On the classification of all self-dual additive codes over GF(4) of length up to 12

Lars Eirik Danielsen *, Matthew G. Parker

The Selmer Center, Department of Informatics, University of Bergen, PB 7800, N-5020 Bergen, Norway.

Abstract

We consider additive codes over GF(4) that are self-dual with respect to the Hermitian trace inner product. Such codes have a well-known interpretation as quantum codes and correspond to isotropic systems. It has also been shown that these codes can be represented as graphs, and that two codes are equivalent if and only if the corresponding graphs are equivalent with respect to local complementation and graph isomorphism. We use these facts to classify all codes of length up to 12, where previously only all codes of length up to 9 were known. We also classify all extremal Type II codes of length 14. Finally, we find that the smallest Type I and Type II codes with trivial automorphism group have length 9 and 12, respectively.

Key words: Self-dual codes; Graphs; Local complementation

1 Introduction

An *additive* code, $\mathcal{C}$, over GF(4) of *length* n is an additive subgroup of $\mathrm{GF}(4)^n$. $\mathcal{C}$ contains 2^k codewords for some $0 \leq k \leq 2n$, and can be defined by a $k \times n$ *generator matrix*, with entries from GF(4), whose rows span $\mathcal{C}$ additively. $\mathcal{C}$ is called an $(n, 2^k)$ code. We denote $\mathrm{GF}(4) = \{0, 1, \omega, \omega^2\}$, where $\omega^2 = \omega + 1$. *Conjugation* of $x \in \mathrm{GF}(4)$ is defined by $\overline{x} = x^2$. The *trace map*, $\mathrm{Tr} : \mathrm{GF}(4) \rightarrow \mathrm{GF}(2)$, is defined by $\mathrm{Tr}(x) = x + \overline{x}$. The *Hermitian trace inner product* of two

* Corresponding author.
Email addresses: `larsed@ii.uib.no` (Lars Eirik Danielsen), `matthew@ii.uib.no` (Matthew G. Parker).
URLs: `http://www.ii.uib.no/~larsed/` (Lars Eirik Danielsen), `http://www.ii.uib.no/~matthew/` (Matthew G. Parker).

vectors over GF(4) of length n, $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$, is given by

$$\boldsymbol{u} * \boldsymbol{v} = \mathrm{Tr}(\boldsymbol{u} \cdot \overline{\boldsymbol{v}}) = \sum_{i=1}^{n} \mathrm{Tr}(u_i \overline{v_i}) = \sum_{i=1}^{n} (u_i v_i^2 + u_i^2 v_i) \pmod 2. \tag{1}$$

The *Hamming weight* of $\boldsymbol{u}$, denoted $\mathrm{wt}(\boldsymbol{u})$, is the number of nonzero components of $\boldsymbol{u}$. Observe that $\boldsymbol{u} * \boldsymbol{v} \equiv \mathrm{wt}(\boldsymbol{u} + \boldsymbol{v}) \pmod 2$. We define the *dual* of the code $\mathcal{C}$ with respect to the Hermitian trace inner product, $\mathcal{C}^\perp = \{\boldsymbol{u} \in \mathrm{GF}(4)^n \mid \boldsymbol{u} * \boldsymbol{c} = 0 \text{ for all } \boldsymbol{c} \in \mathcal{C}\}$. $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^\perp$. It has been shown that self-orthogonal additive codes over GF(4) can be used to represent *quantum error-correcting codes* [4]. If $\mathcal{C} = \mathcal{C}^\perp$, then $\mathcal{C}$ is *self-dual* and must be an $(n, 2^n)$ code. Self-dual additive codes over GF(4) correspond to zero-dimensional quantum codes, which represent single quantum states. If the code has high minimum distance, the corresponding quantum state is highly *entangled*.

The *Hamming distance* between $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}$ is $\mathrm{wt}(\boldsymbol{u}-\boldsymbol{v})$. The *minimum distance* of the code $\mathcal{C}$ is the minimal Hamming distance between any two distinct codewords of $\mathcal{C}$. Since $\mathcal{C}$ is an additive code, the minimum distance is also given by the smallest nonzero weight of any codeword in $\mathcal{C}$. A code with minimum distance d is called an $(n, 2^k, d)$ code. The *weight distribution* of the code $\mathcal{C}$ is the sequence $(A_0, A_1, \ldots, A_n)$, where A_i is the number of codewords of weight i. The *weight enumerator* of $\mathcal{C}$ is the polynomial

$$W(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i \tag{2}$$

We distinguish between two types of self-dual additive codes over GF(4). A code is of *Type II* if all codewords have even weight, otherwise it is of *Type I*. It can be shown that a Type II code must have even length. Bounds on the minimum distance of self-dual codes were given by Rains and Sloane [19, Theorem 33]. Let d_I be the minimum distance of a Type I code of length n. Then d_I is upper-bounded by

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

There is a similar bound on d_{II}, the minimum distance of a Type II code of length n,

$$d_{II} \leq 2\left\lfloor \frac{n}{6} \right\rfloor + 2. \tag{4}$$

A code that meets the appropriate bound is called *extremal*. It can be shown that extremal Type II codes must have a unique weight enumerator. Rains and

Sloane [19] also used a linear programming bound, and showed that extremal codes do not exist for all lengths. For instance, there is no self-dual $(13, 2^{13}, 6)$ code. If a code has highest possible minimum distance, but is not extremal, it is called *optimal*. An interesting open problem is whether there exists a Type II $(24, 2^{24}, 10)$ code.

A *linear* code, $\mathcal{C}$, over GF(4) which is self-dual with respect to the *Hermitian inner product*, i.e., $\boldsymbol{u} \cdot \overline{\boldsymbol{v}} = 0$ for all $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}$, is also a self-dual *additive* code with respect to the *Hermitian trace inner product*. However, most of the self-dual additive codes are not linear. Only Type II codes can be linear, since self-dual linear codes over GF(4) must contain codewords of even weight only. It follows that the set of Hermitian self-dual linear codes over GF(4) is a subset of the set of Type II self-dual additive codes over GF(4).

