GRAPH-BASED CLASSIFICATION OF SELF-DUAL ADDITIVE CODES OVER FINITE FIELDS

Lars Eirik Danielsen

Department of Informatics
University of Bergen
PO Box 7803, N-5020 Bergen, Norway

Abstract. Quantum stabilizer states over $\mathbb{F}_m$ can be represented as self-dual additive codes over $\mathbb{F}_{m^2}$. These codes can be represented as weighted graphs, and orbits of graphs under the generalized local complementation operation correspond to equivalence classes of codes. We have previously used this fact to classify self-dual additive codes over $\mathbb{F}_4$. In this paper we classify self-dual additive codes over $\mathbb{F}_9$, $\mathbb{F}_{16}$, and $\mathbb{F}_{25}$. Assuming that the classical MDS conjecture holds, we are able to classify all self-dual additive MDS codes over $\mathbb{F}_9$ by using an extension technique. We prove that the minimum distance of a self-dual additive code is related to the minimum vertex degree in the associated graph orbit. Circulant graph codes are introduced, and a computer search reveals that this set contains many strong codes. We show that some of these codes have highly regular graph representations.

1. Introduction

It is well-known that *self-orthogonal additive codes* over $\mathbb{F}_4$ can be used to represent a class of *quantum error-correcting codes* known as *binary stabilizer codes* [4]. Although the binary stabilizer codes have been studied most, several authors have considered nonbinary stabilizer codes over finite fields [1, 11, 12, 16, 22, 25], cyclic groups [14], and Abelian groups in general [26]. We will focus mainly on codes over finite fields, and exploit the fact that a stabilizer code over $\mathbb{F}_m$ corresponds to a self-orthogonal *additive code* over $\mathbb{F}_{m^2}$. Quantum codes of dimension zero are known as *stabilizer states*, which are entangled quantum states with several possible applications. Stabilizer states correspond to *self-dual* additive codes. It is known that such codes can be represented as graphs [12, 26]. It is also known that two self-dual additive codes over $\mathbb{F}_4$ are equivalent if and only if their corresponding graphs are equivalent, up to isomorphism, with respect to a sequence of *local complementations* [3, 9, 20, 21]. We have previously used this fact to devise a graph-based algorithm with which we classified all self-dual additive codes over $\mathbb{F}_4$ of length up to 12 [7]. Recently, the representation of equivalence classes as graph orbits was generalized to self-dual additive codes over any finite field [2]. In this paper we use graph-based algorithms to classify all self-dual additive codes over $\mathbb{F}_9$, $\mathbb{F}_{16}$, and $\mathbb{F}_{25}$ up to lengths 8, 6, and 6, respectively. We also give upper bounds on the number of codes, derived from *mass formulas*. By using a graph extension technique we find

that there are only three non-trivial self-dual additive MDS codes over $\mathbb{F}_9$, assuming that the classical MDS conjecture holds. We prove that the minimum distance of a self-dual additive code is related to the minimum vertex degree in the associated graph orbit. Finally, we perform a search of *circulant* graph codes, a subclass of the self-dual additive codes, which is shown to contain many codes with high minimum distance. The highly regular graph structures of some of these codes are described.

2. Stabilizer states

Data in a classical computer are typically stored in bits that have values either 0 or 1. Similarly, we can envisage a quantum computer where data are stored in quantum bits, also known as *qubits*, i.e., two-level quantum systems. One qubit can then be described by a vector $|x\rangle = \binom{\alpha}{\beta} \in \mathbb{C}^2$, where $|\alpha|^2$ is the probability of observing the value 0 when we measure the qubit, and $|\beta|^2$ is the probability of observing the value 1. More generally, data could be stored in m-level *qudits*, described by vectors from $\mathbb{C}^m$. Measuring such a qudit would give a result from an alphabet with m symbols. In general, this alphabet could be any finite Abelian group, but we will focus on the case where the alphabet is a finite field. The m vectors $|x\rangle$, $x \in \mathbb{F}_m$, form an orthonormal basis of $\mathbb{C}^m$.

An error operator that can affect a single qudit is represented by a complex *unitary* $m \times m$ matrix, i.e., a matrix U such that $UU^\dagger = I$, where $\dagger$ means conjugate transpose. A state of n qudits is represented by a vector from $\mathbb{C}^{m^n} = \mathbb{C}^m \otimes \cdots \otimes \mathbb{C}^m$. Assuming that errors act independently on each qubit, this state is affected by error operators described by n-fold tensor products of unitary $m \times m$ matrices. In the case of qubits ($m = 2$), we only need to consider errors from the *Pauli group*,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = iXZ = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

due to the fact that these matrices form a basis of all unitary 2×2 matrices. The error X is called a *bit-flip*, since $X|x\rangle = |x+1\rangle$. The error Z is known as a *phase-flip*, since $Z|x\rangle = (-1)^x |x\rangle$. For general qudits that take their values from $\mathbb{F}_m$, we consider the *generalized Pauli group*, $\mathcal{P}_m$, also known as the *discrete Heisenberg-Weyl group*. When our alphabet is a finite field, we must have $m = p^r$, where p is a prime and $r \geq 1$. The errors contained in the generalized Pauli group are *shift errors*, $X(a)|x\rangle = |x+a\rangle$, and *phase errors*, $Z(b)|x\rangle = \omega^{\mathrm{tr}_{m/p}(bx)} |x\rangle$, where $a, b \in \mathbb{F}_m$, ω is a complex p-th root of unity, and $\mathrm{tr}_{m/p} : \mathbb{F}_m \to \mathbb{F}_p$ is the trace function, $\mathrm{tr}_{m/p}(c) = \sum_{i=0}^{r-1} c^{p^i}$. If $m = p$ is a prime, i.e., $r = 1$, the generalized Pauli group is generated by

$$\left\langle X(1) = \begin{pmatrix} 0 & & & \\ \vdots & & I_{m-1} & \\ 0 & & & \\ 1 & 0 & \cdots & 0 \end{pmatrix}, \quad Z(1) = \begin{pmatrix} 1 & & & & 0 \\ & \omega & & & \\ & & \omega^2 & & \\ & & & \ddots & \\ 0 & & & & \omega^{n-1} \end{pmatrix} \right\rangle,$$

where ω is a complex p-th root of unity, and I is the identity matrix of specified dimension.[1] The operators $X(a)$ and $Z(b)$ are obtained by taking the a-th and b-th powers of $X(1)$ and $Z(1)$, respectively. Even if m is not prime, we can still define

---

[1] The set of generators also contains the scalar ω, except for the case $m = 2$, where it contains i, a 4-th root of unity. This overall phase factor can be ignored for our purposes.

qudits that take values from the cyclic group $\mathbb{Z}_m$, and use the same error operators as defined above. However, when m is a prime power, we get much better codes by using a finite field as our alphabet. When we work with qudits that take values from $\mathbb{F}_{p^r}$, where $r > 1$, we use the error group $\{\bigotimes_{i=1}^{r} E_i \mid E_i \in \mathcal{P}_p\}$ [16], i.e., the operators are r-fold tensor products of Pauli matrices from the group $\mathcal{P}_p$. The error bases that we use are examples of *nice error bases* [17].

