Canad. Math. Bull. Vol. **15** (2), 1972

GROUP PARTITION, FACTORIZATION AND THE VECTOR COVERING PROBLEM

BY

M. HERZOG AND J. SCHÖNHEIM

1. Introduction.

1.1. *The covering problem.* Let S_i $(i=1, 2, \ldots, n)$ be given sets containing m_i elements respectively and let

$$S^{(n)} = S_1 \times S_2 \times \cdots \times S_n \tag{1}$$

be their cartesian product. The elements of $S^{(n)}$ will be called *vectors*. The vector $(x_1, x_2, \ldots, x_n)$ *covers* $(y_1, y_2, \ldots, y_n)$ if $x_i = y_i$ for at least $n-1$ values of i. A subset M of $S^{(n)}$ is said to be a *covering* (*perfect covering*) of $S^{(n)}$ if each member of $S^{(n)}$ is covered by at *least* (*exactly*) one member of M. A covering M is said to be *linear* if the sets S_i are groups G_i and M is a subgroup of $G^{(n)} = S^{(n)}$. Denote by $\sigma(n; m_1, m_2, \ldots, m_n)$ the value of min $|M|$ when M runs through all coverings of $S^{(n)}$ and by $\hat{\sigma}(n; m_1, m_2, \ldots, m_n)$ the value of min $|M|$ when the sets S_i are given groups G_i and M runs through all linear coverings of $G^{(n)}$.

The questions arising in connection with the above concepts are

(i) to find exact values or bounds for σ and $\hat{\sigma}$.

(ii) to establish conditions for the existence of linear or nonlinear perfect coverings.

Both questions have been considered so far in particular cases only, namely, both have been asked by Taussky and Todd [1] when

$$S^{(n)} = S^n = S \times S \times \cdots \times S. \tag{2}$$

References and new partial answers to (i) in this case, are given in [2].

For (ii), again in case (2), it is not known whether perfect coverings exist if m, the number of elements of S is not a power q of a prime p. If $m=q$, Zaremba [3, 4] proved, generalizing an earlier result [5] established for $q=p$, that the condition

$$n = q^r - 1/q - 1 \quad \text{for some } n \text{ and } r \tag{3}$$

is necessary and sufficient for the existence of a perfect covering of S^n. He also proved that for n satisfying (3)

$$\sigma(n; q, q, \ldots, q) = q^{n-r} \tag{4}$$

and if S is the additive group of $GF(q)$, then

Received by the editors September 10, 1970.

https://doi.org/10.4153/CMB-1972-038-x Published online by Cambridge University Press

$$\hat{\sigma}(n; q, \ldots, q) = q^{n-r}, \tag{5}$$

however if S is the cyclic group of order q, then

$$\hat{\sigma}(n, q, \ldots, q) > q^{n-r}. \tag{6}$$

The condition (3) is generalized in Theorem 2, §4, while conditions (4), (5), and (6) are generalized in §5.

1.2. *Group factorization and partition.* The mentioned known results have been obtained by a method using factorization and partition of abelian groups. Our results will be obtained by generalizing this method. We will consider only finite abelian groups.

A group $\mathscr{H}$ is said to have a *factorization* $\mathscr{H}=\mathscr{A}+\mathscr{B}$ if there exist two subsets $\mathscr{A}$ and $\mathscr{B}$ of $\mathscr{H}$, such that every element h of $\mathscr{H}$ has a unique representation $h=a+b$, $a\in\mathscr{A}$, $b\in\mathscr{B}$. The problem of finding all factorizations of finite abelian groups is unsolved [6].

A group H is said to have a *partition* $H=G_1 \cup G_2 \cup \cdots \cup G_n$ if H is the union of n of its subgroups, which have pairwise only the zero element in common. The problem of finding all partitions of a finite abelian group is also unsolved.

The covering problem of the former subsection is related (Lemma 6, §4) to factorizations $\mathscr{A}+\mathscr{B}$ of groups $G^{(n)}=G_1\times G_2\times\cdots\times G_n$ such that $\mathscr{A}$ consists of all elements of $G^{(n)}$ having at most one component different from the zero element. We will call such factorizations *one-factorization.*

Zaremba actually proved the existence of an one-factorization of

$$\mathscr{g}^n = \mathscr{g}\times\mathscr{g}\times\cdots\times\mathscr{g} \tag{7}$$

for n satisfying (3), $\mathscr{g}$ being a group of order q. We will generalize this result to

$$\mathscr{g}^{(n)} = \mathscr{g}_1\times\mathscr{g}_2\times\cdots\times\mathscr{g}_n \tag{8}$$

for n satisfying certain conditions, the $\mathscr{g}_i$ being groups of order p^{α_i}.