Example 1 *The unique extremal* $(6, 2^6, 4)$ *code, also known as the* Hexacode*, has a generator matrix*

$$\begin{pmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ \omega & 0 & 0 & \omega & \omega^2 & \omega^2 \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & \omega & 0 & \omega^2 & \omega & \omega^2 \\ 0 & 0 & 1 & \omega & \omega & 1 \\ 0 & 0 & \omega & \omega^2 & \omega^2 & \omega \end{pmatrix}.$$

This code has weight enumerator $W(x, y) = x^6 + 45x^2y^4 + 18y^6$*. It is therefore of Type II, and it can be verified that it is also a linear code.*

Two self-dual additive codes over GF(4), $\mathcal{C}$ and $\mathcal{C}'$, are *equivalent* if and only if the codewords of $\mathcal{C}$ can be mapped onto the codewords of $\mathcal{C}'$ by a map that preserves self-duality. Such a map must consist of a permutation of coordinates (columns of the generator matrix), followed by multiplication of coordinates by nonzero elements from GF(4), followed by possible conjugation of coordinates. For a code of length n, there is a total of $6^n n!$ such maps. The 6 possible transformations given by scaling and conjugation of a coordinate are equivalent to the 6 permutations of the elements $\{1, \omega, \omega^2\}$ in the coordinate. A map that maps $\mathcal{C}$ to $\mathcal{C}$ is called an *automorphism* of $\mathcal{C}$. All automorphisms of $\mathcal{C}$ make up an *automorphism group*, denoted $\mathrm{Aut}(\mathcal{C})$. The number of distinct codes equivalent to $\mathcal{C}$ is then given by $\frac{6^n n!}{|\mathrm{Aut}(\mathcal{C})|}$. By summing the sizes of all equivalence classes, we find the total number of distinct codes of length n, denoted T_n. It was shown by Höhn [16] that T_n is also given by the *mass formula*,

$$T_n = \prod_{i=1}^{n} (2^i + 1) = \sum_{j=1}^{t_n} \frac{6^n n!}{|\mathrm{Aut}(\mathcal{C}_j)|}, \tag{5}$$

where the sum is over all equivalence classes. Similarly, the total number of distinct Type II codes of length n is given by

$$T_n^{\mathrm{II}} = \prod_{i=0}^{n-1}(2^i+1) = \sum_{j=1}^{t_n^{\mathrm{II}}} \frac{6^n n!}{|\operatorname{Aut}(\mathcal{C}_j)|}, \tag{6}$$

where the sum is over the equivalence classes of Type II codes. By assuming that $|\operatorname{Aut}(\mathcal{C}_j)| = 1$ for all j in Eq. (5), we get a lower bound on t_n, the number of inequivalent codes of length n.

$$t_n \geq \left\lceil \frac{\prod_{i=1}^{n}(2^i+1)}{6^n n!} \right\rceil \tag{7}$$

A similar bound on t_n^{II} can be derived from Eq. (6).

We can use the computational algebra system *Magma* [5] to find the automorphism group of a code. Since, at this time, Magma has no explicit function for calculating the automorphism group of an additive code, we use the following method, described by Calderbank et al. [4]. We map the $(n, 2^k)$ additive code $\mathcal{C}$ over GF(4) to the $[3n, k]$ binary linear code $\beta(\mathcal{C})$ by applying the map $0 \mapsto 000$, $1 \mapsto 011$, $\omega \mapsto 101$, $\omega^2 \mapsto 110$ to each generator of $\mathcal{C}$. We then use Magma to find $\operatorname{Aut}(\beta(\mathcal{C})) \cap \operatorname{Aut}(\beta(\mathrm{GF}(4)^n))$, which will be isomorphic to $\operatorname{Aut}(\mathcal{C})$.

If we are given t_n inequivalent codes of length n, i.e., one code from each equivalence class, it is relatively easy to calculate the automorphism group size of each code, as described above, and verify that the mass formula defined by Eq. (5) gives the correct value. But to actually find a set of t_n inequivalent codes, or just the value of t_n, is a hard problem. All self-dual additive codes over GF(4) of length n were first classified, up to equivalence, by Calderbank et al. [4] for $n \leq 5$ and by Höhn [16] for $n \leq 7$. Höhn also classified all Type II codes of length 8. Using a different terminology, the codes of length n were implicitly classified by Hein, Eisert, and Briegel [14] for $n \leq 7$ and by Glynn et al. [12] for $n \leq 9$. These classifications were not verified using the mass formula defined by Eq. (5). Gaborit et al. [9, 10] have classified all extremal codes of length 8, 9, and 11, and all extremal Type II codes of length 12. Bachoc and Gaborit [1] classified all extremal Type II codes of length 10, and they also showed that there are at least 490 extremal Type II codes of length 14 and gave a partial result on the unicity of the extremal Type II code of length 18. A review of the current status of the classification of various types of self-dual codes is given by Huffman [15].

In this paper, we will give a complete classification of all codes of length up to 12, and all extremal Type II codes of length 14. But first, in Section 2, we introduce *isotropic systems* and show that they correspond to self-dual additive codes over GF(4). It is known that isotropic systems can be represented by graphs. In Section 3 we define *graph codes*. Theorem 6 shows that every code can be represented by a graph. This gives us a much smaller set of objects to work with. In Section 4, we introduce *local complementation*, and Theorem 12 states that two codes are equivalent if and only if the corresponding graphs are related via local complementations and graph isomorphism. This implies that classifying codes up to equivalence is essentially the same as classifying orbits of graphs under local complementation. We describe an algorithm for generating such graph orbits in Section 5. This algorithm was used to classify all codes of length up to 12. We show that Type II codes correspond to a special class of graphs and use this fact to classify all extremal Type II codes of length 14. Finally, we determine that the smallest Type I and Type II codes with trivial automorphism group have length 9 and 12, respectively. In Section 6, we conclude and mention some other results.

2 Isotropic Systems

We define a mapping $\phi : \mathrm{GF}(4) \to \mathrm{GF}(2)^2$ by $\phi(x) = (\mathrm{Tr}(x\omega^2), \mathrm{Tr}(x))$, i.e., $0 \mapsto (0,0)$, $1 \mapsto (1,0)$, $\omega \mapsto (0,1)$ and $\omega^2 \mapsto (1,1)$. The reverse mapping $\phi^{-1} : \mathrm{GF}(2)^2 \to \mathrm{GF}(4)$ is given by $\phi^{-1}(a,b) = a+\omega b$. Let $\boldsymbol{u} \in \mathrm{GF}(2)^{2n}$ be written as $\boldsymbol{u} = (\boldsymbol{a}|\boldsymbol{b}) = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n)$. We extend the mapping $\phi : \mathrm{GF}(4)^n \to \mathrm{GF}(2)^{2n}$ by letting $\phi(\boldsymbol{v}) = (\boldsymbol{a}|\boldsymbol{b})$ where $\phi(v_i) = (a_i, b_i)$. Likewise, we define $\phi^{-1} : \mathrm{GF}(2)^{2n} \to \mathrm{GF}(4)^n$ by $\phi^{-1}(\boldsymbol{a}|\boldsymbol{b}) = \boldsymbol{a}+\omega\boldsymbol{b}$. We define the *symplectic inner product* of $(\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}') \in \mathrm{GF}(2)^{2n}$ as $\langle(\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}')\rangle = \boldsymbol{a}\cdot\boldsymbol{b}' + \boldsymbol{b}\cdot\boldsymbol{a}'$. A subset $\mathcal{I} \subset \mathrm{GF}(2)^{2n}$ is called *totally isotropic* if $\langle \boldsymbol{u}, \boldsymbol{v}\rangle = 0$ for all $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{I}$.

Definition 2 *A totally isotropic linear subspace of* $\mathrm{GF}(2)^{2n}$ *with dimension* n *defines an* isotropic system *[2]. An isotropic system can therefore be defined by the row space of a full rank* $n\times 2n$ *binary matrix* $(A|B)$*, where* $AB^T+BA^T = \mathbf{0}$.