Quantum codes are designed to add redundancy in order to protect quantum states against errors due to interference from the environment. A code of *length n* and *dimension k* adds redundancy by encoding k qudits using n qudits. One type of code that exploits the fact that the generalized Pauli group forms a basis for all possible errors is the *stabilizer code* [10]. A *stabilizer* is an Abelian group generated by a set of $n - k$ commuting error operators. An error is detected by measuring the eigenvalues of these operators. If a state is a valid codeword that has not been affected by error, we will observe the eigenvalue $+1$ for all operators. The quantum code, i.e., the set of all valid codewords, is therefore a joint eigenspace of the stabilizer. If there is a detectable error, some eigenvalues would be different from $+1$, due to the commutativity properties of the generalized Pauli matrices. A stabilizer generated by a set of n error operators defines a zero-dimensional quantum code, also known as a *stabilizer state*.[2] The *minimum distance* of a zero-dimensional stabilizer code is simply the minimum nonzero *weight* of all error operators in the stabilizer. The weight of an error operator is the number of $m \times m$ tensor components that are different from the identity matrix. A quantum code of length n, dimension k, and minimum distance d, over the alphabet $\mathbb{F}_m$, is denoted an $[[n, k, d]]_m$ code. Stabilizer states are therefore $[[n, 0, d]]_m$ codes. If the minimum distance, d, is high, the stabilizer state is robust against error, which indicates that it is highly *entangled*. Entangled quantum states have many potential applications, for instance in cryptographic protocols, or as *graph states* [23] which can be used as a resource for quantum computations. In the next section we will also see that zero-dimensional stabilizer codes correspond to an interesting class of classical codes, known as *self-dual additive codes*.

Example 1. A $[[4, 0, 3]]_3$ stabilizer state is obtained from the stabilizer generated by the following error operators.

$$
\begin{aligned}
X(1) &\otimes X(1)Z(2) \otimes I &\otimes X(1), \\
X(1)Z(1) &\otimes X(2) &\otimes X(1)Z(1) \otimes X(1), \\
I &\otimes X(2)Z(2) \otimes X(1)Z(1) \otimes Z(2), \\
X(1) &\otimes X(2)Z(2) \otimes X(2) &\otimes X(2)Z(2).
\end{aligned}
$$

3. Self-dual additive codes

We can represent a stabilizer state over $\mathbb{F}_m$ by an $n \times 2n$ matrix $(A \mid B)$ [1]. The submatrix A represents shift errors, such that $A_{(i,j)} = a$ if $X(a)$ occurs in the j-th tensor component of the i-th error operator in the set of generators. Similarly, the submatrix B represents phase errors.

---

[2]Stabilizer states could also be called one-dimensional quantum codes, since they are one-dimensional Hilbert subspaces. We use the term dimension to mean the number of qudits the code can encode.

Example 2. The matrix corresponding to the stabilizer state in Example 1 is

$$(A \mid B) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 2 & 0 & 0 \\ 1 & 2 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & 0 & 2 & 1 & 2 \\ 1 & 2 & 2 & 2 & 0 & 2 & 0 & 2 \end{pmatrix}.$$

The matrix $(A \mid B)$ generates a code $\mathcal{C}$, and this code is a representation of a stabilizer state. The fact that a stabilizer is an Abelian group translates into the requirement that $\mathcal{C}$ must be *self-dual* with respect to a *symplectic inner product*, i.e.,

$$(a \mid b) * (a' \mid b') = \mathrm{tr}_{m/p}(b \cdot a' - b' \cdot a) = 0, \quad \forall (a \mid b), (a' \mid b') \in \mathcal{C}.$$

We define the *symplectic weight* of a codeword $(a \mid b) \in \mathcal{C}$ as the number of positions i where a_i, b_i, or both are nonzero. (This is the same as the weight of the corresponding Pauli error operator.)

We can also map the linear code of length $2n$ defined above to an additive code over $\mathbb{F}_{m^2}$ of length n. The representation of binary stabilizer codes as self-dual additive codes over $\mathbb{F}_4$ was first demonstrated by Calderbank et al. [4], and generalized to qudits by Ashikhmin and Knill [1], and by Ketkar et al. [16]. An *additive* code, $\mathcal{C}$, over $\mathbb{F}_{m^2}$ of length n is defined as an $\mathbb{F}_m$-linear subgroup of $\mathbb{F}_{m^2}^n$. The code $\mathcal{C}$ contains m^n codewords, and can be defined by an $n \times n$ generator matrix, C, with entries from $\mathbb{F}_{m^2}$, such that any $\mathbb{F}_m$-linear combination of rows from C is a codeword.[3] To get from the stabilizer representation $(A \mid B)$ to the generator matrix C, we simply take $C = A + \omega B$, where ω is a primitive element of $\mathbb{F}_{m^2}$. The code $\mathcal{C}$ will be self-dual, $\mathcal{C} = \mathcal{C}^\perp$, where the dual is defined with respect to the *Hermitian trace inner product*, $\mathcal{C}^\perp = \{ \boldsymbol{u} \in \mathbb{F}_{m^2}^n \mid \boldsymbol{u} * \boldsymbol{c} = 0 \text{ for all } \boldsymbol{c} \in \mathcal{C} \}$. When $m = p$ is prime, the Hermitian trace inner product of two vectors over $\mathbb{F}_{p^2}$ 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

$$\boldsymbol{u} * \boldsymbol{v} = \mathrm{tr}_{p^2/p}(\boldsymbol{u} \cdot \boldsymbol{v}^p) = \boldsymbol{u} \cdot \boldsymbol{v}^p - \boldsymbol{u}^p \cdot \boldsymbol{v} = \sum_{i=1}^n (u_i v_i^p - u_i^p v_i),$$

When $m = p^r$ is not a prime, we use a modification of the Hermitian trace inner product [16],

$$\boldsymbol{u} * \boldsymbol{v} = \mathrm{tr}_{m/p} \left(\frac{\boldsymbol{u} \cdot \boldsymbol{v}^m - \boldsymbol{u}^m \cdot \boldsymbol{v}}{\omega - \omega^m} \right),$$

where ω is a primitive element of $\mathbb{F}_{m^2}$.

The *Hamming weight* of a codeword $\boldsymbol{u} \in \mathcal{C}$, denoted $\mathrm{wt}(\boldsymbol{u})$, is the number of nonzero components of $\boldsymbol{u}$. The *Hamming distance* between $\boldsymbol{u}$ and $\boldsymbol{v}$ 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 over $\mathbb{F}_{m^2}$ with minimum distance d is called an (n, m^n, 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

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

For an additive code over $\mathbb{F}_{m^2}$, all A_i must be divisible by $m - 1$.

---

[3]For additive codes over $\mathbb{F}_4$, each codeword is a sum of rows of the generator matrix. However, we also use the name "additive code" in this more general case.