Zaremba's essential observation is that the one-factorization of (7) depends on the existence of a group H having a partition into n subgroups, each of order q, and the fact that the group

$$G^r = G\times G\times\cdots\times G \tag{9}$$

where G is the additive group of $GF(q)$ has such a partition for n satisfying (3).

We will observe more generally (Theorem 1) that the one factorization of (8) depends on the existence of a group H having a partition into n subgroups of order m_i respectively and that the group G^r for n satisfying certain conditions has such a partition (§3). Consequences regarding problem (ii) will be formulated in §4.

2. **Group partitions leading to one-factorizations.**

THEOREM 1. *If an abelian group G has a partition*

$$G = G_1 \cup G_2 \cup \cdots \cup G_n$$

and if $\mathscr{g}_i$ are abelian groups, $|\mathscr{g}_i| = |G_i|$, $i = 1, 2, \ldots, n$, then the group

$$\mathscr{g}^{(n)} = \mathscr{g}_1 \times \mathscr{g}_2 \times \cdots \times \mathscr{g}_n$$

has a one-factorization $\mathscr{A} + \mathscr{B}$. Moreover, if

$$\mathscr{g}_i \simeq G_i \tag{10}$$

then $\mathscr{B}$ is a subgroup of $\mathscr{g}^{(n)}$.

Proof. First we prove the second part of the theorem. Denote by x_i an element of $\mathscr{g}_i$ and by x_i' its image by (10). Define the mapping

$$\mathscr{g}^{(n)} \in x = (x_1, x_2, \ldots, x_n) \to x_1' + x_2' + \cdots + x_n' = x' \in G,$$

which is clearly a homomorphism. Denote its kernel by $\mathscr{B}$. Let $\mathscr{A}$ be as in §1.2 the set of elements of $\mathscr{g}^{(n)}$ having at most one component different from the zero element. Then $\mathscr{A} + \mathscr{B}$ is an one-factorization. Indeed, if $\mathscr{g}^{(n)} \in g \to g' \in G$ then for some unique $a \in A$, $a \to g'$, $g - a \to 0$ and

$$g = a + b, \qquad a \in \mathscr{A}, \quad b \in \mathscr{B}. \tag{11}$$

Moreover (11) is unique. Indeed $g = a + b = a_1 + b_1$ would imply $a - a_1 = b - b_1 \in \mathscr{B}$, hence $a - a_1 \to 0$ and therefore $a' = a_1'$, implying $a = a_1$ and finally $b = b_1$.

For the first part, let H be the group $G_1 \times G_2 \times \cdots \times G_n$. By the second part of the theorem it has an one-factorization $H = \mathscr{A} + \mathscr{B}$. Let $\mathscr{g}_i \leftrightarrow G_i$ $(i = 1, 2, \ldots, n)$ be a 1–1 correspondence between the elements of $\mathscr{g}_i$ and G_i, the zero elements corresponding to each other. These correspondence induce a 1–1 correspondence between $\mathscr{g}^{(n)}$ and H, the zeros still corresponding. Denote by $\mathscr{A}^*$ and $\mathscr{B}^*$ the subsets of $\mathscr{g}^{(n)}$ being the images of $\mathscr{A}$ and $\mathscr{B}$ respectively. We claim that $\mathscr{A}^* + \mathscr{B}^*$ is a one-factorization of $\mathscr{g}^{(n)}$. Indeed, let $g^* \in \mathscr{g}^{(n)}$ and $g^* \leftrightarrow g \in H$. Let $g = a + b$, $a \in \mathscr{A}$, $b \in \mathscr{B}$ and let $b^* \leftrightarrow b$. Since b differs from g in one component at most, also b^* differs at most in one component from g^*. Therefore we can determine a_1^*, having at most one nonzero component and such that $a_1^* + b^* = g^*$. This representation is unique, since b^* determines a_1^* uniquely and a representation with $b_1^* \neq b^*$ would imply $g = a_2 + b_1$, $b_1 \neq b$, which is impossible.

3. **Groups having prescribed partitions**.

Denote by $G(q)$ the additive group of $GF(q)$.