Theorem 3 *Every self-dual additive code over* $\mathrm{GF}(4)$ *can be uniquely represented as an isotropic system, and every isotropic system can be uniquely represented as a self-dual additive code over* $\mathrm{GF}(4)$.

PROOF. Let $\mathcal{C} \subset \mathrm{GF}(4)^n$ be a self-dual additive code. Map $\mathcal{C}$ to $\mathcal{I} \subset \mathrm{GF}(2)^{2n}$ by mapping each codeword $\boldsymbol{u} \in \mathcal{C}$ to $\phi(\boldsymbol{u}) = (\boldsymbol{a}|\boldsymbol{b}) \in \mathrm{GF}(2)^{2n}$. $\mathcal{I}$ must then be a linear subspace of $\mathrm{GF}(2)^{2n}$ with dimension n. $(\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}') \in \mathcal{I}$ are orthogonal with respect to the symplectic inner product if and only if $\phi^{-1}(\boldsymbol{a}|\boldsymbol{b}), \phi^{-1}(\boldsymbol{a}'|\boldsymbol{b}') \in \mathcal{C}$ are orthogonal with respect to the Hermitian trace inner product, because

$$
\begin{aligned}
&\phi^{-1}(\boldsymbol{a}|\boldsymbol{b}) * \phi^{-1}(\boldsymbol{a}'|\boldsymbol{b}') \\
=& \operatorname{Tr}(\phi^{-1}(\boldsymbol{a}|\boldsymbol{b}) \cdot \overline{\phi^{-1}(\boldsymbol{a}'|\boldsymbol{b}')}) \\
=& \operatorname{Tr}((\boldsymbol{a} + \omega\boldsymbol{b}) \cdot (\boldsymbol{a}' + \overline{\omega}\boldsymbol{b}')) \\
=& (\boldsymbol{a} \cdot \boldsymbol{a}') \operatorname{Tr}(1) + (\boldsymbol{a} \cdot \boldsymbol{b}') \operatorname{Tr}(\overline{\omega}) + (\boldsymbol{b} \cdot \boldsymbol{a}') \operatorname{Tr}(\omega) + (\boldsymbol{b} \cdot \boldsymbol{b}') \operatorname{Tr}(1) \\
=& \boldsymbol{a} \cdot \boldsymbol{b}' + \boldsymbol{b} \cdot \boldsymbol{a}'.
\end{aligned}
$$

Since $\mathcal{C}$ is self-dual, $\boldsymbol{u} * \boldsymbol{v} = 0$ for all $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}$, and $\mathcal{I}$ must therefore be totally isotropic. It follows that $\mathcal{I}$ defines an isotropic system. Likewise, the reverse mapping from an isotropic system to a subset of $\mathrm{GF}(4)^n$ will always give a self-dual additive code over GF(4). $\square$

Example 4 *The row-space of* $(A|B)$ *defines an isotropic system, while* $C = A + \omega B$ *is a generator matrix of the* $(6, 2^6, 4)$ *Hexacode.*

$$
(A|B) = \left(\begin{array}{cccccc|cccccc}
1&0&0&1&0&0&0&0&0&0&1&1\\
0&0&0&0&1&1&1&0&0&1&1&1\\
0&1&0&0&1&0&0&0&0&1&0&1\\
0&0&0&1&0&1&0&1&0&1&1&1\\
0&0&1&0&0&1&0&0&0&1&1&0\\
0&0&0&1&1&0&0&0&1&1&1&1
\end{array}\right)
\qquad
C = \begin{pmatrix}
1&0&0&1&\omega&\omega\\
\omega&0&0&\omega&\omega^2&\omega^2\\
0&1&0&\omega&1&\omega\\
0&\omega&0&\omega^2&\omega&\omega^2\\
0&0&1&\omega&\omega&1\\
0&0&\omega&\omega^2&\omega^2&\omega
\end{pmatrix}
$$

3 Graph Representation

A *graph* is a pair $G = (V, E)$ where V is a set of *vertices*, and $E \subseteq V \times V$ is a set of *edges*. A graph with n vertices can be represented by an $n \times n$ *adjacency matrix* Γ, where $\gamma_{ij} = 1$ if $\{i, j\} \in E$, and $\gamma_{ij} = 0$ otherwise. We will only consider *simple undirected* graphs whose adjacency matrices are symmetric with all diagonal elements being 0. The *neighbourhood* of $v \in V$, denoted $N_v \subset V$, is the set of vertices connected to v by an edge. The number of vertices adjacent to v, $|N_v|$, is called the *degree* of v. The *induced subgraph* of G on $W \subseteq V$ contains vertices W and all edges from E whose endpoints are both in W. The *complement* of G is found by replacing E with $V \times V - E$, i.e., the edges in E are changed to non-edges, and the non-edges to edges. Two graphs $G = (V, E)$ and $G' = (V, E')$ are *isomorphic* if and only if there exists a permutation π of V such that $\{u, v\} \in E \iff \{\pi(u), \pi(v)\} \in E'$. A *path* is a sequence of vertices, $(v_1, v_2, \ldots, v_i)$, such that $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{i-1}, v_i\} \in E$. A graph is *connected* if there is a path from any vertex to any other vertex in the graph.

Definition 5 *A* graph code *is an additive code over* GF(4) *that has a generator matrix of the form* $C = \Gamma + \omega I$*, where* I *is the identity matrix and* Γ *is the adjacency matrix of a simple undirected graph.*

A graph code is always self-dual, since its generator matrix has full rank over GF(2) and $C\overline{C}^{\mathrm{T}}$ only contains entries from GF(2) whose traces must be zero. This construction for self-dual additive codes over GF(4) has also been used by Tonchev [24].

Theorem 6 *Every self-dual additive code over* GF(4) *is equivalent to a graph code.*

PROOF. (This proof is due to Van den Nest, Dehaene, and De Moor [25,26].) We recall that the generator matrix of a self-dual additive code over GF(4) corresponds to an $n \times 2n$ binary matrix $(A|B)$, such that $C = A + \omega B$. The row-space of $(A|B)$, denoted $\mathcal{I}$, defines an isotropic system. We must prove that $\mathcal{I}$ is also generated by $(\Gamma|I)$, where I is the identity matrix and Γ is the adjacency matrix of a simple undirected graph.

The rows of $(A|B)$ can be replaced by any n independent vectors from $\mathcal{I}$. This basis change can be accomplished by $(A'|B') = M(A|B)$, where M is an $n \times n$ invertible binary matrix. If B is invertible, the solution is simple, since $B^{-1}(A|B) = (\Gamma|I)$. Note that Γ will always be a symmetric matrix, since $\Gamma I^{\mathrm{T}} + I\Gamma^{\mathrm{T}} = 0$. If the ith diagonal element of Γ is 1, it can be set to 0 by conjugating column i of $\Gamma + \omega I$.

