Serdica J. Computing **1** (2007), 213–227

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

SOME NEW RESULTS FOR ADDITIVE SELF-DUAL CODES OVER *GF*(4)

Zlatko Varbanov[*]

Abstract. *Additive code $\mathcal{C}$ over $GF(4)$ of length n* is an additive subgroup of $GF(4)^n$. It is well known [4] that the problem of finding stabilizer quantum error-correcting codes is transformed into problem of finding additive self-orthogonal codes over the Galois field $GF(4)$ under a trace inner product. Our purpose is to construct good additive self-dual codes of length $13 \le n \le 21$. In this paper we classify all extremal (optimal) codes of lengths 13 and 14, and we construct many extremal codes of lengths 15 and 16. Also, we construct some new extremal codes of lengths 17,18,19, and 21. We give the current status of known extremal (optimal) additive self-dual codes of lengths 13 to 21.

1. Introduction. After the publication [4], 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, 4, 5, 6, 7, 13] were

ACM Computing Classification System (1998): E.4.

Key words: Additive code, self-dual code, graph code, classification.

[*] Supported by COMBSTRU Research Training Network HPRN-CT-2002-00278 and the Bulgarian National Science Foundation under Grant MM-1304/03.

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 [17, p. 199]. Moreover it was shown in [13, 15, 16] 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. Also, every additive self-dual code over $GF(4)$ can be uniquely represented as an isotropic system, and conversely [5]. These facts motivate the construction of additive self-dual codes over $GF(4)$.

Let $GF(4) = \{0, 1, \omega, \bar{\omega}\}$ with convention that $\bar{\omega} = \omega^2 = 1 + \omega$. An *additive code* $\mathcal{C}$ *over* $GF(4)$ *of length* n is an additive subgroup of $GF(4)^n$. As C is a free $GF(2)$-module, it has size 2^k for some $0 \leq k \leq 2n$. We call C an $(n, 2^k)$ code. It has a basis, as a $GF(2)$-module, consisting of k basis vectors; a generator matrix of C is a $k \times n$ matrix with entries in $GF(4)$ whose rows are a basis of C.

In other words, let C be a code over $GF(4)$ with generator matrix G. If any sum of the rows of G, i.e., any $GF(2)$-linear combination, is a codeword in C, and all codewords in C are $GF(2)$-linear combinations of the rows of G, then C is an additive code.

There is a natural inner product arising from the trace map. The trace map $Tr : GF(4) \to GF(2)$ is given by $Tr(x) = x + x^2$. In particular $Tr(0) = Tr(1) = 0$ and $Tr(\omega) = Tr(\bar{\omega}) = 1$. The *conjugate* of $x \in GF(4)$, denoted $\bar{x}$, is the image of x under the Frobenius automorphism; in other words, $\bar{0} = 0, \bar{1} = 1$, and $\bar{\bar{\omega}} = \omega$.

We now define the *trace inner product* of two vectors $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ in $GF(4)^n$ is

$$x \star y = \sum_{i=1}^{n} Tr(x_i \bar{y}_i) \tag{1}$$

If C is an additive code, its *dual*, denoted $C^\perp$, is the additive code $\{x \in GF(4)^n | x \star c = 0 \text{ for all } c \in C\}$. If C is an $(n, 2^k)$ code, then $\mathcal{C}^\perp$ is an $(n, 2^{2n-k})$ code. As usual, C is *(trace) self-orthogonal* if $C \subseteq C^\perp$, and *(trace) self-dual* if $C = C^\perp$. In particular, if C is self-dual, then 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 [4]. 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, *weight* of a codeword $c \in C$ $(wt(c))$ is the number of nonzero components of c. The minimum weight d of a code C is the smallest weight of any nonzero codewords of $\mathcal{C}$. If C is an additive $(n, 2^k)$ code with minimum weight d then C is called an $(n, 2^k, d)$ code. C is *Type II* code if C is self-dual and all codewords have even weight; *Type II* codes of length n exist only if n is even [7]. If 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*. There is a bound on the minimum weight of an additive self-dual code ([17], 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

