Europ. J. Combinatorics (1986) 7, 11-25

Partitions of Finite Abelian Groups

OLOF HEDEN

1. INTRODUCTION

A collection of subgroups $G_1, G_2, \ldots, G_n$ of a group G constitute a partition of G if every non-zero element of G is in one and only one of the groups $G_1, G_2, \ldots, G_n$. We shall give conditions on the existence of partitions that consist of n_i groups of order q_i $i=1,2,\ldots,k$ and where $q_1<q_2<\cdots<q_k$. We shall always assume that G is a finite abelian group.

If a finite abelian group G has a nontrivial partition then G is elementary abelian of type $(p, p, \ldots, p)$ p a prime, see e.g. [7]. $q_1, q_2, \ldots, q_k$ and the number of elements in G are powers of the same prime p. If $k=2$, $q_1=p^{n'}$, $q_2=p^n$, $n>n'$, $d=\text{g.c.d.}(n, n')$ and if the order of the group G is p^{2n} then it is easy to prove that

$$n_1=s(p^n-1)/(p^d-1), \qquad n_2=p^n+1-s(p^{n'}-1)/(p^d-1). \tag{1}$$

for some integer s, see Proposition 7 in Section 3. We shall show, Theorem 2 in Section 3, that if $p=2$ and $d=1$ then this condition also is sufficient, i.e. to each integer s with $0\leqslant s\leqslant(2^n+1)/(2^{n'}-1)$ there is a partition that satisfies (1). Probably, condition (1) is sufficient for every p and d. In Theorem 1 in Section 3 we shall show that for arbitrary p, n and n' $(n>n')$ there is to every integer s with $0\leqslant s\leqslant m$, m as in Lemma 4 in section 3, a partition which satisfies (1).

In Section 4 we shall show, using a result for mixed perfect codes, that the following condition

$$n_1\geqslant(q_2-1)/(q_1-1) \tag{2}$$

is necessary. A well-known necessary condition is

$$n_1(q_1-1)+n_2(q_2-1)+\cdots+n_k(q_k-1)=q-1, \tag{3}$$

where q denotes the number of elements in G. We shall show in Section 5 that this condition together with the condition (2) is sufficient if $G=\text{GF}(8)\times\text{GF}(2^n)$, $n\geqslant 6$; $GF(q)$ is the Galois field with q elements, and the partition contains one group of order 2^n. However, there is one exception, no partition contains 5 groups of order 2, 3 groups of order 4, 2^n-2 groups of order 8 and one group of order 2^n.

Other results on the existence of partitions of finite Abelian groups are to be found in [1], [4] and [6].

2. PRELIMINARIES

If the groups $G_1, G_2, \ldots, G_n$ constitute a partition of G then each non-zero element of G is in precisely one of the groups $G_1, G_2, \ldots, G_n$. Hence

$$\sum_{i=1}^{n}(|G_i|-1)=|G|-1,$$

where $|G_i|$ denotes the number of elements of G_i. This necessary condition for existence of partitions we shall call the *packing condition.*

0195-6698/86/010011+15 $02.00/0

If a finite abelian group G has a nontrivial partition then G is an elementary abelian group of type $(p, p, \ldots, p)$, see [7]. One consequence of this is the following proposition which we frequently will use.

PROPOSITION 1. *Suppose that G and G' are elementary abelian groups of the same type $(p, p, \ldots, p)$ and suppose that $|G| = |G'|$. If G has a partition containing the groups $G_1, G_2, \ldots, G_n$ then G' has a partition containing groups $G'_1, G'_2, \ldots, G'_n$ where $|G_i| = |G'_i|$ $i = 1, 2, \ldots, n$.*

PROOF. According to our assumptions on G and G' there is an isomorphism $\varphi: G \to G'$. Put $G'_i = \varphi(G_i)$ for $i = 1, 2, \ldots, n$. Since φ is an isomorphism we deduce that the groups $G'_1, G'_2, \ldots, G'_n$ constitute a partition of G'.

The finite field with p^n elements we shall denote by $\mathrm{GF}(p^n)$. The additive group of $\mathrm{GF}(p^n)$ is elementary abelian of type $(p, p, \ldots, p)$. By a partition of $\mathrm{GF}(p^n)$ we shall always mean a partition of the additive group of $\mathrm{GF}(p^n)$.

By $H \times K$ we denote the set $\{(h, k) \mid h \in H, k \in K\}$. If H and K are additive groups we denote by $\{0\} \times K$ the set $\{(0, k) \mid k \in K\}$.

Let H and K be two elementary abelian groups of type $(p, p, \ldots, p)$ and suppose that $|K| = p^n$. We shall often construct partitions of $H \times K$ by using partitions of $H \times \mathrm{GF}(p^n)$ and Proposition 1. If the additive groups $H \times \{0\}$ and $\{0\} \times \mathrm{GF}(p^n)$ are included in the partition of $H \times \mathrm{GF}(p^n)$ then $H \times \{0\}$ and $\{0\} \times K$ are included in the partition of $H \times K$ that you get from Proposition 1.

Consider $S = S_1 \times S_2 \times \cdots \times S_n$ where $S_1, S_2, \ldots, S_n$ are finite nonempty sets. In each of the sets $S_1, S_2, \ldots, S_n$ one element is denoted by 0. The function

$$d(\bar{s}, \bar{t}) = |\{i \mid s_i \neq t_i, i = 1, 2, \ldots, n\}|, \qquad \bar{s} = (s_1, \ldots, s_n) \in S, \quad \bar{t} = (t_1, \ldots, t_n) \in S,$$

defines a metric in S. $d(\bar{s}, \bar{t})$ is usually called the *Hamming distance* between $\bar{s}$ and $\bar{t}$. A subset C of S is a *perfect e-code* if to every $\bar{s} \in S$ there is a unique $\bar{c} \in C$ with $d(\bar{s}, \bar{c}) \leq e$. The elements of C are called *codewords*. If not all the sets $S_1, S_2, \ldots, S_n$ have the same number of elements the code may be called a *mixed perfect code*. The subset

$$S_e(\bar{0}) = \{\bar{s} \in S \mid d(\bar{s}, \bar{0}) \leq e\}, \qquad \bar{0} = (0, 0, \ldots, 0) \in S,$$

is called a *e-sphere* with centre $\bar{0}$. If C is a perfect e-code then the minimum distance betwen codewords is $2e + 1$.

PROPOSITION 2. *If a finite abelian group G has a partition consisting of the groups $G_1, G_2, \ldots, G_n$ then there is a perfect 1-code in $G_1 \times G_2 \times \cdots \times G_n$.*

PROOF. See Theorem 1 in [4].

Suppose that the number of elements in n_i of the sets $S_1, S_2, \ldots, S_n$ are q_i, $i = 1, 2, \ldots, m$. We also suppose that $q_1 < q_2 < \cdots < q_m$ and that $n_1 + n_2 + \cdots + n_m = n$. With the *weight* of an element $\bar{s}$ in S we mean a m-tuple $(d_1, d_2, \ldots, d_m)$ where d_i is the number of non-zero coordinates of $\bar{s}$ belonging to sets of cardinality q_i.

EXAMPLE 1. Let $S = S_1 \times S_2 \times \cdots \times S_5$ where $|S_1| = 4$ and $|S_i| = 2$ for $i \neq 1$. The element $(a_1, a_2, a_3, a_4, 0)$ where $a_i \neq 0$ $i = 1, 2, 3, 4$ has the weight $(3, 1)$.

The *weight enumerator* of a code is defined to be the polynomial

$$C(Z_1, \ldots, Z_m) = \sum Z_1^{d_1} \cdot \ldots \cdot Z_m^{d_m}, \tag{3'}$$

where we sum over all the codewords $\bar{c}$ and where $(d_1, \ldots, d_m)$ is the weight of $\bar{c}$.

EXAMPLE 2. Let S be as in Example 1. If C consists of the words $(a_1, a_2, a_3, 0, 0)$, $(0, a_2, a_3, a_4, 0)$ and $(0, 0, a_3, a_4, a_5)$, where $a_i \neq 0$ $i = 1, 2, \ldots, 5$, then the weight enumerator of C is $Z_1^2 Z_2 + 2Z_1^3$.

