Improvements to the Bounds on Optimal Binary Linear Codes of Dimensions 11 and 12

T. Aaron Gulliver
Department of Electrical and Electronic Engineering
University of Canterbury
Christchurch, New Zealand

Vijay K. Bhargava
Department of Electrical and Computer Engineering
University of Victoria
P.O. Box 3055, MS 8610, Victoria, BC, Canada V8W 3P6

Abstract Eight new codes are presented which improve the bounds on maximum minimum distance for binary linear codes. They are rate $(m-r)/pm, r \geq 1$, r-degenerate quasi-cyclic codes.

Keywords: binary linear codes, quasi-cyclic codes

I. Introduction

Let $V(n,2)$ be an n-dimensional vector space over the binary Galois field $GF(2)$, and denote a k-dimensional subspace of $V(n,2)$ as C. C is said to be an (n,k) binary linear code and can be represented as the rowspace of

[1]This research was supported in part by the Natural Science and Engineering Research Council of Canada

[2]Formerly with the Department of Systems and Computer Engineering, Carleton University, 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6

a $k \times n$ generator matrix

$$G = \begin{bmatrix} g_{0,0} & g_{0,1} & g_{0,2} & g_{0,3} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & g_{1,2} & g_{1,3} & \cdots & g_{0,n-1} \\ g_{2,0} & g_{2,1} & g_{2,2} & g_{2,3} & \cdots & g_{0,n-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & g_{k-1,3} & \cdots & g_{k-1,n-1} \end{bmatrix}. \quad (1)$$

This code contains 2^k codewords corresponding to all possible combinations of the rows of G. The *Hamming weight* of a codeword, $w_H(x)$, $x \in C$, is the number of nonzero elements in x. The *Hamming distance* between two codewords, $d_H(x_i, x_j), x_i \in C$ and $x_j \in C$, is the number of positions in which they differ. The minimum distance of a code is defined as the minimum Hamming distance between codewords

$$d_{min} = \min\{d_H(x_i, x_j); x_i, x_j \in C, x_i \neq x_j.$$

For a linear code, the minimum distance is the minimum Hamming weight of its nonzero codewords

$$d_{min} = \min\{w_H(x_i); x_i \in C, x_i \neq 0.$$

Let A_i be the number of codewords of Hamming weight i in C. Then the numbers $A_0, A_1, \cdots, A_n$, are called the weight distribution of C [1] and therefore

$$\sum_{i=0}^{n} A_i = 2^k.$$

The maximum number of correctable errors in a codeword is given by

$$t = \lfloor \frac{d_{min} - 1}{2} \rfloor,$$

thus it is desirable to find codes which maximize d_{min}. Denote the maximum possible value of d_{min} for an (n, k) binary linear code as $d_2(n, k)$. Codes which have $d_{min} = d_2(n, k)$ are called *optimal*. For binary linear codes, Brouwer and Verhoeff [2] have tabulated bounds on the maximum

possible minimum distance for $k \leq n \leq 127$, and Brouwer [3] maintains an online table of bounds for $k \leq n \leq 256$.

$n_2(d,k)$ has been completely determined for $k \leq 7$ [3]. Conversely, there remain many unknown values of $n_2(d,k)$ for $k > 7$. In this paper, the bounds on eight values of $d_2(n,11)$ and $d_2(n,12)$ are improved.

II. Quasi-Cyclic Codes

A code is called *quasi-cyclic* (QC) if there is some integer p such that every cyclic shift of a codeword by p places is again a codeword [1, 4]. QC codes were first investigated by Townsend and Weldon [5], Karlin [6, 7] and Chen, et al. [4]. The blocklength, n, of a QC code must be a multiple of p, so that $n = mp$ [8]. If $p = 1$, the code is called *cyclic*. QC codes are known to be good codes [9] (unlike the well known BCH codes, which are cyclic codes [10]). In fact it is conjectured that arbitrarily long QC codes meet the Gilbert-Varshamov bound [11] (if arbitrarily large primes exist with 2 as a primitive root). In addition, a connection exists between QC codes and convolutional codes [12].

By rearranging the columns of the generator matrix, G, it can be shown that many QC codes are equivalent to a code composed of $m \times m$ circulant matrices. Thus G can be transformed to

$$G' = [C_0, C_1, C_2, \ldots, C_{p-1}], \tag{2}$$

with C_i an $m \times m$ circulant matrix of the form

$$\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{m-1} \\ c_{m-1} & c_0 & c_1 & \cdots & c_{m-2} \\ c_{m-2} & c_{m-1} & c_0 & \cdots & c_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}, \tag{3}$$

where each successive row is a right cyclic shift of the previous one. 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_i is mapped onto the polynomial, $c_i(x) = c_{i,0} + c_{i,1}x + c_{i,2}x^2 + \cdots + c_{i,m-1}x^{m-1}$ [1]. The $c_i(x)$ are called *defining polynomials* [8]. These codes are a subset of the more general 1-generator QC codes [13], which is in turn a subclass of QC codes. The class of QC codes of the form (2) is known to contain many optimal binary linear codes [14, 15, 16].