Example 3. The stabilizer state in Example 1 corresponds to the following generator matrix of a self-dual additive $(4, 3^4, 3)$ code.

$$C = \begin{pmatrix} 1 & 1+2\omega & 0 & 1 \\ 1+\omega & 2 & 1+\omega & 1 \\ 0 & 2+2\omega & 1+\omega & 2\omega \\ 1 & 2+2\omega & 2 & 2+2\omega \end{pmatrix}.$$

We define two self-dual additive codes, $\mathcal{C}$ and $\mathcal{C}'$ over $\mathbb{F}_{m^2}$, to be *equivalent* if the codewords of $\mathcal{C}$ can be mapped onto the codewords of $\mathcal{C}'$ by a map that preserves the properties of the code, including self-duality. A permutation of coordinates, or columns of a generator matrix, is such a map. Other operations can also be applied to the coordinates of $\mathcal{C}$. Let each element $a + \omega b \in \mathbb{F}_{m^2}$ be represented as $\binom{a}{b} \in \mathbb{F}_m^2$. We can then premultiply this element by a 2×2 matrix. (We could equivalently have applied transformations to pairwise columns of the $2n \times n$ matrix $(A \mid B)$.) It was shown by Rains [22] that by applying matrices from the *symplectic group* $\mathrm{Sp}_2(m)$ to each coordinate, we preserve the properties of the code. (This group contains all 2×2 matrices with elements in $\mathbb{F}_m$ and determinant one.) For self-dual additive codes over $\mathbb{F}_4$, these symplectic operations can be represented more simply as multiplication by nonzero elements from $\mathbb{F}_4$ and conjugation of coordinates. (Conjugation of elements in $\mathbb{F}_{p^2}$ maps x to x^p.) Combined, there are six possible transformations that are equivalent to the six permutations of the elements $\{1, \omega, \omega^2\}$ in the coordinate. The corresponding symplectic group is

$$\mathrm{Sp}_2(2) = \left\langle A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle,$$

where A_1 represents multiplication by ω and A_2 represents conjugation. Including coordinate permutations, there are a total of $6^n n!$ maps for a code of length n.

For codes over $\mathbb{F}_9$, we observe that $\mathrm{Sp}_2(3)$ is a group of order 24 generated by

$$\mathrm{Sp}_2(3) = \left\langle A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle,$$

where A_1 represents multiplication by ω^2 and A_2 represents the map $a + \omega b \mapsto a + b + \omega b$. By taking powers of A_1, we see that we are allowed to multiply a coordinate by $x \in \mathbb{F}_9$ only if $x\bar{x} = 1$. However, if we also conjugate the coordinate, we may multiply by $x \in \mathbb{F}_9$ where $x\bar{x} = 2$. Note that conjugation on its own is not allowed. The 8 operations just described may be combined with the operations represented by A_2 and A_2^2 to give a total of 24 operations. In all there are $24^n n!$ maps that take a self-dual additive code over $\mathbb{F}_9$ to an equivalent code. In general, for codes over $\mathbb{F}_{m^2}$, the number of maps is $|\mathrm{Sp}_2(m)|^n n!$.

A transformation that maps $\mathcal{C}$ to itself 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 a self-dual additive code over $\mathbb{F}_{m^2}$, $\mathcal{C}$, is then given by $\frac{|\mathrm{Sp}_2(m)|^n n!}{|\mathrm{Aut}(\mathcal{C})|}$. The *equivalence class* of $\mathcal{C}$ contains all codes that are equivalent to $\mathcal{C}$. By adding the sizes of all equivalence classes of codes of length n, we find the total number of distinct codes of length n, denoted T_n. The number T_n is also given by a *mass formula*. The mass formula for self-dual additive codes over $\mathbb{F}_4$ was found by Höhn [15]. This result is easily generalized to $\mathbb{F}_{m^2}$.

Theorem 3.1.
$$T_n = \prod_{i=1}^{n}(m^i + 1) = \sum_{j=1}^{t_n} \frac{|\operatorname{Sp}_2(m)|^n n!}{|\operatorname{Aut}(\mathcal{C}_j)|},$$

where t_n is the number of equivalence classes of codes of length n, and $\mathcal{C}_j$ is a representative from each equivalence class.

Proof. Let $M(n,k)$ be the total number of self-orthogonal (n, m^k) codes. One such code, $\mathcal{C}$, can be extended to a self-orthogonal (n, m^{k+1}) code in $m^{2(n-k)} - 1$ ways by adding an extra codeword from $C^\perp$. Each (n, m^{k+1}) code can be obtained in this way from $m^{2(k+1)} - 1$ different (n, m^k) codes. It follows that

$$M(n, k+1) = M(n, k)\frac{m^{2(n-k)} - 1}{m^{2(k+1)} - 1}.$$

Starting with $M(n, 0) = 1$, the recursion gives us the number of self-dual (n, m^n) codes,

$$M(n, n) = \prod_{i=0}^{n-1} \frac{m^{2(n-k)} - 1}{m^{2(k+1)} - 1} = \prod_{i=1}^{n}(m^i + 1). \qquad \square$$

By assuming that all codes of length n have a trivial automorphism group, we get the following lower bound on t_n, the total number of inequivalent codes. Note that when n is large, most codes have a trivial automorphism group, so the tightness of the bound increases with n. Also note that this bound is much tighter than a bound that was derived from results in graph theory by Bahramgiri and Beigi [2].

Theorem 3.2.
$$t_n \geq \left\lceil \frac{c\prod_{i=1}^{n}(m^i + 1)}{|\operatorname{Sp}_2(m)|^n n!} \right\rceil,$$
where $c = 1$ if m is even, and $c = 2$ if m is odd.

Proof. When m is even, the trivial automorphism group includes only the identity permutation, and the result follows from Theorem 3.1. When $m = p^r$ is odd, where p is a prime, the trivial automorphism group also contains the transformation that applies the symplectic operation $\begin{pmatrix} p-1 & 0 \\ 0 & p-1 \end{pmatrix}$ to all coordinates. This operation is equivalent to multiplying each codeword by $p - 1$, and will therefore map an additive code to itself. $\qquad \square$

It follows from the *quantum singleton bound* [18, 22] that any self-dual additive code must satisfy $2d \leq n + 2$. A tighter bound for codes over $\mathbb{F}_4$ was given by Calderbank et al. [4]. Codes that satisfy the singleton bound with equality are known as *maximum distance separable (MDS) codes*. Self-dual MDS codes must have even length, and MDS codes of length two are trivial and exist for all alphabets. The only non-trivial MDS code over $\mathbb{F}_4$ is the $(6, 2^6, 4)$ *Hexacode*. Ketkar et al. [16, Thm. 63] proved that a self-dual additive (n, m^n, d) MDS code must satisfy $n \leq m^2 + d - 2 \leq 2m^2 - 2$. If the famous MDS conjecture holds, then $n \leq m^2 + 1$, or $n \leq m^2 + 2$ when m is even and $d = 4$ or $d = m^2$. Grassl, Rötteler, and Beth [24] showed that MDS codes of length $n \leq m + 1$ always exist.

Self-dual *linear* codes over $\mathbb{F}_{m^2}$ are a subset of the self-dual additive codes. Only additive codes that satisfy certain constraints can be linear. Such constraints for codes over $\mathbb{F}_4$ were described by Van den Nest [20] and by Glynn et al. [9]. An obvious constraint is that all coefficients of the weight enumerator, except A_0, of

a linear code must be divisible by $m^2 - 1$, whereas for an additive code they need only be divisible by $m - 1$.

4. CORRESPONDENCE TO WEIGHTED GRAPHS

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*. Let an *m-weighted graph* be a triple $G = (V, E, W)$ where W is a set of weights from $\mathbb{F}_m$. Each edge has an associated non-zero weight. (An edge with weight zero is the same as a non-edge.) An m-weighted graph with n vertices can be represented by an $n \times n$ *adjacency matrix* Γ, where the element $\Gamma_{(i,j)} = W(\{i, j\})$ if $\{i, j\} \in E$, and $\Gamma_{(i,j)} = 0$ 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 $U \subseteq V$ contains vertices U and all edges from E whose endpoints are both in U. The *complement* of a 2-weighted graph 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 $\{u, v\} \in E \iff \{\pi(u), \pi(v)\} \in E'$. We also require that weights are preserved, i.e., $W_{\{u,v\}} = W_{\{\pi(u),\pi(v)\}}$. 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. A *complete graph* is a graph where all pairs of vertices are connected by an edge. A *clique* is a complete subgraph.