LEMMA 1. *If a finite abelian group G has a partition*

$$G = G_1 \cup G_2 \cup \cdots \cup G_n \tag{12}$$

then G is isomorphic to $G^r(p)$ for some r and G_i $(i = 1, 2, \ldots, n)$ is isomorphic to $G^{\alpha_i}(p)$ for some α_i. Moreover,

https://doi.org/10.4153/CMB-1972-038-x Published online by Cambridge University Press

$$p^r = 1+\sum_{i=1}^{n}(p^{\alpha_i}-1). \tag{13}$$

REMARK 1. If for certain μ, $0\le\mu\le n$, $\alpha_i=1$ for all i satisfying $\mu<i\le n$ then condition (13) becomes

$$n-\mu = \frac{p^r-1}{p-1}+\frac{\mu-\sum_{i=1}^{\mu}p^{\alpha_i}}{p-1}. \tag{14}$$

Proof of Lemma 1. By a known lemma [7] every element of G must be of order p. This proves the first part of the lemma. Counting the number of elements in the left-hand part and right-hand part of (12), we get (13).

In the next lemmas we will establish various sufficient conditions for the existence of a partition (12) for n, r and μ satisfying the necessary condition (13) or (14). Lemma 2 is known and leads to the partition (9), which corresponds to the case where all the α_i's in (13) have the same value $\alpha\ge 1$.

LEMMA 2. *If for some n and r*

$$(q^r-1)/(q-1) = n \tag{15}$$

then the group $G^r(q)$ has a partition

$$G^r(q) = G_1\cup G_2\cup\cdots\cup G_n \tag{16}$$

with

$$G_i \simeq G(q). \tag{17}$$

Proof. Let $\sigma=f_0, f_1, f_2, \ldots, f_{q-1}$ be the elements of $GF(q)$ and let g be a fixed nonzero element of $G^r(q)$. Then the set $S_g=\{gf_i\}_{i=0}^{q-1}$ is a subgroup of $G^r(q)$ isomorphic to $G(q)$. Moreover the sets S_g and $S_{g'}$ either consist of the same elements or have only the zero in common. This and (15) imply (16) and (17).

LEMMA 3. *If for some n, μ and $r=\sum_{i=1}\beta_i$*

$$n-\mu = \left(q^r-\sum_{i=1}^{\mu}q^{\beta_i}+\mu-1)\right)\Big/q-1) \tag{18}$$

then $G^r(q)$ has the partition

$$G^r(q) = G_1\cup G_2\cup\cdots\cup G_n \tag{19}$$

with

$$\begin{aligned} G_i &= G(q^{\beta_i}) \quad \text{for } i = 1, 2, \ldots, \mu \\ G_i &\simeq G(q) \quad \text{for } i = \mu+1, \mu+2, \ldots, n. \end{aligned} \tag{20}$$

Proof. Let G_j $(j=1, 2, \ldots, \mu)$ be the subgroups of $G^r(q)$ consisting of elements with only the $\nu+\sum_{i=1}^{j}\beta_{i-1}$ components, where $\beta_0=0$ and ν runs over the numbers $1, 2, \ldots, \beta_j$, possibly different from zero. Then $G_j\simeq G(q^{\beta_j})$ and these subgroups

https://doi.org/10.4153/CMB-1972-038-x Published online by Cambridge University Press

have pairwise only the zero in common. The number of elements of $G^r(q)$ not members in $G_1 \cup \cdots \cup G_\mu$ is $q^r - \sum_{i=1}^{\mu} q^{p_i} + \mu - 1$ and they can be partitioned, by (18) and by an argument similar to that used in proving Lemma 2, into $n-\mu$ subgroups, of q elements each.

A useful particularization of Lemma 3 is obtained by taking all β_i's but β_1 equal to 1. This gives:

LEMMA 3*. *If for some n, r and β*

$$n-1 = \frac{q^r - q^\beta}{q-1}$$

then $G^r(q)$ has the partition

$$G(q) = G_1 \cup \cdots \cup G_n$$

with $G_1 \simeq G(q^\beta)$ and $G_i \simeq G(q)$ for $i=2, 3, \ldots, n$.

LEMMA 4. *Denote* max $\alpha_i = \alpha$. *If for some n, μ and $r \geq k\alpha$*

$$n-\mu = \left(q^r - \sum_{i=1}^{\mu} q^{\alpha_i} + \mu - 1\right) \Big/ (q-1) \tag{21}$$

and

$$(q^{\alpha k} - 1)/(q^\alpha - 1) \geq \mu$$

then the group $G^r(q)$ has the partition:

$$G^r(q) = G_1 \cup \cdots \cup G_n \tag{22}$$

with

$$\begin{aligned} G_i &\simeq G(q^{\alpha_i}), \quad i = 1, 2, \ldots, \mu \\ G_i &\simeq G(q), \quad\ \ i = \mu+1, \mu+2, \ldots, n. \end{aligned}$$

