JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **23**, No. 1, March 2010

TRIPLE CIRCULANT CODES BASED ON QUADRATIC RESIDUES

Sunghyu Han*

Abstract. One of the most interesting classes of algebraic codes is the class of quadratic residue (QR) codes over a finite field. A natural construction doubling the lengths of QR codes seems to be the double circulant constructions based on quadratic residues given by Karlin, Pless, Gaborit, et. al. In this paper we define a class of triple circulant linear codes based on quadratic residues. We construct many new optimal codes or codes with the highest known parameters using this construction. In particular, we find the first example of a ternary $[58, 20, 20]$ code, which improves the previously known highest minimum distance of any ternary $[58, 20]$ codes.

1. Introduction

One of the classical problems in algebraic coding theory is to find linear (or nonlinear) codes with the highest minimum distance given the code lengths and cardinalities. Geometrically, this problem corresponds to an extremal problem in the Hamming space. Furthermore, finding good linear or nonlinear codes may affect the sphere packing problems in Euclidean spaces [2]. When the code rate is $1/2$, quadratic residue (QR) codes have been an interesting family of codes with high minimum distances. Some examples of extended quadratic residue codes include the famous binary $[24, 12, 8]$ Golay code, the ternary $[12, 6, 6]$ Golay code, and the $[6, 3, 4]$ hexacode over $GF(4)$. It is still hard to determine the minimum distances of long binary QR codes as well as their asymptotic relative minimum distances (see [9], [11]).

Besides, Karlin [8] and Pless [10] found many good codes by systematic double circulant codes over $GF(2)$ and $GF(3)$ using quadratic

Received November 10, 2009; Accepted February 16, 2010.
2000 Mathematics Subject Classification: Primary 94B05.
Key words and phrases: double circulant codes, quadratic residues, triple circulant codes.

residues respectively. In [3], Gaborit gave a double circulant code scheme which generalizes the constructions of Karlin and Pless over any field and for any length $n = p^m$, where p is an odd prime. Furthermore, Karlin considered binary circulant $[3p+1, p+1]$ and $[3p, p]$ codes using quadratic residues and nonresidues [8].

The purpose of this paper is to generalize Karlin's latter construction using Gaborit's general scheme [3]. Our construction produces many good (extended) triple circulant codes over various finite fields. We give such codes over finite fields $GF(p)$, when $p = 2, 3, 4, 5, 7, 8$, and 9. Most of our codes are inequivalent to the codes in the Magma database [1]. In particular, we give a new $[58, 20, 20]$ ternary linear code which is better than any previously known $[58, 20, 19]$ codes. We also give a general result related to the automorphism groups of our codes. We have used Magma [1] for computations.

2. Preliminaries

First we describe some definitions from [10], [3]. We let l be a power of a prime number and q be a power of an odd prime number, and let $GF(l)$ ($GF(q)$, respectively) be the finite field with l (q, respectively) elements. Let r, s and t be elements of $GF(l)$. Assume that a is a one-to-one mapping from the set of integers $0, 1, \ldots, q-1$ to $GF(q)$. In the case when q is a prime, we choose a to be the identity. We now set the matrix $Q_q(r, s, t)$ to be the $q \times q$ matrix on $GF(l)$ labeled on its rows and its columns by the elements of $GF(q)$: $a(0), a(1), a(2), \ldots, a(q-1)$. The entries q_{ij} in $Q_q(r, s, t)$ for $0 \le i, j \le q-1$ are defined as $q_{ij} := \chi(a(j) - a(i))$, where χ: $GF(q) \to GF(l)$ is given by $\chi(0) = r$, $\chi(a(k)) = s$ if $a(k)$ is a nonzero quadratic residue in $GF(q)$, and $\chi(a(k)) = t$ if $a(k)$ is a quadratic nonresidue in $GF(q)$ for $0 \le k \le q-1$.

Now we are ready to describe our construction. Let $\alpha, \beta, r_1, s_1, t_1, r_2, s_2$, and t_2 be elements of $GF(l)$. We define $[3q, q]$ and $[3q+1, q+1]$ linear codes over $GF(l)$ using the following matrices, respectively:

$$P_q(r_1, s_1, t_1, r_2, s_2, t_2) = [I_q \mid Q_q(r_1, s_1, t_1) \mid Q_q(r_2, s_2, t_2)],$$

$$B_q(\alpha, \beta, r_1, s_1, t_1, r_2, s_2, t_2) = \left[\begin{array}{c|c|c|c} 1 & 0 \cdots 0 & \alpha \ \cdots \ \alpha & \beta \ \cdots \ \beta \\ \hline 0 & & & \\ \vdots & I_q & Q_q(r_1, s_1, t_1) & Q_q(r_2, s_2, t_2) \\ 0 & & & \end{array}\right].$$