Definition 4.1. A *graph code* is an additive code over $\mathbb{F}_{m^2}$ that has a generator matrix of the form $C = \Gamma + \omega I$, where I is the identity matrix, ω is a primitive element of $\mathbb{F}_{m^2}$, and Γ is the adjacency matrix of a simple undirected m-weighted graph.

Theorem 4.2. *Every self-dual additive code over $\mathbb{F}_{m^2}$ is equivalent to a graph code.*

Proof. The generator matrix, C, of a self-dual additive code over $\mathbb{F}_{m^2}$ corresponds to an $n \times 2n$ matrix $(A \mid B)$ with elements from $\mathbb{F}_m$, such that $C = A + \omega B$. We must prove that an equivalent code is generated by $(\Gamma \mid I)$, where I is the identity matrix and Γ is the adjacency matrix of a simple undirected m-weighted graph. A basis change can be accomplished by $(A' \mid B') = M(A \mid B)$, where M is an $n \times n$ invertible matrix with elements from $\mathbb{F}_m$. If B has full rank, the solution is simple, since $B^{-1}(A \mid B) = (\Gamma' \mid I)$. We obtain $(\Gamma \mid I)$ after changing the diagonal elements of Γ' to 0, by appropriate symplectic transformations. Any two rows of $(\Gamma \mid I)$ will be orthogonal with respect to the symplectic inner product, which means that $\Gamma I^{\mathrm{T}} - I \Gamma^{\mathrm{T}} = 0$, and it follows that Γ will always be a symmetric matrix. In the case where B has rank $k < n$, we can perform a basis change to get

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

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 $(A' \mid B')$ defines a self-dual code, 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 $B_1 = (B_{11} \mid B_{12})$ where B_{11} is a $k \times k$ invertible matrix. We also write $A_2 = (A_{21} \mid A_{22})$ where A_{22} has size $(n - k) \times (n - k)$. Assume that there exists an $\boldsymbol{x} \in \mathbb{F}_m^{n-k}$ such that
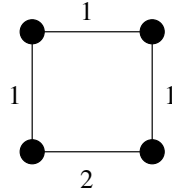
Figure 1: Graph Representation of the $(4, 3^4, 3)$ Code

$A_{22}\boldsymbol{x}^{\mathrm{T}} = 0$. 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 $\boldsymbol{y} \in \mathbb{F}_m^k$. 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. Two of the symplectic operations that we can apply to columns of a generator matrix are $\begin{pmatrix} 0 & m-1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ m-1 & 0 \end{pmatrix}$. This means that we can interchange column i of A' and column i of B' if we also multiply one of the columns by $m-1$. In this way we swap the i-th columns of A' and B' for $k < i \leq n$ to get $(A'' \mid B'')$. Since B_{11} and A_{22} are invertible, B'' must also be an invertible matrix. We then find $B''^{-1}(A'' \mid B'') = (\Gamma \mid I)$, and set all diagonal elements of Γ to 0 by symplectic transformations. $\qquad\square$

Example 4. The matrix from Example 2 can be transformed into the following matrix, using the method given in the proof of Theorem 4.2.

$$(\Gamma \mid I) = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

This means that the stabilizer state from Example 1 is equivalent to the graph code generated by $C = \Gamma + \omega I$. The graph defined by Γ is depicted in Fig. 1.

Note that Theorem 4.2 is a generalization of the same theorem for codes over $\mathbb{F}_4$ [7], which was proved by Van den Nest et al. [21]. The fact that stabilizer codes can be represented by graphs was also shown by Schlingemann and Werner [26] and by Grassl, Klappenecker, and Rötteler [12].

We have seen that every m-weighted graph represents a self-dual additive code over $\mathbb{F}_{m^2}$, and that every self-dual additive code over $\mathbb{F}_{m^2}$ can be represented by an m-weighted 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 is an adjacency matrix of an unlabeled simple undirected m-weighed graph.

5. Graph equivalence and code equivalence

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 $\Gamma' + \omega I$, which are generator matrices for equivalent codes. It follows that two codes are equivalent if their corresponding graphs are isomorphic. However, the symplectic transformations that map a code to an equivalent code do
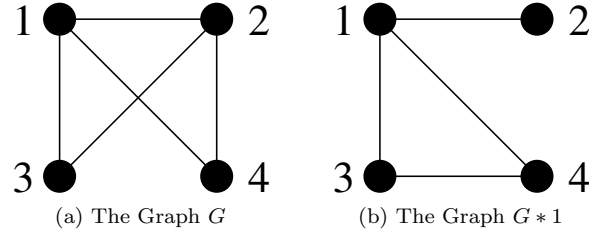
(a) The Graph G (b) The Graph $G * 1$

Figure 2: Example of Local Complementation

not in general produce isomorphic graphs, but we will see that they can be described as graph operations.

It is known that two self-dual additive codes over $\mathbb{F}_4$ are equivalent if and only if their corresponding graphs are equivalent, up to isomorphism, with respect to a sequence of *local complementations* [3, 9, 20, 21]. We have previously used this fact to devise a graph-based algorithm with which we classified all self-dual additive codes over $\mathbb{F}_4$ of length up to 12 [7].

Definition 5.1 ([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 $G * v$ by replacing the induced subgraph of G on N_v by its complement.

Theorem 5.2 ([3, 9, 20, 21]). *Two self-dual additive codes over $\mathbb{F}_4$, $\mathcal{C}$ 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'.*

The LC operation can be generalized to weighted graphs, and it was first shown by Bahramgiri and Beigi [2] that the equivalence of nonbinary stabilizer states over $\mathbb{F}_m$, i.e., self-dual additive codes over $\mathbb{F}_{m^2}$, can be described in terms of graph operations.[4]

Definition 5.3 ([2]). Given an m-weighted graph $G = (V, E, W)$ and a vertex $v \in V$, *weight shifting* on v by $a \in \mathbb{F}_m \setminus \{0\}$ transforms G into $G \circ_a v$ by multiplying the weight of each edge incident on v by a.

Definition 5.4 ([2]). Given an m-weighted graph $G = (V, E, W)$ and a vertex $v \in V$, *generalized local complementation* on v by $a \in \mathbb{F}_m \setminus \{0\}$ transforms G into $G *_a v$. Let Γ and Γ' be the adjacency matrices of G and $G *_a v$, respectively. Then $\Gamma'_{(i,j)} = \Gamma_{(i,j)} + a\Gamma_{(v,i)}\Gamma_{(v,j)}$, for all $i \neq j$, and $\Gamma'_{(i,i)} = 0$ for all i.