$$d_I \leq \begin{cases} 2\lfloor n/6 \rfloor + 1, & n \equiv 0 \pmod 6; \\ 2\lfloor n/6 \rfloor + 3, & n \equiv 5 \pmod 6; \\ 2\lfloor n/6 \rfloor + 2, & \text{otherwise} \end{cases} \tag{2}$$

$$d_{II} \leq \ 2\lfloor n/6 \rfloor + 2$$

A code that meets the appropriate bound is called *extremal.* If the code is not extremal but no code of the given type can exist with a larger minimum weight then the code is called *optimal. Type II* codes meeting the bound d_{II} have a unique weight enumerator [7]. This property is not true for *Type I* codes.

We say that two additive codes C_1 and C_2 are *equivalent* provided there is a map sending the codewords of C_1 onto the codewords of 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 C, denoted $Aut(C)$, consists of all maps which permute coordinates, scale coordinates, and conjugate coordinates that send codewords of C to codewords of 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 $(2, 2^2)$ codes with generator matrices

$$\begin{pmatrix} 1 & 1 \\ \omega & \omega \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ \omega & \bar{\omega} \end{pmatrix}$$

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

All additive self-dual codes over $GF(4)$ of length n have previously been classified, up to equivalence, by Calderbank et al. [4] for $n \leq 5$, by Höhn [13] for $n \leq 7$, by Hein et al. [12] for $n \leq 7$, by Glynn et al. [9] for $n \leq 9$, and by Danielsen and Parker [5] for $n \leq 12$. Höhn [13] also classified all *Type II* codes of length 8 and Danielsen and Parker [5] classified all extremal *Type II* codes of length 14. Gaborit et al. [6, 7] have classified all extremal codes of length 8, 9, 11, and 12. Bachoc and Gaborit [1] classified all extremal *Type II* codes of length 10. Gulliver and Kim [11] classified the extremal circulant codes for $n \leq 15$ and the extremal 4-circulant codes of lengths 4, 6, 8, 12, 14, and 16 and most codes of length 10. Furthermore, Gulliver and Kim classified the extremal bordered 4-circulant codes of lengths 3, 5, 7, 9, 11, 13, 15, and 17, and constructed many good circulant, 4-circulant, and bordered 4-circulant codes for $n \leq 27$. A review of the current status of the classification of various types of self-dual codes is given by Huffman [14].

Our purpose is to classify the optimal additive self-dual codes of length 13 (no extremal code of this length) and the extremal additive self-dual codes of length 14. We also construct good codes for lengths $15 \leq n \leq 21$. We give the current status of known extremal (or optimal) additive *Type I* or *Type II* codes of lengths 13 to 21 in Table 1. In this table, we list our numbers of *Type I* (*Type II*) additive self-dual codes in the fourth (seventh) column and compare them with the old numbers of self-dual *Type I* (*Type II*) codes in the third (sixth) column. When the number in the column is exact (without $\geq$), the classification of those codes is complete.

2. Preliminaries.

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

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

If there are no nonzero vectors of weight $< d$ in $C^{\perp}$ in the above theorem, C is pure (or nondegenerate); otherwise it is impure (or degenerate) [4]. 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 [4].

The *Hermitian inner product* is defined as

$$x.y = x_1\overline{y_1} + x_2\overline{y_2} + \ldots x_n\overline{y_n} \in GF(4)$$

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

Theorem 2.2 (Theorem 3, [4])**.** *A linear code 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 described in the next section.

3. Techniques.

3.1. Shortening and lengthening. The following two methods were described in [7]. If C is an additive self-dual $(n,2^n,d)$ code, we can obtain a self-dual code of length $n-1$ by a process called *shortening.* Let G be a generator matrix of C. Choose any column of G, say the i^{th} one. By row reducing G, we can make all the entries of column i equal to 0 except one or two entries (which are $1,\omega$ or $\bar{\omega}$). The *shortened code of C on coordinate i*, denoted C', is the code with generator matrix G' obtained from G by eliminating one row of G with a nonzero entry in column i and then eliminating column i. If there is only one nonzero entry in column i of G, then C' is C shortened in usual sense. Clearly C' is an additive self-dual $(n-1,2^{n-1},d')$ code with $d' \leq d-1$.