Proof. Let $r = k\alpha + \beta$, $\beta \geq 0$, $(q^{k\alpha}-1)/(q^\alpha - 1) = \mu + v$, $v \geq 0$. By Lemma 3* $G^r(q)$ has the partition

$$G^r(q) = H_1 \cup \cdots \cup H_m$$

with $H_1 \simeq G(q^{k\alpha})$, $H_i \simeq G(q)$, $i = 2, 3, \ldots m$, and $m-1 = q^{k\alpha}(q^\beta - 1)/(q-1)$. Since $H_1 \simeq G(q^{k\alpha}) \simeq G^k(q^\alpha)$, H_1 has by Lemma 2 the partition

$$H_1 = D_1 \cup D_2 \cup \cdots \cup D_{\mu+v}$$

with $D_i \simeq G(q^\alpha)$, $i = 1, 2, \ldots, \mu+v$. For each $i = 1, 2, \ldots, n$, D_i has by Lemma 3* a partition

$$D_\mu = F_{i1} \cup \cdots \cup F_{in_i} \tag{23}$$

with $F_{i\nu} \simeq G(q^{\alpha_i})$ and $F_{in} \simeq G(q)$ for $\nu > 1$, while for $i > \mu$, D_i has by Lemma 2 a partition (23) with $F_{i\nu} = G(q)$ for every ν. Moreover, for each $i \leq \mu$,

$$n_i = \frac{q^\alpha - q^{\alpha_i}}{q-1} + 1,$$

https://doi.org/10.4153/CMB-1972-038-x Published online by Cambridge University Press

whereas $n_i=(q^\alpha-1)/(q-1)$ if $i>\mu$. In order to conclude the proof of the lemma set $G_i=F_{i1}$, $i=1, 2, \ldots, \mu$, and for $i>\mu$ let G_i run over all other subgroups, each of order g, of the above successive partitions. Counting all members of the partition we get the number m given by (21). This completes the proof.

4. **Perfect coverings.** We return now to problem (ii). First we will establish a necessary condition for the existence of perfect coverings.

LEMMA 5. *For the existence of a perfect covering of* (1) *it is necessary that*

$$\prod_{i=1}^{\mu} m_i \Big/ \left(1-n+\sum_{i=1}^{n} m_i\right) = \text{integer}. \tag{24}$$

Proof. The number of vectors covered by a given vector is $1-n+\sum_{i=1}^{n} m_i$. The total number of vectors of (1) being $\prod_{i=1}^{n} m_i$, left side part of (24) must be an integer.

We will use the following particularization of Lemma 5.

LEMMA 5*. *Let $m_i=q^{\alpha_i}$. For the existence of a perfect covering of* (1) *in this case it is necessary that for some r:*

$$1-n+\sum_{i=1}^{n} q^{\alpha_i} = q^r. \tag{25}$$

REMARK 2. If for some μ, $\alpha_i=1$ for all $i>\mu$, then (25) becomes

$$n-\mu = \frac{q^r-1}{q-1}+\frac{\mu-\sum_{i=1}^{\mu} q^{\alpha_i}}{q-1}. \tag{26}$$

This generalizes the necessity of (3).

The first sufficient condition is given in the following:

LEMMA 6. *If a group $G^{(n)}=G_1\times G_2\times\cdots\times G_n$ has an one-factorization and S_i $(i=1, 2, \ldots, n)$ are sets with $|S_i|=|G_i|$ then (1) has a perfect covering.*

Proof. If $\mathscr{A}+\mathscr{B}$ is the assumed one-factorization of $G^{(n)}$ then $\mathscr{B}$ is clearly a perfect covering of $G^{(n)}$. Let $S_i\leftrightarrow G_i$ be any 1–1 correspondence between the elements of S_i and G_i. Then the elements of $S^{(n)}$ corresponding to $\mathscr{B}$ form the required covering.