Theorem 5.5 ([2]). *Two self-dual additive codes over $\mathbb{F}_{m^2}$, $\mathcal{C}$ and $\mathcal{C}'$, with graph representations G and G', are equivalent if and only if we get a graph isomorphic to G' by applying some finite sequence of weight shifts and generalized local complementations to G.*

---

[4]Bahramgiri and Beigi [2] only state their theorem for $\mathbb{F}_m$ where m is prime, but the result holds for any finite field, as their proof does not depend on m being prime.
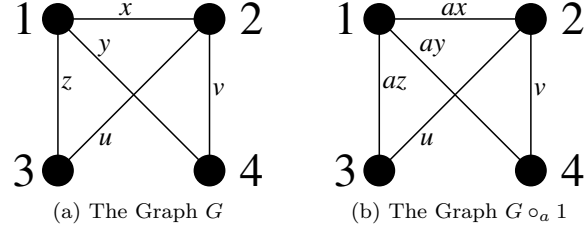
(a) The Graph G (b) The Graph $G \circ_a 1$

Figure 3: Example of Weight Shifting

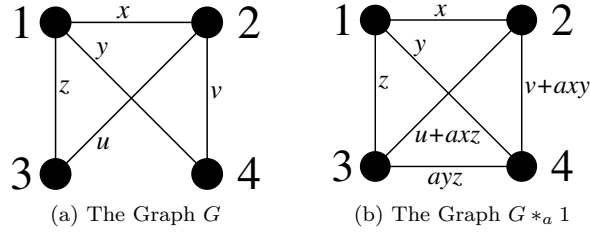(a) The Graph G (b) The Graph $G *_a 1$

Figure 4: Example of Generalized Local Complementation

A proof of Theorem 5.5 was given by Bahramgiri and Beigi [2], as a generalization of the proof given by Van den Nest et al. [21] for self-dual additive codes over $\mathbb{F}_4$.

Definition 5.6. The *LC orbit* of a weighted graph G is the set of all non-isomorphic graphs that can be obtained by performing any sequence of weight shifts and generalized LC operations on G.

Theorem 5.7. *The minimum distance of a self-dual additive (n, m^n, d) code is equal to $\delta + 1$, where δ is the minimum vertex degree over all graphs in the associated LC orbit.*

Proof. A vertex with degree $d - 1$ in the LC orbit corresponds to a codeword of weight d, and we will now show that such a vertex always exists. Choose any graph representation of the code and let $G = (\Gamma \mid I)$ be the corresponding generator matrix. Find a codeword c of weight d generated by G. Let the i-th row of G be one of the rows that c is linearly dependent on. Apply symplectic transformations to the coordinates of the code such that c is mapped to c' with 1 in coordinate $n + i$, and with 0 in all other of the last n coordinates. Since we do not care about changes in the corresponding first n coordinates, as long as the symplectic weight of c is preserved, there will always be transformations that achieve this. Apply the same transformations to the columns of G, and then replace the i-th row with c', to get G'. Note that the right half of G' still has full rank, so we can transform G' into a matrix of the form $(\Gamma' \mid I)$ by Gaussian elimination, where the symplectic weight of the i-th row is d. Finally, we set all diagonal elements of Γ' to zero by appropriate symplectic transformations. Vertex i of the graph with adjacency matrix Γ' has degree $d - 1$. $\square$

6. CLASSIFICATION

It follows from Theorem 5.5 that two self-dual additive codes over $\mathbb{F}_{m^2}$ are equivalent if and only if their graph representations are in the same LC orbit. The LC orbit of a graph can easily be generated by a recursive algorithm. We have used the program *nauty* [19] to check for graph isomorphism.

Let $\boldsymbol{G}_{n,m}$ be the set consisting of all non-isomorphic simple undirected connected m-weighted graphs on n vertices. Note that 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, m^n, d) code and $\mathcal{C}'$ an $(n', m^{n'}, d')$ 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 $(n + n', m^{n+n'}, \min\{d, d'\})$ 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 m-weighted graphs on n vertices is a partitioning of $\boldsymbol{G}_{n,m}$ into $i_{n,m}$ disjoint sets. $i_{n,m}$ is also the number of indecomposable self-dual additive codes over $\mathbb{F}_{m^2}$ of length n, up to equivalence. Let $\boldsymbol{L}_{n,m}$ be a set containing one representative from each LC orbit of connected m-weighted graphs on n vertices. The simplest algorithm for finding such sets of representatives is to start with the set $\boldsymbol{G}_{n,m}$ and generate LC orbits of its members until we have a partitioning of $\boldsymbol{G}_{n,m}$. The following more efficient technique is based on a method described by Glynn et al. [9]. Let the $m^n - 1$ *extensions* of an m-weighted 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, using all possible combinations of edge weights. The set $\boldsymbol{E}_{n,m}$, containing $i_{n-1,m}(m^{n-1} - 1)$ graphs, is formed by making all possible extensions of all graphs in $\boldsymbol{L}_{n-1,m}$.

Theorem 6.1. $\boldsymbol{L}_{n,m} \subset \boldsymbol{E}_{n,m}$, *i.e., the set $\boldsymbol{E}_{n,m}$ will contain at least one representative from each LC orbit of connected m-weighted graphs on n vertices.*

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

The set $\boldsymbol{E}_{n,m}$ will be much smaller than $\boldsymbol{G}_{n,m}$, so it will be more efficient to search for a set of LC orbit representatives within $\boldsymbol{E}_{n,m}$. Another fact that simplifies our classification algorithm is that weight shifting and generalized local complementation commute. This means that to generate the LC orbit of a weighted graph, we may first generate the orbit with respect to generalized local complementation only, and then apply weight shifting to the resulting set of graphs.

Using the described techniques, we were able to classify all self-dual additive codes over $\mathbb{F}_9$, $\mathbb{F}_{16}$, and $\mathbb{F}_{25}$ up to lengths 8, 6, and 6, respectively. Table 1 gives the values of $i_{n,m}$, the number of distinct LC orbits of connected m-weighted graphs on n vertices, which is also the number of inequivalent indecomposable self-dual additive codes over $\mathbb{F}_{m^2}$ of length n. The total number of inequivalent codes of length n, t_n, is shown in Table 2 together with lower bounds derived from Theorem 3.2. The

Table 1: Number $(i_{n,m})$ of Indecomposable Codes of Length n over $\mathbb{F}_{m^2}$

n	$i_{n,2}$	$i_{n,3}$	$i_{n,4}$	$i_{n,5}$
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1
4	2	3	3	3
5	4	5	6	7
6	11	21	25	38
7	26	73		
8	101	659		
9	440			
10	3,132			
11	40,457			
12	1,274,068			

numbers t_n are easily derived from the numbers i_n by using the *Euler transform* [27],

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

Tables 3, 4, and 5 list by minimum distance the numbers of indecomposable codes over $\mathbb{F}_9$, $\mathbb{F}_{16}$, and $\mathbb{F}_{25}$. A database containing one representative from each equivalence class is available at `http://www.ii.uib.no/~larsed/nonbinary/`. For the classification of self-dual additive codes over $\mathbb{F}_4$, we refer to previous work [7], and the web page `http://www.ii.uib.no/~larsed/vncorbits/`.

