Circulant Based Extremal Additive Self-Dual Codes over GF(4)

T. Aaron Gulliver
Department of Electrical and Computer Engineering
University of Victoria
P.O. Box 3055, STN CSC, Victoria, B.C.
Canada V8W 3P6
and
Jon-Lark Kim
Department of Mathematics
810 Oldfather Hall, P.O. Box 880323
University of Nebraska–Lincoln,
Lincoln, NE, 68588-0323, USA

Abstract

It is well known [2] that the problem of finding stabilizer quantum-error-correcting codes is transformed into the problem of finding additive self-orthogonal codes over the Galois field GF(4) under a trace inner product. Our purpose is to classify the extremal additive circulant self-dual codes of lengths up to 15, and construct good codes for lengths $16 \leq n \leq 27$. We also classify the extremal additive 4-circulant self-dual codes of lengths $4, 6, 8, 12, 14$, and 16 and most codes of length 10, and construct good codes of even lengths up to 22. Furthermore, we classify the extremal additive bordered 4-circulant self-dual codes of lengths $3, 5, 7, 9, 11, 13, 15$ and 17, and construct good codes for lengths $19, 21, 23$, and 25. We give the current status of known extremal (or optimal) additive self-dual codes of lengths 12 to 27.

Index Terms Additive codes, circulant codes, 4-circulant codes, quantum codes.

1 Introduction

After the publication of [2], additive self-orthogonal codes over GF(4) under a trace inner product became of interest because of their correspondence to additive (or stabilizer) quantum-error-correcting codes (QECC throughout this paper). Several papers, for example, [1],[2],[3],[4],[6], [10] were devoted to classifying or constructing additive self-dual codes over GF(4). The Gray image of additive self-dual codes over GF(4) produces isodual binary codes [14, p. 199]. Moreover it was shown in [6],[11],[12] that certain vectors in some additive self-dual codes over GF(4) hold generalized t-designs as well as classical t-designs with possibly repeated blocks. These facts motivate the construction of additive self-dual quantum codes. As it is difficult to construct good quantum codes in general, we consider three simple constructions. One uses a circulant matrix over GF(4) and the others use four circulant matrices over GF(4). As will be shown, these constructions give many extremal self-dual codes. Our 4-circulant construction over GF(4) as well as the bordered 4-circulant construction are new although the circulant construction is well-known [15]. We next give some basic definitions about additive codes over GF(4) from [2],[4].

Let $\mathrm{GF}(4) = \{0, 1, \omega, \overline{\omega}\}$ with the convention that $2 = \omega$ and $3 = \overline{\omega}$ where $\overline{\omega} = \omega^2 = 1+\omega$. An *additive code* $\mathcal{C}$ *over* GF(4) *of length* n is an additive subgroup of $\mathrm{GF}(4)^n$. As $\mathcal{C}$ is a free GF(2)-module, it has size 2^k for some $0 \le k \le 2n$. We call $\mathcal{C}$ an $(n, 2^k)$ code. It has a basis, as a GF(2)-module, consisting of k basis vectors; a *generator matrix* of $\mathcal{C}$ is a $k \times n$ matrix with entries in GF(4) whose rows are a basis of $\mathcal{C}$. There is a natural inner product arising from the trace map. The *trace* map $\mathrm{Tr} : \mathrm{GF}(4) \to \mathrm{GF}(2)$ is given by

$$\mathrm{Tr}(x) = x + x^2.$$

In particular $\mathrm{Tr}(0) = \mathrm{Tr}(1) = 0$ and $\mathrm{Tr}(\omega) = \mathrm{Tr}(\overline{\omega}) = 1$. The *conjugate* of $x \in \mathrm{GF}(4)$, denoted $\overline{x}$, is the image of x under the Frobenius automorphism; in other words, $\overline{0} = 0$ $\overline{1} = 1$, and $\overline{\overline{\omega}} = \omega$. We now define the *trace inner product* of two vectors $\mathbf{x} = x_1x_2\cdots x_n$ and $\mathbf{y} = y_1y_2\cdots y_n$ in $\mathrm{GF}(4)^n$ to be

$$\mathbf{x}\star\mathbf{y} = \sum_{i=1}^{n} \mathrm{Tr}(x_i\overline{y_i}).$$

If $\mathcal{C}$ is an additive code, its *dual*, denoted $\mathcal{C}^\perp$, is the additive code $\{\mathbf{x} \in \mathrm{GF}(4)^n \mid \mathbf{x}\star\mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}$. If $\mathcal{C}$ is an $(n, 2^k)$ code, then $\mathcal{C}^\perp$ is an $(n, 2^{2n-k})$ code. As usual, $\mathcal{C}$ is (*trace*) *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^\perp$, and (*trace*) *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. In particular, if $\mathcal{C}$ is self-dual, then $\mathcal{C}$ is an $(n, 2^n)$ code. We remark that additive self-dual codes over GF(4) exist for any length n since the identity matrix I_n clearly generates a self-dual $(n, 2^n, 1)$ code. Any GF(4)-linear code is self-orthogonal under the Hermitian inner product if and only if it is a self-orthogonal additive code under the trace inner product [2]. Any linear Hermitian self-dual $[n, k, d]$ code is an additive self-dual $(n, 2^n, d)$ code. For example, the $[6, 3, 4]$ *Hexacode* is an additive self-dual $(6, 2^6, 4)$ code.

As usual, the *weight* $\mathrm{wt}(\mathbf{c})$ of $\mathbf{c} \in \mathcal{C}$ is the number of nonzero components of $\mathbf{c}$. The minimum weight d of $\mathcal{C}$ is the smallest weight of any nonzero codeword in $\mathcal{C}$. If $\mathcal{C}$ is an $(n, 2^k)$ additive code of minimum weight d, $\mathcal{C}$ is called an $(n, 2^k, d)$ code. $\mathcal{C}$ is *Type II* if $\mathcal{C}$ is self-dual and all codewords have even weight; Type II codes of length n exist only if n is even [4]. If $\mathcal{C}$ is self-dual but some codeword has odd weight (in which case the code cannot be GF(4)-linear), the code is *Type I* (see [14, Section 4.2]). There is a bound on the minimum weight of an additive self-dual code [14, Theorem 33]. If d_I and d_{II} are the minimum weights of additive self-dual Type I and Type II codes, respectively, of length $n > 1$, then

$$d_I \leq \begin{cases} 2\left\lfloor \frac{n}{6} \right\rfloor + 1 & \text{if } n \equiv 0 \pmod 6 \\ 2\left\lfloor \frac{n}{6} \right\rfloor + 3 & \text{if } n \equiv 5 \pmod 6 \\ 2\left\lfloor \frac{n}{6} \right\rfloor + 2 & \text{otherwise} \end{cases} \tag{1}$$

$$d_{II} \leq 2\left\lfloor \frac{n}{6} \right\rfloor + 2. \tag{2}$$

A code that meets the appropriate bound is called *extremal*. Note that (2) is the same as saying that $d = 2m + 2$ if $n = 6m + 2(i-1)$, with $i = 1, 2$, or 3. Type II codes meeting the bound d_{II} have a unique weight enumerator. This property is not true for Type I codes. A self-dual (with respect to the Hermitian inner product) linear code over GF(4) also satisfies (2), and such an extremal code is a $[6m, 3m, 2m + 2]$ code.