In the case where B has rank $k < n$, we can perform a basis change to get

$$(A'|B') = \left(\begin{array}{c|c} A_1 & B_1 \\ A_2 & \mathbf{0} \end{array}\right),$$

where B_1 is a $k \times n$ matrix with full rank, and A_1 also has size $k \times n$. Since the row-space of $(A'|B')$ is totally isotropic, and B' contains an all-zero row, it must be true that $A_2 B_1^{\mathrm{T}} = \mathbf{0}$. A_2 must have full rank, and the row space of B_1 must be the orthogonal complement of the row space of A_2.

We assume that $B_1 = (B_{11}|B_{12})$ where B_{11} is a $k \times k$ invertible matrix. We also write $A_2 = (A_{21}|A_{22})$ where A_{22} has size $(n-k) \times (n-k)$. Assume that there exists an $\boldsymbol{x} \in \mathrm{GF}(2)^{n-k}$ such that $A_{22}\boldsymbol{x}^{\mathrm{T}} = 0$. Then the vector $\boldsymbol{v} = (0, \ldots, 0, \boldsymbol{x})$ of length n satisfies $A_2\boldsymbol{v}^{\mathrm{T}} = 0$. Since the row space of B_1 is the orthogonal complement of the row space of A_2, we can write $\boldsymbol{v} = \boldsymbol{y}B_1$ for some $\boldsymbol{y} \in \mathrm{GF}(2)^k$. We see that $\boldsymbol{y}B_{11} = 0$, and since B_{11} has full rank, it must therefore be true that $\boldsymbol{y} = 0$. This means that $\boldsymbol{x} = 0$, which proves that A_{22} is an invertible matrix.

Interchanging column i of A' and column i of B' corresponds to multiplication by ω^2 followed by conjugation of the ith column of $A' + \omega B'$. We can therefore swap the ith columns of A' and B' for $k < i \leq n$ to get $(A''|B'')$. Since B_{11}

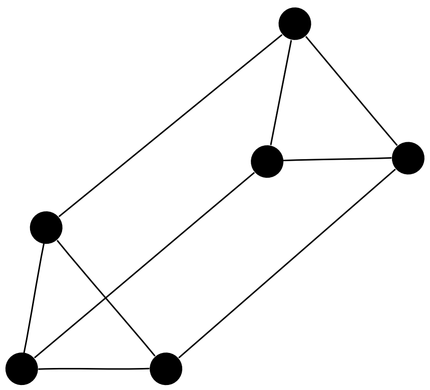

Fig. 1. Graph Representation of the Hexacode

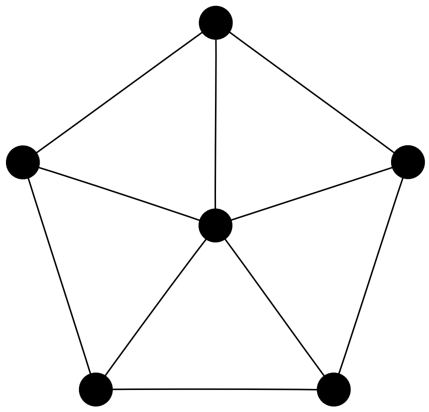

Fig. 2. Alternate Graph Representation of the Hexacode

and A_{22} are invertible, B'' must also be an invertible matrix. We then find $B''^{-1}(A''|B'') = (\Gamma|I)$, and set all diagonal elements of Γ to 0. $\square$

Example 7 *Let $C = A+\omega B$ be the generator matrix of the $(6, 2^6, 4)$ Hexacode given in Example 4. By the method described in the proof of Theorem 6, we find $C' = \Gamma+\omega I$, which generates an equivalent graph code. Γ is the adjacency matrix of the graph shown in Fig. 2.*

$$(A|B) = \left(\begin{array}{cccccc|cccccc} 1&0&0&1&0&0&0&0&0&0&1&1 \\ 0&0&0&0&1&1&1&0&0&1&1&1 \\ 0&1&0&0&1&0&0&0&0&1&0&1 \\ 0&0&0&1&0&1&0&1&0&1&1&1 \\ 0&0&1&0&0&1&0&0&0&1&1&0 \\ 0&0&0&1&1&0&0&0&1&1&1&1 \end{array}\right) \qquad (\Gamma|I) = \left(\begin{array}{cccccc|cccccc} 0&0&1&0&1&1&1&0&0&0&0&0 \\ 0&0&1&1&0&1&0&1&0&0&0&0 \\ 1&1&0&0&0&1&0&0&1&0&0&0 \\ 0&1&0&0&1&1&0&0&0&1&0&0 \\ 1&0&0&1&0&1&0&0&0&0&1&0 \\ 1&1&1&1&1&0&0&0&0&0&0&1 \end{array}\right)$$

$$C' = \begin{pmatrix} \omega&0&1&0&1&1 \\ 0&\omega&1&1&0&1 \\ 1&1&\omega&0&0&1 \\ 0&1&0&\omega&1&1 \\ 1&0&0&1&\omega&1 \\ 1&1&1&1&1&\omega \end{pmatrix}$$

Theorem 6 was first proved by Bouchet [3] in the context of isotropic systems, and later by Schlingemann [20] in terms of *quantum stabilizer states*. Proofs of Theorem 6 have also been given by Schlingemann and Werner [21], by Grassl, Klappenecker, and Rötteler [13], by Glynn et al. [11,12], and by Van den Nest et al. [25, 26].

Swapping vertex i and vertex j of a graph with adjacency matrix Γ can be accomplished by exchanging column i and column j of Γ and then exchanging row i and row j of Γ. We call the resulting matrix Γ'. Exactly the same column and row operations map $\Gamma+\omega I$ to $\Gamma'+\omega I$. These matrices generate equivalent

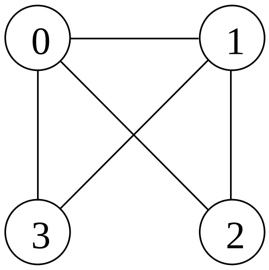

Fig. 3. The Graph G

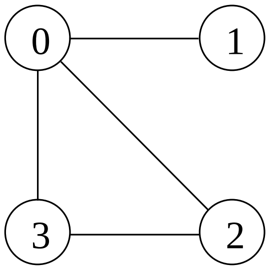

Fig. 4. The LC Image G^0

codes. It follows that two codes are equivalent if their corresponding graphs are isomorphic.

We have seen that every graph represents a self-dual additive code over GF(4), and that every self-dual additive code over GF(4) can be represented by a graph. It follows that we can, without loss of generality, restrict our study to codes with generator matrices of the form $\Gamma + \omega I$, where Γ are adjacency matrices of unlabeled simple undirected graphs.

