Some Nonbinary Power Residue Codes[1]

T. Aaron Gulliver
Department of Electrical and Electronic Engineering
University of Canterbury
Christchurch, New Zealand
gulliver@elec.canterbury.ac.nz
and
Vijay K. Bhargava
Department of Electrical and Computer Engineering
University of Victoria
P.O. Box 3055, MS 8610,
Victoria, B.C. Canada V8W 3P6
bhargava@ece.uvic.ca.

Abstract

Nonbinary power residue codes are constructed using the relationship between these codes and quasi-cyclic codes. Eleven of these codes exceed the known lower bounds on the maximum possible minimum distance of a linear code.

Keywords: power residues, quasi-cyclic codes, optimal codes

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

1 Introduction

Let $GF(q)$ denote the Galois field of q elements, and let $V(n,q)$ denote the vector space of all ordered n-tuples over $GF(q)$. A linear $[n,k]$ code C of length n and dimension k over $GF(q)$ is a k-dimensional subspace of $V(n,q)$. An $[n,k,d]$ code is an $[n,k]$ code with minimum Hamming distance d. The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{x \in GF(p)^n | \, x \cdot y = 0 \text{ for all } y \in C\}$. Let A_i be the number of codewords of weight i in C. Then the numbers $A_0, \cdots, A_n$ form the weight distribution of C.

A central problem in coding theory is that of optimising one of the parameters n, k and d for given values of the other two. One version is to find $d_q(n,k)$, the largest value of d for which there exists an $[n,k,d]$ code over GF(q). Another is to find $n_q(k,d)$, the smallest value of n for which there exists an $[n,k,d]$ code over GF(q). A code which achieves either of these values is called *optimal*. Tables of bounds on $n_q(k,d)$ for $q = 2,3,4,5,7,8$ and 9 are maintained by Brouwer [2].

The Griesmer bound is a well-known lower bound on $n_q(k,d)$

$$n_q(k,d) \geq g_q(k,d) = \sum_{j=0}^{k-1} \lceil \frac{d}{q^j} \rceil, \tag{1}$$

where $\lceil x \rceil$ denotes the smallest integer $\geq x$. For $k \leq 2$, the Griesmer bound is met for all q and d. In addition, most values of $n_q(3,d)$ have been determined [2]. For larger dimensions, far less is known. Eleven codes are presented here which improve the lower bounds on minimum distance ($q \leq 9$). Two of these codes meet the upper bound and so are optimal. Codes over larger fields are given for which tables of bounds do not yet exist ($q > 9$), but eleven meet the Griesmer bound (1). These codes are presented in the next section.

2 Power Residue Codes

The search for optimal codes is difficult because of the large number of possible generator matrices. This problem is very acute for codes over nonbinary fields, where an exhaustive search of all codes is not tractable even for small dimensions. For larger dimensions, constructive techniques can be used. In this paper, the class of power residue (PR) codes are considered.

Power residue codes are cyclic codes which can be transformed into quasi-cyclic (QC) codes using the Normal Basis Theorem [3]. The resulting QC codes over GF(3) and GF(4) have previously been used to initialise stochastic search algorithms [5, 6]. The codes obtained confirm that many PR codes are good codes [1]. This motivates the investigation of these codes over other fields in search of those which improve the bounds on minimum distance. In this paper PR codes are constructed over GF(q) for $q = 5, 7, 8, 9, 11, 13, 16, 17$ and 19. The technique employed to find these codes is presented below.

Let m be the order of q mod n, ($q^m \equiv 1 \bmod n$), n a prime. Then if m divides $(n-1)$, i.e., $n = ems + 1$, a cyclic (n, em), es-th power residue code C exists. Using a normal basis, C can be transformed into an equivalent code C^* formed of $m \times m$ circulant matrices and the all 1's column. The punctured code resulting from deleting the all 1's column is called *quasi-cyclic*.