We define $C(P_q)$ to be the code over $GF(l)$ generated by

$$P_q := P_q(r_1, s_1, t_1, r_2, s_2, t_2),$$

and $C(B_q)$ to be the code over $GF(l)$ generated by

$$B_q := B_q(\alpha, \beta, r_1, s_1, t_1, r_2, s_2, t_2).$$

Note that the codes Karlin constructed in [8] are special cases of ours given by $C(P_q(r, 1, 0, r, 0, 1))$ and $C(B_q(1, 1, r, 1, 0, r, 0, 1))$ over $GF(2)$ where q is a prime, $r = 0$ if $q \equiv 3 \pmod 8$, and $r = 1$ if $q \equiv -3 \pmod 8$. When q is a prime, P_q is equivalent to a systematic quasi-cyclic code of order 3, since $Q_q(r, s, t)$ is a circulant matrix.

3. Square root bound and automorphism group

In this section we discuss the square root bound of the code $C(P_p)$ over $GF(2)$ and the automorphism groups of $C(P_q)$ and $C(B_q)$ over $GF(l)$.

THEOREM 3.1. (Square root bound)

(i) *Let $p \equiv \pm 3 \pmod 8$ be a prime. For any $r, s, t \in GF(2)$, the minimum distance d_p of $C(P_p(0, 1, 0, r, s, t))$, $C(P_p(0, 0, 1, r, s, t))$, $C(P_p(r, s, t, 0, 1, 0))$, and $C(P_p(r, s, t, 0, 0, 1))$ over $GF(2)$ is*

$$d_p \geq \frac{2(p + \sqrt{p})}{\sqrt{p} + 3}.$$

(ii) *Let $p \equiv -1 \pmod 8$ be a prime. For any $r, s, t \in GF(2)$, the minimum distance d_p of $C(P_p(0, 1, 0, r, s, t))$, $C(P_p(0, 0, 1, r, s, t))$, $C(P_p(r, s, t, 0, 1, 0))$, and $C(P_p(r, s, t, 0, 0, 1))$ over $GF(2)$ is $d_p \geq \sqrt{p}$.*

(iii) *Let $p \equiv 1 \pmod 8$ be a prime. For any $r, s, t \in GF(2)$, the minimum distance d_p of $C(P_p(1, 1, 0, r, s, t))$, $C(P_p(1, 0, 1, r, s, t))$, $C(P_p(r, s, t, 1, 1, 0))$, and $C(P_p(r, s, t, 1, 0, 1))$ over $GF(2)$ is $d_p \geq \sqrt{p}$.*

Proof. For (i), the binary code $C(P_p(0, 1, 0, r, s, t))$ punctured on the last column block is identical with the double circulant quadratic residue codes C_p defined in [6] by Helleseth and Voloch. Thus its minimum distance d_p follows from [6, Theorem 1]. In a similar manner, one can see that this is true for $C(P_p(0, 0, 1, r, s, t))$, $C(P_p(r, s, t, 0, 1, 0))$, and $C(P_p(r, s, t, 0, 0, 1))$.

When $p \equiv -1 \pmod 8$, $C(P_p(0, 1, 0, r, s, t))$ punctured on the first and last column block is the well known quadratic residue code, hence

satisfies $d_p \geq \sqrt{p}$ (see [7, Ch. 6]). Similarly when $p \equiv 1 \pmod 8$, $C(P_p(1,1,0,r,s,t))$ punctured on the first and last column block is the well known quadratic residue code, hence satisfies $d_p \geq \sqrt{p}$ (see [7, Ch. 6]). Similarly, for each case the remaining three codes satisfy the square root bound. Thus this proves items (ii) and (iii). □

Next we discuss the automorphism groups of $C(P_q)$ and $C(B_q)$. It turns out that they contain a relatively large subgroup. First we define $\mathrm{Aut}(P_q)$ to be the automorphism group of $C(P_q)$, and $\mathrm{Aut}(B_q)$ to be the automorphism group of $C(B_q)$.

Let

$$e_0 = (1,0,\ldots,0), \ldots, e_i = (0,\ldots,0,1^{i+1},0,\ldots,0), \ldots, e_{q-1} = (0,\ldots,0,1)$$

be a set of basis vectors in $GF(l)^q$. For each b in $GF(q)$ we define the shift transformation $S(b)$ by $e_i S(b) = e_{a^{-1}[a(i)+b]},\ 0 \leq j \leq q-1$, and for any $b \neq 0$ in $GF(q)$ we define $T(b^2)$, the square transformation, by $e_i T(b^2) = e_{a^{-1}[b^2 a(i)]},\ 0 \leq j \leq q-1$.