4 Local Complementation

Definition 8 *Given a graph $G = (V, E)$ and a vertex $v \in V$, let $N_v \subset V$ be the neighbourhood of v.* Local complementation *(LC) on v transforms G into G^v. To obtain G^v, we replace the induced subgraph of G on N_v by its complement. It is easy to verify that $(G^v)^v = G$.*

Example 9 *We will perform local complementation on vertex 0 of the graph G, shown in Fig. 3. We see that the neighbourhood of 0 is $N_0 = \{1, 2, 3\}$ and that the induced subgraph on the neighbourhood has edges $\{1, 2\}$ and $\{1, 3\}$. The complement of this subgraph contains the single edge $\{2, 3\}$. The resulting LC image, G^0, is seen in Fig. 4.*

Example 10 *Consider the graph shown in Fig. 1, whose corresponding graph code is the Hexacode. An LC operation on any vertex of this graph produces the graph shown in Fig. 2. An LC operation on the vertex in the centre of the graph shown in Fig. 2 gives the same graph, up to isomorphism. LC operations on any of the other five vertices produces the graph shown in Fig. 1.*

Theorem 11 *Let Γ be the adjacency matrix of the graph $G = (V, E)$, and Γ^v be the adjacency matrix of G^v, for any $v \in V$. The codes generated by $C = \Gamma + \omega I$ and $C' = \Gamma^v + \omega I$ are equivalent.*

PROOF. We show that C can be transformed into C' by using only operations that map a code to an equivalent code. Each row and each column of C correspond to a vertex in V. Let N_v denote the neighbourhood of v. For all $i \in N_v$, add row v of C to row i of C. Multiply column v of C by ω and then conjugate the same column. Finally, conjugate column i of C, for all $i \in N_v$. The resulting matrix is C'. $\square$

Theorem 12 *Two self-dual additive codes over* GF(4)*,* $\mathcal{C}$ *and* $\mathcal{C}'$*, with graph representations* G *and* G'*, are equivalent if and only if there is a finite sequence of not necessarily distinct vertices* $(v_1, v_2, \ldots, v_i)$*, such that* $(((G^{v_1})^{v_2})^{\cdots})^{v_i}$ *is isomorphic to* G'*.*

Sketch of proof Let Γ be the adjacency matrix of G, and let $\mathcal{C}_G$ be the code generated by $\Gamma + \omega I$. Likewise, let Γ' be the adjacency matrix of G', and let $\mathcal{C}'_G$ be the code generated by $\Gamma' + \omega I$. If the codewords of $\mathcal{C}$ are mapped onto the codewords of $\mathcal{C}'$ by one of the $6^n n!$ combinations of coordinate permutations, coordinate scalings, and coordinate conjugations, then there must also be a transformation from this set that maps the codewords of $\mathcal{C}_G$ onto the codewords of $\mathcal{C}'_G$. Consequently, we only need to consider those transformations that map a graph code to another graph code. The codes obtained by the $n!$ possible permutations of coordinates correspond to graph isomorphisms.

Let $C = \Gamma + \omega I$ be transformed into $C' = A + \omega B$ by coordinate scalings and conjugations. Then C' is a graph code if and only if B is invertible and all diagonal elements of $B^{-1}A$ are zero. It is easy to verify that conjugation of column i of C' has no effect on B, but flips the value of the ith diagonal element of $B^{-1}A$. Given a combination of column scalings on C such that the resulting B is invertible, there must therefore be a unique combination of column conjugations on C such that the resulting $B^{-1}A$ has zero diagonal. We must therefore show that any combination of column scalings on C that give an invertible B can be performed by a sequence of LC operations on G.

Multiplying column i of C by ω^2 replaces column i of I with column i of Γ. Multiplying column i of C by ω adds column i of Γ to column i of I. It is then possible to show which of the 3^n possible scalings do not give an invertible B. A vertex v of G corresponds to a column of Γ. The neighbourhood of v, N_v, corresponds to a set of columns of Γ. We know from Theorem 11 that an LC operation on vertex i of G corresponds to a scaling of column i of C by ω followed by conjugation of column i and all columns in N_i. Observe that conjugating a coordinate followed by a scaling by ω is equivalent to scaling by ω^2 followed by conjugation. Note in particular that the local complementations $((G^i)^j)^i$, where i and j are adjacent vertices, are equivalent to scaling both column i and column j of C by ω^2. It can be verified that any combination of column scalings that map a graph code to a graph code can be implemented as a sequence of LC operations. The exact algorithm for finding this sequence of LC operations is quite involved, and we refer to the proof by Van den Nest et al. [25, 26] for the details. □

Bouchet [3] first proved Theorem 12 in terms of isotropic systems. The same result was discovered by Van den Nest et al. [25, 26] in terms of quantum stabilizer states, and by Glynn et al. [11, 12] using finite geometry.

5 Classification

Definition 13 *The* LC orbit *of a graph G is the set of all unlabeled graphs that can be obtained by performing any sequence of LC operations on G.*

It follows from Theorem 12 that two self-dual additive codes over GF(4) are equivalent if and only if their graph representations are in the same LC orbit. As an example, the two graphs shown in Fig. 1 and Fig. 2 make up a complete LC orbit, and are thus the only possible graph representations of the Hexacode. The LC orbit of a graph can easily be generated by a recursive algorithm. We have used the program *nauty* [18] to check for graph isomorphism.

Let $\boldsymbol{G}_n$ be the set of all unlabeled simple undirected connected graphs on n vertices. Connected graphs correspond to *indecomposable* codes. A code is decomposable if it can be written as the *direct sum* of two smaller codes. For example, let $\mathcal{C}$ be an $(n, 2^n, d)$ code and $\mathcal{C}'$ an $(n', 2^{n'}, d')$ code. The direct sum, $\mathcal{C} \oplus \mathcal{C}' = \{u||v \mid u \in \mathcal{C}, v \in \mathcal{C}'\}$, where $||$ means concatenation, is an $(n+n', 2^{n+n'}, \min\{d, d'\})$ code. It follows that all decomposable codes of length n can be classified easily once all indecomposable codes of length less than n are known.

The set of all distinct LC orbits of connected graphs on n vertices is a partitioning of $\boldsymbol{G}_n$ into i_n disjoint sets. i_n is also the number of indecomposable self-dual additive codes over GF(4) of length n, up to equivalence. Let $\boldsymbol{L}_n$ be a set containing one representative from each LC orbit of connected graphs on n vertices. We have devised several algorithms [7] for finding such sets of representatives. The simplest approach is to start with the set $\boldsymbol{G}_n$ and generate LC orbits of its members until we have a partitioning of $\boldsymbol{G}_n$. The following more efficient technique was described by Glynn et al. [12]. Let the $2^n - 1$ *extensions* of a graph on n vertices be formed by adding a new vertex and joining it to all possible combinations of at least one of the old vertices. The set $\boldsymbol{E}_n$, containing $i_{n-1}(2^{n-1} - 1)$ graphs, is formed by making all possible extensions of all graphs in $\boldsymbol{L}_{n-1}$.

