A Search for New Optimal Singly-Even Self-Dual Codes of Length 48

Kristy Mitchell
Fayetteville State University
Faculty Mentor: Vassil Yorgov
Fayetteville State University

ABSTRACT

The best binary self-dual singly-even codes of length 48 have minimal weight 10 and are called optimal. There are 75 such codes found by Harada at al. in 2005. We use the method for constructing self-dual codes via automorphism of order three to find 102 optimal self-dual singly-even codes of length 48. We use computer algebra system Magma to construct the codes to compute their weight enumerators and automorphism groups. Each of our codes has exactly 768 vectors of weight 10 and automorphism group of order 3 or 6. As a result, the pool of known optimal singly-even self-dual codes of length 48 is increased to 177. We check that all these codes are pair wise inequivalent.

PRELIMINARIES

Prior to the start of this paper, it is necessary that certain terms be defined. We assume the reader has a background in Linear Algebra and Modern Algebra. Let $GF(q)$ be a finite field with q elements (where $q = p^s$ and p is prime) and n be a positive integer. Let$GF(q)^n$ denote the vector space of all n-tuples with entries from $GF(q)$. Any k dimensional linear subspace of $GF(q)^n$ is called a $[n,k]$ code. The number n is called the *block length* of the code. Any k by n matrix with row space equal to an $[n,k]$ code C is called a *generator matrix* of C. The *weight* of a vector $v \in GF(q)^n$, $wt(v)$, is the number of nonzero entries of v. The smallest weight of the nonzero code vectors is known as the *minimum weight* of the code. An $[n,k]$ code is called an $[n,k,d]$ code if its minimum weight is d. Codes are used for error correction when information is sent via noisy channels.

Example. The matrix

$$G_8 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

generates an [8,4,4] self-dual binary (over $GF(2)$) code, C_8. We will illustrate how error correction works with C_8. For us, a piece of information which has to be transmitted is a binary vector, u, of length 4. We encode u into a vector $v = uG_8$ from C_8, where uG_8 is the usual multiplication of a vector and a matrix over $GF(2)$. Then we send v through the channel. The noise introduces errors and the received vector is $v' = v + e$, where e is the error vector of 8 bits. In general, v' is not in C_8. The *Hamming distance* between two vectors x and z from $GF(2)^8$ is $d(x,z) = wt(x - z)$. In other words, $d(x,z)$ equals the number of entries where x and z differ. We decode v' to a closest vector from C_8 with respect to the Hamming distance. That vector corresponds to a unique vector of four bits under reversed encoding. We will show that when $wt(e) \leq 1$, that vector is exactly u. It can be checked that the distance between any two different vectors in C_8 is at least 4. It follows that the spheres in $GF(2)^8$ with radius one centered at the code vectors of C_8 are disjoint. As $d(v',v) = wt(v' - v) = wt(e) = 1$, v' is in a unique sphere of radius one centered in v. Therefore, the procedure described above recovers the vector u. Thus the code C_8 can correct one error.

For any real number r, let $\lfloor r \rfloor$ denote the largest integer not greater than r. In general, an $[n,k,d]$ code over $GF(q)$ can correct up to $\lfloor (d-1)/2 \rfloor$ errors [8]. Codes with larger minimum weight have better error-correcting capabilities. Many of the known good codes have additional properties as being self-dual or having automorphisms. Under the *inner product* $\langle u,v \rangle = u_1v_1 + \cdots + u_nv_n$ in $GF(2)^n$, the *dual code* of C is $C^{\perp\prime} = \{v \in GF(2)^n \mid \langle u,v \rangle = 0 \ \forall \ u \in C\}$. A code C is *self-dual* if $C^{\perp\prime} = C$. Furthermore, a *doubly-even* code is a self-dual code that has only weights divisible by 4; otherwise the code is known as *singly-even.*

The following bound on the minimum distance d of a binary self-dual $[n, n/2, d]$ code is obtained in [9]:

$$d \leq \begin{cases} 4\lfloor n/24 \rfloor + 6 & \text{if } n \equiv 22 \pmod{24}; \\ 4\lfloor n/24 \rfloor + 4 & \text{otherwise.} \end{cases}$$

If a self-dual code meets the upper bound, it is known as *extremal.* Any extremal code of length a multiple of 24 must be *doubly-even* [9]. Two binary codes are called *equivalent* if one can be obtained

from the other by only permuting the entries of its vectors using a single permutation. Up to equivalence, there are unique extremal codes of length 24 and 48 [8], [5].