In [3] we proved that if C is a perfect code then

$$C(Z_1, \ldots, Z_m) = A_{\bar{0}} \prod_1^m (1 + (q_i - 1)Z_i)^{n_i} + \sum A_{\bar{x}} \prod_1^m (1 + (q_1 - 1)Z_i)^{n_i - x_i}(1 - Z_i)^{x_i} \tag{4}$$

for some numbers $A_{\bar{0}}$ and $A_{\bar{x}}$ and where we sum over those $\bar{x} = (x_1, \ldots, x_m)$ which satisfy a certain equation. If the perfect code is a perfect 1-code then this equation is

$$1 + \sum_{i=1}^m [(n_i - x_i)(q_i - 1) - x_i] = 0, \qquad x_i \text{ integer}, \qquad 0 \leq x_i \leq n_i, \quad i = 1, 2, \ldots, m. \tag{5}$$

Since

$$|S_1(\bar{0})| = 1 + \sum_{i=1}^m n_i(q_i - 1),$$

equation (5) can be written

$$\sum_{i=1}^m x_i q_i = |S_1(\bar{0})|, \qquad x_i \text{ integer}, \quad 0 \leq x_i \leq n_i, \quad i = 1, 2, \ldots, m. \tag{5'}$$

Let P be a subset $\{i_1, \ldots, i_p\}$ of $\{1, 2, \ldots, m\}$. To each m-tuple $\bar{y} = (y_1, \ldots, y_m)$ we denote by $\bar{y}_P$ the p-tuple $(y_{i_1}, \ldots, y_{i_p})$. The *weight enumerator according to P* of a code we define to be

$$C_P(Z_1, \ldots, Z_m) = C(Z_{i_1}, \ldots, Z_{i_p}) = \sum Z_{i_1}^{d_{i_1}} \ldots Z_{i_p}^{d_{i_p}} \tag{6}$$

where we sum over all words in the code of weight $(d_1, \ldots, d_m)$ where $d_j = 0$ if $j \notin P$.

EXAMPLE 3. Let S and C be as in Example 2 and let $P = \{1\}$. Then

$$C_P(Z_1, Z_2) = 2Z_1^3$$

PROPOSITION 3. *$C_P(1, 1, \ldots, 1)$ is the number of words in C with $d_j = 0$ if $j \notin P$.*

PROOF. If we substitute Z_{i_v} by 1, $v = 1, 2, \ldots, p$, then each term in the sum (6) will equal 1.

PROPOSITION 4. *If C is a perfect 1-code then the weight enumerator according to the subset $P = \{i_1, \ldots, p_p\}$ of $\{1, 2, \ldots, m\}$ can be written*

$$C_p(Z_1, \ldots, Z_m) = A_{\bar{0}} \prod_{v=1}^p (1 + (q_{i_v} - 1)Z_{i_v})^{n_{i_v}} + \sum A_{\bar{x}} \prod_{v=1}^p (1 + (q_{i_v} - 1)Z_{i_v})^{n_{i_v} - x_{i_v}}(1 - Z_{i_v})^{x_{i_v}} \tag{7}$$

where we sum over those $\bar{x} = (x_{i_1}, \ldots, x_{i_p})$ for which $\bar{x} = \bar{y}_P$ for some $\bar{y}$ that satisfies (5).

PROOF. If we substitute $Z_i = 0$ if $i \notin P$ in the equation (3) for $C(Z_1, \ldots, Z_m)$ we get (6). If we perform the same substitution in (4) we get (7).

PROPOSITION 5. *If there is a perfect* 1*-code in S then there are at least m distinct m-tuples* $(x_1, \ldots, x_m)$ *that satisfy* (5).

PROOF. See Theorem 1 in [3].

The following proposition can be proved in the same was as Theorem 1 in [3].

PROPOSITION 6. *Suppose that P is a subset of* $\{1, 2, \ldots, m\}$ *and that the number of elements in P is p. If there is a perfect* 1*-code in S then there are at least p distinct p-tuples* $\bar{x} = (x_{i_1}, \ldots, x_{i_p})$ *with* $\bar{x} \neq \bar{0}$ *for which* $\bar{x} = \bar{y}_P$ *for some m-tuple y satisfying* (5).

EXAMPLE 4. There will not be a perfect 1-code in $S_1 \times \cdots \times S_{39}$ where $|S_1| = |S_2| = |S_3| = 2$, $|S_i| = 8$ if $i = 4, 5, \ldots, 39$. In this case Equation (5′) will be

$$2x_1 + 8x_2 = 256, \qquad x_1 \text{ and } x_2 \text{ integers}, \quad 0 \leq x_1 \leq 3, \quad 0 \leq x_2 \leq 36.$$

The only solution of this equation is $x_1 = 0$, $x_2 = 32$. Thus by Proposition 5 or 6 and Proposition 2 GF(256) will not have a partition consisting of 3 groups of order 2 and 36 groups of order 8. This has also been proved by Bu [1]. He used a different method.

3. CONSTRUCTIONS

PROPOSITION 7. *Suppose that G is a group of order* p^{m+n}, $m \geq n$ *and p a prime. If G has a partition which consists of one group of order* p^m, $p^m - x$ *groups of order* p^n *and y groups of order* $p^{n'}$ *where* $n > n'$ *then, with* $d = \text{g.c.d.}(n', n)$,

$$x = s(p^{n'} - 1)/(p^d - 1) \quad \text{and} \quad y = s(p^n - 1)/(p^d - 1),$$

for some integers s with $0 \leq s \leq p^m(p^d - 1)/(p^{n'} - 1)$.

PROOF. From the packing condition we deduce that

$$x(p^n - 1) = y(p^{n'} - 1).$$

Since $\text{g.c.d.}(p^n - 1, p^{n'} - 1) = p^d - 1$, see, for example, the proof of 4.10 in [8], $(p^n - 1)/(p^d - 1)$ divides y.

In this section we shall give values of s of which the necessary condition of the proposition is sufficient.

We say that a group is *K′-stable* if G is a subgroup of the additive group of a field K, K' a subfield of K and $kg \in G$ for each $k \in K'$ and $g \in G$.

LEMMA 1. *Let K be a finite field. Suppose that* $G_1, G_2, \ldots, G_k$ *are K-stable subgroups of a K-stable group G and that* $|G_i| = |K|$ *for* $i = 1, 2, \ldots, k$, $G_i \cap G_j = \{0\}$ *if* $i \neq j$. *If K′ is a subfield of K and H a K′-stable subgroup of G satisfying*

$$H \subset G_1 \cup \cdots \cup G_k \quad \text{and} \quad |H \cap G_i| = |K'|, \quad i = 1, 2, \ldots, k$$

then there are K′-stable subgroups $H = H_0, H_1, \ldots, H_l$ *of G satisfying* $|H_i| = |H|$ $i = 0, 1, \ldots, l \bigcup_{i=0}^{l} H_i = \bigcup_{j=1}^{k} G_j$ *and* $H_i \cap H_j = \{0\}$ *if* $i \neq j$ $l = (|K| - 1)/(|K'| - 1) - 1$.

PROOF. Let $\beta_0, \beta_1, \ldots, \beta_l$ be a system of coset representatives of the multiplicative group K'^* of K' in the multiplicative group K^* of K. We put $H_i = \{\beta_i h \mid h \in H\}$ $i = 0, 1, \ldots, l$. Since G is K-stable the groups $H_0, H_1, \ldots, H_l$ are in G. We first show that the union of the groups H_i $i = 0, 1, \ldots, l$ equals the union of the groups G_i $i = 1, 2, \ldots, k$.

The groups $G_1, G_2, \ldots, G_k$ are K-stable and thus K'-stable. Consequently this is also true for $H \cap G_i$ $i = 1, 2, \ldots, k$. As $|H \cap G_i| = |K'|$ there is to each i $i = 1, 2, \ldots, k$ an $\alpha_i \in G_i$ with $H \cap G_i = \{k\alpha_i \mid k \in K'\}$. Since G_i is K-stable we deduce that $\beta_j k\alpha_i \in G_i$ for each $j = 0, 1, \ldots, l$ and $k \in K'$. Consider two elements $x = \beta_\mu k\alpha_i$ and $x' = \beta_\nu k'\alpha_i$ where, to avoid trivialities, we assume that k and k' are non-zero elements of K'. As $\beta_0, \beta_1, \ldots, \beta_l$ is a system of coset representatives of K'^* in K^* we conclude that if $\nu \neq \mu$ then $x \neq x'$. Consequently

$$|\{\beta_\mu k\alpha_i \mid k \in K' \mu = 0, 1, \ldots, l\}| = (l+1)(|K'| - 1) + 1 = |K|$$

and thus, since $|G_i| = |K|$, G_i consists precisely of the elements $\beta_j k\alpha_i$, $k \in K'$, and $j = 0, 1, \ldots, l$. Hence the groups G_i, $i = 1, 2, \ldots, k$, are subsets of the union of the groups $H_0, H_1, \ldots, H_l$. Consequently the union of the groups $G_1, G_2, \ldots, G_k$ is a subset of the union of $H_0, H_1, \ldots, H_l$. On the other hand, as the groups $G_1, G_2, \ldots, G_k$ are K-stable, each of the groups $H_0, H_1, \ldots, H_l$ is a subset of the union of the groups $G_1, G_2, \ldots, G_k$. Hence this is also true for the union of $H_0, H_1, \ldots, H_l$.