Theorem 14 *$\boldsymbol{L}_n \subset \boldsymbol{E}_n$, i.e., the set $\boldsymbol{E}_n$ will contain at least one representative from each LC orbit of connected graphs on n vertices.*

PROOF. Let $G = (V, E) \in \boldsymbol{G}_n$, and choose any subset $W \subset V$ of $n-1$ vertices. By doing LC operations on vertices in W, we can transform the induced subgraph of G on W into one of the graphs in $\boldsymbol{L}_{n-1}$ that were extended when $\boldsymbol{E}_n$ was constructed. It follows that for all $G \in \boldsymbol{G}_n$, some graph in the LC orbit of G must be part of $\boldsymbol{E}_n$. $\square$

The set $\boldsymbol{E}_n$ will be much smaller than $\boldsymbol{G}_n$, so it will be more efficient to search for a set of LC orbit representatives within $\boldsymbol{E}_n$. It is also desirable to partition the set $\boldsymbol{E}_n$ such that graphs from two different partitions are guaranteed to belong to different LC orbits. We can then consider each partition independently, which reduces the amount of memory required and allow for parallel processing. To do this, we must have some property that is invariant over the LC orbit and that can be calculated quickly.

The special form of the generator matrix of a graph code makes it easier to find the number of codewords of weight $i < n$. If $\mathcal{C}$ is generated by $C = \Gamma + \omega I$, then any codeword formed by adding i rows of C must have weight at least i. This means that we can find the *partial weight distribution* of $\mathcal{C}$, $(A_0, A_1, \ldots, A_j)$, for some $j < n$, by only considering codewords formed by adding j or fewer rows of C. We calculate the partial weight distribution, for a suitable choice of j, of all codes corresponding to graphs in $\boldsymbol{E}_n$. Codes with different partial weight distribution can never be equivalent, so we partition $\boldsymbol{E}_n$ such that graphs corresponding to codes with the same partial weight distribution are always in the same partition.

Using the described techniques, and a parallel cluster computer, we were able to classify all self-dual additive codes over GF(4) of length up to 12. The results have been verified by checking that the sizes of all LC orbits add up to the number of graphs in $\boldsymbol{G}_n$. The sizes of the automorphism groups of all codes have also been calculated, and it has been verified that that the mass formulas defined by Eq. (5) and Eq. (6) give the correct values. Table 1 gives the values of i_n, the number of distinct LC orbits of connected graphs on n vertices, which is also the number of inequivalent indecomposable codes of length n. The table also gives the values of i_n^{II}, the number of indecomposable Type II codes. The total number of inequivalent codes of length n, t_n, and the total number of Type II codes of length n, t_n^{II}, are shown in Table 2. The numbers t_n are easily derived from the numbers i_n by using the *Euler transform* [23],

Table 1
Number of Indecomposable (i_n) and Indecomposable Type II (i_n^{II}) Codes of Length n

n	1	2	3	4	5	6	7	8	9	10	11	12
i_n	1	1	1	2	4	11	26	101	440	3,132	40,457	1,274,068
i_n^{II}		1		1		4		14		103		2,926

Table 2
Total Number (t_n) and Number of Type II (t_n^{II}) Codes of Length n

n	1	2	3	4	5	6	7	8	9	10	11	12
t_n	1	2	3	6	11	26	59	182	675	3,990	45,144	1,323,363
t_n^{II}		1		2		6		21		128		3,079

Table 3
Number of Indecomposable Codes of Length n and Minimum Distance d

$d\backslash n$	2	3	4	5	6	7	8	9	10	11	12
2	1	1	2	3	9	22	85	363	2,436	26,750	611,036
3				1	1	4	11	69	576	11,200	467,513
4					1		5	8	120	2,506	195,455
5										1	63
6											1
All	1	1	2	4	11	26	101	440	3,132	40,457	1,274,068

$$
\begin{aligned}
c_n &= \sum_{d|n} d i_d \\
t_1 &= c_1 \\
t_n &= \frac{1}{n}\left(c_n + \sum_{k=1}^{n-1} c_k t_{n-k}\right).
\end{aligned}
$$

The numbers t_n^{II} are similarly derived from i_n^{II}. The values of i_n and t_n can be found as sequences A090899 and A094927 in *The On-Line Encyclopedia of Integer Sequences* [22]. Table 3 and Table 4 list by minimum distance the numbers of indecomposable codes and the total numbers of codes. [1] Table 5 and Table 6 similarly list the numbers of Type II codes by minimum distance. The numbers of Type I codes can be obtained by subtracting the numbers of Type II codes from the total numbers. The number of distinct weight enumerators of all codes of length n and minimum distance d can be found in Table 7. There are obviously too many codes to give a complete list here, but a database containing one representative from each equivalence class, with information about weight enumerators, automorphism groups, etc., is available on-line [6].

Our results give a complete classification of the extremal Type I $(10, 2^{10}, 4)$ and $(12, 2^{12}, 5)$ codes. These classifications were previously unknown. The 101

[1] Note that some authors [10, 15] give 3 as the total number of self-dual $(7, 2^7, 3)$ codes. The correct number is 4.

Table 4
Total Number of Codes of Length n and Minimum Distance d

$d\backslash n$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	2	3	6	11	26	59	182	675	3,990	45,144
2		1	1	3	4	13	29	107	416	2,618	27,445	615,180
3					1	1	4	11	69	577	11,202	467,519
4						1		5	8	120	2,506	195,456
5											1	63
6												1
All	1	2	3	6	11	26	59	182	675	3,990	45,144	1,323,363

Table 5
Number of Indecomposable Type II Codes of Length n and Minimum Distance d

$d\backslash n$	2	4	6	8	10	12	14
2	1	1	3	11	84	2,133	?
4			1	3	19	792	?
6						1	1,020
Total	1	1	4	14	103	2,926	?

Table 6
Total Number of Type II Codes of Length n and Minimum Distance d

$d\backslash n$	2	4	6	8	10	12	14
2	1	2	5	18	109	2,285	?
4			1	3	19	793	?
6						1	1,020
Total	1	2	6	21	128	3,079	$\geq$ 1,727,942

Table 7
Number of Distinct Weight Enumerators of All Codes of Length n and Minimum Distance d

$d\backslash n$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	2	3	5	10	23	46	116	320	909	3,312
2		1	1	2	4	11	21	64	187	549	2,249	11,419
3					1	1	2	4	15	33	125	625
4						1		2	2	7	28	178
5											1	2
6												1
All	1	2	3	5	10	23	46	116	320	909	3,312	15,537

extremal Type I $(10, 2^{10}, 4)$ codes have 6 distinct weight enumerators,

$$\begin{aligned}
W_{10,1}(x,y) &= x^{10} + 10x^6y^4 + 72x^5y^5 + 160x^4y^6 + 240x^3y^7 + 285x^2y^8 + \\
&\quad 200xy^9 + 56y^{10}, \\
W_{10,2}(x,y) &= x^{10} + 14x^6y^4 + 64x^5y^5 + 156x^4y^6 + 256x^3y^7 + 281x^2y^8 + \\
&\quad 192xy^9 + 60y^{10}, \\
W_{10,3}(x,y) &= x^{10} + 18x^6y^4 + 56x^5y^5 + 152x^4y^6 + 272x^3y^7 + 277x^2y^8 + \\
&\quad 184xy^9 + 64y^{10}, \\
W_{10,4}(x,y) &= x^{10} + 22x^6y^4 + 48x^5y^5 + 148x^4y^6 + 288x^3y^7 + 273x^2y^8 + \\
&\quad 176xy^9 + 68y^{10}, \\
W_{10,5}(x,y) &= x^{10} + 26x^6y^4 + 40x^5y^5 + 144x^4y^6 + 304x^3y^7 + 269x^2y^8 + \\
&\quad 168xy^9 + 72y^{10}, \\
W_{10,6}(x,y) &= x^{10} + 30x^6y^4 + 32x^5y^5 + 140x^4y^6 + 320x^3y^7 + 265x^2y^8 + \\
&\quad 160xy^9 + 76y^{10}.
\end{aligned}$$