The best codes in the class of singly-even self-dual codes of length 48 have minimum distance 10 [3]. Such codes are called *optimal.* We investigate the optimal self-dual singly-even [48,24,10] codes.

Let A_k be the number of words of weight k in a code C. Then the polynomial

$$\sum_{k=0}^{n} A_k y^k$$

of the variable y is called the *weight enumerator of* C. The weight enumerator provides information about the distribution of weights in the code. Since permuting entries in a vector does not change its weight, equivalent codes have equal weight enumerators.

Example. The weight enumerator of C_8 is $1 + 14y^4 + y^8$ because this code has the zero vector, the all one vector, and 14 vectors of weight 4.

There are two possible weight enumerators for optimal self-dual singly-even $[48, 24, 10]$ codes [3]:

$$W_{48,1} = 1 + 704y^{10} + 8976y^{12} + 56896y^{14} + \cdots \text{ and}$$
$$W_{48,2} = 1 + 768y^{10} + 8592y^{12} + 57600y^{14} + \cdots .$$

All self-dual codes which have weight enumerator $W_{48,1}$ are known. Proposition 3.7 from [4] states that there are exactly ten inequivalent such codes. Each of these ten codes is a neighbor of the unique extremal code of length 48, q_{48}[8, section 6.5]. A *neighbor* of q_{48} is any code generated by $q_{48} \cap \langle v \rangle$ and v for some $v \notin q_{48}$, where $\langle v \rangle$ is the code generated by v. All $[48, 24, 10]$ neighbors of q_{48} are determined in [4]. There are 74 such codes up to equivalence. The first ten of the neighbors of q_{48} have weight enumerator $W_{48,1}$, and the remaining 64 of them have weight enumerator $W_{48,2}$. A $[48, 24, 10]$ self-dual code with weight enumerator $W_{48,2}$ which is not a neighbor of q_{48} is also provided there.

In this work, we show that there are new, previous unknown $[48, 24, 10]$ self-dual codes with weight enumerator $W_{48,2}$. We find 102 such codes.

METHODS

We use the method of constructing self-dual codes with automorphisms developed in [6] and [10]. A permutation is called an *automorphism* of a code if it sends the code to itself. We look for codes which have automorphism of order 3 with no fixed coordinate positions. Let C be a binary self-dual code having length 48 and automorphism

$$\sigma = (1,2,3)(4,5,6)\cdots(46,47,48)$$

of order 3 with 16 disjoint 3-cycles.

We denote the cycle position sets σ by $\Omega_1 = \{1,2,3\}, \ldots, \Omega_{16} = \{46,47,48\}$. Let

$$F_\sigma(C) = \{v \in C : v\sigma = v\} \text{ and}$$
$$E_\sigma(C) = \{v \in C : wt(v|\Omega_i) \equiv 0 \pmod 2, i = 1,2,\ldots,16\}$$

where $v|\Omega_i$ is the restriction of v to Ω_i. For example, if $v = 101000 \ldots 110$ is a vector from $E_\sigma(C)$, then $v|\Omega_1 = 101$, $v|\Omega_2 = 000$, ..., $v|\Omega_{16} = 110$ are vectors of length three of even weight. If $v = 000111 \ldots 111$ is a vector from $F_\sigma(C)$, then $v|\Omega_1 = 000$, $v|\Omega_2 = 111$, ..., $v|\Omega_{16} = 111$ are repetition vectors of length three.

It is known [6], that $F_\sigma(C)$ and $E_\sigma(C)$ are linear subspaces and the following lemma holds.

Lemma 1 *The code C is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$.*

Example. The code C_8 has automorphism $\lambda = (1,2,3)(4,5,6)$ of order 3 with two 3-cycles and two fixed points. The subcodes $F_\lambda(C_8)$ and $E_\lambda(C_8)$ are generated by the matrices $\begin{pmatrix}1&1&1&0&0&0&1&0\\0&0&0&1&1&1&0&1\end{pmatrix}$ and $\begin{pmatrix}0&1&1&0&1&1&0&0\\1&0&1&1&0&1&0&0\end{pmatrix}$ correspondingly. Because λ has two fixed points, the vectors from $E_\lambda(C_8)$ must end with two zeros by an extension of the definition.