It remains to prove that $H_i \cap H_j = \{0\}$ if $i \neq j$. Suppose that $x \in H_i \cap H_j$ where $i \neq j$. Then $x = \beta_i k\alpha_\nu = \beta_j k'\alpha_\mu$ where β_i, β_j, k, k', α_ν and α_μ are as above. We consider two cases. *Case 1:* $\nu \neq \mu$. Then $x \in G_\nu \cap G_\mu$, i.e. $x = 0$. *Case 2:* $\nu = \mu$. Since β_i and β_j are distinct coset representatives we deduce that $k = k' = 0$. Consequently $x = 0$.

Let $G = K \times K$ where K is a finite field. It is easy to check that the sets $K_\alpha = \{(k, \alpha k) \mid k \in K\}$, $\alpha \in K$, are subgroups of $K \times K$ which together with the group $\{0\} \times K$ constitute a partition of $K \times K$. We denote this partition by π_K.

Suppose that K' is a subfield of K and that K is a finite field. The group of automorphisms of K over K' is cyclic, see [5, p. 185] Let σ denote an element that generates this group. To each K'-stable subgroup H of K we define a K'-stable subgroup H^σ of $G = K \times K$ by

$$H^\sigma = \{(x, \sigma(x)) \mid x \in H\}.$$

Lemma 2. *If $G' \in \Pi_K$ then either $G' \cap H^\sigma = \{0\}$ or $|G' \cap H^\sigma| = |K'|$.*

Proof. Supppose that $(x, \sigma(x))$ and $(y, \sigma(y))$ with $x \neq 0$ and $y \neq 0$ are in the same group K_α of the partition Π_K of G. Then

$$\frac{\sigma(x)}{x} = \frac{\sigma(y)}{y} = \alpha.$$

Hence $\sigma(x)/\sigma(y) = x/y$, i.e. $\sigma(x/y) = x/y$. Since σ generate the Galois group of K over K' we deduce that x/y belongs to the fixed field of the Galois group, i.e. $x/y \in K'$. Then $x = yk$ for some $k \in K'$. The number of elements in $K_\alpha \cap H^\sigma$ is consequently at most $|K'|$.

If $(x, \sigma(x)) \in K_\alpha$ then, since $\sigma(kx) = \sigma(k)\sigma(x) = k\sigma(x)$, $(kx, \sigma(kx)) \in K_\alpha$ for each $k \in K'$. Consequently the number of elements in $K_\alpha \cap H^\sigma$ is 1 or at least $|K'|$.

Lemma 3. *If $H_1 \cap H_2 = \{0\}$, H_1 and H_2 K'-stable, $K_\alpha \in \Pi_K$ and $|H_1^\sigma \cap K_\alpha| > 1$ then $|H_2^\sigma \cap K_\alpha| = 1$.*

Proof. According to the assumption there is $x \in H_1 \setminus \{0\}$ with $\sigma(x)/x = \alpha$. If $|H_2^\sigma \cap K_\alpha| > 1$ then there is $y \in H_2 \setminus \{0\}$ with $\sigma(y)/y = \alpha$. As in the proof of Lemma 2 we deduce that $x = ky$ for some $k \in K'$. As H_2 is K'-stable we conclude that $x \in H_2$ which gives a contradiction.

Since the additive group of every field K has K'-stable subgroups, K' a subfield of K, it is possible, by using Lemma 1 and 2, to construct partitions of $K \times K$ which consists of groups of two or more distinct orders. If we use Lemma 3 and the following lemmas we get a better result.

LEMMA 4. *Suppose that d divides both n and n', $n>n'$, and that $n=kn'+r$ where $n'\leq r<2n'$. Let*

$$m=\begin{cases} p^{n-n'}+p^{n-2n'}+\cdots+p^{n-kn'}+1, & \text{if } r\neq n', \\ (p^n-1)/(p^{n'}-1), & \text{if } r=n', \end{cases}$$

Then $\mathrm{GF}(p^n)$ *has a partition Π which consists of one group of order p^r and $m-1$* $\mathrm{GF}(p^d)$*-stable groups $H_1, H_2, \ldots, H_{m+1}$ each of order $p^{n'}$.*

PROOF. *Case 1: $r=n'$.* Then n' divides n and hence $\mathrm{GF}(p^{n'})$ is a subfield of $\mathrm{GF}(p^n)$. In the same way as in the proof of Lemma 2 in [4] we construct a partition of $\mathrm{GF}(p^n)$. $p^{n'}$ is the order of the groups in this partition. From the construction in [4] it follows that these groups are $\mathrm{GF}(p^{n'})$-stable and thereby also $\mathrm{GF}(p^d)$-stable. *Case 2: $r\neq n'$.* Consider the additive group of $\mathrm{GF}(p^n)$ as a vectorspace over $\mathrm{GF}(p^d)$. According to the paragraph after the proof of Lemma 4 in [1], this vector space has a partition Π which consists of one subvectorspace of dimension r/d over $\mathrm{GF}(p^d)$ and $m-1$ subvectorspaces of dimension n'/d over $\mathrm{GF}(p^d)$. These vectorspaces are $\mathrm{GF}(p^d)$-stable subgroups of $\mathrm{GF}(p^n)$ and contain p^r respectively $p^{n'}$ elements.

LEMMA 4'. *With the same assumptions as in Lemma 4,* $\mathrm{GF}(p^n)$ *has a partition Π' that consists of m* $\mathrm{GF}(p^d)$*-stable groups $H_1, H_2, \ldots, H_m$ each of order $p^{n'}$ and groups of order p^d.*

PROOF. If $r=n'$ this is trivial by Lemma 4. If $r\neq n'$ then $r>n'$. The vector space of dimension r/d over $\mathrm{GF}(p^d)$ in the partition Π of the proof of Lemma 4 has a partition in one $\mathrm{GF}(p^d)$-stable group H_m of order $p^{n'}$ and groups of order p^d.

THEOREM 1. *Suppose that $n=kn'+r$ where $n'<r<2n'$ and suppose that d divides both n and n'. Let m be as in Lemma 4. To each integer s with $0\leq s\leq m$* $\mathrm{GF}(p^n)\times\mathrm{GF}(p^n)$ has a partition that besides $\{0\}\times\mathrm{GF}(p^n)$ *and* $\mathrm{GF}(p^n)\times\{0\}$ *consists of $p^n-1-s(p^{n'}-1)/(p^d-1)$ groups of order p^n and $s(p^n-1)/(p^d-1)$ groups of order $p^{n'}$.*

PROOF. By Lemma 4', $\mathrm{GF}(p^n)$ has m $\mathrm{GF}(p^d)$-stable subgroups $H_1, H_2, \ldots, H_m$ with $H_i\cap H_j=\{0\}$ if $i\neq j$. Let Π_K be defined as in the paragraph before Lemma 2. By Lemma 3, the groups $H_1, H_2, \ldots, H_m$ divides the groups of Π_K in m distinct subclasses $S_1, S_2, \ldots, S_m$ which by Lemma 2 satisfies

$$H_i^\sigma\subset\bigcup_{K_\alpha\in S_i}K_\alpha,\qquad |H_i^\sigma\cap K_\alpha|=p^d,\quad K_\alpha\in S_i,\quad i=1,2,\ldots,m.$$

The number of groups in a class S_i is $(p^{n'}-1)/(p^d-1)$. The union of these groups can, according to Lemma 1, be substituted by $(p^n-1)/(p^d-1)$ groups of order $p^{n'}$ which in pair only has the zero in common. If we carry out this substitute in s of the classes $S_1, S_2, \ldots, S_m$ we get the theorem.

REMARK. If $r=0$ then n' divides n. The situation is then almost trivial. In the partition Π_K of $K\times K$, where $K=\mathrm{GF}(p^n)$, each group has a partition in $(p^n-1)/(p^{n'}-1)$ groups of order $p^{n'}$.

Examples indicate that the theorem is true for each integer s with $0\leq s\leq p^n(p^d-1)/(p^{n'}-1)$. We show that this is the case if $p=2$ and $d=1$.