Table 8
Number of Extremal Type I $(10, 2^{10}, 4)$ Codes with Weight Enumerator w and Automorphism Group of Size a

$a\backslash w$	$W_{10,1}$	$W_{10,2}$	$W_{10,3}$	$W_{10,4}$	$W_{10,5}$	$W_{10,6}$	All
1		3					3
2	2	9	7	2			20
4	5	9	7	1			22
6	1			1			2
8	1	4	3		1		9
12		1					1
16	1	1	6	5	3		16
32	2	2	2	1	2		9
40	1						1
48	1			3			4
64			2				2
128		2					2
192		1	2		1		4
256						2	2
320	1					1	2
384						1	1
3840						1	1
All	15	32	29	13	7	5	101

Table 9
Number of Extremal Type I $(12, 2^{12}, 5)$ Codes with Weight Enumerator w and Automorphism Group of Size a

$a\backslash w$	$W_{12,1}$	$W_{12,2}$	All
1		25	25
2		23	23
3		1	1
4	3	4	7
6	1	3	4
8		2	2
24		1	1
All	4	59	63

Table 8 lists the number of such codes by weight enumerator and automorphism group size. The 63 extremal Type I $(12, 2^{12}, 5)$ codes have 2 distinct weight enumerators,

$$\begin{aligned}
W_{12,1}(x, y) = {} & x^{12} + 40x^7y^5 + 212x^6y^6 + 424x^5y^7 + 725x^4y^8 + 1080x^3y^9 + \\
& 980x^2y^{10} + 504xy^{11} + 130y^{12}, \\
W_{12,2}(x, y) = {} & x^{12} + 48x^7y^5 + 188x^6y^6 + 432x^5y^7 + 765x^4y^8 + 1040x^3y^9 + \\
& 972x^2y^{10} + 528xy^{11} + 122y^{12}.
\end{aligned}$$

Table 9 lists the number of such codes by weight enumerator and automorphism group size.

By observing that graphs corresponding to Type II codes have a special property, we are able to extend our classification to all the 1,020 extremal Type II $(14, 2^{14}, 6)$ codes. It was previously shown by Bachoc and Gaborit [1] that there are at least 490 such codes.

Theorem 15 *Let* Γ *be the adjacency matrix of the graph* G. *The code* $\mathcal{C}$ *generated by* $\Gamma + \omega I$ *is of Type II if and only if* G *is* anti-Eulerian*, i.e., if all its vertices have odd degree.*

PROOF. From the definition of the Hermitian trace inner product it follows that $\boldsymbol{u} * \boldsymbol{v} = 0$ when $\mathrm{wt}(\boldsymbol{u} + \boldsymbol{v})$ is even. This means that $\mathcal{C}$ is self-dual only if the sum of any two codewords of $\mathcal{C}$ has even weight. Thus all codewords with odd weight must appear as rows of all generator matrices of $\mathcal{C}$, and a code is of Type II if and only if all rows of one generator matrix of the code have even weight. Thus $\mathcal{C}$ is of Type II if and only if all rows of $\Gamma + \omega I$ have even weight, which means that all rows of Γ must have odd weight. □

An anti-Eulerian graph is the complement of an *Eulerian graph*, i.e., a graph where all vertices have even degree. It is easy to show that all anti-Eulerian graphs must have an even number of vertices, and it follows that all Type II codes must have even length. To classify Type II codes of length 14, we proceed as follows. We take the set $\boldsymbol{L}_{12}$ containing 1,274,068 LC orbit representatives of graphs on 12 vertices. All these graphs are then extended, but in a slightly different way than earlier. To each graph we add one vertex and join it to all possible combinations of at least one of the old vertices. To each obtained graph we then add a second vertex and join it to those of the 13 other vertices that have even degree. (If the result is not a connected anti-Eulerian graph, it is rejected.) By an argument similar to Theorem 14, it can be shown that all graphs corresponding to Type II codes of length 14 must be part of this extended set. Classifying all Type II codes of length 14 turned out to be infeasible with our computational resources. Even when using partitioning by partial weight distribution, the largest partitions were too large to be processed. However, we were able to generate the LC orbits of all graphs corresponding to $(14, 2^{14}, 6)$ codes. Extremal Type II codes have a unique weight enumerator, and the weight enumerator of a $(14, 2^{14}, 6)$ code must be

$$W_{14}(x, y) = x^{14} + 273x^8y^6 + 2457x^6y^8 + 7098x^4y^{10} + 6006x^2y^{12} + 549y^{14}.$$

Table 10 lists the number of codes by automorphism group size. Note that codes with 21, 168, and 2184 automorphisms were previously unknown. Generator matrices of the codes are available on-line [6].

As mentioned before, the set of self-dual *linear* codes over GF(4) is a subset of the self-dual additive codes of Type II. Note that conjugation of sin-

Table 10
Number of $(14, 2^{14}, 6)$ Codes with Automorphism Group of Size a

a	
1	625
2	258
3	27
4	38
6	27
8	13
12	7
18	1
21	1
24	16
28	1
36	1
48	1
84	1
168	1
2184	1
6552	1
All	1020

gle coordinates does not preserve the linearity of a code. It was shown by Van den Nest [25] that the code $\mathcal{C}$ generated by a matrix of the form $\Gamma + \omega I$ can not be linear. However, if there is a linear code equivalent to $\mathcal{C}$, it can be found by conjugating some coordinates. Conjugating coordinates of $\mathcal{C}$ is equivalent to setting some diagonal elements of Γ to 1. Let A be a binary diagonal matrix such that $\Gamma + A + \omega I$ generates a linear code. Van den Nest [25] proved that $\mathcal{C}$ is equivalent to a linear code if and only if there exists such a matrix A that satisfies $\Gamma^2 + A\Gamma + \Gamma A + \Gamma + I = 0$. A similar result was found by Glynn et al. [12]. Using this method, it is easy to check whether the LC orbit of a given graph corresponds to a linear code. However, self-dual linear codes over GF(4) have already been classified up to length 16, and we have not found a way to extend this result using the graph approach.