We say that two additive codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are *equivalent* provided there is a map sending the codewords of $\mathcal{C}_1$ onto the codewords of $\mathcal{C}_2$ where the map consists of a permutation of coordinates, followed by a scaling of coordinates by elements of GF(4), followed by conjugation of some of the coordinates. The *automorphism group* of $\mathcal{C}$, denoted $\mathrm{Aut}(\mathcal{C})$, consists of all maps which permute coordinates, scale coordinates, and conjugate coordinates that send codewords of $\mathcal{C}$ to codewords of $\mathcal{C}$.

We remark that it is possible that an additive code which is not linear can be equivalent under the definition of the equivalence of additive codes to a linear code over $GF(4)$. For example, consider two additive self-dual additive $(2, 2^2)$ codes with generator matrices

$$\begin{bmatrix} 1 & 1 \\ \omega & \omega \end{bmatrix} \text{and} \begin{bmatrix} 1 & 1 \\ \omega & \overline{\omega} \end{bmatrix}.$$

The first code is linear but the second is not. However they are equivalent by conjugating the second column of the first generator matrix.

Our purpose is to classify the extremal additive circulant self-dual codes of lengths up to 15 and construct good codes for lengths $16 \leq n \leq 27$. We also classify the extremal additive 4-circulant self-dual codes of lengths $4, 6, 8, 12, 14$, and 16 and most codes of length 10, and construct good codes for even lengths up to 22. Furthermore we classify the extremal additive bordered 4-circulant self-dual codes of lengths $3, 5, 7, 9, 11, 13, 15$ and 17 and construct good codes of lengths $19, 21$ and 23. We give the current status of known extremal (or optimal) additive Type I or Type II codes of lengths 12 to 27 in Table 1 as lengths ≤ 11 except $n = 10$ for Type I codes were done [1],[4],[6]. In this table, we list our numbers of Type I (Type II) self-dual codes in the fourth (seventh) column and compare them with the old numbers of Type I (Type II) self-dual codes in the third (sixth) column. When there are at least two possibilities for d, the old and new numbers of Type I or Type II codes mean the number of Type I or Type II codes with the lower bound for d. For example, for $n = 26$ there are at least 14 Type I codes with $d_I = 8$ whose existence was not known previously. When there is no reference in the New No. column of the table, codes with this distance are given in this paper.

2 Preliminaries

We first state the relationship between QECC and additive self-orthogonal codes over GF(4).

Theorem 2.1 (Theorem 2, [2]). *Suppose that $\mathcal{C}$ is an additive trace self-orthogonal $(n, 2^{n-k})$ code of $\mathrm{GF}(4)^n$ such that there are no vectors of weight $< d$ in $\mathcal{C}^\perp \backslash \mathcal{C}$. Then an additive quantum-error-correcting code with parameters $[[n, k, d]]$ is obtained.*

If there are no nonzero vectors of weight $< d$ in $\mathcal{C}^\perp$ in the above theorem, $\mathcal{C}$ is *pure* (or *nondegenerate*); otherwise it is *impure* (or *degenerate*) [2]. An $[[n, k, d]]$ QECC can correct $[(d-1)/2]$ errors, where k is the number of *encoded qubits* (*quantum bits*). An $[[n, 0, d]]$ code is pure by convention and corresponds to an additive self-dual $(n, 2^n, d)$ code [2].

The *Hermitian inner product* is defined as

$$\mathbf{x} \cdot \mathbf{y} = x_1\overline{y_1} + \cdots + x_n\overline{y_n} \in \mathrm{GF}(4),$$

for two vectors $\mathbf{x} = (x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_n)$ in $\mathrm{GF}(4)^n$.

Theorem 2.2 (Theorem 3, [2]). *A linear code $\mathcal{C}$ is self-orthogonal with respect to the trace inner product if and only if it is self-orthogonal with respect to the Hermitian inner product.*

Corollary 2.3. *There does not exist a linear trace self-dual $(n, 2^n)$ code of odd length n.*

We have found many good self-dual $[[n, 0]]$ (i.e. $(n, 2^n)$) codes using constructions based on circulant matrices. In the following sections we explain our construction methods. We did an exhaustive search up to length 15 (cyclic case), 16 (4-circulant case), and 17 (bordered 4-circulant case) in order to classify our codes. Then we determined the equivalence of two additive codes over GF(4) using the techniques in [4]. Therefore in the following, all codes have been obtained up to equivalence, except where noted otherwise. In what follows we use the convention that $2 = \omega$ and $3 = \overline{\omega}$.

3 Extremal additive circulant self-dual codes

An *additive circulant* $(n, 2^n)$ *code* over GF(4) has a circulant generator matrix of the following form

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ & & & \cdots & & \\ a_2 & a_3 & a_4 & \cdots & a_n & a_1 \end{pmatrix}, \tag{3}$$

where $a_i \in \mathrm{GF}(4)$ for $i = 1, \cdots, n$. Clearly an additive circulant $(n, 2^n)$ code generates an additive cyclic $(n, 2^n)$ code and so is generated by $(a_1 a_2 \cdots a_n)$ (with its cyclic shifts). It is known [2, Theorem 14] that any additive cyclic code over GF(4) is generated by one or two generators. Finding all additive (self-orthogonal) cyclic codes over GF(4) becomes infeasible for large lengths, say, ≥ 32 because there are many possibilities to check [2, Theorem 14]. We restrict our attention to one generator cyclic (i.e. one circulant matrix) codes because of their simple construction.

In this section, we classify the extremal additive circulant self-dual codes of lengths $3 \leq n \leq 15$ and construct good codes for lengths $16 \leq n \leq 30$.

The complete classification of extremal self-dual $[[n, 0, d]]$ codes of lengths $2 \leq n \leq 7$ was done in [6]. We will compare the equivalence of our circulant codes of lengths up to 6 with those in Table 1 and Table 2 of [6]. For this purpose, we explain the notation used in [6]. Let δ_n be the code of length n consisting of all codewords containing only 0's and an even number of 1's. Let ϵ_2 be the $[[2, 0, 2]]$ code. Let $\bar{\mathcal{C}}$ be the subcode of an additive self-dual code $\mathcal{C}$ generated by the weight 1 and 2 codewords of $\mathcal{C}$.

- It is straightforward to check that there is a unique circulant $[[3, 0, 2]]$ code $\mathcal{C}_3$. This code is generated by (211) and has an automorphism group of order 24. Thus $\mathcal{C}_3$ is a cyclic representation of the unique $[[3, 0, 2]]$ code $\mathcal{C}$ in Table 2 of [6] having $\bar{\mathcal{C}}$ as δ_3.

- There are exactly two Type II circulant $[[4, 0, 2]]$ codes $\mathcal{C}_{4,1}$ and $\mathcal{C}_{4,2}$ with generators (2010) and (2111), respectively. $\mathcal{C}_{4,1}$ has an automorphism group of order 288 and $\mathcal{C}_{4,2}$ has 192. It is easy to see that $\mathcal{C}_{4,1}$ is equivalent to the code [6] with $\bar{\mathcal{C}}$ as ϵ_2^2 and $\mathcal{C}_{4,2}$ to the code [6] with $\bar{\mathcal{C}}$ as δ_4. As there are only two Type II $[[4, 0, 2]]$ codes [6] we have shown that these codes have cyclic representations. There is only one Type I circulant $[[4, 0, 2]]$ code $\mathcal{C}_4$ which is generated by (1210), and has an automorphism group of order 32. This is equivalent to the unique Type I $[[4, 0, 2]]$ code [6] having $\bar{\mathcal{C}}$ as δ_2^2. For length $n = 5$ there is only one Type I circulant $[[5, 0, 3]]$ code $\mathcal{C}_5$ with generator (12100) with an automorphism group of order 120. This is equivalent to the unique Type I $[[5, 0, 3]]$ code in Table 2 of [6].

