied combinatorial structures. Their history goes back to L. Euler [4].

In this section we will show that permutations can be used to construct factorizations of a group G that has a subgroup H of type (n, n) and $|G : H| \geq 2$. Then we will show that Latin squares that are generalizations of permutations can be used to construct factorizations of a group G that has a subgroup H of type (n, n, n) and $|G : H| \geq 2$.

First we consider the simpler case of the permutations. Let G be a group of type (m, n, n) with basis elements x, y, z, where $|x| = m$, $|y| = |z| = n$. Suppose that $f(0), f(1), \ldots, f(n-1)$ is a permutation of the elements $0, 1, \ldots, n-1$. Set

$$\begin{aligned} A_1 &= \langle y \rangle, \\ A_2 &= \langle z \rangle, \\ A_3 &= \{y^i z^{f(i)} : \ 0 \leq i \leq n-1\}. \end{aligned}$$

Note that the products A_1A_3, A_2A_3 are simultaneous factorizations of the subgroup $H = \langle y, z \rangle$ of G and $B = \langle x \rangle$ is a complete set of representatives in G modulo H. Here $|G : H| = m$. Therefore, by Lemma 1, G has a factorization $G = DC$, where $|D| = mn$, $|C| = n$. In fact there is an astronomical number of these factorizations. There are $n!$ choices for the permutation f. (The choice when f is the identity permutation gives a trivial factorization.) By our first construction from Section 4, the factors C and D are in the following forms

$$\begin{aligned} C &= A_3, \\ D &= b_1 D_1 \cup \cdots \cup b_m D_m, \end{aligned}$$

where $D_i \in \{A_1, A_2\}$. This gives 2^m choices for $D_1, \ldots, D_m$. (The choices when all D_i are equal produce not particularly interesting factorizations.) The elements $b_1, \ldots, b_m$ form a complete set of representatives modulo H with $b_1 = e$. Therefore there are $(n^2)^{m-1}$ choices for the elements $b_2, \ldots, b_m$.

Let G be a group of type (m, n, n, n) with basis elements x, y, z, w, where $|x| = m$, $|y| = |z| = |w| = n$. An n by n Latin square can be described by the n^2 triples $[i, j, f(i, j)]$, $0 \leq i, j \leq n-1$, where $f(i, j)$ is the symbol in the jth position in the ith row. Set

$$\begin{aligned} A_1 &= \langle y \rangle, \\ A_2 &= \langle z \rangle, \\ A_3 &= \langle w \rangle, \\ A_4 &= \{y^i z^j w^{f(i,j)} :\ 0 \leq i, j \leq n-1\}. \end{aligned}$$

Let us observe that the products A_1A_4, A_2A_4, A_3A_4 form simultaneous factorizations of the subgroup $H = \langle y, z, w \rangle$ of G, $B = \langle x \rangle$ is a complete set of representatives in G modulo H and $|G : H| = m$. Consequently, by Lemma 1, there is a factorization $G = DC$ of G, where $|C| = n^2$, $|D| = mn$. We then can go on to construct factorizations $G = DC$ of a group G that has a subgroup H of type (n, n, n, n) and $|G : H| \geq 2$ using Latin cubes in place of Latin squares. Needles to say that the number of these factorization is very large. But there are further possibilities to enlarge the collection of factorizations we have constructed. By Proposition 3 of [17], in a factorization $G = DC$ the factor D can be replaced by D^i to get the factorization $G = D^iC$ whenever i is relatively prime to $|D|$. The set D^i is not necessarily distinct from D. For example if D is a union of cyclic subgroups of G, then plainly $D^i = D$ for each integer i. C. Okuda [9] singled out and studied factorizations in which the factors are unions of cyclic subsets. In order to get interesting factorizations we have to assume that there is an integer i such that i is relatively prime to $|D|$ and $D^i \neq D$. In this case the products DC and D^iC are simultaneous factorizations of G and using the first construction from Section 4 one can construct a factorization a group that contains G as a subgroup. Suppose next that in the factorization $G = DC$, $|D| = |C|$ and there are integers i, j such that $G = D^iC^j$ is a factorization and $D^i \neq D$, $C^j \neq C$.

Now the products

$$DC,\ DC^j,\ D^iC,\ D^iC^j$$

are factorizations of G simultaneously. Using the second construction from Section 4 we can construct a factorization of a group that contains G as a subgroup. In the factorizations constructed so far one of the factors does not span the whole group which is factored. On the other hand for the majority of the finite abelian groups there are factorizations in which both factors span the whole group as shown in [21]. These "full-rank" factorizations cannot be the result of the constructions described in Section 4. However the "full-rank" factorizations can be the starting point of our constructions. In summary there is a bewildering variety of factorizations of finite abelian groups.

6. Disjoint Latin squares. Let f, g be permutations of $0, 1, \ldots, n-1$ such that $f(0) = g(0)$ and $f(i) \neq g(i)$ for $1 \leq i \leq n-1$. We will say that f and g are disjoint permutations. In this section we will show that disjoint permutations can be used to construct factorizations of a group G that has a subgroup H of type (n, n) and the index $|G : H|$ is a composite number. Then we show that an extension of disjoint permutations the disjoint Latin squares can be used to construct factorizations for a group G that admits a subgroup H of type (p, p, p) and the index $|G : H|$ is a composite number.