THEOREM 2. *Suppose that $n = kn' + r$ where $0 < r < n'$. $\mathrm{GF}(2^n) \times \mathrm{GF}(2^n)$ has for each integer s where $0 \leq s \leq (2^n - 2^r)/(2^{n'} - 1)$ a partition that besides $\{0\} \times \mathrm{GF}(2^n)$ and $\mathrm{GF}(2^n) = \{0\}$ consists of $s(2^n - 1)$ groups of order $2^{n'}$ and $2^n - 1 - s(2^{n'} - 1)$ groups of order 2^n.*

PROOF. Let h be any element of $\mathrm{GF}(2^n)$ and let σ_h denote the map

$$\sigma_h : x \to hx + x^2$$

from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2^n)$. As σ_h is a homomorphism we conclude that for any subgroup H of the additive group of $\mathrm{GF}(2^n)$ the subset

$$H^{\sigma_h} = \{(x, \sigma_h(x)) \mid x \in H\}$$

of $\mathrm{GF}(2^n) \times \mathrm{GF}(2^n)$ is a group. Consider the partition Π_K of $\mathrm{GF}(2^n) \times \mathrm{GF}(2^n)$, defined in the paragraph following the proof of Lemma 1 in this section, and the subgroups K_α, $\alpha \in \mathrm{GF}(2^n)$, of this partition. An element $(x, \sigma_h(x))$, $x \neq 0$, of H^{σ_h} belongs to K_α if and only if $\sigma_h(x) = \alpha x$, i.e. from the definition of σ_h, $\alpha = h + x$. Further

$$H^{\sigma_h} \cap (\{0\} \times \mathrm{GF}(2^n)) = \{(0, 0)\}.$$

We conclude that

$$|H^{\sigma_h} \cap K_\alpha| = 2 \qquad \text{for} \quad \alpha \in h + (H \backslash \{0\})$$

and that

$$H^{\sigma_h} \subset \bigcup_{\alpha \in h + (H \backslash \{0\})} K_\alpha.$$

(If h happens to belong to $H \backslash \{0\}$ then $|H^{\sigma_h} \cap K_0| = 2$. Below we shall always choose h such that h does not belong to $H \backslash \{0\}$.)

Now we can use Lemma 1 to substitute all the groups K_α where $\alpha \in h + (H \backslash \{0\})$ by subgroups with the same order as H and that only have the element $(0, 0)$ in common. If we choose subgroups H of $\mathrm{GF}(2^n)$ and elements h of $\mathrm{GF}(2^n)$ in such a manner that the sets $h + (H \backslash \{0\})$ mutually are disjoint we can perform many such substitutions.

Let G denote the additive group of $\mathrm{GF}(2^n)$. As $n = kn' + r$ there are subgroups $H_1, H_2, \ldots, H_k$ of G, each of order $2^{n'}$, and a subgroup H' of G of order 2^r such that

$$G = H_1 \times H_2 \times \cdots \times H_k \times H'.$$

As distinct cosets of H_1 are disjoint we conclude that the sets

$$h + (H_1 \backslash \{0\}) h \in \{0\} \times H_2 \times \cdots \times H_k \times H'$$

are mutually disjoint. Further all elements of G except the elements of the group $\{0\} \times H_2 \times \cdots \times H_k \times H'$ belong to the union of these sets. Proceeding in the same way we consider for $i \in \{1, 2, \ldots, k\}$ the subsets

$$h + (H_i \backslash \{0\}) \text{ where } h \in \{0\} \times \cdots \times \{0\} \times H_{i+1} \cdots \times H_k \times H', \quad i \leq k$$

of G. These sets are mutually disjoint and the number of such sets equals $(2^n - 2^r)/(2^{n'} - 1)$. Hence the theorem follows from Lemma 1.

We now consider partitions of $\mathrm{GF}(p^n) \times \mathrm{GF}(p^m)$, where $m > n$, that beside the groups $\{0\} \times \mathrm{GF}(p^m)$ and $\mathrm{GF}(p^n) \times \{0\}$ contain groups of order p^n respectively $p^{n'}$, $n > n'$.

The following lemma will be of great importance in the sequel.

LEMMA 5. *Suppose that $G = H \times K$ and that the group K has a partition which consists of the groups $K_1, K_2, \ldots, K_n$. If each of the groups $H \times K_i$, $i = 1, 2, \ldots, n$, has a partition Π_i that besides $H \times \{0\}$ and $\{0\} \times K_i$ consists of groups $L_j^i, j = 1, 2, \ldots, m_i$, then* *the groups* $H\times\{0\}$, $\{0\}\times K$ *and the groups* L_j^i, $i=1,2,\dots,n$, $j=1,2,\dots,m_i$ *constitute a partition* Π *of* G.

PROOF. We show that G is the union of the groups in Π. That the intersection of two distinct groups only is the element $(0,0)$ can be proved in a similar manner.

The elements $(h,0)$ and $(0,k)$ $h\in H$, $k\in K$ are in the groups $H\times\{0\}$ and $\{0\}\times K$. If $h\neq 0$ and $k\neq 0$ then (h,k) belongs to one of the groups $H\times K_i$ and thus to one of the groups L_j^i.

THEOREM 3. *Suppose that* $t=kn+r$ *where* $k\geq 1$ *and* $n<r<2n$ *and suppose that* $n=k'n'+r'$ *where* $n'<r'<2n'$. *Let* $d=\text{g.c.d.}(n,n')$ *and put*

$$m'=p^{n-n'}+p^{n-2n'}+\cdots+p^{n-kn'}+1$$

$$m=p^{t-n}+p^{t-2n}+\cdots+p^{t-kn}+1.$$

The group $\mathrm{GF}(p^n)\times\mathrm{GF}(p^t)$ *has for each integer* s *with* $0\leq s\leq m\cdot m'$ *a partition that besides* $\{0\}\times\mathrm{GF}(p^t)$ *and* $GF(p^n)\times\{0\}$ *contains* $p^t-1-s(p^{n'}-1)/(p^d-1)$ *groups of order* p^n *and* $s(p^n-1)/(p^d-1)$ *groups of order* $p^{n'}$.

PROOF. According to Lemma 4′, $\mathrm{GF}(p^t)$ has a partition that consists of m groups $K_1,K_2,\dots,K_m$ of order p^n and one group K of order p^r. Each group $\mathrm{GF}(p^n)\times K_i$, $i=1,2,\dots,m$, has, by Theorem 1 and Proposition 1 in Section 2, for every s' with $0\leq s'\leq m'$ a partition that besides $\{0\}\times K_i$ and $\mathrm{GF}(p^n)\times\{0\}$ consists of $s'(p^n-1)/(p^d-1)$ groups of order $p^{n'}$ and $p^n-1-s'(p^{n'}-1)/(p^d-1)$ groups of order p^n. The group $\mathrm{GF}(p^n)\times K$ has a partition that consists of $\{0\}\times K$, $\mathrm{GF}(p^n)\times\{0\}$ and groups of order p^n. (We construct this partition in the same way as the partition Π_K is constructed. Let H be a subgroup of order p^n of $\mathrm{GF}(p^r)$. Put $H_\alpha=\{(h,\alpha h)\mid h\in H\}$ $\alpha\in\mathrm{GF}(p^r)$. $\{0\}\times\mathrm{GF}(p^r)$ and the groups $H_\alpha\alpha\in GF(p^r)$ constitute a portion of $H\times GF(p^r)$. Since $|H|=|\mathrm{GF}(p^n)|$ and $|\mathrm{GF}(p^r)|=|K|$ we can use Proposition 1 in Section 2.)

By Lemma 5 the theorem is proved.

If n divides t we can do even more.

THEOREM 3′. *Suppose that* $t=kn$ *where* $k\geq 2$ *and suppose that* $n=k'n'+r'$ *where* $n'<r'<2n'$. *Let* $d=\text{g.c.d.}(n,n')$ *and let* m' *be as in Theorem 3. Put*

$$m=(p^t-1)/(p^n-1).$$

The group $\mathrm{GF}(p^n)\times\mathrm{GF}(p^t)$ *has for each integer* s *with* $0\leq s\leq m\cdot m'$ *a partition that besides* $\{0\}\times\mathrm{GF}(p^t)$ *and* $\mathrm{GF}(p^n)\times\{0\}$ *contains* $p^t-1-s(p^{n'}-1)/(p^d-1)$ *groups of order* p^n *and* $s(p^n-1)/(p^d-1)$ *groups of order* $p^{n'}$.

The proof is the same as the proof of Theorem 3.

In the two theorems above we considered partitions of $\mathrm{GF}(p^n)\times\mathrm{GF}(p^t)$ where $t\geq 2n$. The next lemma can be used to construct partitions where $n<t<2n$.

LEMMA 6. *Suppose that* $G=\mathrm{GF}(p^n)\times\mathrm{GF}(p^t)$ *where* $2<n\leq t$ *and suppose that* G *has a partition* Π *that besides* $\{0\}\times\mathrm{GF}(p^t)$ *and* $\mathrm{GF}(p^n)\times\{0\}$ *consists of groups of order* p^n *and groups of order* p^{n-1}. *Let* $G'=H\times\mathrm{GF}(p^t)$ *where* H *is a subgroup of* $\mathrm{GF}(p^n)$ *of order* p^{n-1}.

The groups $G'\cap L$ $L\in\Pi$ *constitute a partition* Π' *of* G'. Π' *contains besides* $H\times\{0\}$ *and* $\{0\}\times\mathrm{GF}(p^t)$ *groups of order* p^{n-1} *and of order* p^{n-2}. *The number of groups in* Π' *of order* p^{n-2} *does not depend on the choice of the group* H'.

The construction in this lemma is the same as in Lemma 5 of [1]. The proof also will almost be the same.