Knowing $F_\sigma(C)$ and $E_\sigma(C)$, we can recover C. For that reason, we consider some additional properties of these two subcodes. A vector v belongs to $F_\sigma(C)$ if and only if v belongs to C and v is constant on each cycle. We use a projection π: $F_\sigma(C) \to F_2^{16}$ by $(v^\pi)_i = v_j$ for some $j \in \Omega_i$, $i = 1,2,\ldots,16$. The map π is called a contraction map because for each set of cycle positions, Ω_i, π replaces the three equal entries of v with one of them.

Example. The matrix $\begin{pmatrix}1&0&1&0\\0&1&0&1\end{pmatrix}$ generates the contracted code $\pi(F_\lambda(C_8))$. One can check that this is a $[4,2]$ binary self-dual code. As we will see in the next theorem, the contracted code is always self-dual.

Let P be the subset of the factor ring $GF(2)[x]/(x^3-1)$ consisting of all even weight polynomials. Denote $e = x + x^2$, $xe = 1 + x^2$, and $x^2e = 1 + x$. It is easy to check that $P = \{0, e, xe, x^2e\}$ is a field with 4 elements. Hence, P is isomorphic to $GF(4)$. For v in $E_\sigma(C)$ and for j in $\{1,2,\ldots,16\}$, we map the restriction $v|\Omega_j = (v_{3j-2}, v_{3j-1}, v_{3j})$ into $v_{3j-2} + v_{3j-1}x, v_{3j}x^2$. This polynomial belongs to P because the weight of (v_0, v_1, v_2) is even. Thus, we define a map φ: $E_\sigma(C) \to P^{16}$.

A *Hermitian* inner product in P^{16} is defined with

$$\langle u, v\rangle = u_1w_1^2 + u_2w_2^2 + \cdots + u_{16}w_{16}^2$$

A *Hermitian self-dual code* is self-dual with respect to this inner product. The inner product is similar to the Hermitian inner product in complex vector spaces. Complex conjugation is an automorphism of order two in the complex number field. In the definition above, it is replaced with squaring which is an automorphism of order two of $P = GF(4)$.

Example. Lets delete the last two coordinates of $E_\lambda(C_8)$ and denote the result by $E_\lambda(C_8)^*$. The code $E_\lambda(C_8)^*$ is generated by the matrix $\begin{pmatrix}0&1&1&0&1&1\\1&0&1&1&0&1\end{pmatrix}$. Replacing the restrictions of the rows on Ω_1 and Ω_2 with the corresponding elements from P produces the matrix $\begin{pmatrix}e&e\\xe&xe\end{pmatrix}$. Since the second row is a multiple of the first row, this matrix generates a $[2,1]$ code over $GF(4)$. One can check that this is a Hermitian self-dual code.

The method we use relies on the following theorem which is a specialization of a result in [6].

Theorem 2 *A binary code C of length 48 with an automorphism σ is self-dual if and only if the following two conditions hold:*
(i) $C_\pi = \pi(F_\sigma(C))$ is a self-dual binary code of length 16;
(ii) $C_\varphi = \pi(E_\sigma(C))$ is a Hermitian self-dual code of length 16 over $GF(4)$.

Complete classifications of the binary self-dual codes of length 16 and of the Hermitian self-dual codes of length 16 over $GF(4)$ are presented in [7] and [2]. By selecting one code of each type, applying

the inverse maps of π and φ, and combining them in different ways we can obtain many $[48,24]$ self-dual binary codes with automorphism σ can be obtained in this way.

RESULTS

Let σ be an automorphism of a $[48,24,10]$ self-dual code C with weight enumerator $W_{48,2}$.

Lemma 3 *The code C_π is equivalent to the $[16,8,4]$ binary self-dual code F_{16} given in [7].*

Proof. It is pointed out in the previous section that C_π is a binary self-dual code of length 16. A weight 3 vector from C_π corresponds to a weight 9 vector from C. Since the minimal weight of C is 10, the minimal weight of C_π is at least 4. Up to equivalence, there are three such codes [7]. The first two of them have weight enumerator

$$W_1 = 1 + 28y^4 + 198y^8 + 28y^{12} + y^{16}.$$

The third one, F_{16}, has weight enumerator

$$W_2 = 1 + 12y^4 + 64y^6 + 102y^8 + 64y^{10} + 12y^{12} + y^{16}.$$

Let A_i and a_i be the number of vectors of weight i in the code C and C_π, correspondingly. The orbit $\{v, v\sigma, v\sigma^2\}$ of a vector v from C under σ has length 1 or 3 because the order of σ is 3. The length of the orbit $\{v, v\sigma, v\sigma^2\}$ is one if and only if v is in $F_\sigma(C)$. These orbits form a partition C. Hence, $A_{3i} \equiv a_i \pmod 3$ for $0 \le i \le 16$. These conditions do not hold for W_1 since $A_{12} \equiv 8592 \equiv 0 \pmod 3$ and $a_4 = 28 \equiv 1 \pmod 3$. An easy check shows that the conditions hold for W_2.