We can reverse shortening by *lengthening* an additive self-dual $(n-1,2^{n-1}, d')$ code C' to obtain an additive self-dual $(n,2^n,d)$ code C. To do this, take a generator matrix G' and adjoin an arbitrary n^{th} row x at the bottom. Then add an n^{th} column on the right according to the following scheme: First place 1 in the n^{th} row. Second place 0 or ω in each of the first $n-1$ rows so that each of the new length n rows is orthogonal to the length n bottom row. (Note that if we begin with two orthogonal rows of length $n-1$ and want to adjoin a nonzero element to one of the rows, we must adjoin the same nonzero element to the other row if we wish to create two orthogonal rows of length n.) The resulting matrix

$$G = \left(\begin{array}{c|c} G' & \begin{matrix} 0 \\ \text{or} \\ \omega \end{matrix} \\ \hline x & 1 \end{array}\right)$$

clearly generates an additive self-dual $(n,2^n,d)$ code with $d \leq d'+1$. If the new row of length $n-1$ added to the bottom of G' is already in C', the lengthened code is a direct sum of C' and the $(1,2,1)$ code generated by I_1.

Lemma 3.1 (Lemma 3.12, [7]). *Other possible constructions generate equivalent codes:*

$$\left(\begin{array}{c|c} G' & \begin{matrix} 0 \\ \textit{or} \\ \bar{\omega} \end{matrix} \\ \hline x & 1 \end{array}\right), \left(\begin{array}{c|c} G' & \begin{matrix} 0 \\ \textit{or} \\ 1 \end{matrix} \\ \hline x & \omega \end{array}\right), \left(\begin{array}{c|c} G' & \begin{matrix} 0 \\ \textit{or} \\ \bar{\omega} \end{matrix} \\ \hline x & \omega \end{array}\right), \left(\begin{array}{c|c} G' & \begin{matrix} 0 \\ \textit{or} \\ 1 \end{matrix} \\ \hline x & \bar{\omega} \end{array}\right), \left(\begin{array}{c|c} G' & \begin{matrix} 0 \\ \textit{or} \\ \omega \end{matrix} \\ \hline x & \bar{\omega} \end{array}\right)$$

As a result of this lemma, the definition of lengthening can be expanded to allow us to lengthen using any of these six matrices. Up to equivalence lengthening and shortening are inverse operations. Thus we have the following theorem.

Theorem 3.2 (Theorem 3.13, [7]). *Every additive self-dual* $(n-1, 2^{n-1})$ *code is shortened from an additive self-dual* $(n, 2^n)$ *code, and every additive self-dual* $(n, 2^n)$ *code is lengthened from an additive self-dual* $(n-1, 2^{n-1})$ *code.*

3.2. Graph codes. A *graph* is a pair $G = (V, E)$, where $V = \{v_0, v_1, \ldots, v_n\}$ is a set of n *vertices* (or *nodes*), and E is a set of distinct pairs of elements from V, i.e., $E \subseteq V \times V$. A pair $\{v_i, v_j\} \in E$ is called *edge*. We will only consider *undirected* graphs, which are graphs where E is a set of distinct unordered pairs of elements from V. Furthermore, the graphs we will look at will all be *simple* graphs, which are graphs with no self-loops, $\{v_i, v_i\} \notin E$. A graph may be represented by an *adjacency matrix* Γ. This is a $|V| \times |V|$ matrix where $\Gamma_{i,j} = 1$ if $\{v_i, v_j\} \in E$ and $\Gamma_{i,j} = 0$ otherwise. For simple graphs, the adjacency matrix must have 0's on the diagonal, i.e., $\Gamma_{i,i} = 0$. The adjacency matrix of an undirected graph will be symmetric, i.e., $\Gamma_{i,j} = \Gamma_{j,i}$

A *graph code* is an additive self-dual code over $GF(4)$ with generator matrix $C = \Gamma + \omega I$ where I is the identity matrix and Γ is the adjacency matrix of a simple undirected graph, which must be symmetric with 0's along the diagonal.