Let G be a group of type (kn, mn) with basis elements x, y, where $|x| = kn$, $|y| = mn$. Assume that f, g are disjoint permutations of $0, 1, \ldots, n-1$. Set

$$\begin{aligned}
A_1 &= \langle x^k \rangle,\\
A_2 &= \langle y^m \rangle,\\
B_1 &= \{x^{ki} y^{mf(i)} :\ 0 \leq i \leq n-1\},\\
B_2 &= \{x^{ki} y^{mg(i)} :\ 0 \leq i \leq n-1\}.
\end{aligned}$$

One can verify that the products

$$A_1B_1,\ A_1B_2,\ A_2B_1,\ A_2B_2$$

are simultaneous factorizations of the subgroup $H = \langle x^k, y^m \rangle$ of G and $|G : H| = km$. One can choose B and C such that B, C are normalized subsets, the product BC is direct and is a complete set of representatives in G modulo H. Now Lemma 2 is applicable and gives that there is a factorization $G = DE$ of G.

Let us turn to the Latin squares. Consider two Latin squares given in the forms

$$[i, j, f(i, j)],\ [i, j, g(i, j)], \quad 0 \le i, j \le n-1,$$

where $f(0,0) = g(0,0)$ and $f(i,j) \ne g(i,j)$ when $(i,j) \ne (0,0)$. We will say that the Latin squares are disjoint. Disjoint Latin squares can be used to construct factorizations.

Let G be a group of type (kn, mn, n) with basis elements x, y, z, where $|x| = kn$, $|y| = mn$, $|z| = n$. Set

$$\begin{aligned} A_1 &= \langle x^k \rangle, \\ A_2 &= \langle y^m \rangle, \\ A_3 &= \langle z \rangle, \\ B_1 &= \{x^{ki} y^{mj} z^{f(i,j)} :\ 0 \le i, j \le n-1\}, \\ B_2 &= \{x^{ki} y^{mj} z^{g(i,j)} :\ 0 \le i, j \le n-1\}. \end{aligned}$$

One can verify that the products

$$A_1B_1,\ A_1B_2,\ A_2B_1,\ A_2B_2,\ A_3B_1,\ A_3B_2$$

are simultaneous factorizations of the subgroup $H = \langle x^k, y^m \rangle$ of G and $|G : H| = km$. By Lemma 2, there is a factorization $G = DE$ of G. From our point of view the most important fact is that there is a very large variety of such factorizations.

7. Finite projective spaces. Let p be a prime and let $n \ge 2$ be an integer. Let G be a finite abelian group and let $G = B_1 \cdots B_s H$ be a factorization of G, where H is an elementary p-group of rank n and $|B_1| \ge 2, \dots, |B_s| \ge 2$. Suppose that

$$B_i = \{b_{i,1}, \dots, b_{i,r(i)}\}.$$

Let $L_1, \dots, L_n, M_1, \dots, M_n$ be subgroups of H of order p such that $H = X_1 \cdots X_s$, where $X_i \in \{L_i, M_i\}$ for each i, $1 \le i \le n$. Set

$$\begin{aligned} A_1 &= b_{1,1}L_1 \cup b_{1,2}M_1 \cup \cdots \cup b_{1,r(1)}M_1, \\ &\ \vdots \\ A_n &= b_{n,1}L_n \cup b_{n,2}M_n \cup \cdots \cup b_{n,r(n)}M_n. \end{aligned}$$

The computation

$$\begin{aligned} A_1 \cdots A_n &= \prod_{i=1}^{n} (b_{i,1} L_i \cup b_{i,2} M_i \cup \cdots \cup b_{i,r(i)} M_i) \\ &= B_1 \cdots B_n H \\ &= G \end{aligned}$$

shows that $G = A_1 \cdots A_n$ is a factorization of G.

As H is an elementary p-group of rank n it can be viewed as an n-dimensional affine space over $\mathrm{GF}(p)$. The subgroups $L_1, \ldots, L_n, M_1 \ldots, M_n$ of order p can be viewed as 1-dimensional subspaces in $[\mathrm{GF}(p)]^n$. The 1-dimensional subspaces of $[\mathrm{GF}(p)]^n$ form the points of in the $(n-1)$-dimensional projective space over $\mathrm{GF}(p)$. This is the geometrical interpretation we will use. Plainly the product $X_1 \cdots X_n$ is equal to H if the points $X_1, \ldots, X_n$ span an $(n-1)$-dimensional projective space. The next lemma shows that if $p \geq 3$, then there is a suitable choice for the points in each dimension.

