On the Classification of All Self-Dual Additive Codes over GF(4) of Length up to 12

Lars Eirik Danielsen and Matthew G. Parker
The Selmer Center, Department of Informatics, University of Bergen,
PB 7800, N-5020 Bergen, Norway.
{larsed,matthew}@ii.uib.no
http://www.ii.uib.no/~{larsed,matthew}

Abstract

We consider additive codes over GF(4) that are self-dual with respect to the Hermitian trace inner product. It has been shown that these codes can be represented as graphs, and that two codes are equivalent iff 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.

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*, $\mathrm{Tr} : \mathrm{GF}(4) \mapsto \mathrm{GF}(2)$, is defined by $\mathrm{Tr}(x) = x + \overline{x}$. The *Hermitian trace inner product* of two 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 $\boldsymbol{u} * \boldsymbol{v} = \sum_{i=1}^{n} \mathrm{Tr}(u_i \overline{v_i})$. We define the *dual* of the code $\mathcal{C}$ with respect to this 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* [1]. If $\mathcal{C} = \mathcal{C}^\perp$, then $\mathcal{C}$ is *self-dual* and must be an $(n, 2^n)$ code.

The *Hamming weight* of $\boldsymbol{u} \in \mathcal{C}$ is the number of nonzero components of $\boldsymbol{u}$. The *minimum distance* of the code $\mathcal{C}$ is the minimal 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. We distinguish between two types of codes. A code is of *type II* if all codewords have even weight, otherwise it is of *type I*. A type II code must have even length. Bounds on the minimum distance of self-dual codes were given by Rains and Sloane [2]. A code that meets the appropriate bound is called *extremal*.

Two self-dual additive codes over GF(4), $\mathcal{C}$ and $\mathcal{C}'$, are *equivalent* iff the codewords of $\mathcal{C}$ can be mapped onto the codewords of $\mathcal{C}'$ by a map that 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. Those maps that map $\mathcal{C}$ to $\mathcal{C}$ make up the automorphism group of $\mathcal{C}$, denoted $\operatorname{Aut}(\mathcal{C})$. The number of distinct codes equivalent to $\mathcal{C}$ is then given by $\frac{6^n n!}{|\operatorname{Aut}(\mathcal{C})|}$. 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 [3] that T_n is also given by the *mass formula*,

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

where the sum is over all equivalence classes.

All self-dual additive codes over GF(4) of length n have previously been classified, up to equivalence, by Calderbank et al. [1] for $n \leq 5$, by Höhn [3] for $n \leq 7$, by Hein et al. [4] for $n \leq 7$, and by Glynn et al. [5] for $n \leq 9$. Höhn [3] also classified all type II codes of length 8. Gaborit et al. [6] classified all extremal codes of length 8, 9, 11, and 12. Bachoc and Gaborit [7] classified all extremal type II codes of length 10.

2 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 *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* iff 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 1. 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 $C^T \overline{C}$ 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 [8].

Theorem 2. *Every self-dual additive code over* GF(4) *is equivalent to a graph code.*

Theorem 2 was first proved by Bouchet [9] in the context of isotropic systems, and later by Schlingemann [10] in terms of *quantum stabilizer states.* It can be shown that isotropic systems, quantum stabilizer states, and self-dual additive codes over GF(4) are equivalent objects. Proofs of Theorem 2 have also been given by Grassl et al. [11], by Glynn et al. [5, 12], and by Van den Nest et al. [13].

Definition 3. 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.

Theorem 4. *Two self-dual additive codes over* GF(4)*,* $\mathcal{C}$ *and* $\mathcal{C}'$*, with graph representations* G *and* G'*, are equivalent iff 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'*.*

Bouchet [9] first proved Theorem 4 in terms of isotropic systems. The same result was discovered by Van den Nest et al. [13] in terms of quantum stabilizer states, and by Glynn et al. [5, 12] using finite geometry.

3 Classification

Definition 5. The *LC orbit* of a graph G is the set of all non-isomorphic graphs that can be obtained by performing any sequence of LC operations on G.

The LC orbit of a graph can easily be generated by a recursive algorithm. We have used the program *nauty* (`http://cs.anu.edu.au/~bdm/nauty/`) to check for graph isomorphism.

Let $\boldsymbol{G}_n$ be the set of all non-isomorphic 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 [14] for classifying codes by finding such sets of representatives. The simplest approach is to start with the set $\boldsymbol{G}_n$ and partition it into LC orbits. A more efficient technique was described by Glynn et al. [5]. 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 6. $\boldsymbol{L}_n \subset \boldsymbol{E}_n$*, i.e., the set* $\boldsymbol{E}_n$ *will contain at least one representative from each LC orbit of connected graphs on* n *vertices.*

Table 1: Number of Indecomposable (i_n) and Possibly Decomposable (t_n) Self-Dual Additive Codes over GF(4) 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
t_n	1	2	3	6	11	26	59	182	675	3,990	45,144	1,323,363

Table 2: Number of Indecomposable Self-Dual Additive Codes over GF(4) 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
Total	1	1	2	4	11	26	101	440	3,132	40,457	1,274,068

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 in two different partitions are guaranteed to be inequivalent. 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 $\boldsymbol{E}_n$. We then partition $\boldsymbol{E}_n$ such that graphs corresponding to codes with the same partial weight distribution are 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 calculating the sizes of the automorphism groups of all codes, and then checking that the mass formula defined by Eq. (1) gives 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 total number of inequivalent codes, t_n, is easily derived from the numbers i_n. The values of i_n and t_n can also be found as sequences A090899 and A094927 in *The On-Line Encyclopedia of Integer Sequences* [15]. Table 2 lists the numbers of indecomposable codes by minimum distance, and Table 3 lists the numbers of type II codes by minimum distance. A database containing one representative from each LC orbit, with information about orbit size, weight distribution, etc., is available at `http://www.ii.uib.no/~larsed/vncorbits/`.

Table 3: Number of Indecomposable (Possibly Decomposable) Type II Self-Dual Additive Codes over GF(4) of Length n and Minimum Distance d

$d\backslash n$	2	4	6	8	10	12
2	1 (1)	1 (2)	3 (5)	11 (18)	84 (109)	2,133 (2,285)
4			1 (1)	3 (3)	19 (19)	792 (793)
6						1 (1)
Total	1 (1)	1 (2)	4 (6)	14 (21)	103 (128)	2,926 (3,079)

4 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-dual with respect to the Hermitian trace inner product. Using this method to classify all codes of length 13 is not feasible with the available computational resources.

An interesting problem, posed by Höhn [3], 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. The smallest type II code with trivial automorphism group has length 12.

The graph representation of a self-dual additive code over GF(4) can also give information about the properties of the code. Tonchev [8] 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* [14,16]. Glynn [5] 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 small *independent sets* [14,16].

Acknowledgement We would like to thank Philippe Gaborit for his helpful comments.

References

[1] A. R. Calderbank, E. M. Rains, P. M. Shor, and 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.

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

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

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

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

[6] P. Gaborit, W. C. Huffman, J.-L. Kim, and 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.

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

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

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

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

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

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

[13] M. Van den Nest, J. Dehaene, and 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`.

[14] 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.

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

[16] L. E. Danielsen and M. G. Parker, Spectral orbits and peak-to-average power ratio of Boolean functions with respect to the $\{I, H, N\}^n$ transform, to appear in the proceedings of Sequences and Their Applications (SETA'04), Lecture Notes in Comput. Sci., Springer-Verlag, `arXiv:cs.IT/0504102`, 2005.