Example:

$$\Gamma = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad C = \Gamma + \omega I = \begin{pmatrix} \omega & 1 & 1 \\ 1 & \omega & 1 \\ 1 & 1 & \omega \end{pmatrix}$$

A graph code is always self-dual, since its generator matrix has full rank over $GF(2)$ and $C\overline{C}^T$ only contains entries from $GF(2)$ whose traces must be zero. This construction for additive self-dual codes over $GF(4)$ has also been used by Tonchev [20].

Schlingemann [18] first proved the following theorem in terms of *quantum stabilizer states.*

Theorem 3.3 (Schlingemann and Werner [18, 19], Grassl et al. [10], Glynn et al. [8, 9]). *For any self-dual quantum code, there is an equivalent graph code. This means that there is a one-to-one correspondence between the set of simple undirected graphs and the set of additive self-dual codes over* $GF(4)$.

We have seen that every graph represents an additive self-dual code over $GF(4)$, and that every additive self-dual code over $GF(4)$ can be represented by a graph. It follows from Theorem 3.3 that, without loss of generality, we can restrict our study of additive self-dual codes over $GF(4)$ to those with generator matrices of the form $\Gamma + \omega I$.

Proposition 3.4. *If G is a generator matrix of a graph code C of length n, and x is a binary vector, then*

$$G' = \left(\begin{array}{c|c} G & x^t \\ \hline x & \omega \end{array}\right)$$

is a generator matrix of a graph code of length $n+1$.

Proof. Each row of G has only one element ω, and this element is in a different position in each row. All other elements in G are 0 or 1. But $Tr(0) = Tr(1) = 0$. Therefore, the trace inner product of every two rows depends only on the positions of the elements ω in these rows. It is easy to see that in this symmetric form of G' we have two possibilities of the trace inner product of every two rows:

$$0 + \cdots + 0 + Tr(\omega * 0) + 0 + \cdots + 0 + Tr(0 * \omega) + 0 + \cdots + 0 = 0$$

or

$$0 + \cdots + 0 + Tr(\omega * 1) + 0 + \cdots + 0 + Tr(1 * \omega) + 0 + \cdots + 0 = 0$$

Therefore, the trace inner product of every two rows is 0 and G' is a generator matrix of a graph code of length $n+1$. □

Similar construction methods, by making all possible extensions of all connected graphs on n vertices were described in [5, 9]. Also, this construction is similar to the second construction from Lemma 3.1 but here x is a binary vector. Therefore, the construction from Proposition 3.4 is 'easier' and 'faster' than the constructions from Lemma 3.1.

The special form of the generator matrix of a graph code makes it easier to find the distance of the code. An $[[n, 0, d]]$ code has 2^n codewords, but if the generator matrix is given in graph form, it is not necessary to check all the codewords to find the distance of the code. If we have found a codeword s, where $wt(s) \leq e$, we know that no codeword formed by adding e or more rows of the generator matrix can have lower weight.

4. Results.

Using the techniques described in the previous section we obtain many results for additive self-dual codes of lengths $13 \leq n \leq 21$. We use the program package $Q-Extension$ [2, 3] to obtain the number of nonequivalent codes of any length and the orders of their automorphism groups. By lengthening of graph codes we classify all optimal codes of length 13 and all extremal codes of length 14.