- There is only one Type I circulant $[[6, 0, 3]]$ code $\mathcal{C}_6$ with generator (121000) and an automorphism group order 48. This is equivalent to the unique Type I $[[6, 0, 3]]$ code in Table 2 of [6]. There is exactly one Type II circulant $[[6, 0, 4]]$ code generated by (321100).

This is a cyclic representation of the linear $[6, 3, 4]$ Hexacode over GF(4), which is in fact the unique Type II $[[6, 0, 4]]$ code.

From these results, we note that any extremal additive self-dual $[[n, 0, d]]$ code of length $n \leq 6$ has a cyclic representation as given above.

- There is only one Type I circulant optimal $[[7, 0, 3]]$ code $\mathcal{C}_7$ which is generated by (1210000) with $W_7(y) = 1 + 7y^3 + 21y^4 + 42y^5 + 42y^6 + 15y^7$ and an automorphism group of order 14. $\mathcal{C}_7$ must be equivalent to one of the three Type I $[[7, 0, 3]]$ codes in Table 1 of [6]. For length $n = 8$, there is only one Type II circulant $[[8, 0, 4]]$ code which is generated by (31201000) with $W_8(y) = 1 + 42y^4 + 168y^6 + 45y^8$ and an automorphism group of order 336. We checked that this code is equivalent to QC_8d in [4]. This code can be used for decoding one of the five classical binary doubly-even self-dual $[32, 16, 8]$ codes. (see [5].) For $n = 9$, there is only one Type I circulant $[[9, 0, 4]]$ code generated by (121210000) with $W_9(y) = 1 + 18y^4 + 72y^5 + 120y^6 + 144y^7 + 117y^8 + 40y^9$ and an automorphism group of order 18. This code is equivalent to QC_9h [4].

- There are exactly three Type I circulant $[[10, 0, 4]]$ codes $\mathcal{C}_{10,1}, \mathcal{C}_{10,2}$ and $\mathcal{C}_{10,3}$, generated by (1121100000), (1212100000) and (3122001000), respectively. $\mathcal{C}_{10,1}$ and $\mathcal{C}_{10,2}$ have weight enumerator $W_{10,1}(y) = 1+30y^4+32y^5+140y^6+320y^7+265y^8+160y^9+76y^{10}$, and $\mathcal{C}_{10,3}$ has weight enumerator $W_{10,2}(y) = 1+10y^4+72y^5+160y^6+240y^7+285y^8+200y^9+56y^{10}$. In the case of Type II codes, there are exactly 5 circulant $[[10, 0, 4]]$ codes $\mathcal{C}_{10,4}, \mathcal{C}_{10,5}, \mathcal{C}_{10,6}, \mathcal{C}_{10,7}$, and $\mathcal{C}_{10,8}$. They are generated by (3211110000), (3212110000), (2132210000), (1210001000), and (2220001000), respectively. All of these Type II codes have weight enumerator $W_{10,3}(y) = 1 + 30y^4 + 300y^6 + 585y^8 + 108y^{10}$. $\mathcal{C}_{10,5}$ is equivalent to d_{10}^{+} [14, Table XIV] or E_{10} in the notation of [13]. $\mathcal{C}_{10,6}$ is equivalent to e_5^{2+} [14, Table XIV] or B_{10} in the notation of [13]. Hence the remaining three codes are not equivalent to the two Hermitian linear $[10, 5, 4]$ codes over $GF(4)$.

Since there are many Type I and Type II $[[10, 0, 4]]$ codes [1],[4], we do not consider their equivalence further.

- We determined that there is no Type I circulant $[[11, 0, 5]]$ code even though there is a unique Type I $[[11, 0, 5]]$ code [4]. For length $n = 12$, there is only one circulant Type I $[[12, 0, 5]]$ code $\mathcal{C}_{12,1}$ with generator (102120100000). It has weight enumerator $W_{12,1}(y) = 1 + 48y^5 + 188y^6 + 432y^7 + 765y^8 + 1040y^9 + 972y^{10} + 528y^{11} + 122y^{12}$ and an automorphism group of order 24. Since this group order is distinct from those of the seven currently known codes in [4], $\mathcal{C}_{12,1}$ is new. For Type II codes of length 12, we know from [2] or [4] that there is only one circulant $[[12, 0, 6]]$ code, called the *dodecacode*.

- For $n = 13$, there are exactly two Type I optimal circulant $[[13, 0, 5]]$ codes $\mathcal{C}_{13,1}$ and $\mathcal{C}_{13,2}$, generated by (1023201000000) and (1203021000000), respectively. $\mathcal{C}_{13,1}$ has group order 52 and $\mathcal{C}_{13,2}$ has 156. Both have weight enumerator $W_{13,1}(y) = 1 + 39y^5 + 156y^6 + 468y^7 + 1053y^8 + 1690y^9 + 2028y^{10} + 1716y^{11} + 858y^{12} + 183y^{13}$. There are five previously known Type I $[[13,0,5]]$ codes. Four of these codes have weight enumerator $W_{13,2}(y) = 1+15y^5+236y^6+\cdots$ [4] and another is the shortened code q'_{14} from the extended quadratic residue code q_{14} which has weight enumerator $W_{13,1}$ and group order 156. We checked by Magma that $\mathcal{C}_{13,2}$ and q'_{14} are equivalent. Hence $\mathcal{C}_{13,1}$ is new.

- For $n = 14$, we obtained exactly three Type II circulant $[[14,0,6]]$ codes $\mathcal{C}_{14,1}, \mathcal{C}_{14,2}$, and $\mathcal{C}_{14,3}$. They are generated by

$$(21130201000000), (23331211000000) \text{ and } (13332120100000),$$

respectively. All three have weight enumerator $W_{14}(y) = 1 + 273y^6 + 2457y^8 + 7098y^{10} + 6006y^{12} + 549y^{14}$. We note that $\mathcal{C}_{14,1}$ is new since its group order 2184 was previously unknown [1]. Comparing these results with [1], we have the following.

Proposition 3.1. *There are at least 491 Type II* $[[14,0,6]]$ *codes.*

- For length $n = 15$, there are exactly three Type I circulant $[[15,0,6]]$ codes $\mathcal{C}_{15,1}, \mathcal{C}_{15,2}$, and $\mathcal{C}_{15,3}$. They are generated by

$$(123232100000000), (332021101000000) \text{ and } (332012201000000),$$

respectively. They have weight enumerator $W_{15}(y) = 1 + 145y^6 + 420y^7 + \cdots$. $\mathcal{C}_{15,2}$ is equivalent to c_{15} in Table 1 of [2], but the remaining codes are not equivalent to the two previously known $[[15,0,6]]$ codes [4]. Hence we have the following.

