Canad. Math. Bull. Vol. 18 (1), 1975

GROUP PARTITIONS AND MIXED PERFECT CODES

BY
BERNT LINDSTRÖM

ABSTRACT. Let G be a finite abelian group of the order p^r and type $(p, \ldots, p)$, where p is a prime. A necessary and sufficient condition is determined for the existence of subgroups $G_1, G_2, \ldots, G_n$, one of the order p^a and the rest of the order p^b, such that $G=G_1 \cup G_2 \cup \cdots \cup G_n$ and $G_i \cap G_j=\{\theta\}$ when $i\neq j$.

A group G is said to have a *partition of the type* $G_1 \cup G_2 \cup \cdots \cup G_n$ if G is the union of subgroups $G_1', G_2', \ldots, G_n'$ which have pairwise only the neutral element G in common and G_i' is isomorphic to $G_i (G_i' \simeq G_i)$ for $i=1, 2, \ldots, n$. If $G_i'=G_i$ for $i=1, 2, \ldots, n$ we have a *group partition* $G=G_1 \cup G_2 \cup \cdots \cup G_n$.

Let $G^r(p)$ denote the elementary abelian group of order p^r and type $(p, \ldots, p)$ for a prime p.

The following lemma was proved by M. Herzog and J. Schönheim in [2].

LEMMA 1. *If a finite abelian group G has a partition $G_1 \cup G_2 \cup \cdots \cup G_n$, then G is isomorphic to $G^r(p)$ for some r, and G_i $(i=1, 2, \ldots, n)$ is isomorphic to $G^{m_i}(p)$ for some m_i and a fixed prime p. Moreover*

$$p^r = 1+\sum_{i=1}^{n}(p^{m_i}-1). \tag{1}$$

The condition (1) *is necessary, but not sufficient, for the existence of a partition of G of the type $G^{m_1}(p) \cup G^{m_2}(p) \cup \cdots \cup G^{m_n}(p)$. The following condition* (2) *is also necessary*

$$m_i+m_j \leq r, \quad when \quad 1 \leq i < j \leq n. \tag{2}$$

In order to prove (2) consider the subgroup H_{ij} generated by the elements of $G_i \cup G_j$. When $h \in H_{ij}$ we have $h=a+b$ for $a \in G_i$, $b \in G_j$, which are uniquely determined since $G_i \cap G_j=\{\theta\}$. The order of H_{ij} is therefore $p^{m_i+m_j} \leq p^r$, and (2) follows.

Some sufficient conditions for the existence of group partitions were found by M. Herzog and J. Schönheim in [2]. Our main result is a necessary and sufficient condition for a special case. We first prove

LEMMA 2. *If $r=a+b$, where $a \geq b$, then there is a partition of the type*

$$G^r(p) = G^a(p) \cup G^b(p) \cup \cdots \cup G^b(p).$$

Received by the editors November 2, 1973 and, in revised form, March 6, 1974.

https://doi.org/10.4153/CMB-1975-011-2 Published online by Cambridge University Press

Proof. Consider $G^r(p)$, $G^a(p)$ and $G^b(p)$ as vector spaces over the prime field $GF(p)$. $G^r(p)$ is the direct product of $G^a(p)$ and $G^b(p)$. Since $b \le a$, we can determine linearly independent $g_1, g_2, \ldots, g_b \in G^a(p)$. Let $v_1, v_2, \ldots, v_b$ be a basis of $G^b(p)$.

Identify $G^a(p)$ and $GF(p^a)$ and consider the products $gg_i \in GF(p^a)$, when $g \in GF(p^a)$, as elements of $G^a(p)$. In the direct product $G^r(p)$ are (gg_i, v_i), $i=1, \ldots, b$, a basis of a b-dimensional subspace G_b.

If $G^a(p)$ is identified with the subspace in $G^r(p)$ of all vectors $(x_1, \ldots, x_a, 0, \ldots, 0)$, then we get $G^a(p) \cap G_b = \{\theta\}$ easily.