We use

$$MF_{16} = \begin{pmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&0&0&1&1&1&1&1&1&1&0&0&0&0&0&0 \\ 1&0&0&0&0&1&1&1&1&1&1&1&0&0&0&0 \\ 1&0&0&0&0&0&0&1&1&1&1&1&1&1&0&0 \\ 1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1 \\ 1&1&0&1&0&0&0&0&0&0&0&1&0&0&1&1 \\ 1&1&0&0&0&1&0&0&0&0&0&0&0&1&1&1 \\ 1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&1 \end{pmatrix}$$

as a generator matrix of F_{16}. Lets denote G_1 the automorphism group of F_{16}. Applying the Magma function *AutomorphismGroup* shows that the order of G_1 is 72728.

Lemma 4 *The code C_φ is a $[16,8,6]$ Hermitian self-dual code over $GF(4)$ equivalent to one of the codes $D_{16,i}$, $52 \le i \le 55$, given in [2].*

Proof. Each nonzero entry of a vector from C_φ contributes 2 to the weight of the corresponding vector from $E_\sigma(C)$. Hence the minimum weight of C_φ is at least 5. Any Hermitian self-dual code contains only vectors of even weight. Thus, the minimum weight of C_φ is at least 6. Among all $[16,8]$ Hermitian self-dual code over $GF(4)$ listed in [2], only the codes $D_{16,i}$, $52 \le i \le 55$, meet this requirement.

The following generator matrices for the codes $D_{16,i}$, $52 \le i \le 55$, are provided in [2]:

$$M_{52} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & w & w^2 & w^2 & w & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & w & w^2 & w^2 & w \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & w & 1 & 0 & 1 & w & w^2 & w^2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & w^2 & w & 1 & 0 & 1 & w & w^2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & w^2 & w^2 & w & 1 & 0 & 1 & w \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & w & w^2 & w^2 & w & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & w & w^2 & w^2 & w & 1 & 0 \end{pmatrix}$$

$$M_{53} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & w & 0 & 0 & w & 0 & 0 & w^2 & w^2 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & w & 0 & w & 0 & 0 & 0 & 0 & 0 & w^2 & w^2 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & w & 0 & w & 0 & w^2 & 0 & 0 & 0 & w^2 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & w & 0 & w & w^2 & w^2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & w & 0 & 0 & w & 0 & 0 & w^2 & w^2 & 0 & 0 \\ 0 & 0 & w^2 & 0 & 0 & w^2 & 0 & w & 0 & w^2 & 0 & 0 & 0 & w^2 & 0 & w \\ 0 & w^2 & 0 & w^2 & 0 & 0 & 0 & 0 & w & 0 & w^2 & w & 0 & 0 & w^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & w & 0 & 0 & w & 1 & w^2 & 0 & 0 & w \end{pmatrix}$$

$$M_{54} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & w & w^2 & w & 0 & 0 & 0 & 0 & 0 & w^2 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & w & w^2 & w & w^2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & w & 0 & 0 & w & w^2 & 0 & w^2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & w^2 & w & 0 & 0 & w & 0 & 0 & w^2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & w & w^2 & w & 0 & 0 & 0 & 0 & 0 & w^2 & 0 \\ 0 & 1 & 0 & w^2 & 0 & w & 1 & w^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w \\ 0 & w & 1 & 0 & w^2 & 0 & 0 & 1 & w^2 & 0 & 0 & w & 0 & 0 & 0 & 0 \\ 0 & 0 & w & 1 & 0 & w^2 & 0 & 0 & 1 & w^2 & 0 & 0 & w & 0 & 0 & 0 \end{pmatrix}$$

$$M_{55} = \begin{pmatrix} w & 1 & w & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & w & 1 & w & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & w & 1 & w & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & w & 1 & w & 0 \\ w & 0 & w & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & w & 0 & w & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & w & 0 & w & 1 & 0 & 0 & 1 & 0 \\ 1 & w^2 & 0 & w^2 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Here $GF(4) = \{0,1,w,w^4\}$ with $w^2 = 1 + w$.