A rate $1/s$ QC code has an $m \times ms$ generator matrix of the form

$$G = [B_1, B_2, \ldots, B_s], \tag{2}$$

where B_i is an $m \times m$ circulant matrix given by

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{m-1} \\ b_{m-1} & b_0 & b_1 & \cdots & b_{m-2} \\ b_{m-2} & b_{m-1} & b_0 & \cdots & b_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ b_1 & b_2 & b_3 & \cdots & b_0 \end{bmatrix}, \tag{3}$$

with $b_i \in$ GF(q). The algebra of $m \times m$ circulant matrices over GF(q) is isomorphic to the algebra of polynomials in the ring GF(q)$[x]/(x^m - 1)$ if B_i is mapped onto the polynomial

$$b_i(x) = b_{0,i} + b_{1,i}x + b_{2,i}x^2 + \cdots + b_{m-1,i}x^{m-1},$$

formed from the entries in the first row of B_i [7]. The $b_i(x)$ are called *defining polynomials*.

To illustrate the construction of PR codes, consider the following example. Let $n = 11$ and $q = 5$, then $5^5 = 3125 \equiv 1 \pmod{11}$. Thus we have an (11,5) PR code over GF(5) composed of two 5×5 circulant matrices

and an all 1's column, (in this case $e = 1, s = 2$ and $m = 5$). By definition [3], this is a cyclic code over GF(5) with generator matrix

$$G = [1, \alpha, \alpha^1, \alpha^2, \ldots, \alpha^{10}], \tag{4}$$

where α is a primitive 11th root of unity over GF(5). To form the circulant matrices, the columns of G are rearranged according to the cyclic classes mod 11 over GF(5), i.e.

$$\begin{array}{ccccccc} \{ & x_1, & qx_1, & q^2x_1, & q^3x_1, & q^4x_1 & \}; \\ \{ & x_2, & qx_2, & q^2x_2, & q^3x_2, & q^4x_2 & \} \end{array}$$

Substituting $x_1 = 1, x_2 = 2$ and $q = 5$, we obtain

$$\begin{array}{ccccc} 1, & 5, & 3, & 4, & 9 \\ 2, & 10, & 6, & 8, & 7 \end{array}$$

Thus G becomes

$$G = [1, \alpha, \alpha^5, \alpha^3, \alpha^4, \alpha^9, \alpha^2, \alpha^{10}, \alpha^6, \alpha^8, \alpha^7], \tag{5}$$

Now, if these columns are represented in terms of a Normal Basis, α^5 becomes a cyclic shift of α, α^3 becomes a cyclic shift of α^5, and so on. (A normal basis can be formed from the roots of a primitive polynomial of degree m with linearly independent roots, as found in [4].) The resulting generator matrix is of the form

$$\begin{aligned} G &= [1, C_1, C_2], \\ &= \begin{bmatrix} 1 & 0 & 3 & 3 & 2 & 1 & 3 & 3 & 3 & 3 & 0 \\ 1 & 1 & 0 & 3 & 3 & 2 & 0 & 3 & 3 & 3 & 3 \\ 1 & 2 & 1 & 0 & 3 & 3 & 3 & 0 & 3 & 3 & 3 \\ 1 & 3 & 2 & 1 & 0 & 3 & 3 & 3 & 0 & 3 & 3 \\ 1 & 3 & 3 & 2 & 1 & 0 & 3 & 3 & 3 & 0 & 3 \end{bmatrix}. \end{aligned} \tag{6}$$

This code has weight distribution

Weight	Count
0	1
6	220
7	220
8	880
9	660
10	924
11	220

and the dual code has minimum distance 5. Both of these codes are optimal.

The related [10,5] QC code formed by deleting the all 1's column has weight distribution

Weight	Count
0	1
5	120
6	240
7	720
8	780
9	960
10	304

and is also optimal.

The PR codes are formulated according to (4) instead of the more common dual representation because the weight distribution of G can easily be computed.