Proposition 3.2. *There are at least four inequivalent Type I* $[[15,0,6]]$ *codes.*

For lengths $n \geq 16$, it is not practical to check all generators. Instead, we considered a large number of generators, and constructed a number of circulant self-dual additive codes.

- For length $n = 16$ we found one Type I circulant $[[16,0,6]]$ code $\mathcal{C}_{16,1}$ with generator (1012321010000000). It has weight enumerator $W_{16,1}(y) = 1 + 120y^6 + 352y^7 + 1218y^8 + 3712y^9 + 7184y^{10} + 11328y^{11} + 14968y^{12} + 13952y^{13} + 8568y^{14} + 3424y^{15} + 709y^{16}$. We also found five Type II $[[16,0,6]]$ codes. They are generated by

$$(3103320010000000), (3120101010000000), (2110032010000000),$$
$$(2222120110000000) \text{ and } (2132000210000000),$$

respectively. These have the same automorphism group order 32 and weight enumerator $W_{16,2}(y) = 1 + 168y^6 + 2610y^8 + 14448y^{10} + 29400y^{12} + 17640y^{14} + 1269y^{16}$.

- For length $n = 17$ we found one Type I circulant $[[17,0,7]]$ code $\mathcal{C}_{17,1}$ with generator (12022202100000000). It has weight enumerator $W_{17}(y) = 1 + 408y^7 + 1530y^8 + 3400y^9 + 8160y^{10} + 17136y^{11} + 25704y^{12} + 28560y^{13} + 24480y^{14} + 15096y^{15} + 5661y^{16} + 936y^{17}$ and group order 16320. We checked with Magma that $\mathcal{C}_{17,1}$ is equivalent to the code S'_{18} shortened by deleting the first column from the unique linear Hermitian $[18, 8, 8]$ code S_{18} in [14, p. 277] (note that S_{18} is the extended cyclic code of length 18 over GF(4).)

For length $n = 18$ we did not not find any circulant Type I $[[18, 0, 7]]$ or Type II $[[18, 0, 8]]$ codes.

- For length $n = 19$ we found four Type I circulant $[[19, 0, 7]]$ codes $\mathcal{C}_{19,1}, \mathcal{C}_{19,2}, \mathcal{C}_{19,3}$ and $\mathcal{C}_{19,4}$. They are generated by

$$(1021112010000000000), (1021312010000000000),$$
$$(1023132010000000000) \text{ and } (1201310210000000000),$$

respectively. They have weight enumerator $W_{19}(y) = 1 + 228y^7 + 1026y^8 + 3496y^9 + 10488^{10} + 25308y^{11} + 50616y^{12} + 82992y^{13} + 106704y^{14} + 105564y^{15} + 79173y^{16} + 42408y^{17} + 14136y^{18} + 2148y^{19}$. The codes $\mathcal{C}_{19,1}, \mathcal{C}_{19,2}$, and $\mathcal{C}_{19,3}$ have group order 38, and $\mathcal{C}_{19,4}$ has group order 114.

- For length $n = 20$ we obtained two Type II circulant $[[20, 0, 8]]$ codes $\mathcal{C}_{20,1}, \mathcal{C}_{20,2}$. They are generated by (31133302001000000000) and (33232100011000000000), respectively. $\mathcal{C}_{20,1}$ has group order 6840 and $\mathcal{C}_{20,2}$ has group order 40. These have weight enumerator $W_{20}(y) = 1 + 1710y^8 + 20976y^{10} + \cdots$. We checked by Magma that $\mathcal{C}_{20,1}$ and $\mathcal{C}_{20,2}$ are not equivalent to the known two Hermitian linear $[20, 10, 8]$ codes [9] since the latter codes have group orders 8640 and 11520 as additive codes.

We could not find a Type I circulant $[[21, 0, 8]]$ code even though there exists a cyclic $[[21, 0, 8]]$ code with two generators in [14, Table XIV].

- For length $n = 22$ we obtained 14 Type II circulant $[[22, 0, 8]]$ codes. Their group orders are either 44 or 132. Their weight enumerator is $W_{22}(y) = 1 + 990y^8 + 18480y^{10} + \cdots$. Two of these codes are generated by (1110222231202211000000) and (2222113202202211000000) with group orders 44, 132, respectively.

- For length $n = 23$ we found two Type I circulant $[[23, 0, 8]]$ codes $\mathcal{C}_{23,1}$ and $\mathcal{C}_{23,2}$, with weight enumerators $W_{23,1}(y) = 1+598y^8+1564y^9+\cdots$ and $W_{23,2}(y) = 1+322y^8+2208y^9+\cdots$, respectively. Note that 8 is the highest known minimum weight for this length. The two codes are generated by

$$(11233133211000000000000) \text{ and } (12213122100000000000000),$$

respectively. Only one Type I circulant $[[23, 0, 8]]$ code, denoted c_{23}, was given in Table XV of [14]. We checked that $\mathcal{C}_{23,1}$ is equivalent to c_{23}. Hence $\mathcal{C}_{23,2}$ is new. For length $n = 24$ we found 51 Type II circulant $[[24, 0, 8]]$ codes. Unfortunately we could not find an extremal $[[24, 0, 10]]$ code, the existence of which would be quite interesting.

- For length $n = 25$ only one circulant code, denoted c_{25} was given in Table XV of [14]. It has $A_8 = 300$ and $A_{10} = 1275$. we obtained 13 Type I circulant $[[25, 0, 8]]$ codes with distinct weight distributions from c_{25}. For length $n = 26$ we constructed 14 Type I circulant $[[26, 0, 8]]$ codes with distinct weight distributions. Their group orders are either 52 or 104. For length $n = 27$ we found 15 Type I circulant $[[27, 0, 8]]$ codes with distinct weight distributions. All have group order 54. We also found one Type II circulant $[[28, 0, 10]]$ code $\mathcal{C}_{28,1}$, one Type I circulant $[[29, 0, 11]]$ code $\mathcal{C}_{29,1}$ and one Type II circulant $[[30, 0, 12]]$ code $\mathcal{C}_{30,1}$. We checked using Magma that $\mathcal{C}_{30,1}$ is equivalent to the extended quadratic residue code XQ_{29} and that $\mathcal{C}_{29,1}$ is equivalent to the code XQ'_{29} shortened from XQ_{29}. We remark that XQ'_{29} is different from the quadratic residue code Q_{29} which is a linear $[29, 15, 11]$ code over GF(4). It is easy to check that $\mathcal{C}_{28,1}$ is not linear. $\mathcal{C}_{28,1}$ has the same weight enumerator (see Table 2) as the three linear Hermitian self-dual $[28, 14, 10]$ codes [7],[8]. As linearity is not invariant under the equivalence of additive codes (see the remark following the equivalence definition in the Introduction), $\mathcal{C}_{28,1}$ may be equivalent to a shortened code from XQ'_{29} or one of the three linear Hermitian self-dual $[28, 14, 10]$ codes [7],[8]. We were unable to determine equivalence in either case.

We give generators for the codes of lengths 25 to 30 in Table 2. Here we omit zeros on the right of each generator. For lengths $n = 25, 26$ and 27 we give only five codes to save space. The complete list of codes can be obtained from the authors.

We summarize what is currently known about circulant $[[n, 0, d]]$ codes in Table 3. As before when there are at least two possibilities for d, our numbers of Type I or Type II codes mean the number of Type I or Type II codes with the lower bound for d.