Noting that the $C(P_q)$ and $C(B_q)$ are invariant under the action of $S(b)$ and $T(b^2)$ acting simultaneously on the three blocks of size p using the ideas in [3] or [10], we have the following.

THEOREM 3.2. *Let q be a power of an odd prime and l be a power of a prime. Then both $Aut(P_q)$ and $Aut(B_q)$ contain the group generated by permutation matrices corresponding to $S(b)$ and $T(b^2)$ and the global scalar multiplications by nonzeros, whose order is $q \cdot \frac{q-1}{2} \cdot (l-1)$.*

REMARK 3.3. The group orders in the conclusion of Theorem 3.2 are tight in the following sense:

$$|\mathrm{Aut}(B_{29}(0,1,0,0,1,0,1,0))| = 406 \text{ with } l = 2,$$
$$|\mathrm{Aut}(B_5(1,1,0,0,1,0,1,2))| = 20 \text{ with } l = 3,$$
$$|\mathrm{Aut}(P_7(0,0,1,1,2,1))| = 42 \text{ with } l = 3,$$
$$|\mathrm{Aut}(B_7(1,1,0,0,1,1,2,1))| = 42 \text{ with } l = 3,$$
$$|\mathrm{Aut}(B_{19}(0,1,1,0,1,0,1,2))| = 342 \text{ with } l = 3,$$
$$|\mathrm{Aut}(B_5(1,1,0,0,1,1,2,3))| = 40 \text{ with } l = 5,$$
$$|\mathrm{Aut}(P_7(0,0,1,1,2,3))| = 84 \text{ with } l = 5,$$
$$|\mathrm{Aut}(B_5(1,1,1,0,3,6,1,5))| = 60 \text{ with } l = 7,$$
$$|\mathrm{Aut}(P_7(0,1,2,0,1,5))| = 126 \text{ with } l = 7,$$
$$|\mathrm{Aut}(B_7(1,1,0,0,1,1,5,6))| = 126 \text{ with } l = 7.$$

4. Construction results

In this section we present construction results using $C(P_q)$ and $C(B_q)$. We have constructed several good linear codes over various finite fields including $GF(2)$, $GF(3)$, $GF(4)$, $GF(5)$, $GF(7)$, $GF(8)$, and $GF(9)$. To save space, we only show our results on optimal codes or codes with the best known parameters in Tables 1-7. The codes with other values of q are available upon request. In each table, the first column denotes the size of the ground field $GF(q)$, the second column gives the code length, the third column gives the code dimension, the fourth column shows the maximum minimum distance d_{max} among various $C(P_q)$ or $C(B_q)$, and the fifth column gives the best known minimum distance of linear codes (see [4]) of the same length and dimension as our code. In the sixth column, we compare our maximum minimum distance d_{max} with the best known minimum distance of linear codes and present a generator matrix P_q or B_q which corresponds to the maximum minimum distance code. (For Table 1 through Table 5, we give the order of automorphism group for the corresponding code.) The seventh column of Table 1 gives the total number of inequivalent codes $C(P_q)$ or $C(B_q)$ with d_{max} for all possibilities of $a, b, r_1, s_1, t_1, r_2, s_2, t_2$ except for the case $q = 29$, in which case we find one code with the best known minimum distance because of calculation complexity. In Table 3, w denotes a primitive element of $GF(4)$ satisfying $w^2 + w + 1 = 0$. Similarly, in Table 6, w denotes a primitive element of $GF(8)$ satisfying $w^3 + w + 1 = 0$, and in Table 7, w denotes a primitive element of $GF(9)$ satisfying $w^2 + 2w + 2 = 0$.

In particular, we construct a new $[58, 20, 20]$ ternary linear code which is better than previously known $[58, 20, 19]$ codes [5].

THEOREM 4.1. *The code $C(B_{19}(0, 1, 1, 0, 1, 0, 1, 2))$ is a $[58, 20, 20]$ ternary linear code.*

We note that the second row of $B_{19}(0, 1, 1, 0, 1, 0, 1, 2)$ is the following.

