SOLUTION TO A PROBLEM OF A. D. SANDS

by OWEN H. FRASER and BASIL GORDON

(Received 17 October, 1977)

Let G be a finite additive abelian group, and suppose that A and B are subsets of G. We say that $G = A \oplus B$ if every element $g \in G$ can be uniquely written in the form $g = a + b$, where $a \in A$, $b \in B$. The study of such decompositions (usually called *factorizations* in the literature) was initiated by G. Hájos [3] in connection with his solution to a problem of Minkowski in the geometry of numbers.

Several problems concerning Hájos factorizations are collected in [2]. The current (1977) status of these problems is the following. Problem 77, in its original form, was solved in the negative by A. D. Sands [4]. However a revised version of the problem, in which the word "subgroup" is replaced by "periodic subset", is still open. Problem 78 was solved by Sands [5], [6]. An affirmative answer to problem 79 can be derived from the work of Sands. Problem 80 is still open. Problem 81 was solved in the negative by Sands [7]. Problem 82 was solved in the negative by the present authors [1]. Finally, problem 83 is still open.

In his paper disposing of problem 81, Sands posed still another question, viz. if $G \neq \{0\}$, and $G = A \oplus B$, where $0 \in A$, $0 \in B$, must one of the sets A, B be contained in some proper subgroup of G? The purpose of the present paper is to answer this question in the negative.

To obtain a counterexample, let G be the vector space F_p^n of all ordered n-tuples $(x_1, \ldots, x_n)$, where the x_i lie in the field $F_p = \{0, 1, \ldots, p-1\}$ of integers (mod p). As an additive group, G is the direct sum of n cyclic groups of order p. Moreover the subgroups of G are the subspaces of the vector space F_p^n.

We now recall some terminology from the theory of error-correcting codes (see for example [9]). The *Hamming distance* $d(\mathbf{u}, \mathbf{v})$ between two vectors $\mathbf{u} = (x_1, \ldots, x_n)$ and $\mathbf{v} = (y_1, \ldots, y_n)$ in F_p^n is defined to be the number of integers i such that $x_i \neq y_i$. With respect to this distance, the sphere of radius e and center $\mathbf{u} \in F_p^n$ is the set $S_e(\mathbf{u}) = \{\mathbf{v} \in F_p^n \mid d(\mathbf{u}, \mathbf{v}) \leq e\}$. A *perfect e-error-correcting code* is a set C of vectors $\mathbf{u} \in F_p^n$ such that F_p^n is the disjoint union of the spheres $S_e(\mathbf{u})$, $\mathbf{u} \in C$. In the terminology of Hájos factorizations, this amounts to the requirement that $F_p^n = C \oplus S_e(\mathbf{0})$.

The *linear* perfect error-correcting codes C (i.e. those where C is a subspace of F_p^n) have all been determined [10]. These, however, are of no use for our present purpose. Of more interest is the fact that there exist *non-linear* perfect codes. An account of them can be found, for example, in van Lint's book [9]. In his terminology, the codes we use here are actually "equivalent" to linear codes. To construct them, we first form the *Hamming codes*, which are obtained as follows.

Let $n = (p^r - 1)/(p - 1)$, and let H be an r by n matrix whose columns are all the nonzero vectors $(a_1, \ldots, a_n) \in F_p^n$ such that the first nonzero component a_i is equal to 1.

For example, if $p=5$ and $r=2$, we have $n=6$, and we can take

$$H=\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{bmatrix}.$$

Let $C=\{\mathbf{u}\in F_p^n \mid H\mathbf{u}^t=0\}$. It can be shown that C is a perfect one-error-correcting code, called a Hamming code.

For example, in the above case $p=5$, $r=2$, C consists of all vectors $\mathbf{u}=(x_1,\ldots,x_6)\in F_5^6$ such that

$$\begin{aligned} x_2+x_3+\ x_4+\ x_5+\ x_6&=0,\\ x_1+x_3+2x_4+3x_5+4x_6&=0. \end{aligned}$$

These vectors form a four-dimensional subspace C of F_5^6; a basis of C is given by the vectors $\mathbf{u}_1=(4,4,1,0,0,0)$, $\mathbf{u}_2=(3,4,0,1,0,0)$, $\mathbf{u}_3=(2,4,0,0,1,0)$, and $\mathbf{u}_4=(1,4,0,0,0,1)$.

