On Minimum Distance Bounds for Abelian Codes

Roberta Evans Sabin

Computer Science Department, Loyola College, 4501 N. Charles St., Baltimore, Maryland 21210-2699, USA

Received December 3, 1990; revised version April 27, 1992

Abstract. This paper is an exposition of two methods of formulating a lower bound for the minimum distance of a code which is an ideal in an abelian group ring. The first, a generalization of the cyclic BCH (Bose–Chaudhuri–Hocquenghem) bound, was proposed by Camion [2]. The second method, presented by Jensen [4], allows the application of the BCH bound or any of its improvements by viewing an abelian code as a direct sum of concatenations of cyclic codes. This second method avoids the mathematical analysis required for a direct generalization of a cyclic bound to the abelian case. It can produce a lower bound that improves the generalized BCH bound. We present simple algorithms for 1) deriving the generalized BCH bound for an abelian code 2) determining direct sum decompositions of an abelian code to concatenated codes and 3) deriving a bound on an abelian code, viewed as a direct sum of concatenated codes, by applying the cyclic BCH bound to the inner and outer code of each concatenation. Finally, we point out the applicability of these methods to codes that are not ideals in abelian group rings.

Keywords: Error-correcting codes, Algebraic block codes, Minimum distance, BCH Bound, Concatenated codes, Mattson–Solomon polynomial, Discrete Fourier transform

1 Introduction

Let $G_M$ represent the cyclic group of order $M$. Let $G = G_{M_1} \times G_{M_2} \times \cdots \times G_{M_k}$ and consider ideals in $FG$ where for field $F$, $\text{char}(F) \mid \text{order}(G)$. When $k = 1$, these ideals are the familiar cyclic codes. We use the term abelian code for an ideal in $FG$ where $k > 1$. Like their cyclic counterparts, these codes have a well-defined structure: minimal codes form a direct sum decomposition of $FG$; each code is generated by a unique idempotent generator; the set of idempotent generators sum to unity in $FG$ and are mutually orthogonal.
To find lower bounds on the minimum distance of these codes, methods analogous to those used with cyclic codes [6] may be employed. The traditional BCH (Bose–Chaudhuri–Hocquenghem) bound for cyclic codes is a result of the one-to-one correspondence that exists between the elements of the underlying abelian group and that group’s irreducible group characters. Camion [2] used this correspondence to generalize the BCH bound to the abelian case. An abelian codeword, like its cyclic counterpart, may be associated with a polynomial, its discrete Fourier transform. An abelian code can be identified with one such polynomial, called the support. As in the cyclic case, the relationship between the discrete Fourier transform of any codeword and the support of the code and the fact that such a polynomial can be inverted to recover a codeword is important in the establishment of the bound. Unlike the cyclic case, however, the support polynomial contains more than one indeterminate and thus requires more complicated analysis. We present Camion’s method of deriving the generalized BCH bound in a simplified form along with an algorithm that determines the bound by manipulating the matrix form of the support polynomial.

An alternate approach to establishing a lower bound on the minimum distance of an abelian code was presented by Jensen [4]. Any code in $F(G_{M_1} \times G_{N})$ may be viewed as the direct sum of concatenations of cyclic outer and inner codes, and the bound on generalized concatenated codes [1] may be applied. A minimum distance bound is set by using minimum distances of the constituent cyclic codes. We show that this approach, which can be extended to codes in $F(G_{M_1} \times G_{M_2} \times \cdots \times G_{M_n})$, produces a lower bound on minimum distance that frequently improves the BCH bound. We demonstrate simple algorithms that reveal the concatenated structure of an abelian code and arrive at this lower bound. Finally we point out the applications and limitations of these methods in determining lower bounds for non-abelian codes which are ideals in metacyclic group rings [8].

Note 1: In this paper, for any $G$, elements of $F G$ are represented as polynomials in which the elements of $G$ are indeterminate; alternatively, elements of $F G$ are represented as order($G$)-tuples of elements of $F$ ordered according to the lexicographic ordering of the polynomial representation.

Note 2: In the following discussion, the term “polynomial” is used to refer exclusively to non-zero polynomials. Similarly, unless otherwise stated, “codeword” refers to a non-zero codeword.

2 The BCH Bound Generalized to the Abelian Case

We begin by describing abelian codes in a way that is analogous to that used for cyclic codes. If $G$ is abelian, $G$ is isomorphic to the direct product of 1 or more cyclic groups. If $G = G_{M_1} \times G_{M_2} \times \cdots \times G_{M_n}$, code $C$ in $F G$ may be identified by a set of zeros or by irreducible group characters, which are valued at zero for all codewords [3]. The sequence of characters evaluated for any element of $F G$ is the discrete Fourier transform of that element and, written in polynomial form, is referred to as the Mattson–Solomon (M–S) polynomial. As with cyclic codes, given any generator of a code, we identify with the code a unique M–S polynomial, the support of the