[2] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 284–287, Mar. 1974.

[3] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Inform. Theory*, vol. 13, pp. 260–269, Apr. 1967.

[4] V. Zyablov and V. Sidorenko, "Bounds on complexity of trellis decoding of linear block codes," *Probl. Inform. Transm.*, pp. 3–9, July–Sept. 1993 [in Russian].

[5] V. Zyablov and V. Sidorenko, "Soft-decision decoding of partial-unit memory codes," *Probl. Inform. Transm.*, vol. 28, no. 1, pp. 22–27, Jan.–Mar. 1992 [in Russian]; pp. 18–22, July 1992 [in English].

[6] U. Dettmar and U. Sorger, "On maximum-likelihood decoding of unit memory codes," in *Proc. 6th Joint Swedish–Russian Int. Workshop Inform. Theory* (Molle, Sweden), Aug. 1993, pp. 184–188.

[7] J. P. M. Schalkwijk, A. J. Vink, and K. A. Post, "Syndrome decoding of binary rate k/n convolutional codes," *IEEE Trans. Inform. Theory*, vol. 24, pp. 553–562, Sept. 1978.

[8] G. D. Forney, Jr., "Convolutional codes I: Algebraic structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720–738, Nov. 1970.

[9] G. D. Forney, Jr., "Coset codes—part II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, Sept. 1988.

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-Cyclic 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 $m \times m$ circulant matrices. Let

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

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

$$C = \begin{bmatrix} c_0 & c_1 & \cdots & c_{m-1} \\ c_{m-1} & c_0 & \cdots & c_{m-2} \\ \cdots & \cdots & \cdots & \cdots \\ c_1 & c_2 & \cdots & c_0 \end{bmatrix}. \tag{2}$$

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 $c_0(x), c_1(x), \cdots, c_{p-1}(x)$ be the polynomials corresponding to circulant $m \times m$ matrices $C_0, C_1, \cdots, C_{p-1}$. Seguin and Drolet [5] defined 1-generator quasi-cyclic codes. The order of a 1-generator QC code V is defined as

$$h(x) = (x^m + 1)/\gcd\{x^m + 1, c_0(x), c_1(x), \cdots, c_{p-1}(x)\} \tag{3}$$

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 $[pm, k]$ 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, $i = 1, 2, \cdots, m-1$.

The search is initialized with r given generator polynomials $c_0(x), c_1(x), \cdots, c_{r-1}(x)$, 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 $c_r(x)$ and $c_{r+1}(x)$ must be chosen from two sets of polynomials $S_t(x)$ and $S_q(x)$, respectively, where

$$wt(c_0(x)) + wt(c_1(x)) + \cdots + wt(c_{r-1}(x)) + t + q > d.$$

Only the polynomials in the chosen sets are examined exhaustively. For each possible choice, the program produces its codewords 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

Manuscript received November 8, 1993; revised January 26, 1994. This paper was presented in part at ISIT '94, Norway, 1994.

The author was with the Department of Electrical Engineering, Linköping University, Sweden. He is now in the Technical Department, University of Kristianstad, 281 38 Hässleholm, Sweden.

IEEE Log Number 9404936.

TABLE I
NEW QUASI-CYCLIC CODES

QC Code	d_{min}	d_{BV}	m	$c_i(x)$
[60, 19]	18	17-20	20	3, 415, 463357
[81, 20]	26	25-30	27	4551, 72341, 33267167
[66, 21]	20	19-22	22	3, 10567, 443671
[82, 21]	25	24-30	41	16051207, 1136315123
[84, 20]	28	27-32	21	215, 157, 10345, 2737733
[100,20]	34	33-40	25	41, 515433, 1367143, 3237107

significant coefficient on the right, where d_{BV} is the bound on the minimum distance given in [6].