Theorem 4.1. *There are* 85845 *nonequivalent additive self-dual* $(13, 2^{13}, 5)$ *codes,* 2 *nonequivalent* $(14, 2^{14}, 6)$ *Type I codes, and* 1020 *nonequivalent* $(14, 2^{14}, 6)$ *Type II codes.*

Proof. To obtain all nonequivalent optimal codes of length 13 we use the generator matrices of graph codes of length 12 and minimum distance $d \geq 4$ obtained in [5]. By lengthening of graph codes, after exhaustive computer search we obtain exactly 85845 nonequivalent additive self-dual codes of length 13.

To obtain all nonequivalent extremal codes of length 14 we use the obtained generator matrices of codes of length 13. After exhaustive computer search we obtain that there exist 2 nonequivalent additive self-dual *Type I* codes of length 14 ($C_{14,1}$ and $C_{14,2}$) and 1020 nonequivalent additive self-dual *Type II* codes of length 14. The generator matrices of the codes $C_{14,1}$ and $C_{14,2}$ are:

$$G_{14,1} = \begin{pmatrix}
\omega & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & \omega & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & \omega & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & \omega & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & \omega & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & \omega & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & \omega & 0 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \omega & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & \omega & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & \omega & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & \omega & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & \omega & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & \omega
\end{pmatrix},$$

$$G_{14,2} = \begin{pmatrix}
\omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & \omega & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & \omega & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & \omega & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & \omega & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & \omega & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & \omega & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & \omega & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & \omega & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & \omega & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \omega & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & \omega
\end{pmatrix}$$

Their weight enumerators and group orders are:
$1 + 177z^6 + 512z^7 + 1177z^8 + 2304z^9 + 3578z^{10} + 4096z^{11} + 2934z^{12} + 1280z^{13} + 325z^{14}, |AUT(C_{14,1})| = 24$ and
$1 + 161z^6 + 576z^7 + 1113z^8 + 2240z^9 + 3738z^{10} + 4032z^{11} + 2870z^{12} + 1344z^{13} + 309z^{14}, |AUT(C_{14,2})| = 48$ □

Corollary 4.2. *There are exactly* 85845 *nonequivalent* $[[13, 0, 5]]$ *quantum error-correcting codes and* 1022 *nonequivalent* $[[14, 0, 6]]$ *quantum error-correcting codes.*

Danielsen and Parker [5] firstly classified $(14, 2^{14}, 6)$ *Type II* codes. The most important result in Theorem 4.1 is that there exist $(14, 2^{14}, 6)$ *Type I* codes. Therefore, the minimum distance of extremal *Type I* codes of length 14 is exactly 6 (in [14], 5 or 6).

In the same way, we construct many extremal codes of lengths 15 and 16. We obtain 2114 new $(15, 2^{15}, 6)$ codes, 8354 new *Type I* $(16, 2^{16}, 6)$ codes, and 84 new *Type II* $(16, 2^{16}, 6)$ codes (it is known [11] that there are at least 28 nonequivalent $(16, 2^{16}, 6)$ *Type II* codes). Hence we have the following.

Theorem 4.3. *There are at least* 2118 *nonequivalent additive self-dual* $(15, 2^{15}, 6)$ *codes, at least* 8369 *nonequivalent* $(16, 2^{16}, 6)$ *Type I codes, and at least* 112 *nonequivalent* $(16, 2^{16}, 6)$ *Type II codes.*

Corollary 4.4. *There are at least* 2118 $[[15, 0, 6]]$ *QECC, and at least* 8481 $[[16, 0, 6]]$ *QECC.*

Rains and Sloane [17] constructed an additive self-dual $(17, 2^{17}, 7)$ code with group order 16320. By lengthening it we construct new extremal *Type I* $(18, 2^{18}, 7)$ code $C_{18,1}$. It is the first constructed extremal *Type I* code of length 18. Its weight enumerator is $1 + 224z^7 + 1570z^8 + 3360z^9 + 9560z^{10} + 21184z^{11} + 38136z^{12} + 53312z^{13} + 54160z^{14} + 44640z^{15} + 26085z^{16} + 8352z^{17} + 1560z^{18}$, and its group order is 320. By shortening it we obtain new additive self-dual $(17, 2^{17}, 7)$ code C_{17} with generator matrix

$$G_{17} = \begin{pmatrix}
\omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \omega
\end{pmatrix}$$