4 Extremal additive 4-circulant self-dual codes

A 4-*circulant additive* $(n, 2^n)$ *code* of even length n has the following generator matrix

$$\begin{pmatrix} I_{n/2} & A_{n/2} \\ B_{n/2} & I_{n/2} \end{pmatrix}, \tag{4}$$

where $I_{n/2}$ is an identity matrix of size $n/2$ and $A_{n/2}, B_{n/2}$ are circulant matrices of the form (3).

A trivial example of both circulant and 4-circulant self-dual code is a $(2, 2^2, 2)$ code with generator matrix

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

This is equivalent to the linear code i_2 with generator matrix

$$\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}.$$

It is easy to see that there is only one self-dual $(2, 2^2, 2)$ code up to isomorphism.

Using the construction method (4), we obtained several new extremal additive self-dual codes which are 4-circulant. We classify the extremal additive 4-circulant self-dual codes of lengths $4, 6, 8, 12, 14$, and 16 and most codes of length 10. We also give several good codes with even lengths up to 22. Let matrices A_n and B_n in (4) have first rows r_1 and r'_1, respectively. In the following we only give $(r_1)(r'_1)$ to denote the corresponding 4-circulant code and refer to Section 3 for the weight enumerators, when possible.

- For length $n = 4$, there is only one Type II 4-circulant $[[4, 0, 2]]$ code. It is generated by (20)(20) and has group order 288. Also there is only one Type I 4-circulant $[[4, 0, 2]]$ code. It is generated by (20)(21) and has group order 32.

- For length $n = 6$, there is a unique Type II 4-circulant $[[6, 0, 4]]$ code. It has generators (211)(211). It is equivalent to the linear $[6, 3, 4]$ Hexacode. There is a unique Type I 4-circulant $[[6, 0, 3]]$ code. It is generated by (220)(202).

- For length $n = 8$, there are exactly two Type II 4-circulant $[[8, 0, 4]]$ codes, which are generated by (1210)(1012) and (3210)(3102), respectively. The automorphism group orders are 8064 and 336, respectively. Furthermore, there are exactly two Type I 4-circulant $[[8, 0, 4]]$ codes, which are generated by (1210)(1112) and (2220)(2122) and have group orders 128 and 384, respectively. See [4] for the equivalence with the known $[[8, 0, 4]]$ codes.

- For length $n = 10$, there are exactly 6 Type II 4-circulant $[[10, 0, 4]]$ codes, all with weight enumerator $W_{10,3}$. There are only two Type I 4-circulant $[[10, 0, 4]]$ codes, both with weight enumerator $W_{10,1}$. We list their generators below, with the first six corresponding to the Type II codes and the last two corresponding to the Type I codes.

(12100)(01102), (12100)(10012), (12100)(11112),
(22200)(20022), (21111)(21111), (22211)(31132),
(21200)(21120) and (22220)(20222).

Finally, we found that there are 91 Type I 4-circulant $[[10, 0, 4]]$ codes with $W_{10,2}$ before checking equivalence. We were not able to check the equivalence of these codes using Magma. One of these codes is generated by (22220)(30322). Thus we have shown that there are at least 9 4-circulant $[[10, 0, 4]]$ codes with three different weight enumerators.

- For length $n = 12$, there are no 4-circulant $[[12, 0, 6]]$ codes. However there are exactly two Type I 4-circulant $[[12, 0, 5]]$ codes with generators (122100)(011022) and (331200)(310202), denoted $D_{12,1}$ and $D_{12,2}$, respectively. Both have weight enumerator $W_{12,1}$. $D_{12,1}$ has an automorphism group of order 24 while $D_{12,2}$ has order 6. It was determined that $D_{12,1}$ is equivalent to $\mathcal{C}_{12,1}$ in Section 3, but $D_{12,2}$ is not equivalent to any of the seven previously known codes given in Table 4 of [4]. Considering the results from Section 3 we have the following.

Proposition 4.1. *There are at least 9 inequivalent Type I* $[[12, 0, 5]]$ *codes.*

- For length $n = 14$, there are exactly four Type II 4-circulant $[[14, 0, 6]]$ codes with generators

$$\begin{array}{ll} (1121100)(1001121), & (1222100)(1001222), \\ (1232100)(0110232) & \text{and } (1232100)(1001232). \end{array}$$

They have weight enumerator W_{14}. Exactly five Type I 4-circulant $[[14, 0, 5]]$ codes were obtained with the following generators

$$\begin{array}{lll} (1221000)(0101022), & (2332000)(2010222), & (2332000)(3000322), \\ (2233220)(2022332) & \text{and } (2313200)(3113202). & \end{array}$$

The first two codes have weight enumerator $W_{14,1}(y) = 1 + 28y^5 + 133y^6 + \cdots$, the third and fourth codes have $W_{14,2}(y) = 1 + 14y^5 + 147y^6 + \cdots$, and the fifth has $W_{14,3}(y) = 1 + 42y^5 + 119y^6 + \cdots$.

- For length $n = 16$, there are exactly 28 Type II 4-circulant $[[16, 0, 6]]$ codes, and all have weight enumerator $W_{16,2}$. There are exactly 15 Type I 4-circulant $[[16, 0, 6]]$ codes with either weight enumerator $W_{16,1}$ or one of the following

$$\begin{array}{ll} W_{16,3}(y) = 1 + 64y^6 + 464y^7 + \cdots, & W_{16,4}(y) = 1 + 72y^6 + 448y^7 + \cdots, \\ W_{16,5}(y) = 1 + 88y^6 + 416y^7 + \cdots, & W_{16,6}(y) = 1 + 96y^6 + 400y^7 + \cdots, \\ W_{16,7}(y) = 1 + 104y^6 + 384y^7 + \cdots, & W_{16,8}(y) = 1 + 128y^6 + 336y^7 + \cdots, \\ W_{16,9}(y) = 1 + 136y^6 + 320y^7 + \cdots. & \end{array}$$

We give their generators in Table 4. It is known [1] that there are many Type II $[[16, 0, 6]]$ codes. However, only three examples of Type I $[[16, 0, 6]]$ codes were given in [4]. Hence we have the following.

Proposition 4.2. *There are at least 15 Type I* $[[16, 0, 6]]$ *codes.*

This completes the classification of extremal 4-circulant codes of even lengths up to 16 (except 10). For higher lengths, we constructed a large number of codes. The results are summarized below.

We determined that a 4-circulant $[[18, 0, 8]]$ code does not exist. For length $n = 20$ we found three Type II 4-circulant $[[20, 0, 8]]$ codes, denoted $D_{20,1}, D_{20,2}, D_{20,3}$. They have weight enumerator W_{20} and group orders $20, 11520$ and 8640, respectively. We checked by Magma that $D_{20,2}$ and $D_{20,3}$ are equivalent to the two Hermitian linear $[20, 10, 8]$ codes in the Figure 3 and 4 of [9]. Furthermore, there are at least three Type I 4-circulant $[[20, 0, 8]]$ codes. For length $n = 22$ there are at least 67 Type II 4-circulant $[[22, 0, 8]]$ codes with weight enumerator W_{22}. They have group orders $11, 22$, or 44. Previously, only 46 Type II $[[22, 0, 8]]$ codes were known from [14, Table XIV] and [10, Table VIII]. Hence many of our codes are new. We list only 10 of these codes in Table 5. Even though we could not find a Type I circulant $[[22, 0, 8]]$ code, we did obtain a Type I 4-circulant $[[22, 0, 8]]$ code. This is generated by (23223121000)(31110302332) and has group order 22 and weight enumerator $1 + 638y^8 + 2464y^9 + \cdots$. This is the first example of a Type I $[[22, 0, 8]]$ code. Generators for other codes of length 22 are given in Table 5.