We shall now prove that $G_g \cap G_h = \{\theta\}$, when $g, h \in GF(p^a)$ and $g \ne h$. If

$$\sum_{i=1}^{b} x_i(gg_i, v_i) = \sum_{i=1}^{b} y_i(hg_i, v_i),$$

where all $x_i, y_i \in GF(p)$, then it follows that $x_i = y_i$ $(i=1, \ldots, b)$ since $v_1, v_2, \ldots, v_b$ are linearly independent. Then we have in $GF(p^a)$

$$\sum_{i=1}^{b} x_i(g-h)g_i = 0.$$

If we divide by $g-h \ne 0$ and use the linear independence of $g_1, \ldots, g_b$, then it follows that $x_i = y_i = 0$ $(i=1, \ldots, b)$, and we have proved that $G_g \cap G_h = \{\theta\}$. Observe that each subspace G_g is isomorphic to $G^b(p)$.

The union of $G^a(p)$ and all G_g, $g \in GF(p^a)$, is $G^r(p)$, for the number of elements in the union is $p^a + p^a(p^b - 1) = p^r$. This completes the proof.

THEOREM 1. *A necessary and sufficient condition for the existence of a partition of $G^r(p)$ of the type $G^a(p) \cup G^b(p) \cup j \cdot \cdot \cup G^b(p)$ in n subgroups is that both*

$$p^r = p^a + (n-1)(p^b - 1), \tag{3}$$

and

$$a+b \le r, \qquad a \ge b. \tag{4}$$

Proof. The necessity of (3) follows by (1). The inequality $a+b \le r$ in (4) is a special case of (2). We shall prove that $a \ge b$ is necessary.

$G^r(p)$ is a vector space over $GF(p)$. We choose a basis of $G^r(p)$ such that $G^a(p)$ will be the subspace of vectors with the last $r-a$ components 0. Let $\mathrm{E} = e^{2\pi i/p}$ and define two functions λ and μ from $G^r(p)$ into the complex numbers by

$$\lambda(x_1, \ldots, x_r) = \varepsilon^{x_1}, \qquad \mu(x_1, \ldots, x_r) = \varepsilon^{x_r}.$$

We write for brevity $(x_1, \ldots, x_r) = \mathbf{x}$ and $G^r(p) = G$, and find that

$$\sum_{\mathbf{x} \in G} \lambda(\mathbf{x}) = \sum_{\mathbf{x} \in G} \mu(\mathbf{x}) = 0. \tag{5}$$

Let s be the number of subgroups $G_i \simeq G^b(p)$ in the partition of G with $x_1 = 0$ when $\mathbf{x} \in G_i$. Let t be the number of subgroups $G_i \simeq G^b(p)$ in the partition of G

with $x_r=0$ when $\mathbf{x}\in G_i$. We find easily that

$$(6)\qquad \sum_{i=1}^{n}\sum_{\mathbf{x}\in G_i}\lambda(\mathbf{x}) = sp^b \quad\text{and}\quad \sum_{i=1}^{n}\sum_{\mathbf{x}\in G_i}\mu(\mathbf{x}) = p^a+tp^b,$$

where the sums run over all (n) subgroups in the partition of G. Then we find that the sums are respectively

$$\sum_{\mathbf{x}\in G}\lambda(\mathbf{x})+(n-1)\lambda(\theta) \quad\text{and}\quad \sum_{\mathbf{x}\in G}\mu(\mathbf{x})+(n-1)\mu(\theta),$$

and it follows by (5) and (6), and since $\lambda(\theta)=\mu(\theta)=1$, that $(s-t)p^b=p^a$. Hence $a\geq b$, and the necessity of (3) and (4) is proved.

Then we assume that the conditions (3) and (4) are satisfied. By (3) and since p is a prime it follows that b divides $r-a$. We write $r=a+kb$ for an integer k, with $k\geq 1$ by (4). Since $a\geq b$ by (4), we now find by Lemma 2 a partition of $G^r(p)$ of the type

$$\begin{aligned} G^{a+kb}(p) &= G^{a+(k-1)b}(p)\cup G^b(p)\cup\cdots\cup G^b(p) = \cdots \text{ (by induction)}\\ &= G^a(p)\cup G^b(p)\cup\cdots\cup G^b(p), \end{aligned}$$

which completes the proof of Theorem 1.

We shall indicate briefly the close relationship between group partitions and mixed perfect codes.

Let $G_1, G_2, \ldots, G_n$ be finite groups and $W_n=G_1\times G_2\times\cdots\times G_n$ the direct product. A subset C of W_n is called a *mixed code*. When all the groups $G_1, G_2, \ldots, G_n$ are isomorphic the prefix "mixed" is usually omitted. If C is a subgroup of W_n, then C is called a *group code*.