PROOF. Trivially, $G' \cap (\mathrm{GF}(p^n) \times \{0\}) = H \times \{0\}$ and $G' \cap (\{0\} \times \mathrm{GF}(p^t)) = \{0\} \times \mathrm{GF}(p^t)$.

Note that if $L \in \Pi \backslash (\mathrm{GF}(p^n) \times \{0\} \cup \{0\} \times \mathrm{GF}(p^t))$ then those elements h of $\mathrm{GF}(p^n)$ for whicn there is $k_h \in \mathrm{GF}(p^t)$ with $(h, k_h) \in L$ consitute a subgroup of $\mathrm{GF}(p^n)$ with the same order as L, else L should contain an element $(0, k)$ where $k \neq 0$, which contradicts our assumption on L. We denote this subgroup of $\mathrm{GF}(p^n)$ by L_1.

$\mathrm{GF}(p^n)$ is a vectorspace over $\mathrm{GF}(p)$ of dimension n. If H is a subspace of $\mathrm{GF}(p^n)$ of dimension $n-1$ and L' another subspace of $\mathrm{GF}(p^n)$ then

$$\dim L' \cap H = \dim L' \quad \text{or} \quad \dim L' - 1.$$

By this and the observation above we conclude that Π' besides $H \times \{0\}$ and $\{0\} \times \mathrm{GF}(p^t)$ consists of groups of order p^{n-1} or p^{n-2}.

By the packing condition the number of groups in Π is uniquely determined by the number of groups in Π of order p^{n-1}. On the other hand, the number of groups of Π' of order p^{n-2} is uniquely determined by the number of groups of Π'. Since $n > 2$, Π and Π' contains the same number of groups. Now the proof of Lemma 6 is complete.

REMARK. If $n = 2$ then the situation is trivial. Every abelian group of order p^2 and type (p, p) has a partition that consists of $p+1$ groups of order p.

From Lemma 6 we can deduce results analogous to those in Theorem 1, 2 and 3. We give an example that we need in Section 5.

EXAMPLE. Let $G = \mathrm{GF}(16) \times \mathrm{GF}(16)$. By Theorem 2, G has one partition Π_1 which consists of $\mathrm{GF}(16) \times \{0\}$, $\{0\} \times \mathrm{GF}(16)$, 8 groups of order 16 and 15 groups of order 8. G has also one partition Π_2 which consists of $\mathrm{GF}(16) \times \{0\}$, $\{0\} \times \mathrm{GF}(16)$, one group of order 16 and 30 groups of order 8.

Let H be a subgroup of $\mathrm{GF}(16)$ of order 8 and put $G' = H \times \mathrm{GF}(16)$. The groups $G' \cap L$, $L \in \Pi_i$ $i = 1$ or 2 constitutes a partition Π_i' of G'. Π_i' contains besides $H \times \{0\}$ and $\{0\} \times \mathrm{GF}(16)$: 9 groups of order 8 and 14 groups of order 4, if $i = 1$; 3 groups of order 8 and 28 groups of order 4, if $i = 2$.

4. SOME NECESSARY CONDITIONS

The set of groups of least order in a partition Π of a group G we shall call the *tail* of the partition. The number of groups in the tail we shall call the *length of the tail.* In this section we show that the tail of a partition has a certain minimal length.

Suppose that the partition Π of G consists of n_i groups of order q_i, $i = 1, 2, \ldots, m$, and suppose that $q_1 < q_2 < \cdots < q_m$.

LEMMA 7. *If a finite abelian group G has a partition Π then*

$$n_1 \geq q_2 / q_1.$$

PROOF. There is a perfect 1-code in the direct product of the groups in the partition Π, Proposition 2 in Section 2. According to Proposition 6 in the same section there is at least one m-tuple $(x_1, x_2, \ldots, x_m)$ with $x_1 \neq 0$ and $0 \leq x_i \leq n_i$, $i = 1, 2, \ldots, m$, satisfying

$$x_1 q_1 + x_2 q_2 + \sum_{i=3}^{m} x_m q_m = |S_1(0)|. \tag{8}$$

Since G is a finite abelian group, $q_i = p^{t_i}$ for $i = 1, 2, \ldots, m$, where p is a prime. $|S_1(0)| = p^t$ since $|S_1(0)| = |G|$. Since $t_1 < t_2 < \cdots < t_m < t$ we deduce from Equation (8) that q_2 divides

x_1q_1. Consequently q_2/q_1 divides x_1. Since $x_1 \neq 0$ we must have $x_1 \geq q_2/q_1$ and thus $n_1 \geq q_2/q_1$.

THEOREM 4. *If a finite abelian group has a partition Π then*

$$n_1 \geq (q_2-1)/(q_1-1).$$

PROOF. Suppose that G has a partition Π with $n_1 < (q_2-1)/(q_1-1)$. In the direct product of the groups in the partition there is a perfect 1-code, Proposition 2 in Section 2. If an m-tuple $(x_1, x_2, \ldots, x_m)$ satisfies Equation (5′) in Section 2 then, by the proof of Lemma 7 q_2/q_1 divides x_1. Further, from our assumption on n_1 and by Lemma 7, we deduce that $q_2/q_1 \leq n_1 < 2q_2/q_1$. Now, by Proposition 4 in Section 2, the weight enumerator according to the subset $\{1\}$ of $\{1, 2, \ldots, m\}$ may be written

$$C(Z_1) = A(1+(q_1-1)Z_1)^{n_1} + B(1+(q_1-1)Z_1)^{n_1-x_1}(1-Z_1)^{x_1} \tag{9}$$

where $x_1 = q_2/q_1$ and where A and B are constants.

As the minimum distance between codewords is 3 and as the word $(0, 0, \ldots, 0)$ belongs to the code there are no codewords of weight $(d_1, 0, \ldots, 0)$ where $d_1 = 1$ or 2. Thus

$$C(Z_1) = 1 + \text{terms of degree} \geq 3. \tag{10}$$

If we calculate the coefficients of 1 and Z_1 in (9) and use (10) we get two equations for A and B. These equations have the solution

$$A = 1 - n_1(q_1-1)/q_2, \qquad B = n_1(q_1-1)/q_2. \tag{11}$$

By Proposition 3 in Section 2 we now get that the number of words of weight $(d_1, 0, \ldots, 0)$ in the code is

$$C(1) = (1 - n_1(q_1-1)/q_2)q_1^{n_1}. \tag{12}$$

On the other hand, since the minimum distance between codewords is 3, we can have at most $q_1^{n_1}/(1+n_1(q_1-1))$ such words. If $n_1 < (q_2-1)/(q_1-1)$ this number if according to (12) less than $C(1)$, which gives a contradiction.

The inequality in the theorem may not be improved generally. GF(p^4), i.e. has a partition that consists of p^2+1 groups H_i, $i = 1, 2, \ldots, p^2+1$, each of order p^2. H_1 has a partition consisting of $p+1$ groups L_i $i = 1, 2, \ldots, p+1$ each of order p. The groups $L_1, \ldots, L_{p+1}, H_2, \ldots, H_{p^2+1}$ constitute a partition with $n_1 = (q_2-1)/(q_1-1)$.

In [6] Lindström proved that if a partition of a finite abelian group consists of one group of order p^a and groups of order p^b then $a \geq b$. This result follows from Theorem 1 since we never have $n_1 = 1$.

We need the following result in Section 5.

THEOREM 5. *A finite abelian group G never has a partition Π with n_i groups of order 2^i, $i = 1, 2, \ldots, m$, where $n_1 = 5$ and $n_2 = 3$.*

PROOF. Suppose that G has such a partition. By Proposition 2 in Section 2, there is a perfect 1-code in the direct product of the groups in the partition. By Proposition 5 in Section 2 there is at least m m-tuples satisfying

$$2x_1 + 4x_2 + \sum_{i=3}^{m} 2^i x_i = 2^t, \qquad x_i \text{ integer}, \quad 0 \leq x_i \leq n_i, \tag{13}$$

where $|S_1(0)| = 2^t$. From this equation we deduce that $x_1 \equiv 0 \pmod 2$ and if $x_1 = 0$ then $x_2 \equiv 0 \pmod 2$. Further if $(x_1, x_2, \ldots, x_m)$ and $(x_1', x_2', \ldots, x_m')$ are two m-tuples satisfying

(13) and $x_1 = x'_1$ then $x_2 \equiv x'_2 \pmod 2$. Now the weight enumerator according to the subset $\{1, 2\}$ of $\{1, 2, \ldots, m\}$ can, by Proposition 4 in Section 2, be written

$$\begin{aligned} C(Z, U) = {} & A(1+3Z)^3(1+U)^5 + A'(1+3Z)(1-Z)^2(1+U)^5 \\ & + B(1+3Z^2)(1-Z)(1+U)^3(1-U)^2 + B'(1-Z)^3(1+U)^3(1-U)^2 \\ & + C(1+3Z)^3(1+U)(1-U)^4 + C'(1+3Z)(1-Z)^2(1+U)(1-U)^4 \end{aligned} \tag{14}$$

($Z_1 = U$ and $Z_2 = Z$) for some constants A, A', B, B', C and C'. As in the proof of Theorem 4 we get that

$$C(Z, U) = 1 + \text{terms of degree} \geqslant 3.$$

Thus the coefficients of Z, U, Z^2, U^2 and ZU in (14) are zero. If we use this we can calculate the constants $A, A', \ldots, C'$. We get that $A = 1/64$, $A' = 3/64$, $B = 12/64$, $B' = 28/64$, $C = -1/64$ and $C' = 21/64$. If we use these values of $A, A', \ldots, C'$ and calculate the coefficient of Z^2U^2 in (14) we get -6 which is impossible.