Lemma 3. *Let p be an odd prime and let $n \geq 2$ be an integer. There are points $L_1, \ldots, L_n, M_1, \ldots, M_n$ in the $(n-1)$-dimensional projective space over $\mathrm{GF}(p)$ such that the points $X_1, \ldots, X_n$ span the whole $(n-1)$-dimensional projective space where $X_i \in \{L_i, M_i\}$ for each i, $1 \leq i \leq n$.*

Proof. Consider first the $n = 2$ special case. Let the points L_1, L_2, M_1, M_2 be defined by coordinates in the following way

$$\begin{aligned} L_1 &: (1,0), & M_1 &: (1,1), \\ L_2 &: (0,1), & M_2 &: (1,2). \end{aligned}$$

Note that none of the determinants

$$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 \\ 1 & 2 \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix}$$

is zero in $\mathrm{GF}(p)$ for $p \geq 3$ and so each of the four pairs

$$L_1, L_2, \quad L_1, M_2, \quad M_1, L_2, \quad M_1, M_2$$

spans a 1-dimensional projective space over $\mathrm{GF}(p)$.

Let us turn to the $n = 3$ case. Let the points L_1, L_2, L_3, M_1, M_2, M_3

given in the following way

$$\begin{aligned} L_1 &: (1,0,0), & M_1 &: (1,1,0), \\ L_2 &: (0,1,0), & M_2 &: (1,2,0), \\ L_3 &: (0,0,1), & M_2 &: (0,0,2). \end{aligned}$$

Let $X_i \in \{L_i, M_i\}$ for some i, $1 \leq i \leq 3$. We claim that X_1, X_2, X_3 span a 2-dimensional projective space over $\mathrm{GF}(p)$. Indeed, if $X_3 = L_3$, then the $n = 2$ special case gives that the points X_1, X_2 span a 1-dimensional projective space. Clearly L_3 is not in this space and so the points X_1, X_2, X_3 span a 2-dimensional projective space. The case when $X_3 = M_3$ can be settled in a similar manner.

The proof can be completed by an induction on n. $\square$

8. *Z*-subsets. A subset A of an abelian group G is called a Z-subset if $A^k \subseteq A$ for each $k \in Z$. Clearly a Z-subset of G is a union of cyclic subsets of G. The concept, that was introduced by C. Okuda [9] in 1975, is not as artificial as it might look at the first glance. Let q be a power of a prime. If C is a perfect e-error correcting linear code of length n over the alphabet $\{0, 1, \ldots, q-1\}$, then $[\mathrm{GF}(q)]^n = S + C$ is an additive factorization, where S is the Hamming sphere of radius e centered at the origin. Here C is a subgroup of $[\mathrm{GF}(q)]^n$ and so it is obviously a Z-subset. Further S is a Z-subset too. Thus factorizations with Z-subset factors occur naturally in coding theory.

We present a factorization construction of [9] by Z-subsets. Let p be an odd prime. Let G be a group of type (p, p, p, p) with basis elements x, y, u, v. Set

$$\begin{aligned} A &= \langle x \rangle \cup \langle xy \rangle \cup \cdots \cup \langle xy^{p-1} \rangle \cup \langle yu \rangle, \\ B &= \langle u \rangle \cup \langle y^2uv \rangle \cup \cdots \cup \langle y^2uv^{p-1} \rangle \cup \langle v \rangle. \end{aligned}$$

We claim that $G = AB$ is a factorization of G. We will verify that $|A| = |B| = p^2$ and $AA^{-1} \cap BB^{-1} = \{e\}$. To prove $|A| = p^2$ note that A is a union of $p+1$ distinct subgroups of order p. This will give that $|A| = (p+1)(p-1)+1 = p^2$. It remains to show that

$$\begin{aligned} \{e\} &= \langle x \rangle \cap \langle xy^{\alpha} \rangle, & 1 \leq \alpha \leq p-1, \\ \{e\} &= \langle x \rangle \cap \langle yu \rangle, & \\ \{e\} &= \langle xy^{\alpha} \rangle \cap \langle xy^{\beta} \rangle, & 1 \leq \alpha < \beta \leq p-1, \\ \{e\} &= \langle xy^{\alpha} \rangle \cap \langle yu \rangle, & 1 \leq \alpha \leq p-1. \end{aligned}$$

As an illustration let us check the third one. Suppose that $(xy^{\alpha})^i = (xy^{\beta})^j$ for some i, j, $0 \leq i, j \leq p-1$. Since x, y, u, v is a basis of G it follows that

$$\begin{array}{rcrcl} i & - & j & = & 0, \\ \alpha i & - & \beta j & = & 0. \end{array}$$

The equations hold in $\mathrm{GF}(p)$. The determinant of the system is not zero and so it follows that $i = j = 0$ as required. The proof of $|B| = p^2$ is similar.