We summarize what is currently known about 4-circulant $[[n, 0, d]]$ codes in Table 6.

5 Extremal additive bordered 4-circulant codes

In the previous section we dealt with 4-circulant self-dual codes. As these codes have even length, we consider a class of bordered 4-circulant codes which have odd length. A *bordered 4-circulant additive* $(n, 2^n)$ *code* of odd length n has the following generator matrix

$$\begin{pmatrix} e & d & c \\ a & I_{(n-1)/2} & A_{(n-1)/2} \\ b & B_{(n-1)/2} & I_{(n-1)/2} \end{pmatrix}, \tag{5}$$

where a and d are all-one vectors of length $(n-1)/2$, and b and c are all-two vectors of length $(n-1)/2$. e is one of $0, 1, 2$, or 3, and $A_{(n-1)/2}$ and $B_{(n-1)/2}$ are circulant matrices.

- For length $n = 3$, there is only one Type I bordered 4-circulant $[[3, 0, 2]]$ code. It is generated by (1)(2) with $e = 2$. This code is equivalent to $\mathcal{C}_3$ in Section 3.

- For length $n = 5$, there is only one Type I bordered 4-circulant $[[5, 0, 3]]$ code. It is generated by (30)(12) with $e = 2$. This code is equivalent to $\mathcal{C}_5$ in Section 3.

- For length $n = 7$, there are exactly two Type I bordered 4-circulant $[[7, 0, 3]]$ codes $BD_{7,1}$ and $BD_{7,2}$. $BD_{7,1}$ is generated by (330)(121) with $e = 0$. It has weight enumerator $W_{7,1} = 1 + 3y^3 + 29y^4 + \cdots$. $BD_{7,2}$ is generated by (300)(122) with $e = 3$. It has weight enumerator $W_{7,2}(y) = 1 + 7y^3 + 21y^4 + \cdots$ with group order 336. We note that neither of these codes is equivalent to the unique circulant $[[7, 0, 3]]$ code $\mathcal{C}_7$. Hence $BD_{7,1}, BD_{7,2}$, and $\mathcal{C}_7$ are the three Type I $[[7, 0, 3]]$ codes in Table 1 of [6].

- For length $n = 9$, there are exactly two Type I bordered 4-circulant $[[9, 0, 4]]$ codes. One is generated by (2010)(1222) with $e = 2$. It has weight enumerator W_9 given in Section 3, but is not equivalent to the circulant code because it has a different group order 64. The second code is generated by (2010)(0232) with $e = 2$. It has weight enumerator $W_{9,1}(y) = 1 + 26y^4 + 48y^5 + 136y^6 + \cdots$, so neither bordered code is equivalent to the unique Type I circulant $[[9, 0, 4]]$ code.

- For length $n = 11$ we have found exactly seven Type I bordered 4-circulant $[[11, 0, 4]]$ (there is no bordered $[[11, 0, 5]]$ code). Five of these codes have $e = 0$ with generators (22000)(02220), (33000)(02320), (33000)(02220), (13310)(22211), (13310)(23211), respectively. Two of these codes have $e = 3$ with generators (13100)(22221), (13100)(23321), respectively.

• For length $n = 13$ we have shown that there are exactly four Type I bordered 4-circulant $[[13, 0, 5]]$ codes. All codes have $e = 2$ with generators (331200)(132020), (331200)(033120), (321210)(132020), (321210)(133021), respectively. The first three codes have weight enumerator $W_{13,1}$ in Section 3. The fourth code has the weight enumerator given in [4] and group order 6. We checked that the second code is equivalent to q'_{14}, but the rest are not equivalent to the six codes described in Section 3. Hence we have the following.

Proposition 5.1. *There are at least* 9 *inequivalent Type I* $[[13, 0, 5]]$ *codes.*

• For length $n = 15$ we have shown that there is only one Type I bordered 4-circulant $[[15, 0, 6]]$ code BD_{15}. BD_{15} is generated by (1233210)(2321001) with $e = 0$. It has weight enumerator $W_{15,1}(y) = 1 + 161y^6 + 308y^7 + \cdots$ and group order 28. BD_{15} is equivalent to the code given in Example 3.14 of [4].

• For length $n = 17$, there are exactly 12 Type II bordered 4-circulant $[[17, 0, 6]]$ codes (there is no bordered $[[17, 0, 7]]$ code). For example, one of these codes is generated by (11311000)(23332202) with $e = 2$.

• For length $n = 19$ (respectively 21), we found at least 20 Type I bordered 4-circulant $[[19, 0, 6]]$ codes (respectively $[[21, 0, 7]]$ codes) with distinct weight distributions. For example, the code with $e = 2$ and generators (121210000)(232232020) produces a $[[19, 0, 6]]$ code, and the code with $e = 2$ and generators (1232100000)(2333332010) produces a $[[21, 0, 7]]$ code. These codes have distance one less than optimal according to Table XIV of [14].

• For length 23 we have at least 7 Type I bordered 4-circulant $[[23, 0, 8]]$ codes with distinct weight distributions. Note that $d = 8$ for length $n = 23$ is the highest known minimum weight. All codes have $e = 2$ with the following generators

(31322110000)(03222231012), (11313110000)(33223320202),
(13313310000)(32332301210), (23322120000)(02232120010),
(23322120000)(03222121101), (22211201000)(03232203200),
(20332110100)(02232330112),

and $A_8 = 550, 506, 528, 594, 616, 572, 704$, respectively.

Including the results from Section 3, we have the following.

Proposition 5.2. *There are at least* 9 *inequivalent Type I* $[[23, 0, 8]]$ *codes with distinct weight distributions.*

• For length 25 we have at least 16 Type I bordered 4-circulant $[[25, 0, 8]]$ codes with distinct weight distributions different from those of circulant $[[25, 0, 8]]$ codes in Section 3. We list some of them. All codes have $e = 2$ with the following generators.

$$
\begin{array}{ll}
(211231010000)(023333321122), & (211231010000)(132233331122) \\
(211231010000)(133223231032), & (211231010000)(023233231132) \\
(213112010000)(032232302202), & (213112010000)(133323212302) \\
(213112010000)(023332203312), & (113212010000)(232332202002)
\end{array}
$$

Including the results from Section 3, we have the following.

Proposition 5.3. *There are at least* 30 *inequivalent Type I* $[[25, 0, 8]]$ *codes with distinct weight distributions.*

We summarize what is currently known about bordered 4-circulant $[[n, 0, d]]$ codes in Table 7.

6 Conclusion

We have classified the extremal circulant $[[n, 0]]$ self-dual codes of lengths $n \le 15$ and constructed some good codes for lengths $16 \le n \le 30$. We have also classified the extremal 4-circulant $[[n, 0]]$ self-dual codes of lengths $n = 4, 6, 8, 12, 14,$ and 16 and most codes of length $n = 10$, and constructed good codes for lengths $n = 20$ and 22. Moreover we have classified the extremal additive bordered 4-circulant self-dual codes of odd lengths from 3 to 17, and constructed good codes for lengths $19, 21, 23,$ and 25.