Taking into consideration also the results of §3 we can formulate now the results of this section as follows:

THEOREM 2. *For the existence of a perfect covering of the set $S^{(n)}=S_1\times S_2\times\cdots\times S_n$, with $|S_i|=q^{\alpha_i}$, $\max\alpha_i=\alpha$, $\alpha_i=1$ for $i>\mu$ it is necessary that for some r*

$$n-\mu = \frac{q^r-1}{q-1}+\frac{\mu-\sum_{i-1}^{\mu} q^{\alpha_i}}{q-1} \tag{27}$$

and it is sufficient that (27) *and one of the following conditions hold*:

(28) $$\alpha_i = \alpha, \quad i = 1, 2, \ldots, n$$

(29) $$\sum_{i=1}^{\mu} \alpha_i = r$$

(30) $$r \geq k\alpha, \quad \text{where } (q^{k\alpha}-1)/(q^{\alpha}-1) \geq \mu.$$

Proof. The necessity of (27) follows from Lemma 5*, Remark 2. For the sufficiency, supposing (28), (29), or (30) the conditions of Lemmas 2, 3, or 4 are respectively satisfied. Therefore the existence of partitions (16), (19), or (22) follows. This implies, by Theorem 1, the existence of an one-factorization of $G^{(r)}$ which by Lemma 6 leads to the required covering.

5. **Bounds.** Restricting our attention to coverings M of sets (1) with $m_i = q^{\alpha_i}$ we can state now

PROPOSITION 1. *If (27) and one of (28), (29), or (30) are satisfied, then*

(31) $$\sigma(n; q^{\alpha_1}, \ldots, q^{\alpha_n}) = q^{\sum_{i=1}^{n} \alpha_i - r}.$$

Proof. (31) is a consequence of (25), of the fact that $|M|$ is the right side part of (24) and of the existence of a perfect covering, by Theorem 2.

PROPOSITION 2. *Under the assumptions of Proposition 1 and if $S_i = G(q^{\alpha_i})$, then*

$$\hat{\sigma}(n; q^{\alpha_1}, \ldots, q^{\alpha_n}) = \sigma(n, q^{\alpha_1}, \ldots, q^{\alpha_n}) = q^{\sum_{i=1}^{n} \alpha_1 - r}.$$

Proof. By Theorem 1 the one-factorizations used in order to construct the coverings of Theorem 2 are linear coverings.

PROPOSITION 3. *Under the assumptions of Proposition 1, if $S_i = G_i$ are groups, and if for some i, G_i is not isomorphic to $G(q^{\alpha_i})$ a perfect covering of $S^{(n)}$ cannot be a subgroup, consequently*

$$\hat{\sigma}(n; q^{\alpha_1}, \ldots, q^{\alpha_n}) > q^{\sum_{i=1}^{n} \alpha_i - r}.$$

Proof. By a well-known property of perfect coverings containing the zero vector, every nonzero member of the covering has at least three nonzero components—and the vectors having two nonzero components are covered by vectors with three components.

Let G_ν be nonisomorphic to $G(q^{\alpha_\nu})$ then there exists $x \in G_\nu$ the order of x being mp, $m > 1$. Let $y \in G_\mu$, $\mu \neq \nu$, y of order p. The vector $(0, \ldots, x, \ldots, y, \ldots, 0)$ having the only nonzero components in the νth and μth position is covered by a vector $(0, \ldots, x, \ldots, y, \ldots, z, \ldots, 0)$.

If the covering would be a subgroup it should contain the vector

$$(0, \ldots, px, \ldots, py, \ldots, pz)$$

having at most two nonzero components. This contradicts the mentioned property. A similar argument has been used in [7] in order to prove (6).

6. **Final remarks**. Unfortunately the methods of this paper do not permit to decide whether a perfect covering of $S^{(n)}$ exists if $|S^n|$ is not a power of a prime.

The topic of this paper is strongly related to single error-correcting codes [8]. However, this point of view will be emphasized elsewhere.

REFERENCES

1. O. Taussky and Y. Todd, *Covering theorems for groups*, Ann. Polon. Math. **21** (1949), 303–308.
2. J. G. Kalbfleisch and R. G. Stanton, *A combinatorial problem in matching*, J. London Math. Soc. **44** (1969), 60–64.
3. S. K. Zaremba, *Covering problems concerning Abelian Groups*, J. London Math. Soc. **27** (1952), 242–246.
4. G. Losey, *Note on a theorem of Zaremba*, J. Comb. Theory, **6** (1969), 208–209.
5. S. K. Zaremba, *A covering theorem for Abelian groups*, J. London Math. Soc. **26** (1950), 71–72.
6. A. D. Sands, *Factorizations of cyclic groups*, Proc. Coll. on Abelian Groups, Akademiai Kiado Budapest (1964), 139–146.
7. R. Baer, *Partitionen endlicher Gruppen*, Math. Z. **75** (1961), 337.
8. B. Lindström, *On group and nongroup perfect codes in q symbols*, Math. Scand. **25** (1969), 145–158.

TEL-AVIV UNIVERSITY,
TEL-AVIV, ISRAEL