We remark that if $\mathcal{C}$ is a self-dual additive code over GF(4) with generator matrix $\Gamma + \omega I$, it can be shown that the additive code over $\mathbb{Z}_4$ generated by $2\Gamma + I$ has the same weight distribution as $\mathcal{C}$. It has also been shown [19] that self-dual additive codes over GF(4) can be mapped to *isodual* binary linear codes, i.e., codes that are equivalent to their duals, by the mapping $0 \mapsto 00$, $1 \mapsto 11$, $\omega \mapsto 01$ and $\omega^2 \mapsto 10$. A code over $\mathbb{Z}_4$ and a binary code obtained from the same self-dual additive code over GF(4) by these two methods are related by the well-known *Gray map*. There are also severals mappings from self-dual additive codes over GF(4) to self-dual and self-orthogonal binary linear codes [10, 16, 17].

An interesting problem, posed by Höhn [16], is to find the smallest code with trivial automorphism group, i.e., automorphism group of size 1. We find that there is no such code of length up to 8, but there is a single code of length 9 with trivial automorphism group. This code has generator matrix

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

The smallest Type II codes with trivial automorphism groups have length 12. One such code is generated by

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

Table 11 lists the numbers of Type I and Type II codes with trivial automorphism group by length and minimum distance. Note that for length 12, almost half the codes have trivial automorphism group. For high lengths, one can expect almost all codes to have trivial automorphism group [16]. This implies that the bound on t_n given by Eq. (7) is tighter for higher n. Observe that in Table 11, no code of minimum distance less than 3 is listed. It is easy to show that all codes with minimum distance 1 or 2 must have nontrivial automorphisms.

6 Conclusions

By using graph representation and equivalence via local complementation, we have classified all additive codes over GF(4) of length up to 12 that are self-

Table 11
Number of Type I (Type II) Codes of Length n and Minimum Distance d with Trivial Automorphism Group

$d\backslash n$	≤ 8	9	10	11	12	14
3		1 (0)	113 (0)	6,247 (0)	392,649 (0)	? (0)
4			3 (0)	1,180 (0)	163,982 (102)	? (?)
5					25 (0)	? (0)
6						? (625)
All	0 (0)	1 (0)	116 (0)	7,427 (0)	556,656 (102)	? (?)

dual with respect to the Hermitian trace inner product. It follows from the bound given by Eq. (7) that there are at least 72,573,549 codes of length 13. It is not feasible to classify all codes of length 13 using our method and the computational resources available to us. We were however able to classify the 1,020 extremal Type II $(14, 2^{14}, 6)$ codes. This was done by exploiting the fact that Type II codes correspond to anti-Eulerian graphs. Finally, we showed that the smallest Type I and Type II codes with trivial automorphism group have length 9 and 12, respectively.

The graph representation of a self-dual additive code over GF(4) can also give information about the properties of the code. Tonchev [24] showed that *strongly regular* graphs give rise to interesting codes. In particular, codes represented by the strongly regular *Paley graphs* are well-known *quadratic residue codes*. We have shown that many extremal and optimal codes can be represented by *nested regular graphs* [7, 8]. Glynn et al. [12] showed that the minimum distance of a code is equal to one plus the minimum *vertex degree* over all graphs in the corresponding LC orbit. We have shown that the LC orbit corresponding to a code with high minimum distance only contains graphs with both small *independent sets* and small *cliques* [7, 8].

Acknowledgements

We would like to thank Philippe Gaborit for his helpful comments. Also thanks to the Bergen Center for Computational Science, whose cluster computer made the results in this paper possible. This research was supported by the Research Council of Norway.

References

[1] C. Bachoc, P. Gaborit, On extremal additive $\mathbb{F}_4$ codes of length 10 to 18, J. Théor. Nombres Bordeaux 12 (2) (2000) 255–271.

[2] A. Bouchet, Isotropic systems, European J. Combin. 8 (3) (1987) 231–244.

[3] A. Bouchet, Graphic presentations of isotropic systems, J. Combin. Theory Ser. B 45 (1) (1988) 58–76.

[4] A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane, Quantum error correction via codes over GF(4), IEEE Trans. Inform. Theory 44 (4) (1998) 1369–1387, `arXiv:quant-ph/9608006`.

[5] J. Cannon, W. Bosma, Handbook of Magma functions, Version 2.11, `http://magma.maths.usyd.edu.au/`, May 2004.

[6] L. E. Danielsen, Database of self-dual quantum codes, `http://www.ii.uib.no/~larsed/vncorbits/`, 2005.

[7] L. E. Danielsen, On Self-Dual Quantum Codes, Graphs, and Boolean Functions, Master's thesis, Department of Informatics, University of Bergen, Norway, `arXiv:quant-ph/0503236`, March 2005.

[8] L. E. Danielsen, M. G. Parker, Spectral orbits and peak-to-average power ratio of Boolean functions with respect to the $\{I, H, N\}^n$ transform, in: Sequences and Their Applications – SETA 2004, vol. 3486 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 2005, pp. 373–388, `arXiv:cs.IT/0504102`.

[9] P. Gaborit, W. C. Huffman, J.-L. Kim, V. Pless, On the classification of extremal additive codes over GF(4), in: Proc. of the 37th Allerton Conference on Communication, Control, and Computing, University of Illinois at Urbana-Champaign, 1999, pp. 535–544.

[10] P. Gaborit, W. C. Huffman, J.-L. Kim, V. Pless, On additive GF(4) codes, in: Codes and Association Schemes, vol. 56 of DIMACS Ser. Discrete Math. Theoret. Comput. Sci., American Mathematical Society, Providence, RI, 2001, pp. 135–149.

[11] D. G. Glynn, On self-dual quantum codes and graphs, submitted to Electron. J. Combin., 2002.

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

[13] M. Grassl, A. Klappenecker, M. Rötteler, Graphs, quadratic forms, and quantum codes, in: Proc. IEEE Int. Symp. Inform. Theory (ISIT 2002), 2002, p. 45.

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

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

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

[17] J.-L. Kim, K. E. Mellinger, V. Pless, Projections of binary linear codes onto larger fields, SIAM J. Discrete Math. 16 (4) (2003) 591–603.

[18] B. D. McKay, nauty User's Guide, `http://cs.anu.edu.au/~bdm/nauty/`, 2003.

[19] E. M. Rains, N. J. A. Sloane, Self-dual codes, in: Handbook of Coding Theory, North-Holland, Amsterdam, 1998, pp. 177–294, `arXiv:math.CO/0208001`.

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

[21] D. Schlingemann, R. F. Werner, Quantum error-correcting codes associated with graphs, Phys. Rev. A 65 (1) (2002) 012308, `arXiv:quant-ph/0012111`.

[22] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, `http://www.research.att.com/~njas/sequences/`.

[23] N. J. A. Sloane, S. Plouffe, The Encyclopedia of Integer Sequences, Academic Press, San Diego, CA, 1995.

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

[25] M. Van den Nest, Local Equivalence of Stabilizer States and Codes, Ph.D. thesis, K. U. Leuven, Leuven, Belgium, May 2005.

[26] M. Van den Nest, J. Dehaene, B. De Moor, Graphical description of the action of local Clifford transformations on graph states, Phys. Rev. A 69 (2) (2004) 022316, `arXiv:quant-ph/0308151`.