Its weight enumerator is $1 + 408z^7 + 1530z^8 + 3400z^9 + 8160z^{10} + 17136z^{11} + 25704z^{12} + 28560z^{13} + 24480z^{14} + 15096z^{15} + 5661z^{16} + 936z^{17}$, and its group order is 960. By lengthening it we construct new *Type I* $(18, 2^{18}, 7)$ code $C_{18,2}$ with group order 40 and the same weight enumerator as $C_{18,1}$. The generator matrices of the codes $C_{18,1}$ and $C_{18,2}$ are

$$G_{18,1} = \begin{pmatrix}
\omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & \omega
\end{pmatrix},$$

$$G_{18,2} = \begin{pmatrix}
\omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & \omega & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & \omega & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & \omega & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & \omega & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \omega & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & \omega & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & \omega & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \omega & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & \omega & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & \omega
\end{pmatrix}$$

Therefore we have

Theorem 4.5. *There are at least* 2 *nonequivalent additive self-dual* $(17, 2^{17}, 7)$ *codes and at least* 2 *nonequivalent* $(18, 2^{18}, 7)$ *Type I codes.*

We know [17] that there exists at least one *Type II* $(18, 2^{18}, 8)$ code. Using it and the two constructed *Type I* codes of length 18, by lengthening we obtain 13 new additive self-dual codes of length 19.

Calderbank et al. [4] constructed additive cyclic self-dual $(21, 2^{21}, 8)$ code. Its group order is 60480 and its weight enumerator is $1 + 630z^8 + 3640z^9 + \cdots + 35028z^{20} + 5016z^{21}$. By shortening it we obtain $(20, 2^{20}, 7)$ additive self-dual code, and by lengthening the shortened code we construct new $(21, 2^{21}, 8)$ code C_{21} with group order 96 and weight enumerator:
$1 + 726z^8 + 3352z^9 + 9888z^{10} + 28560z^{11} + 73860z^{12} + 156360z^{13} + 266880z^{14} + 369504z^{15} + 415857z^{16} + 369960z^{17} + 246624z^{18} + 115728z^{19} + 34740z^{20} + 5112z^{21}$.

Its generator matrix is

$$\begin{pmatrix}
\bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & \omega \\
0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & \omega \\
1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & \omega \\
0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & \omega \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & \omega \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & 0 & \omega \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & 1 & \omega \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 1 & \omega \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 & \omega \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & \bar\omega & \bar\omega & 1 & \omega & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & \omega \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & \omega \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega & 1 & \bar\omega & 0 & \bar\omega & \omega & 1 & \bar\omega & \omega & 1
\end{pmatrix}$$

Hence we have the following.

Theorem 4.6. *There are at least* 17 *nonequivalent additive self-dual* $(19, 2^{19}, 7)$ *codes, and at least* 2 *nonequivalent* $(21, 2^{21}, 8)$ *codes.*

Corollary 4.7. *There are at least two nonequivalent* $[[17, 0, 7]]$ *QECC, at least two nonequivalent* $[[18, 0, 7]]$ *QECC, at least one* $[[18, 0, 8]]$ *QECC, at least* 17 *nonequivalent* $[[19, 0, 7]]$ *QECC, and at least two nonequivalent* $[[21, 0, 8]]$ *QECC.*

In Table 1 we summarize all obtained results for additive self-dual codes and we give the current status of known extremal (or optimal) additive *Type I* or *Type II* codes of lengths 13 to 21.