Note that applying the graph extension technique described previously is equivalent to *lengthening* [8] a self-dual additive code. Given an (n, m^n, d) code, we add a row and column to its generator matrix to obtain an $(n+1, m^{n+1}, d')$ code, where $d' \le d+1$. If follows that given a classification of all codes of length n and minimum distance d, we can classify all codes of length $n+1$ and minimum distance $d+1$. All length 8 codes over $\mathbb{F}_9$ have been classified as described above. By extending the 77 $(8, 3^8, 4)$ codes, we found 4 $(9, 3^9, 5)$ codes, and from those we obtained a single $(10, 3^{10}, 6)$ code. Assuming that the MDS conjecture holds, there are no self-dual additive MDS codes over $\mathbb{F}_9$ with length above 10. This would mean that the three MDS codes with parameters $(4, 3^4, 3)$, $(6, 3^6, 4)$, and $(10, 3^{10}, 6)$ are the only non-trivial self-dual additive MDS codes over $\mathbb{F}_9$. The $(6, 3^6, 4)$ and $(10, 3^{10}, 6)$ are constructed as circulant codes in Section 7. A generator matrix for the $(4, 3^4, 3)$ code is given in Example 4. In fact, a $(4, m^4, 3)$ code, for any $m \ge 3$, is generated by

$$
\begin{pmatrix}
\omega & 1 & 1 & 0 \\
1 & \omega & 0 & 1 \\
1 & 0 & \omega & \alpha \\
0 & 1 & \alpha & \omega
\end{pmatrix},
$$

Table 2: Total Number $(t_{n,m})$ of Codes of Length n over $\mathbb{F}_{m^2}$

n	$t_{n,2}$	$t_{n,3}$	$t_{n,4}$	$t_{n,5}$
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	6	7	7	7
5	11	13	14	15
6	26	39	44	58
7	59	121	?	?
8	182	817	≥ 946	$\geq 21{,}161$
9	675	$\geq 9{,}646$	$\geq 458{,}993$	$\geq 38{,}267{,}406$
10	3,990	$\geq 2{,}373{,}100$		
11	45,144			
12	1,323,363			
13	$\geq 72{,}573{,}549$			

Table 3: Number of Indecomposable Codes of Length n and Distance d over $\mathbb{F}_9$

$d \backslash n$	2	3	4	5	6	7	8	9	10
2	1	1	2	4	15	51	388	?	?
3			1	1	5	20	194	?	?
4					1	2	77	?	?
5								4	?
6									1
All	1	1	3	5	21	73	659	?	?

Table 4: Number of Indecomposable Codes of Length n and Distance d over $\mathbb{F}_{16}$

$d \backslash n$	2	3	4	5	6
2	1	1	2	4	16
3			1	2	6
4					3
5					
6					
All	1	1	3	6	25

where $\alpha \in \mathbb{F}_m \setminus \{0,1\}$. This code has weight enumerator $W(1,y) = 1 + 4(m^2 - 1)y^3 + (m^2 - 3)(m^2 - 1)y^4$.

There are four $(9, 3^9, 5)$ codes, all with weight enumerator $W(1,y) = 1 + 252y^5 + 1176y^6 + 3672y^7 + 7794y^8 + 6788y^9$. None of these are equivalent to circulant graph

Table 5: Number of Indecomposable Codes of Length n and Distance d over $\mathbb{F}_{25}$

$d\backslash n$	2	3	4	5	6
2	1	1	2	4	21
3			1	3	11
4					6
5					
6					
All	1	1	3	7	38

codes. The generator matrices are:

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

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

The two $(7, 3^7, 4)$ codes, the three $(6, 4^6, 4)$, and five of the six $(6, 5^6, 4)$ codes are equivalent to circulant graph codes generated in Section 7. The last $(6, 5^6, 4)$ code has weight enumerator $W(1, y) = 1 + 360y^4 + 3024y^5 + 12240y^6$ and generator matrix

$$
\begin{pmatrix}
\omega & 2 & 2 & 1 & 0 & 0 \\
2 & \omega & 0 & 1 & 4 & 1 \\
2 & 0 & \omega & 0 & 1 & 1 \\
1 & 1 & 0 & \omega & 3 & 4 \\
0 & 4 & 1 & 3 & \omega & 3 \\
0 & 1 & 1 & 4 & 3 & \omega
\end{pmatrix}.
$$

7. CIRCULANT GRAPH CODES

It is clearly infeasible to study all self-dual additive codes of lengths much higher than those classified in the previous section. We therefore restrict our search space to the $m^{\lceil \frac{n-1}{2} \rceil}$ codes over $\mathbb{F}_{m^2}$ of length n corresponding to graphs with *circulant* adjacency matrices. A matrix is circulant if the i-th row is equal to the first row, cyclically shifted $i - 1$ times to the right. We have performed an exhaustive search

Table 6: Highest Found Minimum Distance of Codes over $\mathbb{F}_{m^2}$ of Length n

$n\backslash m$	2	3	4	5
2	**2**	**2**	**2**	**2**
3	**2**	**2**	**2**	**2**
4	2	**3***	**3***	**3***
5	**3**	**3**	**3**	**3**
6	**4**	**4**	**4**	**4**
7	3	**4**	**4**	**4**
8	4	4	4	4
9	4	**5**^{s}	**5**	**5**
10	4	**6**	**6**	**6**
11	**5**^{s}	5	**6**	**6**
12	6	6	6	6
13	5	6	6	**7**
14	6	6	7	**8**
15	6	6	7	7
16	6	6	8	8
17	7	7	8	**9**
18	8*	8	8	**10**
19	7	8		
20	8	8		
21	8*	8		
22	8	9		
23	8	9		
24	8	9		
25	8			
26	8			
27	9^s			
28	10			
29	11			
30	12			

of such graphs, the result of which is summarized in Table 6. This table shows the highest found minimum distance of self-dual additive codes over various alphabets. A code with the given minimum distance has been found in our search, except for the cases marked $*$, where a better code is obtained in some other way and does not have a circulant graph representation,[5] and cases marked s, which are not circulant, but obtained by a trivial *shortening* [8] of a longer circulant code. Minimum distances printed in bold font are optimal according to the quantum singleton bound. If n is even and the quantum singleton bound is satisfied with equality, we have an MDS code.

We here give the first row of a circulant generator matrix for those codes classified in Section 6 that are equivalent to circulant graph codes. There is a unique $(6, 3^6, 4)$ code with weight enumerator $W(1, y) = 1 + 120y^4 + 240y^5 + 368y^6$ generated by

---

[5]See the web page http://www.codetables.de/ for details on how codes over $\mathbb{F}_4$ of length 18 and 21 can be obtained.

(ω01110). There are two inequivalent $(7, 3^7, 4)$ codes generated by (ω110011) and (ω022220), both with weight enumerator $W(1, y) = 1 + 70y^4 + 336y^5 + 812y^6 + 968y^7$. There is a unique $(10, 3^{10}, 6)$ code with weight enumerator $W(1, y) = 1 + 1680y^6 + 2880y^7 + 14040y^8 + 22160y^9 + 18288y^{10}$ generated by (ω012111210). There are three inequivalent $(6, 4^6, 4)$ codes with weight enumerator $W(1, y) = 1 + 225y^4 + 1080y^5 + 2790y^6$ generated by (ω01110), (ω01α10), and (ω01$\alpha^2$10), where $\alpha = \omega^5$ is a primitive element of $\mathbb{F}_4$. There are five inequivalent $(6, 5^6, 4)$ codes generated by (ω01110), (ω01210), (ω02220), (ω10201), and (ω12221), all with weight enumerator $W(1, y) = 1 + 360y^4 + 3024y^5 + 12240y^6$.

For circulant graph codes of higher length that are optimal according to the quantum singleton bound, we find that all codes of the same length have the same weight enumerator. In the list below, we give the first row of one generator matrix for each weight enumerator.

