Double Circulant Self-Dual Codes over GF(5)

T. Aaron Gulliver and Masaaki Harada[1]

Abstract

All distinct double circulant self-dual codes over $GF(5)$, with a minimum weight which is highest among all double circulant self-dual codes, have been found for each length $n \leq 24$. For lengths 14, 16 and 20, these codes are extremal. In this paper, we characterize these extremal double circulant self-dual codes. In particular, a classification of extremal double circulant self-dual codes of length 14 is given. We present other double circulant codes which improve the lower bounds on the highest possible minimum weight. A classification of double circulant self-dual codes with parameters $[18, 9, 7]$ and $[24, 12, 9]$ is also given.

Keywords: self-dual codes, double circulant codes

1 Introduction

A linear $[n, k]$ code C over $GF(p)$ is a k-dimensional vector subspace of $GF(p)^n$, where $GF(p)$ is the Galois field with p elements, p prime. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. Two codes C and C' over $GF(p)$ are *equivalent* if there exists an n by n monomial matrix P over $GF(p)$ with $C' = C \cdot P = \{xP \mid x \in C\}$. The dual code $C^{\perp}$ of C is

[1]T. Aaron Gulliver is with the Department of Electrical and Electronic Engineering, University of Canterbury, Christchurch, New Zealand, gulliver@elec.canterbury.ac.nz. Masaaki Harada is with the Department of Mathematical Sciences, Yamagata University, Yamagata 990, Japan, harada@ksmath1.kj.yamagata-u.ac.jp

defined as $C^{\perp} = \{x \in GF(p)^n |\ x \cdot y = 0 \text{ for all } y \in C\}$. C is *self-dual* if $C = C^{\perp}$.

A *pure double circulant* code has a generator matrix of the form $[\ I\ ,\ R\ ]$ where I is the identity matrix of order n and R is an n by n circulant matrix. A $[2n, n]$ code over $GF(p)$ with generator matrix of the form

$$\begin{bmatrix} & \alpha & \beta & \cdots & \beta \\ & \gamma & & & \\ I & \vdots & & R' & \\ & \gamma & & & \end{bmatrix}, \tag{1}$$

where R' is an $n-1$ by $n-1$ circulant matrix, and α, β and $\gamma \in GF(p)$, is called a *bordered double circulant* code. These two families of codes are collectively called *double circulant* codes [4].

All self-dual codes over $GF(5)$ are classified in [3] for lengths $n \leq 12$. For larger lengths, some interesting self-dual codes were given in [3]. The highest possible minimum weight was also given for lengths $n \leq 24$. A self-dual code with the highest minimum weight is called *extremal.*

By exhaustive search, we have found all distinct double circulant self-dual codes over $GF(5)$ with a minimum weight which is highest among all double circulant self-dual codes for each length $n \leq 24$. For lengths $14, 16$ and 20, these codes are extremal. In Section 2, we characterize these extremal double circulant self-dual codes. In particular, a classification of extremal double circulant self-dual codes of length 14 is given. In Section 3, we present other double circulant codes which improve the lower bounds on the highest possible minimum weight. A classification of double circulant self-dual codes with parameters $[18, 9, 7]$ and $[24, 12, 9]$ is also given. Our notation and terminology for coding theory follow that in [4].

2 Extremal Double Circulant Codes

First we present three lemmas which are useful in checking the equivalences of double circulant self-dual codes. These lemmas can easily be proven.

Lemma 1 *If the matrix* $[\ I\ ,\ A\ ]$ *generates a self-dual code* C *over* $GF(5)$, *then the matrices* $[\ I\ ,\ 4A\ ]$, $[\ I\ ,\ A^T\ ]$ *and* $[\ I\ ,\ 4A^T\ ]$ *also generate self-dual codes which are equivalent to* C.

Lemma 2 *Let C, C', C'' and C''' be codes with generator matrices of the form $[\ I\ ,\ A\ ]$, $[\ I\ ,\ A'\ ]$, $[\ I\ ,\ A''\ ]$ and $[\ I\ ,\ A'''\ ]$, respectively, where*

$$A = \begin{bmatrix} \alpha & \beta & \cdots & \beta \\ \gamma & & & \\ \vdots & & R & \\ \gamma & & & \end{bmatrix}, \quad A' = \begin{bmatrix} -\alpha & \beta & \cdots & \beta \\ -\gamma & & & \\ \vdots & & R & \\ -\gamma & & & \end{bmatrix},$$

$$A'' = \begin{bmatrix} -\alpha & -\beta & \cdots & -\beta \\ \gamma & & & \\ \vdots & & R & \\ \gamma & & & \end{bmatrix} \text{ and } A''' = \begin{bmatrix} \alpha & -\beta & \cdots & -\beta \\ -\gamma & & & \\ \vdots & & R & \\ -\gamma & & & \end{bmatrix},$$

and R is a square matrix. Then C, C', C'' and C''' are equivalent.