These codes are interesting because of their simple structures. Furthermore, we have shown that many of the codes given in this paper are new. It will be very interesting to fill the blanks in Table 1, and also to update the other entries.

Acknowldegement We are thankful to the anonymous referees for their valuable comments.

References

[1] C. Bachoc and P. Gaborit, "On extremal additive GF(4)-codes of lengths 10 to 18," *J. Théorie Nombres Bordeaux,* vol. 12, pp. 225–271, 2000.

[2] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory,* vol. 44, pp. 1369–1387, 1998.

[3] P. Gaborit, W.C. Huffman, J.-L. Kim, and V. Pless, "On the classification of extremal additive codes over GF(4)," *Proc. Allerton Conf. on Communication, Control, and Computing*, Univ. Illinois, Urbana-Champaign, pp. 535–544, Sep. 1999.

[4] P. Gaborit, W.C. Huffman, J.-L. Kim, and V. Pless, "On additive GF(4) codes," *DIMACS Workshop on Codes and Association Schemes,* DIMACS Series in Discrete Math. and Theoret. Computer Science, American Mathematical Society, vol. 56, pp. 135–149, 2001.

[5] P. Gaborit, J.-L. Kim, and V. Pless, "Decoding binary $R(2, 5)$ by hand," *Discrete Math.* vol. 264, pp. 55–73, 2003.

[6] G. Höhn, "Self-dual codes over the Kleinian four group," preprint, 1996. An updated version can be found at http://xxx.lanl.gov/pdf/math.CO/0005266.

[7] W.C. Huffman, "On extremal self-dual quaternary codes of lengths 18 to 28, I," *IEEE Trans. Inform. Theory,* vol. 36, pp. 651–660, May 1990.

[8] W.C. Huffman, "On extremal self-dual quaternary codes of lengths 18 to 28, II," *IEEE Trans. Inform. Theory,* vol. 37, pp. 1206–1216, July 1991.

[9] W.C. Huffman, "Characterization of quaternary extremal codes of lengths 18 and 20," *IEEE Trans. Inform. Theory,* vol. 43, pp. 1613–1616, 1997.

[10] J.-L. Kim, "New self-dual codes over GF(4) with the highest known minimum weights," *IEEE Trans. Inform. Theory,* vol. 47, pp. 1575–1580, Mar. 2001.

[11] J.-L. Kim and V. Pless, "Designs in additive codes over GF(4)," *Proc. Allerton Conf. on Communication, Control and Computing,* pp. 1010–1018, Oct. 2000.

[12] J.-L. Kim and V. Pless, "Designs in additive codes over GF(4)," *Design, Codes, and Cryptography*, vol. 30, pp. 187-199, 2003.

[13] F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane and H.N. Ward, "Self-dual codes over GF(4)", *J. Combin. Theory Ser. A,* vol. 25, pp. 288–318, 1978.

[14] E.M. Rains and N.J.A. Sloane, "Self-dual codes," in *Handbook of Coding Theory,* ed. V. S. Pless and W. C. Huffman, Amsterdam: Elsevier, pp. 177–294, 1998.

[15] M. Ran and J. Snyders, "On cyclic reversible self-dual additive codes with odd length over $\mathcal{Z}_2^2$," *IEEE Trans. Inform. Theory,* vol. 46, pp. 1056–1059, 2001.

Table 1: Number of extremal or optimal additive self-dual codes over GF(4) of lengths $12 \leq n \leq 27$

n	d_I	Old No.(ref)	New No.	d_{II}	Old No.(ref)	New No.
12	5	≥ 7 [4]	≥ 9	6	1 [4]	1 [4]
13	5	≥ 5 [4]	≥ 9	-	-	-
14	5-6	≥ 1 [4]	≥ 5	6	≥ 490[1]	≥ 491
15	6	≥ 2 [4]	≥ 4	-	-	-
16	6	≥ 3 [4]	≥ 15	6	≥ 4 [4]	≥ 28
17	7	$\geq$1 [14]	≥ 1	-	-	-
18	7	? [14]	?	8	≥ 1 [14]	≥ 1 [14]
19	7	≥ 1 [14]	≥ 4	-	-	-
20	8	? [14]	≥ 3	8	≥ 2 [14]	≥ 5
21	8	≥ 1 [14]	≥ 1 [14]	-	-	-
22	8	? [14]	≥ 1	8	≥ 46 [10]	≥ 67
23	8-9	≥ 1 [14]	≥ 2	-	-	-
24	8-9	? [14]	?	8 or 10	≥ 17 [10]	≥ 51
25	8-9	≥ 1 [14]	≥ 30	-	-	-
26	8-10	? [14]	≥ 14	8 or 10	≥ 49 [10]	≥ 49 [10]
27	9-10	≥ 1 [14]	≥ 15	-	-	-

Table 2: Generators for good circulant self-dual codes of lengths 25 to 30

Codes	Generators	A_8	A_9	A_{10}	A_{11}	A_{12}
$\mathcal{C}_{25,1}$	(12332332)	450	525	6560	22800	81100
$\mathcal{C}_{25,2}$	(10212321201)	275	1250	5360	22800	84800
$\mathcal{C}_{25,3}$	(11023332011)	175	1150	6160	23600	82000
$\mathcal{C}_{25,4}$	(11201310211)	175	1250	5800	23800	82600
$\mathcal{C}_{25,5}$	(11220302211)	250	1225	5400	23800	83300
$\mathcal{C}_{26,1}$	(122131221)	247	936	4394	19136	77376
$\mathcal{C}_{26,2}$	(122323221)	91	936	4758	20800	76752
$\mathcal{C}_{26,3}$	(10213131201)	169	1196	4108	18720	79144
$\mathcal{C}_{26,4}$	(10213231201)	182	806	4641	21008	76076
$\mathcal{C}_{26,5}$	(10222322201)	182	910	4537	20176	76908
$\mathcal{C}_{27,1}$	(122131221)	108	657	3537	17739	69300
$\mathcal{C}_{27,2}$	(122323221)	162	705	3483	16875	68652
$\mathcal{C}_{27,3}$	(10212321201)	297	738	3024	16470	68328
$\mathcal{C}_{27,4}$	(10213131201)	189	900	3132	15876	69624
$\mathcal{C}_{27,5}$	(10221312201)	135	630	3618	17442	68544
$\mathcal{C}_{28,1}$	(323131223322011)	0	0	6006	0	122031
$\mathcal{C}_{29,1}$	(120231323132021)	0	0	0	15834	71253
$\mathcal{C}_{30,1}$	(3032120320121101)	0	0	0	0	118755

Table 3: Extremal or optimal additive circulant self-dual codes over GF(4)

n	d_I	No.	n	$d_I; d_{II}$	No.
3	2	1	4	2 ; 2	1; 2
5	3	1	6	3 ; 4	1; 1
7	3	1	8	4 ; 4	0; 1
9	4	1	10	4 ; 4	3; 5
11	5	0	12	5 ; 6	1; 1
13	5	2	14	6 ; 6	0; 3
15	6	3	16	6 ; 6	$\geq 1; \geq 5$
17	7	≥ 1	18	7 ; 8	? ; ?
19	7	≥ 4	20	8 ; 8	? ;≥ 2
21	8	?	22	8 ; 8	? ;≥ 14
23	8-9	≥ 2	24	8-9;8 or 10	? ;≥ 51
25	8-9	≥ 14	26	8-10; 8 or 10	≥ 14 ; ?
27	8-9	≥ 15	28	10; 10	? ;≥ 1
29	11	≥ 1	30	11; 12	? ; ≥ 1