EXAMPLE. Consider GF(64) and a partition of GF(64) that consists of groups of order 2, 4 respectively 8. Let n_1, n_2 and n_3 be as above. Theorem 4 excludes the following 6 possibilities for (n_1, n_2, n_3)

$$(1, 2, 8), (2, 4, 7), (1, 9, 5), (2, 11, 4), (1, 16, 2) \text{ and } (2, 18, 1).$$

These possibilities are, however, not excluded by the packing condition. Theorem 5, but not Theorem 4 or packing condition, exclude $(n_1, n_2, n_3) = (5, 3, 7)$. For all the remaining 3-tuples (n_1, n_2, n_3) that satisfies the packing condition there is a partition as we shall see in the next section.

5. PARTITIONS OF $\mathrm{GF}(8) \times \mathrm{GF}(2^n)$ WHERE $n > 2$

THEOREM 6. *$\mathrm{GF}(8) \times \mathrm{GF}(2^n)$ $n \geqslant 6$ has a partition that besides $\mathrm{GF}(8) \times \{0\}$ and $\{0\} \times \mathrm{GF}(2^n)$ consists of n_i groups of order 2^i $i = 1, 2$ or 3 if and only if n_1, n_2 and n_3 satisfy the following two conditions*:

(a) $n_1 + 3n_2 + 7n_3 = 7 \cdot (2^n - 1)$;

(b) if $n_2 \neq 3$ then $n_1 = 0$ or $n_1 \geqslant 3$; if $n_2 = 3$ then $n_1 > 5$.

That the condition (a) is necessary follows from the packing condition, since the number of elements in the set $\mathrm{GF}(8) \times \mathrm{GF}(2^n) \setminus (\mathrm{GF}(8) \times \{0\} \cup \{0\} \times \mathrm{GF}(2^n))$ is $7 \cdot (2^n - 1)$. From the results of Section 4, as in the example of that section, it follows that condition (b) is necessary. It remains to prove that the conditions (a) and (b) are sufficient.

Let n_1, n_2 and n_3 be as in Theorem 6. We shall say that a partition Π of $H \times K$ where $|H| = 8$ and $|K| = 2^n$ $n \geqslant 3$ is of *type* P_t if

$$n_3 = 2^n - 1 - t, \qquad 0 \leqslant t \leqslant 2^n - 1,$$

$$n_2 = \begin{cases} 7t/3, & \text{if } t \equiv 0 \pmod 3, \\ 7(t-1)/3 + 1, & \text{if } t \equiv 1 \pmod 3, \end{cases}$$

$$n_2 = \begin{cases} 7(t-2)/3 + 3 & \text{if } t \equiv 2 \pmod 3,\ t \neq 2, \\ 2 & \text{if } t = 2. \end{cases}$$

LEMMA 8. *If $G = \mathrm{GF}(8) \times \mathrm{GF}(2^n)$ $n \geqslant 6$ has a partition of type P_t for $t = 0, 1, \ldots, 2^n - 1$ then for each 3-tuple (n_1, n_2, n_3) that satisfies condition (a) and (b) of Theorem 6 there is a partition of G that besides $\mathrm{GF}(8) \times \{0\}$ and $\{0\} \times \mathrm{GF}(2^n)$ consists of n_i groups of order 2^i, $i = 1, 2,$ or 3.*

PROOF. Let Π and Π' be partitions of G that contain the same number of groups of order 8. Suppose that the number of groups in Π of order 2^i, $i=1$ or 2, is n_i and that the corresponding numbers of Π' are n_i', $i=1$ or 2, and suppose that $n_2'<n_2$. Since Π and Π' contains the same number of groups of order 8

$$n_1+3n_2=n_1'+3n_2'.$$

We deduce that 3 divides $n_1'-n_1$. From Π we can construct a partition with n_2' groups of order 4 by splitting up $(n_1'-n_1)/3$ of the groups of order 4 in groups of order 2.

The partitions of type P_t are optimal in the sense that there do not exist partitions which for a given number of groups of order 8 contains more groups of order 4 than those of type P_t. This follows from the results of Section 4.

To show that conditions (a) and (b) of Theorem 1 are sufficient it is, according to Lemma 8, enough to prove the following theorem.

THEOREM 7. GF(8)×GF(2^n) $n\geq 6$ *has a partition of type* P_t *for* $t=0,1,\ldots,2^n-1$.

We shall prove this theorem by induction. However, we need a couple of lemmas.

LEMMA 9. *If* GF(8)×GF(2^n), $n\geq 3$, *has a partition of type* P_t *for* $t\equiv 0 \pmod 3$ $t\leq 2^n-2$ *then* G *has a partition of type* P_{t+1}. G *always has partitions of types* P_0, P_1 *and* P_2.

PROOF. Let Π be a partition of type P_t $t\equiv 0 \pmod 3$. If H is a group of order 8 in Π then H has a partition consisting of one group of order 4 and 4 groups of order 2. If we in Π substitute H by these groups we get a partition of type P_{t+1}.

In the same way we deduce that GF(8)×GF(2^n) always has partitions of type P_0, P_1 and P_2.

LEMMA 10. $G=$ GF(8)×GF(8) *has a partition of type* P_t *for* $t=0,1,2,\ldots,7$.

PROOF. From Theorem 2 in Section 3 and Lemma 9 above we deduce that G has a partition of type P_t for $t=0$, 1, 2, 3, 4, 6 and 7. We now construct a partition of type P_5.

Let ε denote an element of GF(8) that satisfies $\varepsilon^3+\varepsilon+1=0$. Then ε is a primitive element of GF(8), i.e. GF(8) $=\{0,\varepsilon^0,\varepsilon^1,\ldots,\varepsilon^6\}$. Put

$$H_i=\{(k,\varepsilon^i k)\,|\,k\in \mathrm{GF}(8)\},\qquad i=5 \text{ or } 6.$$

H_5, H_6, GF(8)×{0} and {0}×GF(8) constitute together with the following groups a partition of type P_5. In the enumeration below we write $\bar{i}$ instead of ε^i; only elements which are not equal to (0, 0) will be indicated:

$$\{(\bar 0,\bar 2),(\bar 1,\bar 3),(\bar 3,\bar 5)\},\quad \{(\bar 0,\bar 4),(\bar 1,\bar 5),(\bar 3,\bar 0)\},\quad \{(\bar 1,\bar 2),(\bar 2,\bar 4),(\bar 4,\bar 1)\}$$
$$\{(\bar 2,\bar 2),(\bar 3,\bar 4),(\bar 5,\bar 1)\},\quad \{(\bar 3,\bar 3),(\bar 4,\bar 5),(\bar 6,\bar 2)\},\quad \{(\bar 4,\bar 4),(\bar 5,\bar 6),(\bar 0,\bar 3)\}$$
$$\{(\bar 4,\bar 6),(\bar 5,\bar 2),(\bar 0,\bar 0)\},\quad \{(\bar 5,\bar 5),(\bar 6,\bar 0),(\bar 1,\bar 4)\},\quad \{(\bar 5,\bar 0),(\bar 6,\bar 3),(\bar 1,\bar 1)\}$$
$$\{(\bar 6,\bar 6),(\bar 0,\bar 1),(\bar 2,\bar 5)\},\quad \{(\bar 3,\bar 6)\},\quad \{(\bar 4,\bar 0)\},\quad \{(\bar 6,\bar 1)\},\quad \{(\bar 2,\bar 6)\},\quad \{(\bar 2,\bar 3)\}.$$

LEMMA 11. $G=$ GF(8)×GF(16) *has a partition of type* P_t *for* $t=0$, 1, 2, 4, 5, 6, 7, 8, 11, 12, 13, 14 *and* 15.

REMARKS. It is not known to the author of this paper if G has partitions of type P_3, P_9 and P_{10}. Probably there is a partition of type P_{10} and possibly also of type P_9.

PROOF. From the example of Section 3 and from Lemma 9 it follows that G has partitions of type P_t for $t=1, 2, 6, 7, 12$ and 13. GF(16) has a partition that consists of 5 groups of order 4. If we use this partition and apply Lemma 5 in Section 3 we get a partition of type P_{15}.