Lemma 3 *Let C and C' be codes with generator matrices of the form $[\ I\ ,\ A\ ]$ and $[\ I\ ,\ A'\ ]$, respectively. If there are permutation matrices P and Q such that $A' = PAQ$, then the codes C and C' are equivalent.*

2.1 Length 14

Sixteen distinct pure double circulant $[14, 7, 6]$ codes were found. The first row of R for four of these codes is given in Table 1. All codes can be found from the four codes using Lemmas 1 and 2. In the remainder of this paper, we provide only those codes which must be checked further for equivalence. All distinct codes can be found from these, as shown above. Table 2 gives the first row of R' for bordered double circulant codes with these parameters along with the values of α, β and γ in the matrix (1). These codes have the same weight distribution, which is given in Table 3.

Table 1: Pure double circulant $[14, 7, 6]$ codes.

code	first row of R	code	first row of R
$C_{14,1}$	1424110	$C_{14,2}$	4344110
$C_{14,3}$	3414410	$C_{14,4}$	2122311

Let R_i be the matrix R or R' for the code $C_{14,i}$ then it is easy to see that there are permutation matrices P and Q such that $PR_iQ = R_{i+1}$ for $i = 1, 2$ and 5. By Lemma 3, $C_{14,1}, C_{14,2}$ and $C_{14,3}$ are equivalent, and $C_{14,5}$ and $C_{14,6}$ are equivalent.

Table 2: Bordered double circulant $[14, 7, 6]$ codes.

code	first row of R'	α	β	γ	code	first row of R'	α	β	γ
$C_{14,5}$	203410	0	2	2	$C_{14,6}$	201430	0	2	2

Table 3: Weight distribution of the $[14, 7, 6]$ codes.

Weight	Number
0	1
6	252
7	392
8	3472
9	4872
10	16324
11	15848
12	22708
13	10528
14	3728

In order to determine the inequivalence of the remaining codes, a method given in [2] is employed. Let C be a self-dual $[2n, n, d]$ code. Let $M = (m_{ij})$ be the A_d by $2n$ matrix with rows composed of the codewords of weight d in C, where A_i denotes the number of codewords of weight i in C. For an integer k $(1 \leq k \leq 2n)$, let $n(j_1, \ldots, j_k)$ be the number of r $(1 \leq r \leq A_d)$ such that $m_{rj_1} \cdots m_{rj_k} \neq 0$ for $1 \leq j_1 < \ldots < j_k \leq 2n$. We consider the set

$$S = \{n(j_1, \ldots, j_k) | \text{ for any distinct } k \text{ columns } j_1, \ldots, j_k \}.$$

Let $M(k)$ and $m(k)$ be the maximal and minimal numbers in S, respectively. Since two equivalent codes have the same S, these numbers are invariant under the equivalence of codes.

For the remaining three codes, we have determined the values $(M(k), m(k),\ 1 \leq k \leq 5)$, and these are given in Table 4. This table provides the following result:

Theorem 4 *There are exactly three inequivalent extremal double circulant self-dual* $[14, 7, 6]$ *codes. Two of them are pure double circulant.*

Table 4: Inequivalence of the $[14, 7, 6]$ codes.

codes	$M(1)$	$m(1)$	$M(2)$	$m(2)$	$M(3)$	$m(3)$	$M(4)$	$m(4)$	$M(5)$	$m(5)$
$C_{14,1}$	108	108	52	32	20	8	8	0	4	0
$C_{14,4}$	108	108	48	24	20	8	12	0	4	0
$C_{14,5}$	108	108	48	28	20	8	12	0	4	0

2.2 Length 16

Previously, only one extremal $[16, 8, 7]$ code was known, namely Q_{16} [3]. We constructed 16 distinct extremal bordered double circulant self-dual codes with these parameters. Table 5 lists the first row of R' for the two codes which must be checked further for equivalence, along with the values of α, β and γ in the matrix (1). These codes and Q_{16} have the same weight distribution, which is given in Table 6. We have not been able to establish the equivalence or inequivalent of these codes.

Table 5: Bordered double circulant $[16, 8, 7]$ codes.

code	first row of R'	α	β	γ	code	first row of R'	α	β	γ
$C_{16,1}$	4434330	1	2	3	$C_{16,2}$	3323221	1	2	3

Table 6: Weight distribution of the $[16, 8, 7]$ codes.