Now if π_i $(i=1,\ldots,n)$ are permutations of the elements $\{0,1,\ldots,p-1\}$ of F_p, the map

$$\pi:(x_1,\ldots,x_n)\mapsto(\pi_1(x_1),\ldots,\pi_n(x_n))$$

of F_p^n onto itself obviously preserves the Hamming distance. Therefore the image of any perfect e-error-correcting code under this map is again a perfect e-error-correcting code.

In particular, we consider the Hamming code C with $p=5$, $r=2$ discussed above. We choose $\pi_1=\pi_2=(23)$, and let $\pi_3,\ldots,\pi_6$ be the identity maps. Then $\pi(\mathbf{0})=\mathbf{0}$, so $\mathbf{0}\in\pi(C)$. Moreover,

$$\begin{aligned} &\pi(\mathbf{u}_1)=(4,4,1,0,0,0),\ \pi(\mathbf{u}_2)=(2,4,0,1,0,0),\ \pi(\mathbf{u}_3)=(3,4,0,0,1,0),\\ &\pi(\mathbf{u}_4)=(1,4,0,0,0,1),\ \pi(\mathbf{u}_1+\mathbf{u}_2)=(3,2,1,1,0,0), \end{aligned}$$

and

$$\pi(\mathbf{u}_3+\mathbf{u}_4)=(2,2,0,0,1,1).$$

These six vectors are linearly independent, since

$$\begin{vmatrix} 4 & 4 & 1 & 0 & 0 & 0\\ 2 & 4 & 0 & 1 & 0 & 0\\ 3 & 4 & 0 & 0 & 1 & 0\\ 1 & 4 & 0 & 0 & 0 & 1\\ 3 & 2 & 1 & 1 & 0 & 0\\ 2 & 2 & 0 & 0 & 1 & 1 \end{vmatrix}\equiv 1 \pmod 5.$$

Hence $\pi(C)$ is not contained in any proper subspace of F_5^6. Moreover the sphere $S_1(\mathbf{0})$ contains $\mathbf{0}$, and it does not lie in any proper subspace of F_5^6, since it contains e_i. Since $F_5^6=\pi(C)\oplus S_1(\mathbf{0})$, we have answered Sands' question in the negative.

It is easily seen that an infinite number of counterexamples can be constructed by the same method.

In conclusion we remark that Sands' problem for the special case of cyclic groups G was raised earlier by C. Swenson [**8**]. Our methods do not yield counterexamples for this case; thus Swenson's problem remains open.

REFERENCES

1. O. Fraser and B. Gordon, Solution to a problem of L. Fuchs, *Quart. J. Math. Oxford Ser.* **25** (1974), 1–8.

2. L. Fuchs, *Abelian Groups*, 3rd edition (Pergamon, 1960), 331.

3. G. Hájos, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, *Math. Z.* **47** (1941), 427–467.

4. A. D. Sands, On a problem of L. Fuchs, *J. London Math. Soc.* **37** (1962), 277–284.

5. A. D. Sands, The factorization of abelian groups, *Quart. J. Math. Oxford Ser.* **10** (1959), 81–91.

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

7. A. D. Sands, On a conjecture of G. Hájos, *Glasgow Math. J.* **15** (1974), 88–89.

8. C. Swenson, *Direct sum subset decomposition of abelian groups*, Thesis, Washington State University (1972).

9. J. H. van Lint, *Coding Theory* (Springer, 1971), 85–91.

10. J. H. van Lint, Survey of perfect codes, *Rocky Mountain J. Math.* **5** (1975), 199–220.

Los Angeles Valley College
University of California
Los Angeles

https://doi.org/10.1017/S0017089500003803 Published online by Cambridge University Press