Six New Binary Quasi-Cyclic Codes

Zhi Chen

Abstract—Six new quasi-cyclic codes are presented, which improve the lower bounds on the minimum distance for a binary code. A local exhaustive search is used to find these codes and many other quasi-cyclic codes which attain the lower bounds.

Index Terms—Quasi-cyclic codes, best known binary codes, coding and codes.

I. INTRODUCTION

As a generalization of cyclic codes, quasi-cyclic (QC) codes contain many good linear codes. Much work has been done to find good QC codes with the help of computers, and many good QC codes have been found [1]–[4]. It should be noted that an exhaustive search is intractable with the increase in the code dimensions. Gulliver and Bhargava [1]–[3] presented a nonexhaustive method based on the exhaustive method developed by Tilborg [4]. However, it is not feasible to search for codes with large code dimensions, so some other methods should be developed. In this correspondence, a local exhaustive method is used to find good binary QC codes. New QC codes which improve the lower bounds on the minimum distance for a binary linear code are presented, and many other QC codes which attain the best known lower bounds are found.

II. NEW QUASI-CYClical CODES

A code is said to be quasi-cyclic (QC) if a cyclic shift of any codeword by p positions is still a codeword. Thus, a cyclic code is a QC code with p = 1. The block length n of a QC code is a multiple of p, i.e., n = mp. A subset of QC codes can be constructed from m × m circulant matrices. Let

\[ G = [C_0 \ C_1 \ \cdots \ C_{p-1}] \]

where \( C_i \) are circulant matrices, \( i = 0, 1, \ldots, p - 1 \). A circulant matrix \( C \) is defined to be a cyclic square matrix of the form

\[
C = \begin{bmatrix}
C_0 & C_1 & \cdots & C_{m-1} \\
C_{m-1} & C_0 & \cdots & \vdots \\
\vdots & \vdots & \ddots & \vdots \\
C_1 & \cdots & \cdots & C_0
\end{bmatrix}
\]

The algebra of circulant \( m \times m \) matrices over \( GF(2) \) is isomorphic to the algebra of polynomials in the ring \( f(x)/(x^m + 1) \) if \( C \) is mapped onto the polynomial \( c(x) = c_0 + c_1 x + \cdots + c_{m-1} x^{m-1} \). Let \( c(x), c_1(x), \ldots, c_{r-1}(x) \) be the polynomials corresponding to circulant \( m \times m \) matrices \( C_0, C_1, \ldots, C_{r-1} \). Seguin and Drolet [5] defined 1-generator quasi-cyclic codes. The order of a 1-generator QC code \( V \) is defined as

\[ h(x) = (x^m + 1)/\gcd(x^m + 1, c_0(x), c_1(x), \ldots, c_{r-1}(x)) \]

and the dimension \( k \) of \( V \) is equal to the degree of \( h(x) \). If \( h(x) \) has degree \( m \), the dimension of \( V \) is \( k = m \), and (1) is a generator matrix for \( V \). If \( k < m \), a generator matrix for \( V \) can be constructed by deleting \( m - k \) rows of (1). Therefore, a 1-generator QC code is a \([pm,k]_2 \) code.

The quasi-cyclic structure of the code can be used to simplify the search. The first step is to find all polynomials of degree less than \( m \), which are divisible by another polynomial \( a(x) \) of degree \( m - k \) and \( \gcd(x^m + 1, a(x)) = a(x) \). The equivalent polynomials which generate the equivalent codes are eliminated. The remaining polynomials are grouped according to their weights. Let \( S_i(x) \) be sets of such polynomials with weight \( i \), \( i = 1, 2, \ldots, m - 1 \).

The search is initialized with \( r \) given generator polynomials \( c_0(x), c_1(x), \ldots, c_{r-1}(x) \), and an initial value of minimum distance \( d \). To obtain a QC code with \( p = r + 1, r + 2 \), or \( r + 3 \), one, two, or three more generator polynomials are chosen from one, two, or three sets \( S_i(x) \) of polynomials, respectively. For example, to obtain QC code with \( p = r + 2 \) and the minimum distance \( > d \), two polynomials \( c_i(x) \) and \( c_j(x) \) must be chosen from two sets of polynomials \( S_i(x) \) and \( S_j(x) \), respectively, where

\[ \text{wt}(c_i(x)) + \text{wt}(c_j(x)) + \cdots + \text{wt}(c_{r-1}(x)) + i + q > d. \]

Only the polynomials in the chosen sets are examined exhaustively. For each possible choice, the program produces its code-words one by one and checks the weights of the produced codewords. If a nonzero codeword with weight less than or equal to \( d \) is found, the program continues to examine another choice of polynomials. If no nonzero codewords with weights less than or equal to \( d \) are found, a QC code with the minimum distance \( > d \) is constructed, and the program records the new code and updates the minimum distance \( d \). This process is repeated until all possible polynomials in the given sets are investigated.

With this local exhaustive search, many good QC codes have been obtained. Among these, six QC codes improve the lower bounds on the minimum distance for a binary linear code, and 19 entries in the table of [6] are thus updated. Table I lists these codes and their generator polynomials in octal, with the least
TABLE I
New Quasi-Cyclic Codes

<table>
<thead>
<tr>
<th>QC Code</th>
<th>d_{min}</th>
<th>d_{BV}</th>
<th>m</th>
<th>c(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[60, 19]</td>
<td>18</td>
<td>17-20</td>
<td>20</td>
<td>3, 415, 463357</td>
</tr>
<tr>
<td>[81, 20]</td>
<td>26</td>
<td>23-30</td>
<td>27</td>
<td>4551, 72341, 35267167</td>
</tr>
<tr>
<td>[66, 21]</td>
<td>20</td>
<td>19-22</td>
<td>22</td>
<td>3, 10567, 443671</td>
</tr>
<tr>
<td>[82, 21]</td>
<td>25</td>
<td>24-30</td>
<td>41</td>
<td>16051207, 1136315123</td>
</tr>
<tr>
<td>[100, 20]</td>
<td>34</td>
<td>33-40</td>
<td>25</td>
<td>41, 515433, 1367143, 3237107</td>
</tr>
</tbody>
</table>

A local exhaustive search for good quasi-cyclic codes is presented, and new codes have been constructed which improve the lower bounds on the minimum distance for a binary linear code. From these codes, 19 entries in the table of [6] are thus updated. The author is grateful to Prof. I. Ingemarsson for his support and discussion, and to the referees and the Associate Editor for their helpful reviews.

ACKNOWLEDGMENT

The author is grateful to Prof. I. Ingemarsson for his support and discussion, and to the referees and the Associate Editor for their helpful reviews.

REFERENCES