- $(7, 4^7, 4)$, (ω11$\alpha\alpha$11),

$$W(1, y) = 1 + 105y^4 + 1008y^5 + 4830y^6 + 10440y^7.$$

- $(9, 4^9, 5)$, (ω001$\alpha\alpha$100),

$$W(1, y) = 1 + 378y^5 + 3780y^6 + 23220y^7 + 88155y^8 + 146610y^9.$$

- $(10, 4^{10}, 6)$, (ω010α1α010),

$$W(1, y) = 1 + 3150y^6 + 18000y^7 + 111375y^8 + 366000y^9 + 550050y^{10}.$$

- $(11, 4^{11}, 6)$, (ω00α1111α00),

$$W(1, y) = 1 + 1386y^6 + 13860y^7 + 99495y^8 + 505560y^9 + 1511598y^{10}$$
$$+ 2062404y^{11}.$$

- $(7, 5^7, 4)$, (ω011110),

$$W(1, y) = 1 + 140y^4 + 2184y^5 + 17080y^6 + 58720y^7.$$

- $(9, 5^9, 5)$, (ω00211200),

$$W(1, y) = 1 + 504y^5 + 8400y^6 + 84240y^7 + 507420y^8 + 1352560y^9.$$

- $(10, 5^{10}, 6)$, (ω001222100),

$$W(1, y) = 1 + 5040y^6 + 54720y^7 + 508680y^8 + 2704560y^9 + 6492624y^{10}.$$

- $(11, 5^{11}, 6)$, (ω0012222100),

$$W(1, y) = 1 + 1848y^6 + 31680y^7 + 370260y^8 + 2977480y^9$$
$$+ 14282664y^{10} + 31164192y^{11}.$$

- $(13, 5^{13}, 7)$, (ω010011110010),

$$W(1, y) = 1 + 6864y^7 + 118404y^8 + 1538680y^9 + 14867424y^{10}$$
$$+ 97222320y^{11} + 388930776y^{12} + 718018656y^{13}.$$

- $(14, 5^{14}, 8)$, (ω1011331331101),

$$W(1, y) = 1 + 72072y^8 + 816816y^9 + 10474464y^{10} + 90679680y^{11}$$
$$+ 544536720y^{12} + 2010441888y^{13} + 3446493984y^{14}.$$

- $(17, 5^{17}, 9)$, $(\omega 0010111001110100)$,

$$W(1, y) = 1 + 97240y^9 + 1633632y^{10} + 24504480y^{11} + 296652720y^{12}$$
$$+ 2733620400y^{13} + 18749403360y^{14} + 89994568992y^{15}$$
$$+ 269984494620y^{16} + 381154477680y^{17}.$$

- $(18, 5^{18}, 10)$, $(\omega 12134242124243121)$,

$$W(1, y) = 1 + 1050192y^{10} + 11456640y^{11} + 180442080y^{12}$$
$$+ 1964813760y^{13} + 16877613600y^{14} + 107991522432y^{15}$$
$$+ 485972877960y^{16} + 1372155934320y^{17} + 1829541554640y^{18}.$$

As mentioned in the introduction, stabilizer codes can be defined over any Abelian group, not only finite fields. For comparison, we also generated circulant codes over $\mathbb{Z}_4^2$. As expected, the minimum distance of these codes are much worse than for codes over $\mathbb{F}_{16}$. We found a $(7, 4^7, 4)$-code over $\mathbb{Z}_4^2$, but for all other lengths up to 16, the best minimum distance was equal to the best minimum distance of codes over $\mathbb{F}_4$ of the same length.

Gulliver and Kim [13] performed a computer search of circulant self-dual additive codes over $\mathbb{F}_4$ of length up to 30. Their search was not restricted to graph codes, so our search space is a subset of theirs. It is interesting to note that for every length, the highest minimum distance found was the same in both searches. This suggests that the circulant graph code construction can produce codes as strong as the more general circulant code construction. Besides a smaller search space, the special form of the generator matrix of a graph code makes it easier to find the minimum distance, since any codeword obtained as a linear combination of i rows of the generator matrix must have weight at least i. If, for example, we want to determine whether a code has minimum distance at least d, we only need to consider combinations of d or fewer rows of its generator matrix.

Circulant graphs must be *regular*, i.e., all vertices must have the same number of neighbours. We have previously discovered [5, 6] that many strong circulant self-dual additive codes over $\mathbb{F}_4$ can be represented as highly structured *nested clique graphs*. Some of these graphs are shown in Fig. 5. For instance, Fig. 5b shows a graph representation of the $(12, 2^{12}, 6)$ "Dodecacode" consisting of three 4-cliques. The remaining edges form a *Hamiltonian cycle*, i.e., a cycle that visits every vertex of the graph exactly once. Notice that all graphs shown in Fig. 5 have *minimum regular vertex degree*, i.e., each vertex has $d - 1$ neighbours, where d is the minimum distance of the corresponding code.

We have discovered some new highly structured weighted graph representations of self-dual additive codes over $\mathbb{F}_9$ and $\mathbb{F}_{16}$. Fig. 6 shows two interconnected 5-cliques where all edges have weight one, and a 10-cycle where all edges have weight two. The sum of these two graphs, such that no edges overlap, corresponds to the $(10, 3^{10}, 6)$ code. Up to isomorphism, there is only one way to add a Hamiltonian cycle of weight two edges to the double 5-clique, since there cannot be both weight one and weight two edges between the same pair of vertices. The first row of a circulant generator matrix corresponding to this graph is $(\omega 012111210)$.

As a second example, Fig. 7 shows two pairs of 4-cliques, each of which is connected by a length 8 cycle, and two 16-cycles where all edges have weight α and α^2, respectively, where $\alpha = \omega^5$ is a primitive element of $\mathbb{F}_4$. The $(16, 4^{16}, 8)$ code generated by $(\omega 0\alpha^2 1\alpha 100010001\alpha 1\alpha^2)$ corresponds to a sum of these three graphs.
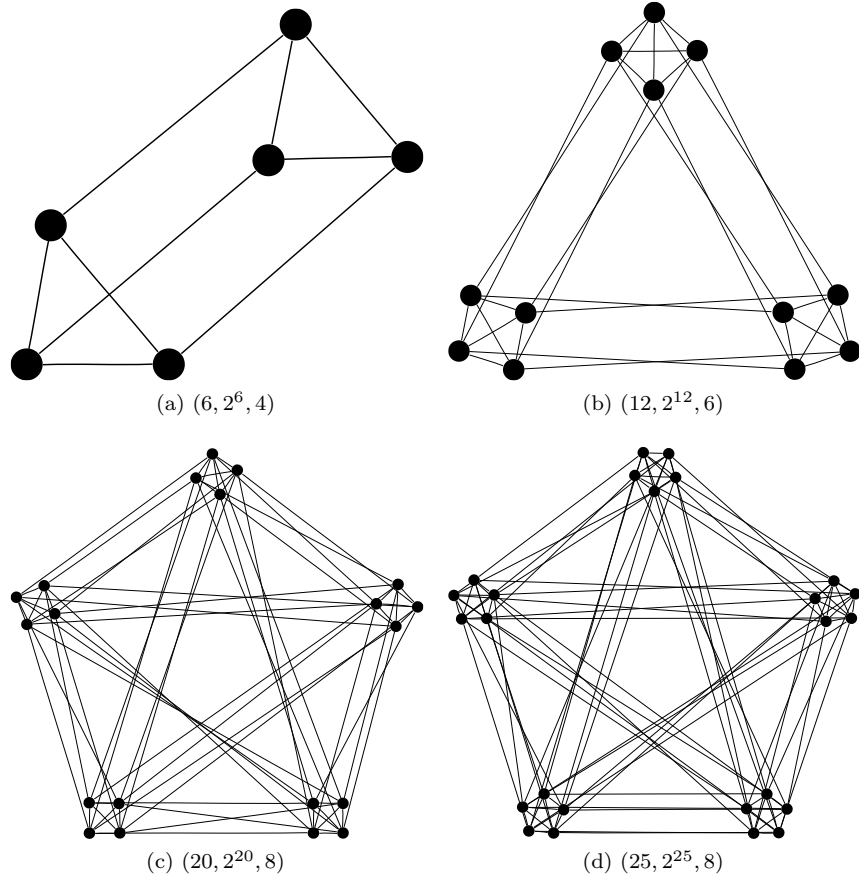
(a) $(6, 2^6, 4)$