Table 4: Generators for 4-circulant self-dual [[16, 0, 6]] codes

Types	Generators
Type II	(32111000)(31110002); (32111000)(31101002); (11211000)(11011020); (11211000)(10001121); (12221000)(01010222); (12221000)(10001222); (12321000)(01010232); (33312000)(31002022); (33312000)(20012032); (33312000)(30103032); (32110100)(31101002); (32110100)(31001102); (21220100)(31001220); (21220100)(20101320); (21220100)(20010221); (21220100)(31011221); (13201100)(10011032); (23021100)(31010202); (22302100)(31002022); (22302100)(30103032); (30332100)(20013220); (30332100)(20102320); (23202010)(30103032); (23121110)(31110212); (33322210)(31023322); (33232210)(31023322); (33232210)(21033232); (32233210)(31023322)
Type I	(11211000)(11111020); (23223200)(30032332); (12221000)(10101222); (21220100)(21111221); (12321000)(10101232); (21321100)(21111221); (33312000)(31012032); (22302100)(30113022); (33212100)(30103032); (21332100)(20102320); (21220100)(30110221); (21220100)(21010321); (30332100)(31012320); (22332200)(21033322); (32121010)(31110212)

Table 5: Generators for good 4-circulant self-dual codes of lengths 20 and 22

Codes	Generators	A_8	A_9	A_{10}	A_{11}	A_{12}	Order
$\mathcal{D}_{20,1}$	(2230312100)(3011303022)	1710	0	20976	0	126540	20
$\mathcal{D}_{20,2}$	(1120202110)(1011202021)	1710	0	20976	0	126540	11520
$\mathcal{D}_{20,3}$	(1121312110)(1011213121)	1710	0	20976	0	126540	8640
$\mathcal{D}_{20,4}$	(2212122010)(3010321212)	990	4160	9552	25920	65820	1920
$\mathcal{D}_{20,5}$	(2313132010)(2101220202)	1070	3840	9712	26880	64460	3840
$\mathcal{D}_{20,6}$	(3222223020)(2030223232)	990	4160	99552	25920	65820	1920
$\mathcal{D}_{22,1}$	(21321110000)(21011100320)	990	0	18480	0	163548	11
$\mathcal{D}_{22,2}$	(21321110000)(20010111320)	990	0	18480	0	163548	11
$\mathcal{D}_{22,3}$	(21321110000)(20110100221)	990	0	18480	0	163548	11
$\mathcal{D}_{22,4}$	(21321110000)(31110101221)	990	0	18480	0	163548	11
$\mathcal{D}_{22,5}$	(11232110000)(01111002320)	990	0	18480	0	163548	22
$\mathcal{D}_{22,6}$	(11232110000)(10110102320)	990	0	18480	0	163548	22
$\mathcal{D}_{22,7}$	(11232110000)(11111102320)	990	0	18480	0	163548	44
$\mathcal{D}_{22,8}$	(11232110000)(10000112321)	990	0	18480	0	163548	44
$\mathcal{D}_{22,9}$	(13311210000)(00101021122)	990	0	18480	0	163548	11
$\mathcal{D}_{22,10}$	(13311210000)(01010031122)	990	0	18480	0	163548	11

Table 6: Extremal or optimal additive 4-circulant self-dual codes over GF(4)

n	$d_I; d_{II}$	No.	n	$d_I; d_{II}$	No.
2	$2; 2$	$0; 1$	14	5 or 6;6	5 or 0;4
4	$2; 2$	$1; 1$	16	$6; 6$	$15; 28$
6	$3; 4$	$1; 1$	18	$7; 8$	$?; ?$
8	$4; 4$	$2; 2$	20	$8; 8$	$\geq 3; \geq 3$
10	$4; 4$	$\geq 1; 6$	22	$8; 8$	$\geq 1; \geq 67$
12	$5; 6$	$2; 0$	24	$9; 10$	$?; ?$

Table 7: Extremal or optimal additive bordered 4-circulant self-dual codes over GF(4)

n	d_I	No.	n	d_I	No.
3	2	1	15	6	1
5	3	1	17	6	12
7	3	2	19	6	≥ 20
9	4	2	21	7	≥ 20
11	4	7	23	8	≥ 7
13	5	4	25	8	≥ 16

Table Captions

Table 1: Number of extremal or optimal additive self-dual codes over GF(4) of lengths $12 \leq n \leq 27$
Table 2: Generators for good circulant self-dual codes of lengths 25 to 30
Table 3: Extremal or optimal additive circulant self-dual codes over GF(4)
Table 4: Generators for 4-circulant self-dual $[[16, 0, 6]]$ codes
Table 5: Generators for good 4-circulant self-dual codes of lengths 20 and 22
Table 6: Extremal or optimal additive 4-circulant self-dual codes over GF(4)
Table 7: Extremal or optimal additive bordered 4-circulant self-dual codes over GF(4)

Biographies of T. Aaron Gulliver and Jon-Lark Kim

Biography of T. Aaron Gulliver (S'81-M'82-SM'96)

T. Aaron Gulliver received the B.Sc.(Eng.) and M.Sc.(Eng.) degrees in Electrical Engineering from the University of New Brunswick, Fredericton, NB, Canada, in 1982 and 1984, respectively, and the Ph.D. degree in Electrical and Computer Engineering from the University of Victoria, Victoria, BC, Canada, in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, Canada. From 1991 to 1995 he was a member of the Department of Systems and Computer Engineering at Carleton University, Ottawa, Canada. From 1996 to 1999 he was at the Department of Electrical and Electronic Engineering at the University of Canterbury, Christchurch, New Zealand. He is now a Professor in the Department of Electrical and Computer Engineering at the University of Victoria.

He was registration chair for the 1995 IEEE International Symposium on Information Theory which was held in Whistler, BC, Canada. He was co-chair of the 2003 Information Theory Workshop held in Paris. Since 2000, he has been the Secretary for the Board of Governors of the IEEE Information Theory Society. He also maintains the website of the society. In 2000, he was awarded a Research Fellowship by the British Columbia Advanced Systems Institute. In 2002, he became a Fellow of the Engineering Institute of Canada. His research interests include coding theory, source coding, cryptography and wireless communications.

Biography of Jon-Lark Kim (S'01-A'03)

Jon-Lark Kim (S'01–A'03) was born in Taejon, Korea, on November 15, 1970. He received the B.S. degree in mathematics from POSTECH, Pohang, Korea, in 1993, the M.S. degree in mathematics from Seoul National University, Seoul, Korea, in 1997, and the Ph.D. degree in mathematics from the University of Illinois at Chicago, in 2002.

Since 2002, he has been with the department of mathematics at the University of Nebraska-Lincoln as a Research Assistant Professor. His areas of interest include algebraic coding theory with connections to combinatorics, graph theory, finite geometry, number theory, and algebraic geometry as well as cryptography using error-correcting codes or elliptic curves.