Let $\pi^{-1}(MF_{16})$ be the 8 by 48 matrix obtained from MF_{16} by repeating each coordinate three times. Let α be a permutation from the symmetric group of degree 16, and let M_i^{α} be the matrix M_i with columns permuted with α where $i \in \{52, 53, 54, 55\}$. Let $\varphi^{-1}(M_i^{\alpha})$ denote the 16 by 48 matrix obtained from M_i^{α} by replacing each of its entries with a matrix block according to the map

$$0 \to \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad 1 \to \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad w \to \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad w^2 \to \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Then the code $C_{i,\alpha}$ generated by the rows of $\pi^{-1}(MF_{16})$ and $\varphi^{-1}(M_i^{\alpha})$ is a binary self-dual [48,24] singly-even code.

Lemma 5 *If α_1 and α_2 belong to the same left coset of the automorphism group G_1 of F_{16}, then the codes C_{i,α_1} and C_{i,α_2} are equivalent.*

Proof. Let $\alpha_2 = \alpha_1 g$ where g is in G_1. The codes C_{i,α_1} *and* C_{i,α_2} are generated by the matrices

$$\begin{pmatrix} \pi^{-1}(MF_{16}) \\ \varphi^{-1}(M_i^{\alpha_1}) \end{pmatrix} \text{ and } \begin{pmatrix} \pi^{-1}(MF_{16}) \\ \varphi^{-1}(M_i^{\alpha_2}) \end{pmatrix}.$$

The matrices

$$\begin{pmatrix} \pi^{-1}(MF_{16}) \\ \varphi^{-1}(M_i^{\alpha_2}) \end{pmatrix} = \begin{pmatrix} \pi^{-1}(MF_{16}) \\ \varphi^{-1}(M_i^{\alpha_1 g}) \end{pmatrix}$$

and

$$\begin{pmatrix} \pi^{-1}(MF_{16})^{g^{-1}} \\ \varphi^{-1}(M_i^{\alpha_1 g g^{-1}}) \end{pmatrix} = \begin{pmatrix} \pi^{-1}(MF_{16})^{g^{-1}} \\ \varphi^{-1}(M_i^{\alpha_1}) \end{pmatrix}$$

Generate equivalent codes. Since g is in the automorphism group of the code F_{16},

$$\begin{pmatrix} \pi^{-1}(MF_{16})^{g^{-1}} \\ \varphi^{-1}(M_i^{\alpha_1}) \end{pmatrix} = \begin{pmatrix} \pi^{-1}(MF_{16}) \\ \varphi^{-1}(M_i^{\alpha_1}) \end{pmatrix}$$

The Lemma follows.

A computer search with Magma [1] over a large number of representatives of left cosets of G_1 in the symmetric group of degree 16 produced 73 permutations α which determine optimal codes $C_{52,\alpha}$, 7 permutations α which determine optimal codes $C_{53,\alpha}$, 5 permutations α which determine optimal codes $C_{54,\alpha}$, and 17 permutations α which determine optimal codes $C_{55,\alpha}$. The 102 permutations are given in Table 1 through Table 4 in the Appendix.

CONCLUSION

We used the Magma function IsEquivalent [1] to check that all of the 102 optimal codes we found in this work are pair wise inequivalent. They are also inequivalent to any of the codes found in [4]. We computed the weight enumerators and automorphism groups of the codes. Each code has weight enumerator $W_{48,2}$, and automorphism group of order 3 or 6. To the best of our knowledge, these codes are previously unknown. As a result of this work, the pool of optimal self-dual codes of length 48 is increased by 102 new codes.

Acknowledgment

The authors are grateful to the anonymous reviewers. Due to their criticism, the quality of the paper was considerably improved.

REFERENCES

[1] W. Bosma and J. Cannon, "Handbook of Magma Functions," University of Sydney, 2001.

[2] J.H. Conway, V. Pless, N.J.A. Sloane, "Self-dual codes over GF(3) and GF(4) of length not exceeding 16," IEEE Trans. Info. Theory 25 (1979), 312-322.

[3] J.H. Conway and N.J.A. Sloane, "A new upper bound on the minimal distance of self-dual codes,"IEEE Trans. Inform. Theory IT-36 (1990), 1319-1333.

[4] M. Harada, M. Kitazume, A. Munemasa, and B. Venkov, "on some self-dual codes and unimodular lattices in dimension 48," European Journal of Combinatorics 26 (2005), 543-557.