In order to prove that $AA^{-1} \cap BB^{-1} = \{e\}$ consider the subgroups

$$\begin{array}{ll} \langle x, xy^{\alpha} \rangle, & \langle u, y^2uv^{\gamma} \rangle, \\ \langle x, yu \rangle, & \langle u, v \rangle, \\ \langle xy^{\alpha}, xy^{\beta} \rangle, & \langle y^2uv^{\gamma}, y^2uv^{\delta} \rangle, \\ \langle xy^{\alpha}, yu \rangle, & \langle y^2uv^{\gamma}, v \rangle. \end{array}$$

We should verify that each subgroup from the first column is distinct from each subgroup from the second column. The subgroups can be paired off in 16 ways. As an illustration we will show that

$$\{e\} = \langle xy^{\alpha}, xy^{\beta} \rangle \cap \langle y^2uv^{\gamma}, y^2uv^{\delta} \rangle.$$

Assume that

$$(xy^{\alpha})^i (xy^{\beta})^j = (y^2uv^{\gamma})^k (y^2uv^{\delta})^l.$$

Since x, y, u, v is a basis of G it follows that

$$\begin{array}{rcrcrcrcl} i & + & j & & & & & = & 0 \\ \alpha i & + & \beta j & - & 2k & - & 2l & = & 0 \\ & & & & k & + & l & = & 0 \\ & & & & \gamma k & + & \delta l & = & 0 \end{array}$$

The last two equations give that $k = l = 0$, then the first two equations give that $i = j = 0$ as required.

It might be disheartening that one must go through the drudgery of checking 16 cases. On the other hand it is quite comforting that we can get away with considering a mere 16 cases independently of the size of the prime p.

9. Exhaustive search. There are occasions when searching for factorizations of a group we have to resort on a computer assisted exhaustive search.

We describe the complementer factor problem and two methods that proved to be useful in practice.

Given a finite abelian group G, a subset A of G such that $|A|$ divides $|G|$. A subset B of G is a called a complementer factor of A in G if $G = AB$ is a factorization of G. The complementer factor problem asks if A has a complementer factor or alternatively asks for finding all possible complementer factors of A in G.

We introduce a graph Γ in the following way. The nodes of Γ are the elements of G. Then compute the set AA^{-1} and set $k = |G|/|A|$. We connect two distinct elements g, h of G with an edge if $gh^{-1} \notin AA^{-1}$. Suppose that Δ is a clique of size k in Γ and that B is the set of the nodes of Δ. Now $BB^{-1} \cap AA^{-1} = \{e\}$ and $|G| = |A||B|$ obviously hold which implies that $G = AB$ is a factorization of G. Therefore in order to decide if A has a complementer factor in G one may check if the graph Γ has a clique of size k. In order to find all complementer factors to A in G we may find all cliques of size k in Γ.

We illustrate the procedure with a toy problem. Let G be a group of type $(4, 4, 2)$ with basis elements x, y, z, where $|x| = |y| = 4$, $|z| = 2$. Let $A = \{e, x, y, x^3y^3z\}$. The group G has 32 elements and A has 4 elements. So a possible complementer factor B must have 8 elements. We list the elements of G in the following way

$$x^0y^0z^0,\ x^0y^0z^1,\ x^0y^1z^0, \ldots, x^3y^3z^1,$$

that is, the exponents of the elements are ordered lexicographically. The graph Γ has 32 nodes and is given by its 32 by 32 incidence matrix which is displayed in Table 1.

Table 1. The incidence matrix of Γ

A	B	C	D
D	A	B	C
C	D	A	B
B	C	D	A

The blocks A, B, C, D are detailed in Table 2. The reader can notice that the matrices B and D are transposes of each other and the matrices A and C are symmetric with respect to the main diagonal.

There are well tested computer programs to find k-cliques in a given graph. See for example [13], [10]. The computation reveals that Γ contains 16

Table 2. Blocks A, B, C, D

	1			1	1		
1				1	1		
			1			1	1
		1				1	1
1	1				1		
1	1			1			
		1	1				1
		1	1			1	

		1		1	1		1
			1	1	1	1	
	1			1		1	1
1					1	1	1
1	1		1			1	
1	1	1					1
1		1	1		1		
	1	1	1	1			

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

			1	1	1	1	
		1		1	1		1
1					1	1	1
	1			1		1	1
1	1	1					1
1	1		1			1	
	1	1	1	1			
1		1	1		1		

cliques of size 8. We list two of them

$$B_1 = \{e, z, y^2, y^2z, x^2, x^2z, x^2y^2, x^2y^2z\},$$
$$B_2 = \{e, z, y^2, y^2z, x^2y^3, x^2y^3z, x^2y, x^2yz\}.$$

One can see that both of them are periodic. The subgroups of periods are $\langle x^2, y^2, z\rangle$, $\langle y^2, z\rangle$ respectively and so B_1 is a subgroup of G.

We turn to an other possible algorithm to tackle the complementer factor problem. Let F be a family of subsets of a universal set U. The k-exact cover problem asks if there are k elements $V_1, \ldots, V_k$ of F such that $V_1, \ldots, V_k$ form a partition of U, that is, $V_1 \cup \cdots \cup V_k = U$ and $V_i \cap V_j = \emptyset$ for each i, j, $1 \leq i < j \leq k$. The complementer factor problem can be reduced to the exact cover problem by setting $U = G$ and $F = \{Ag : \ g \in G\}$. If the sets Ab, $b \in B$ form a partition of G, then clearly $G = AB$ is a factorization of G.