(b) $(12, 2^{12}, 6)$

(c) $(20, 2^{20}, 8)$

(d) $(25, 2^{25}, 8)$

Figure 5: Examples of Nested Clique Graphs Corresponding to Codes over $\mathbb{F}_4$
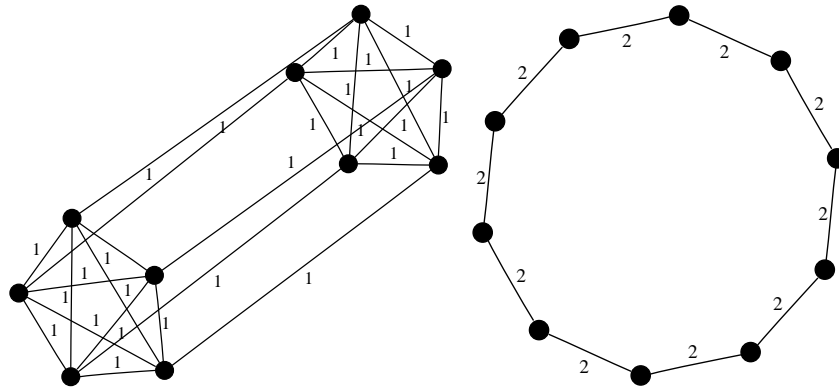

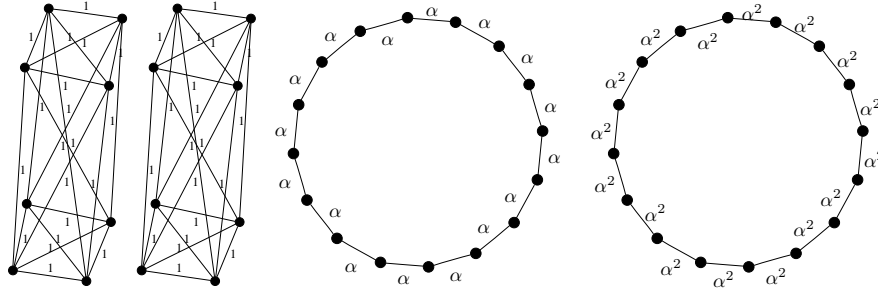Figure 6: Two Graphs Whose Sum Corresponds to the $(10, 3^{10}, 6)$ Code

Figure 7: Three Graphs Whose Sum Corresponds to the $(16, 4^{16}, 8)$ Code

Note that the vertices of the graphs corresponding to circulant $(10, 3^{10}, 6)$ and $(16, 4^{16}, 8)$ graph codes have degree higher than $d-1$. We have tried to obtain similar graph representations for other codes in Table 6, but without success. Many of the circulant graph codes have vertex degree much higher than $d-1$, for instance the $(14, 5^{14}, 8)$ code generated by $(\omega 1221202021221)$, and the $(18, 5^{18}, 10)$ code generated by $(\omega 12134242124243121)$.

ACKNOWLEDGEMENTS

REFERENCES

[1] A. Ashikhmin and E. Knill, *Nonbinary quantum stabilizer codes*, IEEE Trans. Inform. Theory, **47** (2001), 3065–3072.

[2] M. Bahramgiri and S. Beigi, *Graph states under the action of local Clifford group in non-binary case* (2006), preprint, `arXiv:quant-ph/0610267`

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

[4] 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** (1998), 1369–1387.

[5] L. E. Danielsen, "On Self-Dual Quantum Codes, Graphs, and Boolean Functions", Master's thesis, Univ. Bergen, 2005.

[6] 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*, in "Sequences and Their Applications – SETA 2004" (eds. T. Helleseth, D. Sarwate, H.-Y. Song and K. Yang), Springer-Verlag, Berlin, (2005), 373–388.

[7] L. E. Danielsen and M. G. Parker, *On the classification of all self-dual additive codes over* GF(4) *of length up to 12*, J. Combin. Theory Ser. A, **113** (2006), 1351–1367.

[8] P. Gaborit, W. C. Huffman, J.-L. Kim and V. Pless, *On additive* GF(4) *codes*, in "Codes and Association Schemes" (eds. A. Barg and S. Litsyn), Amer. Math. Soc., Providence, RI, (2001), 135–149.

[9] D. G. Glynn, T. A. Gulliver, J. G. Maks and M. K. Gupta, "The Geometry of Additive Quantum Codes" (2004), submitted to Springer-Verlag.

[10] D. Gottesman, "Stabilizer Codes and Quantum Error Correction", Ph.D. thesis, Caltech, 1997.

[11] M. Grassl, T. Beth and M. Rötteler, *On optimal quantum codes*, Internat. J. Quantum Inf., **2** (2004), 55–64.

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

[13] T. A. Gulliver and J.-L. Kim, *Circulant based extremal additive self-dual codes over* GF(4), IEEE Trans. Inform. Theory, **50** (2004), 359–366.

[14] E. Hostens, J. Dehaene and B. De Moor, *Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic*, Phys. Rev. A, **71** (2005), 042315.

[15] G. Höhn, *Self-dual codes over the Kleinian four group*, Math. Ann., **327** (2003), 227–255.

[16] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Trans. Inform. Theory, **52** (2006), 4892–4914.

[17] A. Klappenecker and M. Rötteler, *Beyond stabilizer codes I: Nice error bases*, IEEE Trans. Inform. Theory, **48** (2002), 2392–2395.

[18] E. Knill and R. Laflamme, *Theory of quantum error-correcting codes*, Phys. Rev. A, **55** (1997), 900–911.

[19] B. D. McKay, nauty User's Guide, version 2.2 (2004), `http://cs.anu.edu.au/~bdm/nauty/`.

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

[21] 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** (2004), 022316.

[22] E. M. Rains, *Nonbinary quantum codes*, IEEE Trans. Inform. Theory, **45** (1999), 1827–1832.

[23] R. Raussendorf, D. E. Browne and H. J. Briegel, *Measurement-based quantum computation on cluster states*, Phys. Rev. A, **68** (2003), 022312.

[24] M. Rötteler, M. Grassl and T. Beth, *On quantum MDS codes*, in "Proc. 2004 IEEE Int. Symp. Inform. Theory", (2004), 355.

[25] D. Schlingemann, *Stabilizer codes can be realized as graph codes*, Quantum Inf. Comput., **2** (2002), 307–323.

[26] D. Schlingemann and R. F. Werner, *Quantum error-correcting codes associated with graphs*, Phys. Rev. A, **65** (2002), 012308.

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

E-mail address: larsed@ii.uib.no