If the polynomial $c_i(x)$ representing a circulant matrix C_i contains a factor of $x^m - 1$, then C_i is singular. If all the $c_i(x)$ in a QC code have a common factor of $x^m - 1$, then the QC code is called *degenerate* [8]. Degenerate QC codes are also 1-generator QC codes [13]. The *order* of a 1-generator QC code is defined as [13]

$$h(x) = \frac{x^m - 1}{(x^m - 1, c_0(x), c_1(x), \cdots, c_{p-1}(x))}, \tag{4}$$

and k, the code dimension, is equal to the degree of $h(x)$. If $h(x)$ has degree m, then $k = m$, and (2) is a generator matrix for C. If $\deg(h(x)) = k < m$, a generator matrix can be constructed by deleting $r = m - k$ rows of (2). These are called r-degenerate QC codes.

The QC structure of C can used to be reduce the computational complexity of finding good codes. The first step is to obtain a set of defining polynomials. Consider the set of polynomials of degree $m - 1$ or less. Two polynomials, $c_j(x)$ and $c_i(x)$ can be said to belong to the same equivalence class if

$$c_j(x) = ax^l c_i(x) \bmod (x^m - 1),$$

for some integer $l > 0$ and scalar $a \in \mathrm{GF}(q)\backslash\{0\}$. This means that two polynomials are in the same class if one can be obtained from the other by a cyclic shift, multiplying by a nonzero scalar, or both. Only one polynomial from each class need be considered when constructing QC codes since polynomials from the same class produce equivalent codes [17]. This equivalence relation is induced by the action of a finite group on the set of

m-tuples. Distinct equivalence classes correspond to distinct orbits under the action of this group and so can be enumerated using Burnside's Lemma [17].

Once a set of defining polynomials has been constructed, the weight distributions of the codes generated by the corresponding circulant matrices, C_i, must be computed. This task can be simplified since the Hamming weight of $i_j(x)c_i(x) \bmod (x^m-1)$ is equal to the weight of $ai_j(x)x^l c_i(x) \bmod (x^m-1)$ for all $a \in GF(q)/\{0\}$ and $0 \leq l < m$, so these redundant weights can be eliminated. Arranging the remaining weights in a matrix [14] gives

$$D = \begin{array}{c|cccccc} & i_1(x) & i_2(x) & \cdots & i_j(x) & \cdots & i_y(x) \\ \hline c_1(x) & w_{11} & w_{12} & \cdots & w_{1j} & \cdots & w_{1y} \\ c_2(x) & w_{21} & w_{22} & \cdots & w_{2j} & \cdots & w_{2y} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ c_k(x) & w_{k1} & w_{k2} & \cdots & w_{kj} & \cdots & w_{ky} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ c_z(x) & w_{z1} & w_{z2} & \cdots & w_{zj} & \cdots & w_{zy} \end{array} \tag{5}$$

where $i_j(x)$ is the jth information polynomial, $c_k(x)$ is the kth generator polynomial, and w_{kj} is the Hamming weight of $i_j(x)c_k(x) \bmod (x^m-1)$. Since the $i_j(x)$ and $c_k(x)$ correspond to the set of class representatives, D is a symmetric, square matrix, with $y = z$. The complete weight distribution of any QC code can be constructed from D.

III. New Codes of Dimensions 11 and 12

The algorithm used to construct new codes is based on the approach in [18], but with a heuristic (nonexhaustive) search. The search is initialized with a code of the desired rate, chosen arbitrarily as p rows of D. Clearly the minimum distance of this code is the minimum column sum of these p rows.

To improve the code, a new $c_k(x)$ is found to replace one presently in

the code so that the minimum distance, or the column sum of the p rows, is increased. If one is not found, a selection algorithm is used which provides some degree of randomness, as in [14, 15, 16, 17]. This process is repeated until the required minimum distance is achieved, or a limit on the number of iterations is reached. This approach is used because an exhaustive search is intractable for these code dimensions. Although the resulting codes are not guaranteed to be the best possible, codes which meet or exceed the lower bounds on minimum distance can still be obtained. In this case, eight codes were found which improve the bounds in [2] and [3] on $d_2(n,k)$. Numerous agreements with the tabulated bounds were also found. No codes with dimension $k < 11$ or $k > 12$ were found which improved the known bounds.