We illustrate the procedure with the same choice of G and A as in the previous example. The elements of the family F can be given by a 32 by 32 incidence matrix. The matrix is depicted in Table 3. The blocks A, B are detailed in Table 2. We used D. E. Knuth [8] dancing link algorithm to solve this instance of the exact cover problem and got the same 16 solutions as with the

Table 3. The family F

A	B		
	A	B	
		A	B
B			A

Table 4. Blocks A, B

1		1					
	1		1				
		1		1			
			1		1		
				1		1	
					1		1
1						1	
	1						1

1			1				
	1	1					
		1			1		
			1	1			
				1			1
					1	1	
	1					1	
1							1

k-clique method.

Sometimes only a subset of the factor A is given in the exact cover problem. Both the clique and the exact cover approaches can be extended to this more general situation. It is well-known that the k-clique and the exact cover problems fall into the NP-complete class. This means that in these families of problems there must be computationally demanding instances. However, it is an empirical fact some of the solvable cases played crucial role to settle highly nontrivial problems. As convincing examples we would like to mention [22], [12], [11]. So these exhaustive search techniques can be rightfully listed among the tools of constructing factorizations.

We would like to propose a family of new type of random graphs to test the performance of maximum clique algorithms. Namely, take a finite abelian group of a suitable size. The order of G will be the number of nodes of the graph. Then consider an ascending chain of subgroups

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n \subseteq H_{n+1} = G.$$

From the chain using the Hajós-Sands recursion we have seen in Section 2 construct a factorization $G = B_1 B_2$. Discard B_1 and try to find a complementer factor to B_2 in G. This can be done by constructing the graph Γ above. In order to have a large collection of such graphs and in order to ensure fairness we suggest to pick the functions φ_i randomly so that each φ_i has the some probability

$1/(|D_{i-1}|^{|U_i|})$.

10. Code constructions. Let A be the binary alphabet $\{x, y\}$. The set of all the possible finite words can be formed using letters from A will be denoted by A^*. With the operation of the concatenation of words A^* is a free semigroup generated by the elements of A. The neutral element is the empty word. A nonempty subset C of A^* is called a code if for each $c_1, \dots, c_u, d_1, \dots, d_v \in C$ from

$$c_1 \cdots c_u = d_1 \cdots d_v$$

it follows that $u = v$, then $c_1 \cdots c_u = d_1 \cdots d_u$ implies that $c_1 = d_1, \dots, c_u = d_u$. Once a code C is constructed by deleting elements from C we get new codes. In other words subset of a code is again a code.

In order to refute the so called triangle conjecture P. W. Shor [18] constructed the code listed in Table 5.

Table 5. Shor's code

y	x^3y	x^8y	$x^{11}y$
yx	x^3yx^2	x^8yx^2	$x^{11}yx$
yx^7	x^3yx^4	x^8yx^4	$x^{11}yx^2$
yx^{13}	x^3yx^6	x^8yx^6	
yx^{14}			

Analyzing Shor's code one can come up with the following idea of constructing codes. Let $B = \{b(1), \dots, b(s)\}$ be a set of integers. Suppose $A_1, \dots, A_s$ are subsets of integers such that the sum $A_i + B$ is direct for each i, $1 \le i \le s$. This simply means that

$$a + b = a' + b', \quad a, a' \in A_i, \quad b, b' \in B$$

imply that $a = a'$, $b = b'$. Set

$$C_i = \{x^{b(i)}yx^a : \ a \in A_i\}, \quad 1 \le i \le s.$$

Lemma 4. *The set $C = C_1 \cup \cdots \cup C_s$ is a code over the binary alphabet $\{x, y\}$.*

Proof. It is enough to verify that given a word w that is a product of elements of C then we are able to decompose w into a product of elements of C without any ambiguity.

If the letter y does not appear in w, then w cannot be a product of elements of C. If y appears in w once, then w must be a single code word in C. By counting we can find the number of x's in front of y in w. Let this number be β. If β is equal to one of $b(1), \ldots, b(s)$, say $\beta = b(i)$, then w must belong to C_i. By scanning w we can find the number of x's following y. Let this number be α. If $\alpha \in A_i$, then w must be the code word $x^{b(i)}yx^{\alpha}$ in C.

Consider next the case when y appear in w at least twice. We can find the number of x's in front of the first y and the number of x's between the first and second y. Let these numbers be β and α respectively. There is a $b(i)$ such that $\beta = b(i)$ otherwise w cannot be a product of elements of C. Then α can be represented in the form

$$\alpha = a + b, \quad a \in A_i, \quad b \in B$$

otherwise w is not a product of elements of C. We can chop off the code word $x^{b(i)}yx^{a}$ from the front of w and repeat the procedure with a shorter word. $\square$

Example 3. In case of the code exhibited in Table 5

$$\begin{aligned} B &= \{0, 3, 8, 11\}, \\ A_1 &= \{0, 1, 7, 13, 14\}, \\ A_2 &= \{0, 2, 4, 6\}, \\ A_3 &= \{0, 2, 4, 6\}, \\ A_4 &= \{0, 1, 2\}. \end{aligned}$$

One can verify that the sum $A_i + B$ is direct for each i, $1 \leq i \leq 4$.