Let ε be an element of GF(16) that satisfies $\varepsilon^4+\varepsilon+1=0$. From [2] we deduce that the set $H=\{0, \varepsilon^0, \varepsilon^1, \varepsilon^2, \varepsilon^4, \varepsilon^5, \varepsilon^{10}, \varepsilon^8\}$ is a subgroup of GF(16). We shall now construct partitions of $H\times \mathrm{GF}(16)$. As H and GF(8) have the same number of elements we get, according to Proposition 1 in Section 2, from each partition of $H\times\mathrm{GF}(16)$ a partition of $\mathrm{GF}(8)\times\mathrm{GF}(16)$. Put $H_i=\{(h, \varepsilon^i h)\,|\, h\in H\}$, $i=0, 1, \ldots, 14$. Consider the following 10 subsets of $H\times\mathrm{GF}(16)$ (we write $\bar{\imath}$ instead of ε^i):

$$M_1=\{(\bar{0},\bar{9}),(\bar{1},\overline{10}),(\bar{4},\overline{13})\},\qquad M_2=\{(\bar{8},\bar{2}),(\bar{0},\overline{11}),(\bar{2},\bar{9})\},$$
$$M_3=\{(\bar{1},\overline{12}),(\bar{2},\overline{13}),(\bar{5},\bar{1})\},\qquad M_4=\{(\bar{1},\bar{7}),(\bar{2},\overline{11}),(\bar{5},\bar{8})\},$$
$$M_5=\{(\bar{2},\bar{5}),(\bar{4},\bar{7}),(\overline{10},\overline{13})\},\qquad M_6=\{(\bar{2},\bar{8}),(\bar{4},\bar{0}),(\overline{10},\bar{2})\},$$
$$M_7=\{(\bar{4},\overline{10}),(\bar{5},\overline{14}),(\bar{8},\overline{11})\},\qquad M_8=\{(\bar{5},\overline{12}),(\overline{10},\bar{4}),(\bar{0},\bar{6})\},$$
$$M_9=\{(\overline{10},\bar{6}),(\bar{8},\overline{14}),(\bar{1},\bar{8})\},\qquad M_{10}=\{(\overline{10},\bar{1}),(\bar{8},\bar{0}),(\bar{1},\bar{4})\}.$$

$G_i=M_i\cup\{(0, 0)\}$ is a subgroup of $H\times\mathrm{GF}(16)$, $i=1, 2, \ldots, 10$, and $G_i\subset H_3\cup H_6\cup H_7\cup H_9\cup H_{11}$, for $i=1, 2, \ldots, 10$. Further $G_i\cap G_j=\{(0, 0)\}$ if $i\neq j$. Every element in the set $(H_3\cup H_6\cup H_7\cup H_9\cup H_{11})\setminus\bigcup_{i=1}^{10} G_i$ constitute together with $(0, 0)$ a subgroup of $H\times\mathrm{GF}(16)$. These groups of order 2, the groups $G_1, G_2, \ldots, G_{10}$, the groups H_i for $i=0, 1, 2, 4, 5, 8, 10, 12, 13$ and 14, $H\times\{0\}$ and $\{0\}\times\mathrm{GF}(16)$ constitute a partition of $H\times\mathrm{GF}(16)$. This partition is of type P_5.

We get a partition of type P_8 in a similar way using the following 17 subsets of $H\times\mathrm{GF}(16)$.

$$N_1=\{(\bar{8},\bar{5}),(\bar{0},\overline{12}),(\bar{2},\overline{14})\},\qquad N_2=\{(\bar{5},\bar{4}),(\bar{2},\bar{5}),(\bar{1},\bar{8})\},$$
$$N_3=\{(\bar{5},\bar{1}),(\bar{2},\bar{8}),(\bar{1},\overline{10})\},\qquad N_4=\{(\bar{1},\bar{0}),(\bar{8},\bar{7}),(\overline{10},\bar{9})\},$$
$$N_5=\{(\bar{5},\overline{14}),(\bar{2},\bar{1}),(\bar{1},\bar{7})\},\qquad N_6=\{(\bar{4},\bar{0}),(\bar{1},\overline{14}),(\bar{0},\bar{3})\},$$
$$N_7=\{(\bar{1},\overline{12}),(\bar{8},\bar{2}),(\overline{10},\bar{7})\},\qquad N_8=\{(\overline{10},\bar{6}),(\bar{4},\overline{13}),(\bar{2},\bar{0})\},$$
$$N_9=\{(\bar{4},\bar{3}),(\bar{1},\bar{4}),(\bar{0},\bar{7})\},\qquad N_{10}=\{(\bar{0},\overline{14}),(\overline{10},\overline{13}),(\bar{5},\bar{2})\},$$
$$N_{11}=\{(\overline{10},\bar{4}),(\bar{4},\overline{11}),(\bar{2},\overline{13})\},\qquad N_{12}=\{(\bar{4},\overline{10}),(\bar{1},\overline{13}),(\bar{0},\bar{9})\},$$
$$N_{13}=\{(\bar{0},\bar{6}),(\overline{10},\bar{2}),(\bar{5},\bar{3})\},\qquad N_{14}=\{(\overline{10},\bar{8}),(\bar{4},\bar{7}),(\bar{2},\overline{11})\},$$
$$N_{15}=\{(\bar{0},\overline{13}),(\overline{10},\bar{1}),(\bar{5},\overline{12})\},\qquad N_{16}=\{(\bar{8},\bar{6}),(\bar{5},\overline{11}),(\bar{4},\bar{1})\},$$
$$N_{17}=\{(\bar{8},\bar{0}),(\bar{5},\bar{8}),(\bar{4},\bar{2})\}.$$

All these sets are namely subsets of 8 of the groups $H_0, H_1, \ldots, H_{14}$.

It remains to construct partitions of type P_4, P_{11} and P_{14}. Partitions of type P_{11} and P_{14} we get by completing $M_1, M_2, \ldots, M_{10}$, and $N_1, N_2, \ldots, N_{17}$, respectively, with the following 14 sets.

$$L_1=\{(\bar{0},\bar{0}),(\bar{1},\bar{2}),(\bar{4},\bar{8})\},\qquad L_2=\{(\bar{0},\bar{8}),(\bar{1},\bar{6}),(\bar{4},\overline{14})\},$$
$$L_3=\{(\bar{1},\bar{1}),(\bar{2},\overline{12}),(\bar{5},\overline{13})\},\qquad L_4=\{(\bar{1},\overline{11}),(\bar{2},\bar{2}),(\bar{5},\bar{9})\},$$
$$L_5=\{(\bar{2},\bar{3}),(\bar{4},\overline{12}),(\overline{10},\overline{10})\},\qquad L_6=\{(\bar{2},\overline{10}),(\bar{4},\bar{5}),(\overline{10},\bar{0})\},$$
$$L_7=\{(\bar{4},\bar{4}),(\bar{5},\bar{5}),(\bar{8},\bar{8})\},\qquad L_8=\{(\bar{4},\bar{9}),(\bar{5},\overline{10}),(\bar{8},\overline{13})\},$$
$$L_9=\{(\bar{5},\bar{6}),(\overline{10},\overline{11}),(\bar{0},\bar{1})\},\qquad L_{10}=\{(\bar{5},\bar{0}),(\overline{10},\bar{5}),(\bar{0},\overline{10})\},$$
$$L_{11}=\{(\overline{10},\overline{14}),(\bar{8},\overline{12}),(\bar{1},\bar{5})\},\qquad L_{12}=\{(\overline{10},\bar{3}),(\bar{8},\bar{1}),(\bar{1},\bar{9})\},$$
$$L_{13}=\{(\bar{8},\bar{9}),(\bar{0},\bar{5}),(\bar{2},\bar{6})\},\qquad L_{14}=\{(\bar{8},\bar{3}),(\bar{0},\bar{4}),(\bar{2},\bar{7})\}.$$

We leave it to the reader to construct a partition of type P_4. We shall not need such a partition in the future.

In the proofs below we shall use Lemma 5 in Section 3. To avoid repetition we shall not refer to this lemma every time it will be used.

Note that if we choose partitions of type P_{t_i} in $\mathrm{GF}(8)\times K_i$, $i=1,2,\ldots,n$, and apply Lemma 5 in Section 3 we will not always get a partition of type $P_{t_1+t_2+\cdots+t_n}$. The partition will be of type $P_{t_1+t_2+\cdots+t_n}$ if and only if at least $n-1$ of the numbers $t_1, t_2, \ldots, t_n$ are divisible by 3.

If $|K|=4$ and $|H|=8$ then $H\times K$ has a partition which besides $H\times\{0\}$ and $\{0\}\times K$ consists of 7 groups of order 4. We shall say that this partition is of type L.

