Constructing Single-error-correcting Codes
Using Factorization of finite Abelian Groups

Khalid Amin

University of Bahrain
Department of Mathematics
PO Box 32038
Sakhir, Kingdom of Bahrain

Abstract

Factorization of finite abelian groups was proposed by G. Hajos, when he was attempting to solve a conjecture about tiling by H. Minkowski. Hajos eventually settled this conjecture in its group-theoretic form. Subsequently, the notion of factorization of finite abelian groups was studied in the context of many other fields, ranging from number theory to geometry and coding theory. In this paper, we will use factorization of finite abelian groups to construct a single-error-correcting binary code of length seven and minimum hamming distance three.

1. Introduction

Let $G$ be a finite abelian group written multiplicatively and let $A$ and $B$ subsets of $G$. If it happens that for each element $g \in G$, there exist unique elements $a \in A$ and $b \in B$ such that $g = ab$, we say that we have a factorization of $G$ into the subsets $A$ and $B$. We shall express this by writing $G = AB$. This idea of factorization can be easily generalized to $G = A_1 A_2 \ldots A_k$ for subsets $A_1, A_2, \ldots, A_k$ of $G$. Recall that by the fundamental theorem of finite abelian groups, any finite abelian group is the direct product of cyclic groups. Namely, if $G$ is a finite abelian group of order
For distinct primes $p_1, p_2, \ldots, p_r$, and $\alpha_i$ are non-negative integers, then $G = C_{p_1^{\alpha_1}} \times C_{p_2^{\alpha_2}} \times \ldots \times C_{p_r^{\alpha_r}}$

Where $C_{p_i^{\alpha_i}}$ is a cyclic group of order $p_i^{\alpha_i}$

We say that $G$ is of type $(p_1, p_2, \ldots, p_r)$. In the special case of $p_1 = \ldots = p_r = p$, and $\alpha_i = 1, 1 \leq i \leq r$, we call $G$ an elementary $p$-group. The idea of such type of decomposition of a finite abelian group was initiated by Hajos [2], when he succeeded in giving an answer to a conjecture about tiling by H. Minkowski [4], after first translating it into a question about finite abelian groups. In the study of factorization of finite abelian groups, usually questions are asked as to under what conditions one of the factors must be a subgroup of $G$. With the exception of elementary 2-groups, previous work has lead to formulas giving all factorizations under certain conditions.

The conditions may involve the structure of the group and the number of factors. Alternatively they may involve numerical conditions on the orders of the factors. The best known results of this second type is the famous theorem of L. Redei [5], which asserts that if each of the factors has prime order, then one of the factors must be a subgroup of $G$. This result was further generalized by Sands in [6] to the case when each factor has prime power order. A large body of work on the factorization of abelian groups has been written since Hajos, and are mainly due to N. G. De Bruijn [1] and A. D. Sands [7,8]. For a history of factorization of abelian group, Stein and Szabo, [11] may be consulted.

2. Preliminaries

Let $X$ be an alphabet of $q$ elements and let $S_r(a)$ be the Hamming sphere in $X^n$ centered at $a$ with radius $r$. A subset $B$ is called a perfect error-correcting code with parameters $(n, e, q)$ if the Hamming spheres

$S_r(a), a \in B$

form a partition of $X^n$. Szabo [10,] shows that when the set $X^n$ is endowed with a structure of an abelian group, the existence problem of the perfect error correcting codes is equivalent to what is called the Complementer Subgroup Problem which is stated below:
Given a finite abelian group \( G \) and a subset \( A \) of \( G \) such that \( |A| \) divides \( |G| \). Decide if there is a subgroup \( H \) of \( G \) such that \( G = AH \) is a factorization of \( G \).

Evidently, the complementer subgroup problem is not easily resolved since we do not have an algorithm for producing such a subgroup \( H \) for a given a subset \( A \) of \( G \). However, in certain cases, this is possible. For example, if we let \( G = \langle x \rangle \) be the cyclic group of order 32 with generator \( x \) and the subset \( A = \{ e, x^3 \} \), then direct calculations show that the choice of the subgroup \( H = \langle x^2 \rangle \) generated by \( x^2 \) will give a factorization of \( G \).

3. Result

To achieve the aim of this paper, we choose the elementary 2-group \( G \) of order \( 2^7 = 128 \). That is we choose a group \( G \) which is the direct product of 7 cyclic groups each of order 2, Viz,

\[
G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle \times \langle x_6 \rangle \times \langle x_7 \rangle
\]

where each of \( x_1, x_2, x_3, x_4, x_5, x_6, x_7 \) has order 2.

Let

\[
A = \{ e, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \}
\]

Then it can be easily checked by direct calculation that the choice of the subgroup \( H \) generated by \( x_1 x_2 x_6, x_1 x_3 x_5, x_1 x_4 x_7, x_2 x_3 x_4 \), Viz

\[
H = \langle x_1 x_2 x_6, x_1 x_3 x_5, x_1 x_4 x_7, x_2 x_3 x_4 \rangle
\]

will give a factorization of \( G \). Now, each element \( g \) of \( G \), can be written uniquely in the form

\[
g = x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4} x_5^{\alpha_5} x_6^{\alpha_6} x_7^{\alpha_7}
\]

where \( \alpha_i \in \{0,1\} \) \( 1 \leq i \leq 7 \). Thus we can identify each element \( g \in G \) with the tuples \((\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7)\). Upon expanding, we get
Using the above correspondence, we obtain the following binary code $C$ with 16 codewords:

\[
H = \left\{ e, x_1 x_2 x_6, x_1 x_3 x_5, x_2 x_3 x_4, x_1 x_4 x_7, x_1 x_2 x_4 x_5, x_1 x_3 x_4 x_6, x_1 x_2 x_3 x_7, \\
\quad x_2 x_3 x_5 x_6, x_2 x_4 x_6 x_7, x_3 x_4 x_5 x_7, x_1 x_2 x_4 x_5 x_6 x_7, x_4 x_5 x_6, \\
\quad x_2 x_5 x_7, x_3 x_6 x_7, x_5 x_6 x_7 \right\}
\]

Thus, we have a linear code of length 7 and minimum Hamming distance 3.

**Final Remark**

It would be nice to know if we could find a systemic way of finding the subgroup $H$, since then construction of such codes of any length would follow.

**Acknowledgements.** The author is thankful to the Deanship of Research at the University of Bahrain for their support (Research Project No. 9/2012) during work on this Project.

**References**


Received: March 15, 2014