In the construction above direct sums of subsets of the set of integers were used. Next we use direct sums of subsets of a finite cyclic group. Choose a positive integer n. Let $B = \{b(1), \ldots, b(s)\}$ be a subset of $Z(n)$. We think of $Z(n)$ as the set of elements $0, 1, \ldots, n-1$ with the operation of addition modulo n. Suppose that $A_1, \ldots, A_s$ are subsets of $Z(n)$ such that the sum $A_i + B$ is direct in $Z(n)$ for each i, $1 \leq i \leq s$. Set

$$C_i = \{x^{b(i)}yx^{a} : \ a \in A_i\}, \quad 1 \leq i \leq s.$$

Lemma 5. *The set $C = \{x^n\} \cup C_1 \cup \cdots \cup C_s$ is a code over the alphabet $\{x, y\}$.*

Proof. The proof parallels the proof of Lemma 4. The only difference is that when we count the number of appearances of x we should do so modulo n. $\square$

The morale of this section is that simultaneous factorizations provide another source of codes beside the well-known constructions that yield for example the prefix and postfix codes. We describe two possible approaches in detail.

In the first approach one can start with a normalized factorization $Z(n) = A + C$ of the cyclic group $Z(n)$. Then look for integers $k_1, \dots, k_s$ for which $k_1 A + C, \dots, k_s A + C$ are factorizations of $Z(n)$ simultaneously. Then choosing the subsets $A_1, \dots, A_s$, B such that $A_1 \subseteq k_1 A, \dots, A_s \subseteq k_s A$, $B \subseteq C$ by Lemma 5 we get a code.

In the second approach one can start with a normalized factorization $Z(n) = A + C$ of the cyclic group $Z(n)$. This time consider $H = \langle C \rangle$ and suppose that $H \neq Z(n)$, that is, $Z(n) = A + C$ is not a "full-rank" factorization. Choose elements $a_1, \dots, a_s$ of A. Adding $-a_i$ to both sides of the factorization $Z(n) = A + C$ gives the normalized factorization $Z(n) = (A - a_i) + C$. Restricting this factorization to H results the normalized factorization $H = [(A - a_i) \cap C] + C$. Now the sums

$$[(A - a_1) \cap C] + C, \dots, [(A - a_s) \cap C] + C$$

form s simultaneous factorizations of H. Let us choose the subsets $A_1, \dots, A_s$, B such that

$$A_1 \subseteq [(A - a_1) \cap C] + a_1, \dots, A_s \subseteq [(A - a_s) \cap C] + a_s, \; B \subseteq C.$$

By Lemma 5 we can construct a code.

Arguments similar to those in Section 5 show that there is a ready supply of factorizations of cyclic groups and so a very large variety of codes can be constructed from factorizations.

There is a more profound connection between codes and factoring cyclic groups when one starts with a maximal code and assigns a factorization to the code as described by A. Restivo, S. Salemi, and T. Sportelli [15]. For further details see also C. De Felice [5] and the definitive monograph of J. Berstel and D. Perrin [1].

11. Characters and the covering problem. Let U be a universal set and let F be a family of subsets of U. If $B_1, \dots, B_k$ are subsets of F such that $U = B_1 \cup \cdots \cup B_k$, then we say that $B_1, \dots, B_k$ form a covering of U. The decision version of the k-covering problem is the following. Given a universal set U, a family of subsets F of U and an integer k. Are there k elements $B_1, \dots, B_k$ of F that form a covering of U? The non-decision version of the covering problem seeks of finding a covering or finding all coverings of U by k subsets. We show that factoring a finite abelian group can be related to the covering problem.

For a subset A and for a character χ of a finite abelian group G the complex number

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

will be denoted by $\chi(A)$. If $\chi(A)=0$, then we say that χ annihilates A. The set of all characters of G that annihilates A will be denoted by $\mathrm{Ann}(A)$. The character ε of G defined by $\varepsilon(g)=1$ for each $g\in G$ is called the unit or principal character of G. Let $\mathcal{G}$ be the set of all the characters of G. It is a consequence of the standard orthogonality relations of characters that $G=A_1\cdots A_n$ is a factorization of G if and only if $|G|=|A_1|\cdots|A_n|$ and the sets $\mathrm{Ann}(A_1),\ldots,\mathrm{Ann}(A_n)$ form a covering of $\mathcal{G}\setminus\{\varepsilon\}$. (For the details see [14].)

Let G be a finite abelian group, let $\mathcal{G}$ be the group of characters of G and let L be a family of subsets of G. We construct an $|L|$ by $|\mathcal{G}|$ incidence matrix M. The rows correspond to the elements of L and the columns correspond to the elements of $\mathcal{G}$. Let $m_{A,\chi}$ be a typical component of M, where $A\in L$, $\chi\in\mathcal{G}$. We set

$$m_{A,\chi}=\begin{cases}1, & \text{if} \quad \chi(A)=0,\\ 0, & \text{if} \quad \chi(A)\neq 0.\end{cases}$$

The 1's in the row of A record the annihilator of A. It is clear that the column labeled by the principal character ε of G contains only 0. If the rows corresponding to the sets $A_1,\ldots,A_n$ together contain 1's in each column corresponding to the elements of $\mathcal{G}\setminus\{\varepsilon\}$ and in addition $|G|=|A_1|\cdots|A_n|$ holds, then the product $A_1\cdots A_n$ is a factorization of G.