LEMMA 12. *$G=\mathrm{GF}(8)\times\mathrm{GF}(64)$ has a partition of type P_t for $t=0,1,2,\ldots,63$.*

PROOF. GF(64) has a partition that consists of 9 groups $K_1, K_2, \ldots, K_9$ each of order 8. By Lemma 10, $\mathrm{GF}(8)\times K_i$ has partitions of type P_0, P_3, P_5 and P_6. If we choose partitions of type P_0, P_3 or P_6 in $\mathrm{GF}(8)\times K_i$ for $i=1,2,\ldots,9$ we get partitions of type P_t in G where $t\equiv 0 \pmod 3$ and $t\leq 54$. If we choose a partition of type P_5 in $\mathrm{GF}(8)\times K_1$ and partitions of type P_0, P_3 and P_6 in $\mathrm{GF}(8)\times K_i$ for $i=2,3,\ldots,9$ we get partitions of type P_t where $t\equiv 2 \pmod 3$ and $5\leq t\leq 53$. If we apply Lemma 9 we get partitions of type P_t for the remaining values of t where $0\leq t\leq 55$.

GF(64) has a partition that consists of one group H of order 16 and 16 groups $K_1, K_2, \ldots, K_{16}$ each of order 4. We choose a partition of type L in $\mathrm{GF}(8)\times K_i$, $i=1,2,\ldots,16$, and partitions of type P_t where $t=8$, 11, 12, 13, 14, 15 in $\mathrm{GF}(8)\times H$. From these partitions we get partitions of types P_t of G where $t=56$, 59, 60, 61, 62, 63.

From Lemma 9 we deduce that all that remains to be done is to construct a partition of type P_{57}. From Theorem 2 in Section 3 we know that GF(64) has a partition consisting of 3 groups each of order 8 and 14 groups $L_1, L_2, \ldots, L_{14}$ each of order 4. In $\mathrm{GF}(8)\times L_i$, $i=1,2,\ldots,14$, we choose partitions of type L. In $\mathrm{GF}(8)\times K_i$, $i=1,2,\ldots,14$, we choose partitions of type L. In $\mathrm{GF}(8)\times K_i$, $i=1$ and 2 we choose partitions of type P_6 and in $\mathrm{GF}(8)\times K_3$ a partition of type P_3. Applying Lemma 5 we get a partition of type P_{57}.

LEMMA 13. *$G=\mathrm{GF}(8)\times\mathrm{GF}(128)$ has partitions of type P_t for $t=0,1,2,\ldots,127$.*

PROOF. GF(128) has a partition that consists of one group K of order 16 and 16 groups $K_1, K_2, \ldots, K_{16}$ of order 8. If we choose a partition of type P_0 in $\mathrm{GF}(8)\times K$ and suitable partitions of type P_t in $\mathrm{GF}(8)\times K_i$, $i=1,2,\ldots,16$, we get, as in the proof of Lemma 12 partitions of type P_t of G for $0\leq t\leq 97$. If we choose a partition of type P_{15} in $\mathrm{GF}(8)\times K$ and partitions of $\mathrm{GF}(8)\times K_i$, $i=1,2,\ldots,16$, as above we get partitions of type P_t of G for $t=15$, 16, 18, 19, 20, 21, $\ldots$, 112.

For the remaining values of t, we choose a partition of GF(128) that consists of one group K of order 16, one group K' of order 8 and 35 groups $L_1, L_2, \ldots, L_{35}$ each of order 4. This is a partition of type P_{15} of $G'\times G''$ where $|G'|=8$ and $|G''|=16$. We choose partitions of type L in the groups $\mathrm{GF}(8)\times L_i$, $i=1,2,\ldots,35$, and partitions of $\mathrm{GF}(8)\times K$ and $\mathrm{GF}(8)\times K'$ according to the following table:

Partition of $\mathrm{GF}(8)\times K$ of type P_t where $t=$	5	6	6	6	6	7	8	12	12	12	12	13	14	15	15
Partition of $\mathrm{GF}(8)\times K'$ of type P_t where $t=$	3	3	4	5	6	6	6	3	4	5	6	6	6	6	7

We then get partitions of type P_t where $t=113$, 114, $\ldots$, 127.

LEMMA 14. *Suppose that* $n = n'+2$, $n' \geq 6$. *If* $GF(8)\times GF(2^{n'})$ *has partitions of type* P_t *for* $t = 0, 1, 2, \ldots, 2^{n'}-1$ *then* $G = GF(8)\times GF(2^n)$ *has partitions of type* P_t *for* $t = 0, 1, 2, \ldots, 2^n - 1$.

PROOF. $GF(2^n)$ has a partition that consists of one group K of order 2^{n-3} and 2^{n-3} groups K_i, $i = 1, 2, \ldots, 2^{n-3}$, of order 8. $GF(8)\times K$ has a partition of type P_0. If we choose partitions of suitable types P_t in $GF(8)\times K_i$, $i = 1, 2, \ldots, 2^{n-3}$, as in the proof of Lemma 12, we get partitions of type P_t for $t = 0, 1, 2, \ldots, 6\cdot 2^{n-3}+1$.

$GF(2^n)$ has a partition that consists of one group K' of order 2^{n-2} and 2^{n-2} groups L_i $i = 1, 2, \ldots, 2^{n-2}$ of order 4. In the groups $GF(8)\times L_i$, $i = 1, 2, \ldots, 2^{n-2}$, we choose partitions of type L. According to our assumptions, $GF(8)\times K'$ has partitions of type P_t for $t = 0, 1, 2, \ldots, 2^{n-2}-1$. By using Lemma 5 of Section 3, we get partitions of G of type P_t for $t = 3\cdot 2^{n-2}, 3\cdot 2^{n-2}+1, 3\cdot 2^{n-2}+3, 3\cdot 2^{n-2}+4, \ldots, 2^n-1$.

Finally, we have to construct a partition of type P_t where $t = 6\cdot 2^{n-3}+2$. Let K and K_i, $i = 1, 2, \ldots, 2^{n-3}$, be as above. As $n \geq 8$ K has a partition which consists of one group K'' of order 2^{n-5} and 2^{n-5} groups L_i, $i = 1, 2, \ldots, 2^{n-5}$, each of order 4. If we choose a partition of type P_0 in $GF(8)\times K''$ and partitions of type L in $GF(8)\times L_i$, $i = 1, 2, \ldots, 2^{n-5}$, we get a partition of type P_t, $t = 3\cdot 2^{n-5}$ in $GF(8)\times K$. Using this partition and suitable partitions of type P_t of the groups $GF(8)\times K_i$, $i = 1, 2, \ldots, 2^{n-3}$, we get partitions of type P_t for $3\cdot 2^{n-5}+3 \leq t \leq 3\cdot 2^{n-5}+6\cdot 2^{n-3}+1$. $6\cdot 2^{n-3}+2$ is surely in this interval.

PROOF OF THEOREM 7. According to Lemmas 12 and 13, the theorem is true if $n = 6$ and $n = 7$. By Lemma 14 and induction, the theorem is true for every $n \geq 6$.

REMARK. By lemma 2 in [6] if a finite abelian group G has a partition that consists of the groups $G_1, G_2, \ldots, G_n$ then $|G_i|\cdot|G_j| \leq |G|$ for every i and j, $i \neq j$. Consequently if $G = GF(8)\times GF(2^n)$ has a partition Π that contains one group of order 2^n then the remaining groups in the partition have orders 2, 4 or 8. Thus Theorem 6 gives a necessary and sufficient condition for existence of partitions of G that contains n_1 groups of order 2, n_2 groups of order 4, n_3+1 groups of order 8 and one group of order 2^n.

REFERENCES

1. T Bu, Partitions of a vector space, *Discrete Math.* **31** (1980), 79-83.
2. W. H. Bussey, Galois field tables for $p^n \leq 169$, *Bull. Amer. Math.* **12** (1905-1906), 22-38.
3. O. Heden, A generalised Lloyd theorem and mixed perfect codes, *Math. Scand.* **37** (1975), 13-26.
4. M. Herzog and J. Schönheim, Group partition, factorization and the vector covering problem, *Canad. Math. Bull.* **15**(2) (1972), 207-214.
5. S. Lang, *Algebra*, Addison-Wesley, 1971.
6. B. Lindström, Group partitions and mixed perfect codes, *Canad. Math. Bull.* **18**(1) (1975), 57-60.
7. G. A. Miller, Groups in which all operators are contained in a series of subgroups such that any two have only identity in common, *Bull. Amer. Math.* **12** (1905-1906), 446-449.
8. R-H. Schulz, Uber Blockpläne mit transitiver Dilatationsgruppe, *Math. Zeitschr.* **98** (1967), 60-82.

Received 22 March 1982 and in revised form 18 June 1984

OLOF HEDEN
Department of Mathematics
Royal Institute of Technology,
S-10044 Stockholm, Sweden