01000000000000000000 10110000101011111001 01221111212122221l2

The weight distribution of $C(B_{19}(0, 1, 1, 0, 1, 0, 1, 2))$ is given by

$$\begin{aligned} W_C(1, y) &= 1 + 6614y^{20} + 20862y^{21} + 25650y^{22} + 68172y^{23} + \\ &\quad 193458y^{24} + 437076y^{25} + \cdots . \end{aligned}$$

M. Grassl has figured out that the code $C(B_{19}(0, 1, 1, 0, 1, 0, 1, 2))$ can be constructed as follows [4].

(1) $[1, 1, 1]$ cyclic linear code over $GF(3)$ (the repetition code of length 1)
(2) $[57, 1, 19]$ quasi-cyclic of degree 3 linear code over $GF(3)$ with generating polynomials: $0, 0, x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
(3) $[57, 19, 20]$ quasi-cyclic of degree 3 linear code over $GF(3)$ with generating polynomials: $x^{17}, x^{17} + x^{16} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x + 1, x^{18} + 2x^{16} + x^{15} + x^{14} + 2x^{13} + 2x^{12} + 2x^{11} + 2x^{10} + x^9 + 2x^8 + x^7 + 2x^6 + x^5 + x^4 + x^3 + x^2 + 2x + 2$ (note that it is the code $C(P_{19}(1, 0, 1, 0, 1, 2))$.)
(4) $[57, 20, 19]$ linear code over $GF(3)$, the vector space sum: (2) + (3)
(5) [58, 20, 20] linear code over $GF(3)$, Construction X [9, p.581] using (3), (4) and (1)

REMARK 4.2. Inspired by our code, Grassl constructed a new ternary $[58, 21, 19]$ code which is better than previously known $[58, 21, 18]$ code using $C(P_{19}(1, 0, 1, 0, 1, 2))$ (see [4], [5].)

Acknowledgments

The author wish to thank the reviewers for valuable remarks which are used to improve this article. The author would like to thank J.-L. Kim(University of Louisville) for his helpful discussions on this research. The author also wish to thank M. Grassl for the information about ternary linear codes with parameters $[58, 20, 20]$ and $[58, 21, 19]$.

TABLE 1. Codes obtained from P_q and B_q over $GF(2)$

q	n	k	d_{max}	Linear, d	Comments, a code, $\|Aut\|$	#(Codes)
3	9	3	4	4	optimal, $P_3(0, 0, 1, 0, 1, 1)$, 48	3
3	10	4	4	4	optimal, $B_3(0, 1, 0, 0, 1, 0, 1, 1)$, 192	6
5	15	5	7	7	optimal, $P_5(1, 0, 1, 1, 1, 0)$, 20160	1
5	16	6	6	6	optimal, $B_5(0, 1, 0, 0, 1, 1, 0, 1)$, 120	8
7	21	7	8	8	optimal, $P_7(0, 0, 1, 0, 1, 1)$, 1344	1
7	22	8	8	8	optimal, $B_7(0, 1, 0, 1, 1, 0, 0, 1)$, 1344	1
13	39	13	12	12-13	best known, $P_{13}(0, 0, 1, 0, 1, 0)$, 156	2
19	57	19	16	16-19	best known, $P_{19}(1, 0, 1, 1, 1, 0)$, 342	2
29	87	29	24	24-28	best known, $P_{29}(0, 0, 1, 0, 1, 0)$, 812	≥ 1
29	88	30	23	23-28	best known, $B_{29}(0, 1, 0, 0, 1, 0, 1, 0)$, 406	≥ 1

TABLE 2. Codes obtained from P_q and B_q over $GF(3)$

q	n	k	d_{max}	Linear, d	Comments, a code, $\lvert Aut\rvert$
3	9	3	6	6	optimal, $P_3(0,1,1,1,1,2)$, 864
5	15	5	8	8	optimal, $P_5(0,1,1,0,1,2)$, 80
5	16	6	7	7	optimal, $B_5(1,1,0,0,1,0,1,2)$, 20
7	21	7	10	10	optimal, $P_7(0,0,1,1,2,1)$, 42
7	22	8	9	9-10	best known, $B_7(1,1,0,0,1,1,2,1)$, 42
17	51	17	18	18-23	best known, $P_{17}(0,0,1,0,1,2)$, 272
19	57	19	20	20-26	best known, $P_{19}(0,0,1,1,2,0)$, 684
19	58	20	20	19-26	exceeds, $B_{19}(0,1,1,0,1,0,1,2)$, 342