Weight	Number
0	1
7	448
8	3360
9	4992
10	25536
11	38976
12	91392
13	82880
14	90048
15	41728
16	11264

2.3 Length 20

The extremal double circulant self-dual $[20, 10, 8]$ codes over $GF(5)$ are now described. By exhaustive search, 24 distinct pure double circulant codes were found. These codes can be divided into two classes by comparing their weight distributions, which are given in Table 7. The first row of R for only codes which must be checked further for equivalence is given in Table 8. For the bordered type, we list in Table 9 the first row of R' for the codes, along with the values of α, β and γ in the matrix (1). These codes have weight distribution W_1.

Table 7: Weight distributions of the $[20, 10, 8]$ codes.

	W_1	W_2
Weight	Number	Number
0	1	1
8	2280	1280
9	0	3200
10	23408	24848
11	72960	58560
12	241680	248480
13	437760	464960
14	1203840	1175840
15	1586880	1568000
16	2229840	2267240
17	1901520	1896720
18	1418160	1398960
19	528960	541760
20	118336	115776

Table 8: Pure double circulant $[20, 10, 8]$ codes.

code	first row of R	W	code	first row of R	W
$C_{20,1}$	2442212000	W_1	$C_{20,2}$	1402220240	W_1
$C_{20,3}$	1202320440	W_1	$C_{20,4}$	2423412000	W_1
$C_{20,5}$	2312201010	W_2	$C_{20,6}$	1320221010	W_2

Let R_i be the matrix R or R' for the code $C_{20,i}$ then it is easy to see that there are permutation matrices P and Q such that $PR_iQ = R_{i+1}$ for $i = 1, 3, 5, 7$ and 8. By Lemma 3, $C_{20,i}$ and $C_{20,i+1}$ are equivalent for $i = 1, 3$ and 5, and $C_{20,7}, C_{20,8}$ and $C_{20,9}$ are equivalent. Moreover, from

Table 9: Bordered double circulant $[20, 10, 8]$ codes.

code	first row of R'	α	β	γ
$C_{20,7}$	314322000	0	1	1
$C_{20,8}$	243023100	0	1	1
$C_{20,9}$	432302010	0	1	1

Table 10 we have the following:

Proposition 5 *Any extremal pure double circulant self-dual* $[20, 10, 8]$ *code with weight distribution* W_1 *is equivalent to* $C_{20,1}$ *or* $C_{20,3}$. *There is a unique extremal pure double circulant self-dual* $[20, 10, 8]$ *code with weight distribution* W_2, *up to equivalence. There is a unique extremal bordered double circulant self-dual* $[20, 10, 8]$ *code, up to equivalence.*

Remark. In all codes with weight distribution W_1 (resp. W_2), the nonzero coordinates of the minimum weight codewords form a 3-design (resp. 1-design) which cannot be explained by the Assmus-Mattson theorem (cf. [1]).

Table 10: Inequivalence of the $[20, 10, 8]$ codes.

codes	$M(1)$	$m(1)$	$M(2)$	$m(2)$	$M(3)$	$m(3)$	$M(4)$	$m(4)$	$M(5)$	$m(5)$
$C_{20,1}$	912	912	336	336	112	112	112	16	28	0
$C_{20,3}$	912	912	336	336	112	112	112	16	28	0
$C_{20,5}$	512	512	220	160	92	32	48	0	40	0
$C_{20,7}$	912	912	336	336	112	112	48	16	16	0

3 Largest Minimum Weights for Other Lengths

In the preceding section, extremal double circulant self-dual codes were presented for lengths 14, 16 and 20. In this section, double circulant self-dual codes are given which have the highest minimum weight, d_n, among known self-dual codes of lengths 18, 22 and 24. For lengths 18 and 22, these codes improve the lower bounds on d_n.

3.1 Length 18

It was shown in [3] that the highest possible minimum weight is $d_{18} \leq 8$. We found 12 distinct pure double circulant self-dual $[18, 9, 7]$ codes. The first row of R for only three codes which must be checked further for equivalence is given in Table 11. The weight distributions of these codes are given in Table 12. Let R_i be the matrix R for the code $C_{18,i}$ then it is easy to see that there are permutation matrices P and Q such that $PR_iQ = R_{i+1}$ for $i = 1$ and 2. It was previously not known whether self-dual $[18, 9]$ codes with minimum weight 7 existed.

Therefore we have the following:

Proposition 6 *There is a unique pure double circulant self-dual* $[18, 9, 7]$ *code, up to equivalence. Moreover we have* $7 \leq d_{18} \leq 8$.