Table 1
Number of extremal (optimal) additive self-dual codes over $GF(4)$ of length $13 \geq n \geq 21$

n	d_I	Old No.(ref.)	New No.	n	d_{II}	Old No.(ref)	New No.
13	5	≥ 9 [11]	**85845**	13	–	–	–
14	**6**	? [14]	**2**	14	6	1020 [5]	1020
15	6	≥ 4 [11]	$\geq$ **2118**	15	–	–	–
16	6	≥ 15 [11]	$\geq$ **8369**	16	6	≥ 28 [11]	$\geq$ **112**
17	7	≥ 1 [17]	$\geq$ **2**	17	–	–	–
18	7	? [14]	$\geq$ **2**	18	8	≥ 1 [17]	≥ 1
19	7	≥ 4 [11]	$\geq$ **17**	19	–	–	–
20	8	≥ 3 [11]	≥ 3	20	8	≥ 5 [11]	≥ 5
21	8	≥ 1 [17]	$\geq$ **2**	21	–	–	–

REFERENCES

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

[2] Bouyukliev I. Q-extension – strategy in algorithms. Proceedings of the International Workshop ACCT, Bansko, Bulgaria, 2000, 84–89.

[3] Bouyukliev I. Q-extension. User's guide (version 0.1), preprint, 2005. http://lpmi.vali.bg/iliya/Manuelq.ps.

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

[5] Danielsen L., M. Parker. On the classification of all self-dual additive codes over $GF(4)$ of length up to 12. *J. Combin. Theory Ser. A* **113**, *7* (2006), 1351-1367, arXiv:math.CO/0504522.

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

[7] Gaborit P., W. C. Huffman, J.-L. Kim, V. Pless. On additive GF(4)-codes. DIMACS Workshop on Codes and Association Schemes. *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.* **56**, (2001), 135–149.

[8] Glynn D. On self-dual quantum codes and graphs, April 2002. Submitted to the Electronic Journal of Combinatorics.
http://homepage.mac.com/dglynn/.cv/dglynn/Public/SD-G3.pdf-link.pdf.

[9] Glynn D. G., T. A. Gulliver, J. G. Maks, M. K. Gupta. The geometry of additive quantum codes. Submitted to Springer-Verlag, 2004.

[10] Grassl M., A. Klappenecker, M. Rötteler. Graphs, quadratic forms, and quantum codes. Proceedings of the 2002 IEEE International Symposium on Information Theory, 2002, p. 45.
http://faculty.cs.tamu.edu/klappi/papers/ISIT2002.pdf

[11] Gulliver A. T., J.-L. Kim. Circulant based extremal additive self-dual codes over $GF(4)$. *IEEE Trans. on Inform. Theory* **40** (2004), 359–366.

[12] Hein M., J. Eisert, H. J. Briegel. Multy-party entanglement in graph states,. *Phys. Rev. A* **69**, *6* (2004) 062311, arXiv: quant-ph/0307130.

[13] Höhn G. Self-dual codes over the Kleinian four group. *Math. Ann.* **327**, *2* (2003), 227–255, arXiv:math.CO/0005266.

[14] Huffman W. C. On the classification and enumeration of self-dual codes. *Finite Fields Appl.* **11**, *3* (2005), 451–490.

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

[16] Kim J.-L., V. Pless. Designs in additive codes over $GF(4)$. *Des. Codes Cryptogr.* **30** (2003), 187–199.

[17] Rains E. M., N. J. A. Sloane. Self-dual codes. In: Handbook of Coding Theory (Eds V. S. Pless, W. C. Huffman). Amsterdam, Elsevier, 1998, 177–294.

[18] Schlingemann D. Stabilizer codes can be realized as graph codes. *Quantum Inf. Comput.* **2**, *4* (2002), 307–323, arXiv:quant-ph/0111080.

[19] Schlingemann D., R. F. Werner. Quantum error-correcting codes associated with graphs. *Phys. Rev. A* **65(012308)** (2002), arXiv:quant-ph/0012111.

[20] Tonchev V. D. Error-correcting codes from graphs. *Discrete Math.* **257**, *2–3* (2002), 549–557.

Department of Mathematics and Informatics
Veliko Tarnovo University
5000 Veliko Tarnovo, Bulgaria
e-mail: `vtgold@yahoo.com`

Received October 23, 2006
Final Accepted June 27, 2007