Tables 1 to 9 present the PR codes obtained over GF(5), GF(7), GF(8), GF(9), GF(11), GF(13), GF(16), GF(17) and GF(19), respectively. A superscript ^{o} denotes an optimal code. Optimality was established either by meeting the upper bound in [2] or (1). Codes denoted ^{dz} are those with weights divisible by z. The codes which improve the bounds on minimum distance are denoted by ^{e}, and the defining polynomials for these codes are listed in Table 10 (excluding the all 1's column). The polynomials are listed with the lowest degree coefficient on the left, i.e., 2021 corresponds to the polynomial $x^3 + 2x^2 + 2$. For GF(8), if α is a root of the primitive

polynomial $x^3 + x^2 + 1$ over GF(2), then $2 \equiv \alpha, 3 \equiv \alpha^2$, etc. For GF(9), α is a root of the primitive polynomial $x^2 + x + 2$

References

[1] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw Hill, New York, N.Y., 1969.

[2] A.E. Brouwer, Linear code bound (server), Eindhoven University of Technology, Eindhoven, The Netherlands, `http://www.win.tue.nl/win/math/dw/voorlincod.html`.

[3] C.L. Chen, W.W. Peterson and E.J. Weldon, Jr., "Some results on quasi-cyclic codes," *Inform. and Control*, vol. 15, pp. 407-423, 1969.

[4] T.A. Gulliver, M. Serra and V.K. Bhargava, "The generation of primitive polynomials in GF(q) with independent roots and their applications for power residue codes, VLSI testing and finite field multipliers using normal basis," *Int. J. Electronics*, Vol. 71, No. 4, pp. 559-576, Oct. 1991.

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

[6] T.A. Gulliver and V.K. Bhargava, "Some best rate $1/p$ and $(p-1)/p$ quasi-cyclic codes over GF(3) and GF(4)," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1369-1374, 1992.

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

Table 1: Power Residue Codes Over GF(5)

code	d_{min}	dual code	d_{min}
$(11,5)^o$	6	$(11,6)^o$	5
$(13,4)^o$	8	$(13,9)^o$	4
(19,9)	8	(19,10)	7
$(31,3)^o$	25	$(31,28)^o$	3
(31,6)	19	(31,25)	4
(71,5)	50^{d5}	(71,66)	3
$(71,10)^e$	44	$(71,61)^e$	6
(313,8)	235	(313,305)	4
(521,10)	370	(521,511)	4
(601,12)	430	(601,589)	3
(829,9)	635^{d5}	(829,820)	3
(19531,7)	15625	(19531,19524)	3

Table 2: Power Residue Codes Over GF(7)

PR code	d_{min}	dual code	d_{min}
$(19,3)^o$	15	$(19,16)^o$	3
(19,6)	11	(19,13)	5
(19,9)	9	(19,10)	8
$(29,7)^e$	19	$(29,22)^e$	6
(37,9)	18	(37,28)	5
(43,6)	30	(43,37)	4
(191,10)	137	(191,181)	4
(1063,9)	864	(11063,1054)	3
(1201,8)	980	(1201,1193)	2
(2801,5)	2401^{d2401}	(2801,2796)	3
(4733,7)	4018^{d49}	(4733,4726)	3

Table 3: Power Residue Codes Over GF(8)

PR code	d_{min}	dual code	d_{min}
(7,3)	4	(7,4)	3
$(13,4)^o$	9	$(13,9)^o$	4
(17,8)	6	(17,9)	5
$(19,6)^e$	12	$(19,13)^{eo}$	6
(31,5)	16^{d4}	(31,26)	3
$(73,3)^o$	64	$(73,70)^o$	3
(73,6)	56^{d4}	(73,67)	3
(73,9)	28	(73,64)	3
(127,7)	64^{d16}	(127,120)	3
(151,5)	121	(151,146)	3
(241,8)	194	(241,233)	3
(337,7)	253	(337,330)	3