TABLE 3. Codes obtained from P_q and B_q over $GF(4)$

q	n	k	d_{max}	Linear, d	Comments, a code, $\lvert Aut\rvert$
3	9	3	6	6	optimal, $P_3(1,1,\omega,1,1,\omega^2)$, 162
5	15	5	8	8	optimal, $P_5(1,1,\omega,1,\omega,1)$, 2160
5	16	6	8	8	optimal, $B_5(1,1,1,1,\omega,\omega^2,\omega,\omega^2)$, 8640
7	21	7	11	11	optimal, $P_7(0,1,\omega,0,1,\omega^2)$, 378

TABLE 4. Codes obtained from P_q and B_q over $GF(5)$

q	n	k	d_{max}	Linear, d	Comments, a code, $\lvert Aut\rvert$
3	9	3	6	6	optimal, $P_3(0,1,1,1,1,2)$, 24
3	10	4	6	6	optimal, $B_3(1,1,0,1,1,2,3,3)$, 24
5	16	6	8	8-9	best known, $B_5(1,1,0,0,1,1,2,3)$, 40
7	21	7	11	11-12	best known, $P_7(0,0,1,1,2,3)$, 84

TABLE 5. Codes obtained from P_q and B_q over $GF(7)$

q	n	k	d_{max}	Linear, d	Comments, a code, $\lvert Aut\rvert$
3	9	3	6	6	optimal, $P_3(0,1,1,1,1,2)$, 36
3	10	4	6	6	optimal, $B_3(1,1,0,1,1,2,2,3)$, 36
5	15	5	9	9	optimal, $P_5(0,1,2,0,1,4)$, 120
5	16	6	9	9	optimal, $B_5(1,1,1,0,3,6,1,5)$, 60
7	21	7	12	12-13	best known, $P_7(0,1,2,0,1,5)$, 126
7	22	8	11	11-13	best known, $B_7(1,1,0,0,1,1,5,6)$, 126
11	33	11	16	16-20	best known, $P_{11}(0,1,2,0,1,3)$, 660

TABLE 6. Codes obtained from P_q and B_q over $GF(8)$

q	n	k	d_{max}	Linear, d	Comments
3	9	3	7	7	optimal, $P_3(1,\omega,\omega^5,1,\omega^3,\omega^2)$
3	10	4	6	6	optimal, $B_3(1,1,1,1,\omega,\omega,\omega^2,\omega^4)$
5	16	6	9	9-10	best known, $B_5(1,1,1,\omega,\omega^2,\omega,\omega^5,1)$
7	21	7	12	12-13	best known, $P_7(1,\omega,\omega^2,1,\omega,\omega^4)$

TABLE 7. Codes obtained from P_q and B_q over $GF(9)$

q	n	k	d_{max}	Linear, d	Comments
3	9	3	7	7	optimal $P_3(1, \omega, \omega^3, 1, \omega^3, \omega)$
3	10	4	7	7	optimal $B_3(1, 1, 1, \omega, \omega^3, 2, \omega^7, \omega^5)$
7	21	7	12	12-13	best known $P_7(1, \omega, 2, 1, \omega, \omega^6)$
7	22	8	12	12-13	best known $B_7(1, 1, 1, \omega, 2, \omega, \omega^2, \omega^7)$

References

[1] J. Cannon and C. Playoust, *An Introduction to Magma,* University of Sydney, Sydney, Australia, 1994.

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups,* third ed., Springer, New York, 1999.

[3] P. Gaborit, *Quadratic double circulant codes over fields,* J. Combin. Theory Ser. A **97** (2002) 85–107.

[4] M. Grassl, *Bounds on the minimum distance of linear codes,* online available at http://www.codetables.de. Accessed on 01-08-2008.

[5] M. Grassl, Personal Communication, Jan. **8**, 2008.

[6] T. Helleseth and J. F. Voloch, *Double circulant quadratic residue codes,* IEEE. Trans. Inform. Theory, **50** (2004) 2154–2155.

[7] W. C. Huffman and V. Pless, *Fundamentals of Error-correcting Codes,* Cambridge University Press, Cambridge, 2003.

[8] M. Karlin, *New binary coding results by circulants,* IEEE Trans. Inform. Theory **15** (1969) 81–92.

[9] F. J. McWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* Amsterdam, The Netherlands: North-Holland Mathematical Library, 1977.

[10] V. Pless, *Symmetry codes over $GF(3)$ and new five-designs,* J. Combinatorial Theory, **12** (1972) 119–142.

[11] V. S. Pless and W. C. Huffman, eds., *Handbook of Coding Theory,* Elsevier, Amsterdam, 1998.

*

School of Liberal Arts
Korea University of Technology and Education
Cheonan 330-708, Republic of Korea
E-mail: sunghyu@kut.ac.kr