Table 11: Pure double circulant $[18, 9, 7]$ codes.

code	first row of R	code	first row of R	code	first row of R
$C_{18,1}$	341333100	$C_{18,2}$	303334110	$C_{18,3}$	433031310

Table 12: Double circulant $[18, 9, 7]$ codes.

Weight	Number
0	1
7	72
8	2340
9	5040
10	28152
11	54360
12	185136
13	259560
14	461160
15	411072
16	359640
17	150192
18	36400

3.2 Length 22

We constructed 200 (resp. 144) distinct pure (resp. bordered) double circulant $[22, 11, 8]$ codes with 6 different weight distributions, which are given in Table 13. This establishes that $8 \leq d_{22} \leq 9$. In Table 14, we give only one code for each weight distribution due to space limitations.

Table 13: Weight distributions of the $[22, 11, 8]$ codes.

	W_1	W_2	W_3	W_4	W_5	W_6
Weight	Number	Number	Number	Number	Number	Number
0	1	1	1	1	1	1
8	880	660	440	460	660	660
9	1408	1760	2112	2040	1320	1720
10	16104	16984	17864	17948	18788	17148
11	49984	49280	48576	48600	48840	49240
12	262768	259160	255552	255156	251196	258436
13	593120	594880	596640	597440	605440	595840
14	1925264	1932480	1939696	1939880	1941720	1933320
15	3447488	3445728	3443968	3441680	3418800	3443280
16	7016372	7005240	6994108	6995720	7011840	7005840
17	8760664	8763480	8766296	8768368	8789088	8765808
18	10729400	10739960	10750520	10747500	10717300	10737900
19	8364928	8361760	8358592	8358680	8359560	8361560
20	5364832	5356912	5348992	5350796	5368836	5357996
21	1926144	1932480	1938816	1937680	1926320	1931920
22	368768	367360	365952	366176	368416	367456

Table 14: Double circulant $[22, 11, 8]$ codes.

pure		bordered				
first row of R	distribution	first row of R'	α	β	γ	distribution
24433420000	W_1	4442101200	2	1	1	W_4
34120331000	W_2	2444232200	2	1	1	W_5
32323022100	W_3	2444102010	2	1	1	W_6

3.3 Length 24

For length 24, a self-dual $[24, 12, 9]$ code was constructed in [3]. We found eight distinct bordered double circulant codes with minimum weight $d = 9$. Unfortunately, our search has established that no double circulant self-dual $[24, 12, 10]$ code exists. Thus the existence of a $[24, 12, 10]$ self-dual

code remains an open question. However we give a classification of double circulant self-dual $[24, 12, 9]$ codes. The first row of R' for the eight bordered double circulant codes is given in Table 15 along with the values of α, β and γ. The weight distributions of these codes are listed in Table 16. It follows from Lemmas 1 and 2 that the eight codes are equivalent. Thus we have the following:

Proposition 7 *There is a unique double circulant self-dual* $[24, 12, 9]$ *code, up to equivalence. There is no double circulant self-dual* $[24, 12, d \geq 10]$ *code.*

Table 15: Double circulant $[24, 12, 9]$ codes.

first row of R'	α	β	γ	first row of R'	α	β	γ
32333222320	0	2	2	23222333230	0	2	2
32333222320	0	2	3	23222333230	0	2	3
32333222320	0	3	2	23222333230	0	3	2
32333222320	0	3	3	23222333230	0	3	3

Table 16: Weight distributions of the $[24, 12, 9]$ codes.

Weight	Number
0	1
9	1056
10	11088
11	36960
12	212352
13	591360
14	2382336
15	5287040
16	13796640
17	23037696
18	39528720
19	46163040
20	49252896
21	35604800
22	20240352
23	6832320
24	1161968

Table 17: The highest possible minimum weights.

n	d_n	N_n	n	d_n	N_n	n	d_n	N_n
2	2	1	10	4	3	18	7 or 8	≥ 1 or
4	2	1	12	6	1	20	8	≥ 3
6	4	1	14	6	≥ 3	22	8 or 9	≥ 6 or
8	4	1	16	7	≥ 1	24	9 or 10	≥ 1 or

3.4 Summary

In summary, Table 17 presents the highest possible minimum weight d_n for extremal self-dual codes of length $n \leq 24$, along with the number N_n of known inequivalent codes.

References

[1] E.F. Assmus, Jr., and H.F. Mattson, Jr., *New 5-designs*, J. Combin. Theory 6 (1969) 122–151.

[2] M. Harada, *Extremal ternary self-dual codes and weighing matrices*, submitted.

[3] J.S. Leon, V. Pless and N.J.A. Sloane, *Self-dual codes over $GF(5)$*, J. Combin. Theory Ser. A 32 (1982) 178–194.

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