Table 4: Power Residue Codes Over GF(9)

code	d_{min}	dual code	d_{min}
$(7,3)^o$	5	$(7,4)^o$	4
$(11,5)^o$	6	$(11,6)^o$	5
$(13,3)^{d3}$	9	$(13,10)^o$	3
(13,6)	6	$(13,7)^o$	3
(17,8)	8	(17,9)	7
$(19,9)^o$	10	$(19,10)^o$	9
$(37,9)^e$	23	$(37,28)^e$	7
$(41,4)^{eo}$	34	$(41,37)^o$	4
(41,8)	22	(41,33)	5
$(61,5)^e$	49	$(61,56)^o$	4
$(73,6)^e$	57	(73,67)	3
(193,8)	145	(193,185)	4
(547,7)	470	(547,540)	4
(757,9)	486^{d3}	(757,748)	3
(1093,7)	729^{d243}	(1093,1086)	3

Table 5: Power Residue Codes Over GF(11)

code	d_{min}	dual code	d_{min}
$(7,3)^o$	5	$(7,4)^o$	4
$(19,3)^o$	16	(19,16)	3
(19,6)	12	$(19,13)^o$	6
(37,6)	27	(37,31)	5
(43,7)	30	(43,36)	5
(61,4)	52	(61,57)	4
(3221,5)	2905	(3221,3216)	3

Table 6: Power Residue Codes Over GF(13)

code	d_{min}	dual code	d_{min}
(17,4)	12	(17,13)	4
(61,3)	54	(61,58)	3
(61,6)	47	(61,55)	4
(127,6)	109	(127,121)	4
(157,6)	136	(157,151)	4

Table 7: Power Residue Codes Over GF(16)

code	d_{min}	dual code	d_{min}
(7,3)	4	(7,4)	3
(11,5)	6	(11,6)	5
(13,3)	11	(13,10)	4
(13,6)	6	(13,7)	5
(17,4)	12	(17,11)	4
(29,7)	20	(29,22)	6
(31,5)	16^{d4}	(31,26)	3
(41,5)	33	(41,36)	4
(43,7)	27	(43,36)	5
(113,7)	93	(113,106)	5
(127,7)	64^{d8}	(127,120)	3
(241,6)	216^{d4}	(241,235)	4
$(257,4)^o$	240	(257,253)	4

Table 8: Power Residue Codes Over GF(17)

code	d_{min}	dual code	d_{min}
$(13,6)^o$	8	$(13,7)^o$	7
(29,4)	24	(29,25)	4
$(307,3)^o$	289	$(307,304)^o$	3

Table 9: Power Residue Codes Over GF(19)

code	d_{min}	dual code	d_{min}
(127,3)	118	(127,124)	3
(127,6)	109	(127,121)	4
(151,5)	135	(151,146)	4
(181,4)	167	(181,177)	4
(911,5)	850	(911,906)	3

Table 10: Defining Polynomials for PR Codes

code	q	m	d	$b_i(x)$
[71, 10]	5	5	44	40324, 33422, 34013, 31123, 34140, 33002, 00204, 22120, 24022, 32032, 00334, 41114, 00312, 44401
		row 2		24022, 34003, 44401, 22120, 00312, 40020, 02330, 12331, 32440, 44111, 23342, 32320, 14034, 01334
[29, 7]	7	7	19	1426011, 2310145, 6600564, 5634450
[19, 6]	8	6	12	563521, 473476, 072744
[37, 9]	9	9	23	614450660, 647524066, 646383560, 783821714
[41, 4]	9	4	34	0657, 6818, 6883, 1315, 0221, 2501, 3761, 8838, 8207, 5278
[61, 5]	9	5	49	76466, 33530, 22184, 61755, 81578, 13402, 65466, 73646, 17817, 68662, 17260, 65025
[73, 6]	9	6	57	768418, 831107, 805666, 662512, 024275, 657216, 002342, 641503, 407114, 285414, 881083, 632076