The elements of W_n are n-tuples $\mathbf{x}=(x_1,\ldots,x_n)$, where $x_i\in G_i$ for $i=1,2,\ldots,n$. If also $\mathbf{y}=(y_1,\ldots,y_n)$ belongs to W_n, then we define a *distance* $d(\mathbf{x},\mathbf{y})=|\{i \mid 1\leq i\leq n,\ x_i\neq y_i\}|$. A code C in W_n is *perfect e-error-correcting* if for each $w\in W_n$ there is precisely one $c\in C$ such that $d(w,c)\leq e$.

The "only if" part of the following theorem was proved in [1].

THEOREM 2. *Let $G_1, G_2, \ldots, G_n$ be finite abelian groups. There is an abelian group G with a partition of the type $G_1\cup G_2\cup\cdots\cup G_n$ if and only if there is a perfect* 1*-error-correcting mixed group code C in the direct product $W_n=G_1\times G_2\times\cdots\times G_n$.*

Proof. Suppose we have a partition $G=G_1\cup G_2\cup\cdots\cup G_n$. Then the group code C is the kernel of the homomorphism

$$(x_1, x_2, \ldots, x_n)\to x_1+x_2+\cdots+x_n.$$

The details of the proof can be found in [1], p. 366.

Conversely, let C be a perfect 1-error-correcting mixed group code in W_n. Let G be the factor group W_n/C and h the natural homomorphism $W\to W_n/C$.

https://doi.org/10.4153/CMB-1975-011-2 Published online by Cambridge University Press

We identify G_i with the subgroup in W_n of all $(0, \ldots, 0, x_i, 0, \ldots, 0)$, where $x_i \in G_i$. Put $h(G_i)=G_i'$ for $i=1, 2, \ldots, n$. If $\mathbf{x} \in G_i$ then $d(\mathbf{x}, \theta) \leq 1$. The only $c \in C$ for which $d(c, \theta) \leq 1$ is $c=\theta$. Hence $G_i \cap C=\{\theta\}$, and it follows that G_i and G_i' are isomorphic groups, when $i=1, 2, \ldots, n$.

It is easy to see that G is the union of all G_i', $1 \leq i \leq n$. For if w is any element in W_n, then we can find $c \in C$ and G_i such that $w-c \in G_i$, since C is a 1-error-correcting code. There is only one $c \in C$ such that $d(w, c) \leq 1$, hence it follows that $G_i' \cap G_j'=\{\theta\}$ when $i \neq j$.

We have proved that G has a group partition of the type $G_1 \cup \cdots \cup G_n$, which was to be proved.

We omit the proof of the following result on mixed perfect codes, which generalizes Theorem 2 in [3], since Lenstra's proof is valid with minor changes.

THEOREM 3. *Let $G_1, G_2, \ldots, G_n$ be finite groups (abelian or non-abelian). If there exists a perfect e-error-correcting mixed group code in $G_1 \times G_2 \times \cdots \times G_n$ and $e<n$, then each G_i is abelian and isomorphic to $G^{m_i}(p)$ for a fixed prime p and $i=1, 2, \ldots, n$.*

From the last theorem it follows that the vector covering problem in [2] (on perfect coverings) cannot be solved by the group partition method unless the cardinalities of the sets considered for each coordinate are powers of the same prime.

Finally, observe that Lemma 1 is a consequence of Theorems 2 and 3.

REFERENCES

1. M. Herzog and J. Schönheim, *Linear and nonlinear single-error-correcting perfect mixed codes*, Information and Control **18** (1971), 364–368.

2. M. Herzog and J. Schönheim, *Group partition, factorization and the vector covering problem*, Canad. Math. Bull. **15** (2) (1972), 207–214.

3. H. W. Lenstra, Jr., *Two theorems on perfect codes*, Discrete mathematics **3** (1972), 125–132.

DEPARTMENT OF MATHEMATICS,
UNIVERSITY OF STOCKHOLM,
BOX 6701,
S-113 85 STOCKHOLM,
SWEDEN

EMALJVÄGEN 14V
S-175 73 JÄRFÄLLA
SWEDEN