We illustrate the procedure with a toy example. Let G be a group of type $(2,2,3)$ with basis elements x, y, z, where $|x|=|y|=2$, $|z|=3$. Each element $g\in G$ can be written in the form

$$g=x^a y^b z^c,\quad 0\leq a,b\leq 1,\quad 0\leq c\leq 2.$$

We record g by the exponents a, b, c. Let ρ, σ be a roots of unity of orders 2 and 3 respectively. The character χ of G defined by

$$\chi(x)=\rho^a,\quad \chi(y)=\rho^b,\quad \chi(z)=\sigma^c$$

will be recorded by the exponents a, b, c. The cyclic subset

$$A=\{e,a,a^2,\ldots,a^{r-1}\}$$

Table 6. The incidence matrix

	0	0	0	0	0	0	1	1	1	1	1	1
	0	0	0	1	1	1	0	0	0	1	1	1
	0	1	2	0	1	2	0	1	2	0	1	2
000;2												
001;2												
002;2												
010;2				1	1	1				1	1	1
011;2				1						1		
012;2				1						1		
100;2							1	1	1	1	1	1
101;2							1			1		
102;2							1			1		
110;2				1	1	1	1	1	1			
111;2				1			1					
112;2				1			1					
000;3												
001;3		1	1		1	1		1	1		1	1
002;3		1	1		1	1		1	1		1	1
010;3												
011;3		1	1					1	1			
012;3		1	1					1	1			
100;3												
101;3		1	1		1	1						
102;3		1	1		1	1						
110;3												
111;3		1	1								1	1
112;3		1	1								1	1

will be recorded by $[a, r]$. If $a = x^u y^v z^w$, then $[a, r]$ will be written simply as $u, v, w; r$ The incidence matrix is depicted in Table 6. The reader may notice that the notation $000; 2$ does not correspond to a set of G. In fact it denotes a multiset of G. So the rows of the incidence matrix should be labeled by multisets of G instead of sets. The underlying theory works equally well for multisets. The reader also can check that the rows marked by $101; 2$, $111; 2$, $001; 3$ cover the columns marked by the elements of $\mathcal{G} \setminus \{\varepsilon\}$. These rows record the following sets

$$A_1 = \{e, xz\}, \quad A_2 = \{e, xyz\}, \quad A_3 = \{e, z, z^2\}$$

and $|G| = |A_1||A_2||A_3|$ holds. Therefore $G = A_1A_2A_3$ is a factorization of G. By Rédei's theorem one of the factors A_1, A_2, A_3 must be a subgroup of G. Indeed, here A_3 is a subgroup of G.

Let us cancel now the rows of the incidence matrix that correspond to subgroups of G. In this way the occurring factorizations cannot contain subgroup factors. From Rédei's theorem we know that such factorizations do not exist. However, there are multiple factorizations without subgroup factors and the construction of such factorizations is also related to the covering problem. Namely, if

$$\mathcal{G} \setminus \{\varepsilon\} \subseteq \mathrm{Ann}(A_1) \cup \cdots \cup \mathrm{Ann}(A_n),$$

then the product $A_1 \cdots A_n$ is a multiple factorization of G. The multiplicity of the factorization is of course $(|A_1| \cdots |A_n|)/|G|$.

We say that the row labeled by A dominates the row labeled by A' if $\mathrm{Ann}(A) \subseteq \mathrm{Ann}(A')$. (For example in Table 6 the 15th row dominates the last row.) Deleting row A' from M we get a new incidence matrix M'. Obviously if M contains a covering, then so does M'. In short, the row of A' can be deleted from M.

The column of χ of M records the family of subsets

$$L_\chi = \{A : \ A \in L, \ \chi(A) = 0\}$$

of G. We say that the column of χ dominates the column of χ' if $L_\chi \subseteq L_{\chi'}$. (For example in Table 6 the last column dominates the second column.) Canceling column χ from M we get a new incidence matrix M'. Clearly if M contain a covering, then so does M'. Shortly, one can delete column χ' from M.

Table 7 represents a condensed version of the incidence matrix in Table 6. One can read off from the incidence matrix that the product of the sets

$$\begin{aligned}
A_1 &= \{e, yz\}, \\
A_2 &= \{e, xz\}, \\
A_3 &= \{e, yz, (yz)^2\}, \\
A_4 &= \{e, xz, (xz)^2\}, \\
A_5 &= \{e, xyz, (xyz)^2\},
\end{aligned}$$

form a 9-fold factorization of G.