The eight new codes are listed in Table I. The generator polynomials, $c_i(x)$, are given in octal, with the leading zeros deleted and the least significant coefficient on the left, i.e., 325_8 corresponds to $x^7+x^5+x^3+x+1$. The common factor of all the $c_i(x)$, $(x^m-1)/h(x)$, is also given, along with the minimum distance and the new bound on $d_2(n,k)$, denoted by d_{br}, which appears in [3].

REFERENCES

[1] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, New York: North-Holland, 1977.

[2] A.E. Brouwer and T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes", *IEEE Trans. Inf. Theory*, vol. 39, pp. 662-677, Mar. 1993.

[3] A.E. Brouwer, Table of minimum-distance bounds for linear codes over GF(2), lincodbd server, aeb@cwi.nl, http://www.win.tue.nl/win/math/dw/voorlincod.html. Eindhoven University of Technology, Eindhoven, the Netherlands.

[4] C.L. Chen, W.W. Peterson and E.J. Weldon Jr., "Some results on quasi-cyclic codes," *Inf. and Contr.*, No. 15, pp. 407-423, 1969.

[5] R.L. Townsend and E.J. Weldon Jr., "Self-orthogonal quasi-cyclic codes," *IEEE Trans. Inf. Theory*, vol. 13, pp. 183-195, Apr. 1967.

[6] M. Karlin, "New binary coding results by circulants," *IEEE Trans. Inf. Theory*, vol. 15, pp. 81-92, Jan. 1969.

[7] M. Karlin, "Decoding of circulant codes," *IEEE Trans. Inf. Theory*, vol. 16, pp. 797-802, Nov. 1970.

[8] P.P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes," *Designs, Codes and Crypt.*, vol. 2, pp. 81-91, 1992.

[9] E.J. Weldon Jr., "Long quasi-cyclic codes are good," *IEEE Trans. Inf. Theory*, vol. 13, pp. 130, 1970.

[10] S. Lin and , E.J. Weldon , Jr., "Long BCH codes are bad," *Inf. and Contr.*, vol. 11, pp. 445-451, 1967.

[11] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2," *IEEE Trans. Inf. Theory*, vol. 20, p. 679, 1974.

[12] G. Solomon and H.C.A. van Tilborg, "A connection between block codes and convolutional codes," *SIAM J. Appl. Math.*, vol. 37, pp. 358-369, Oct. 1979.

[13] G.E. Séguin and G. Drolet, "The theory of 1-generator quasi-cyclic codes," preprint, Royal Military College of Canada, Kingston, ON, June 1990.

[14] T.A. Gulliver and V.K. Bhargava, "Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes," *IEEE Trans. Inf. Theory*, vol. 37, pp. 552-555, May 1991.

[15] T.A. Gulliver and V.K. Bhargava, "Nine good rate $(m-1)/pm$ quasi-cyclic codes," *IEEE Trans. Inf. Theory*, vol. 38, pp. 1366-1369, July 1992.

[16] T.A. Gulliver and V.K. Bhargava, "Twelve good rate $(m-r)/pm$ quasi-cyclic codes," *IEEE Trans. Inf. Theory*, vol. 39, pp. 1750-1751, Sept. 1993.

[17] T.A. Gulliver, New optimal ternary linear codes, *IEEE Trans. Inf. Theory*, vol. 41, pp. 1182-1185, July, 1995.

[18] H.C.A. van Tilborg, On quasi-cyclic codes with rate 1/m, *IEEE Trans. Inf. Theory*, vol. 24, pp. 628-629, Sept., 1978.

Table I. QC Codes Which Improve the Bounds on Maximum Minimum Distance for a Binary Linear Code

QC code	m	$(x^m-1)/h(x)$	d_{min}	d_{br}	$c_i(x)$
$(140,11)$	14	13	63	$63-65$	$1277,61,5523,343,6725,5717,1127,3075,1335,13$
$(147,11)$	21	3303	66	$66-69$	$56353,1571733,43747,472531,1153757,212331,30333$
$(150,11)$	15	31	68	$68-70$	$17765,427,5455,1703,1761,445,4223,5165,12465,15467$
$(180,11)$	15	31	82	$82-84$	$2333,7671,13577,2725,737,6555,15467,2167,3075,17237,207,4635$
$(210,11)$	21	3303	98	$98-101$	$1351577,467125,36535,546217,30333,326417,452713,5505,124637$ 447307
$(252,11)$	21	3303	120	$120-122$	$117607,63565,306635,533065,43747,25727,1135737,234715,670711$ $506653,5505,461723$
$(161,12)$	23	6165	72	$72-75$	$1653073,5567373,2727375,360575,1061105,1564517,73467$
$(168,12)$	21	1101	76	$76-80$	$155041,230311,313221,623147,674315,67161,2733267,65363$