For example, the best known binary linear code with block length $n = 60$, dimension $k = 19$ has a minimum distance $d = 17$. Let $a(x) = 1 + x$, $c_0(x) = a(x)$. Then, $S_4(x)$ and $S_{12}(x)$ are formed with $|S_4(x)| = 245$ and $|S_{12}(x)| = 8509$. To find a QC [60, 19] code with minimum distance $d = 18 > 17$, the program chose two polynomials from $S_4(x)$ and $S_{12}(x)$, respectively. There are $245 \times 8509 = 2\ 084\ 705$ possible choices, and this number of choices can be examined in a short time. A [60, 19, 18] code is thus found as listed in Table I. If polynomials are not grouped according to their weights, and an exhaustive method is used, there are still about $(2^{19}/20)^2 = 2.56 \times 2^{28}$ possible choices, although $c_0(x)$ is given, and it may be impossible to try all of these possibilities.

III. CONCLUSION

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. Many other QC codes which attain the lower bounds have been also obtained, and they are available from the author upon the request.

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

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

[2] ——, "Nine good rate $(m - 1)/pm$ quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1366–1369, July 1992.

[3] ——, "Twelve good rate $(m - r)/pm$ quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 39, 1993.

[4] H. C. A. van Tilborg, "On quasi-cyclic codes with rate $1/m$," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 628–630, Sept. 1978.

[5] G. E. Sequin and G. Drolet, "The theory of 1-generator quasi-cyclic codes," manuscript, Dep. Elec. Comput. Eng., Royal Military College of Canada, Kingston, Ont., June 1990.

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

Two New Rate $2/p$ Binary Quasi-Cyclic Codes

T. Aaron Gulliver, *Member, IEEE*, and Vijay K. Bhargava, *Fellow, IEEE*

***Abstract*—A class of rate $2/p$ quasi-cyclic codes can be characterized in terms of $m \times m$ circulant matrices. In this correspondence, two new codes with parameters (80, 10, 35) and (95, 10, 42) are presented which improve the known lower bound on the maximum possible minimum distance. The former code can be extended with an even parity check bit to an (81, 10, 36) code that establishes that $d_2(81, 10) = 36$.**

***Index Terms*—Quasi-cyclic codes, best binary linear codes**

I. INTRODUCTION

A linear (n, k, d) code C over GF(2) can be represented as the rowspace of a $k \times n$ binary generator matrix G with rows composed of k linearly independent codewords of C. One of the most fundamental and challenging problems in coding theory is to find a linear (n, k) code achieving the maximum possible minimum distance d, which is the minimum of the Hamming weights of the 2^k codewords. This is denoted as $d_2(n, k)$. A related problem is that of finding the smallest n such that an (n, k) code exists with a given d. For binary linear codes, Brouwer and Verhoeff [1] have tabulated bounds on $d_2(n, k)$ for n, $k \leq 127$. In this correspondence, a subset of the class of quasi-cyclic codes is investigated to improve these bounds.

A code is called *quasi-cyclic* (QC) if there is some integer s such that every cyclic shift of a codeword by s places is again a codeword [2], [3]. The generator matrices of many QC codes can be characterized in terms of $m \times m$ circulant matrices [2], of the form,

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

so that

$$G = \begin{bmatrix} C_{1,1} & C_{1,2} & C_{1,3} & \cdots & C_{1,p} \\ C_{2,1} & C_{2,2} & C_{2,3} & \cdots & C_{2,p} \\ \vdots & \vdots & \vdots & & \vdots \\ C_{h,1} & C_{h,2} & C_{h,3} & \cdots & C_{h,p} \end{bmatrix}. \tag{2}$$

The ring of $m \times m$ circulant matrices over GF(q) is isomorphic to the algebra of polynomials in the ring $f[x]/(x^m - 1)$ if C_i is mapped onto the polynomial, $c_i(x) = c_{0i} + c_{1i}x + c_{2i}x^2 + \cdots + c_{m-1,i}x^{m-1}$, formed from the entries in the first row of C_i [2].

Most known QC codes have $h = 1$, whereas in the correspondence, new QC codes are constructed with $h = 2$.

Manuscript received October 26, 1993; revised December 30, 1993. This work was supported in part by the Natural Science and Engineering Research Council of Canada.

T. A. Gulliver is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, Ont. K1S 5B6, Canada.

V. K. Bhargava is with the Department of Electrical and Computer Engineering, Victoria, B.C. V8W 3P6, Canada.

IEEE Log Number 9405084.