In this construction the type of the group G was $(2, 2, 3)$. Let us now consider a group of type $(2, 2, p)$. In other words let us replace the number 3 by

Table 7. A condensed incidence matrix

	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
011;2	1				1	
101;2			1		1	
111;2	1		1			
011;3				1		
101;3		1				
111;3						1

an odd prime p in the above construction. Let x, y, z, be the basis elements of G, where $|x| = |y| = 2$, $|z| = p$. Set

$$\begin{aligned} A_1 &= \{e, yz\}, \\ A_2 &= \{e, xz\}, \\ A_3 &= \{e, yz, \ldots, (yz)^{p-1}\}, \\ A_4 &= \{e, xz, \ldots, (xz)^{p-1}\}, \\ A_5 &= \{e, xyz, \ldots, (xyz)^{p-1}\}. \end{aligned}$$

Let us choose a non-identity character χ of G and try to show that $\chi(A_i) = 0$ for some i, $1 \le i \le 5$.

Suppose first that $\chi(z) = 1$. Since χ is not the identity character either $\chi(x) \neq 1$ or $\chi(y) \neq 1$. This means that at least one of $\chi(x)$ and $\chi(y)$ is equal to -1. If $\chi(x) = -1$, then $\chi(A_2) = 0$. If $\chi(y) = -1$, then $\chi(A_1) = 0$. For the remaining part of the argument we may assume that $\chi(z) \neq 1$, that is, $\chi(z)$ is a complex root of unity of order p. If $\chi(x) = 1$, then $\chi(A_4) = 0$. If $\chi(y) = 1$, then $\chi(A_3) = 0$. We are left with the case when $\chi(x) = \chi(y) = -1$. Now $\chi(xy) = 1$ and so $\chi(A_5) = 0$. Thus the product $A_1 \cdots A_5$ is a p^2-fold factorization of G.

REFERENCES

[1] J. Berstel, D. Perrin. Theory of Codes. Pure and Applied Mathematics, vol. **117**. Academic Press, New York, 1985.

[2] N. G. De Bruijn. On the factorization of finite abelian groups. *Indagationes Math.* **15** (1953), 258–264.

[3] M. Dinitz. Full rank tilings of finite abelian groups. *SIAM J. Discrete Math.* **20**, *1* (2006), 160–170.

[4] L. Euler. Opera Omnia vol. **7**, Berlin, Teubner, 1923, 391–392.

[5] C. De Felice. An application of Hajós factorization to variable-length codes. *Theoret. Comput. Sci.* **164**, *1–2* (1996), 223–252.

[6] O. Fraser, B. Gordon. Solution to a problem of A. D. Sands. *Glasgow Math. J.* **20**, *2* (1979), 115–117.

[7] G. Hajós. Sur la factorisation des groupes abéliens. *Časopis Pěs. Mat. Fys.* **74** (1950), 157–162.

[8] D. E. Knuth. Dancing links. In: Millennial Perspectives in Computer Science (Eds J. Davies, B. Roscoe, J. Woodcock) Basingstoke, Palgrave Macmillan, 2000, 187–214.

[9] C. Okuda. The factorization of abelian groups. Ph.D. Thesis, The Pennsylvania State University, 1975.

[10] P. R. J. Östergård. A fast algorithm for the maximum clique problem. *Discrete Appl. Math.* **120**, *1–3* (2002), 197–207.

[11] P. R. J. Östergård, S. Szabó. Elementary p-groups with the Rédei property. *Internat. J. Algebra Comput.* **17**, *1* (2007), 171–178.

[12] P. R. J. Östergård, A. Vardy. Resolving the existence of full-rank tilings of binary Hamming spaces. *SIAM J. Discrete Math.* **18**, *2* (2004), 382–387.

[13] P. M. Pardalos, J. Xue. The maximum clique problem. *J. of Global Optim.* **4**, *3* (1994), 301–328.

[14] L. Rédei. Die neue Theorie der endlichen Abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós. *Acta Math. Acad. Sci. Hungar.* **16** (1965), 329–373.

[15] A. Restivo, S. Salemi, T. Sportelli. Completing codes. *RAIRO Inform. Théor. Appl.* **23**, *2* (1989), 135–147.

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

[17] A. D. Sands. Replacement of factors by subgroups in the factorization of abelian groups, *Bull. London Math. Soc.* **32**, *3* (2000), 297–304.

[18] P. W. Shor. A counterexample to the triangle conjecture, *J. Combin. Theory Ser. A* **38**, *1* (1985), 110–112.

[19] S. K. Stein. A symmetric star body that tiles but not as a lattice. *Proc. Amer. Math. Soc.* **36** (1972), 543–548.

[20] S. Szabó. A type of factorization of finite abelian groups. *Discrete Math.* **54**, *1* (1985), 121–125.

[21] S. Szabó. Constructions related to the Rédei property. *J. London Math. Soc. (2)* **73**, *3* (2006), 701–715.

[22] A. Trachtenberg, A. Vardy. Full-rank tilings of $\mathbb{F}_2^8$ does not exist. *SIAM J. Discrete Math.*, **16**, *3* (2003), 390–392.

Institute of Mathematics and Informatics
University of Pécs
Ifjúság u. 6
7624 Pécs, Hungary
e-mail: `sszabo7@hotmail.com`

Received February 9, 2018