Dual Codes of Systematic Group Codes over Abelian Groups

A. A. Zain, B. Sundar Rajan

Department of Electrical Engineering, Indian Institute of Technology, Delhi, Hauz Khas, New Delhi 110016, India. email: bsrajan@ee.iitd.ernet.in

Received March 7, 1995; revised version April 3, 1996

Abstract. For systematic codes over finite fields the following result is well known: If $[I | P]$ is the generator matrix then the generator matrix of its dual code is $[-P^t | I]$. The main result is a generalization of this for systematic group codes over finite abelian groups. It is shown that given the endomorphisms which characterize a group code over an abelian group, the endomorphisms which characterize its dual code are identified easily. The self-dual codes are also characterized. It is shown that there are self-dual and MDS group codes over elementary abelian groups which can not be obtained as linear codes over finite fields.

Keywords: Self-dual codes, Endomorphisms, Group codes, Dual codes.

1. Introduction

Study of codes over groups is motivated by the observation [7-9] that when more than two signals are used for transmission, a group structure, instead of the finite field structure traditionally assumed, for the alphabet is matched to the relevant distance measure. The Hamming distance properties of codes over groups have been studied in [5] and in [1] construction of group codes over abelian groups is given in terms of a 'parity check' matrix.

It is well known that binary linear codes are matched to binary signalling over an Additive White Gaussian Noise (AWGN) channel, in the sense that the squared Euclidean distance between two signal points in the signal space corresponding to two codewords is proportional to the Hamming distance between codewords. Similarly, linear codes over $\mathbb{Z}_p$ are matched to M-PSK modulation systems for an AWGN channel [11, 12]. The general problem of matching signal sets to linear codes over general algebraic structure of groups has been studied in [7-9]. Also, group codes constitute an important ingredient for the construction of Geometrically Uniform codes [4]. This motivates the study of codes over groups.

Part of this correspondence was presented in 1994 International Symposium on Information Theory, Trondheim, Norway, June 1994
both abelian and nonabelian. In [1] construction of group codes over abelian
groups that mimics the construction of algebraic codes over finite fields is consider-
ed and it is shown that the construction can be on the basis of a parity check matrix
which provides the relevant information about the minimum Hamming distance of
the code. The parity check symbols are seen as images of certain homomorphisms
from \( G^k \) to \( G \).

In this correspondence the dual code of a group code over an abelian group is
characterized in terms of the endomorphisms of the abelian group. The study of dual
codes is motivated by the fact that the weight distributions of the code and its dual
are related for group codes over abelian groups [3]. It is shown that the endomor-
phisms of the dual code for a given code is related to the defining endomorphisms of
the code, and in terms of appropriate matrix representations for the endomorphisms
the relation is relatively simple. For the special case of codes over cyclic groups the
colorization turns out to be straight forward, i.e., the endomorphisms defining
the code and its dual are inverses in the group of endomorphisms. This special case
actually corresponds to linear codes over residue class rings of integers. The
necessary and sufficient conditions on the defining endomorphisms are obtained for
the code to be self-dual.

In Sect. II the description of group codes in terms of endomorphisms is given.
The characterization of dual codes is obtained in Sect. III. The special cases of group
codes over cyclic groups and elementary abelian groups are discussed in Sect. IV.
Section V deals with self-dual codes. Some concluding remarks and suggestions for
further work are given in Section VI.

II. Group codes over abelian groups

Let \( G \) be a finite abelian group. The subgroups of \( G^n \) are called length \( n \) group codes.
A group code isomorphic to \( G^k \) for some \( k < n \), is called an information set
supporting group code [1]. Information set supporting group codes are equivalent
to systematic group codes. An instance of group codes that do not support an
information set is where in none of the components all the elements of \( G \) appear. In
this paper only information set supporting group codes are under consideration.

**Definition 1.** [1] A \((n, k)\) systematic group code over an abelian group \( G \) is
a subgroup of \( G^n \) with order \( |G|^k \) described by \( n-k \) homomorphisms \( \phi_j, \)
\( j = 1, 2, \ldots, n-k \), of \( G^k \) onto \( G \). Its codewords are \( (x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) \), where

\[
x_{k+j} = \phi_j(x_1, \ldots, x_k) = \bigoplus_{l=1}^{k} \phi_j(e, \ldots, e, x_l, e, \ldots, e) \quad (1)
\]

with \( e \) and \( \bigoplus \) denoting the identity element and the group operation of \( G \),
respectively.

In (1), the term \( \phi_j(e, \ldots, e, x_l, e, \ldots, e) \) can be replaced by an endomorphism of \( G \),
say, \( \psi_{l, j} \). With this notation the code is defined by the set of endomorphisms \( \{\psi_{l, j}, \)
\( l = 1, 2, \ldots, k \) and \( j = 1, 2, \ldots, n-k \} \) and (1) can be rewritten as

\[
x_{k+j} = \phi_j(x_1, \ldots, x_k) = \bigoplus_{l=1}^{k} \phi_j(e, \ldots, e, x_l, e, \ldots, e) = \bigoplus_{l=1}^{k} \psi_{l, j}(x_l). \quad (2)
\]