[5] S.K.Houghten, C.W.H. Lam, L.H. Thiel and J.A. Parker, "The extended quadratic residue code is the only (48, 24,12) self-dual doubly-even code," IEEE Trans. Info. Theory 49 (2003), 53-59.

[6] W.C. Huffman, "Automorphisms of codes with application to extremal doubly-even codes of length 48," IEEE Trans. Inform. Theory 28 (1982), 511-521.

[7] V.Pless, "A classification of self-orthogonal codes over GF(2)," Discrete Math 3 (1972), 209-246.

[8] V. Pless, "Introduction to the theory of error-correcting codes," Wiley, John & Sons, 1998.

[9] E. M. Rains, "Shadow bounds for self-dual codes," IEEE. Trans. Inform. Theory IT-44 (1998), 134-139.

[10] V.Y. Yorgov, "A method for constructing inequivalent self-dual codes with applications to length 56," IEEE Trans. Inform. Theory 33 (1987), 77-82.

APPENDIX

Table 1: The Codes $C_{52,\alpha}$

Code	α	Code	α
1	(9, 12, 14, 15, 13, 11)	2	(9, 12, 15, 13, 11, 10)
3	(9, 14, 12, 15, 13, 11)	4	(9, 15, 13, 10)
5	(8, 9, 15, 13, 10, 11)	6	(8, 12, 15, 13, 11)
7	(7, 11, 13, 8, 10, 15)	8	(7, 11)(8, 10, 9, 15, 13)
9	(7, 11, 8)(9, 15, 13, 10)	10	(7, 10, 14)(9, 11, 15)
11	(7, 10, 15, 13, 11)	12	(7, 10)(8, 15, 9)
13	(7, 10, 13, 11, 14, 12)(8, 15, 9)	14	(7, 10)(8, 9)(11, 14, 12, 13)
15	(7, 12)(8, 11)(9, 15, 13, 10)	16	(7, 9, 11, 13, 10)
17	(7, 9, 11, 13, 14)	18	(7, 9, 11)(13, 14)
19	(7, 9, 11, 10, 13)	20	(7, 9, 11)(10, 13)
21	(7, 9, 13)(10, 11)	22	(7, 9, 13, 11, 10, 15)
23	(7, 9, 13, 14, 11)(10, 15)	24	(7, 9, 15, 10)(11, 13)
25	(7, 9, 14, 12, 13, 11)	26	(7, 9, 14, 12)(11,13)
27	(7, 9, 10)	28	(7, 9, 12, 14)(11, 13)
29	(7, 9, 13, 8, 12, 14)(10, 15)	30	(7, 9, 11, 13, 8, 14)(10, 15)
31	(7, 9, 12)(8, 13, 11)	32	(7, 9, 15)(8, 13, 11)
33	(7, 9, 8, 10, 11, 13)	34	(7, 15, 9, 10)
35	(7, 15, 9, 10, 13)	36	(7, 15, 10)(11, 13)
37	(7, 15, 9, 13)(10, 11)	38	(7, 15, 10, 14)(9, 13, 11)
39	(7, 15)(8, 13, 11)	40	(7, 15, 9, 12)(8, 13, 11)
41	(7, 15, 9)(8, 10, 11)	42	(7, 13, 14, 9, 11, 15)
43	(7, 13, 14)(9, 11)	44	(7, 13, 14, 15)(9, 11)
45	(7, 13, 11, 9, 14, 12, 15)	46	(7, 13, 12, 15)(9, 14, 11, 10)
47	(7, 13, 11)(10, 15)	48	(7, 13, 11, 9, 12, 14, 15)
49	(7, 13, 15)(9, 10, 11)	50	(7, 13, 10, 9, 15)
51	(7, 14, 11, 15, 9, 8, 12)	52	(7, 8, 13, 11)(9, 10, 15, 12)
53	(7, 8, 13, 11, 9, 14, 15)	54	(6, 11, 7, 10)(8, 15, 9)
55	(6, 11, 15, 10, 13)	56	(6, 11, 13)(12, 14)
57	(6, 11, 8, 13)(9, 15)	58	(6, 10, 7, 15, 9)(11, 12, 13)
59	(6, 10, 13, 11, 12, 7, 9)	60	(6, 10, 9, 14)(11, 12, 15, 13)
61	(6, 10, 15, 13, 11, 12, 9)	62	(6, 12, 14)(9, 15, 13, 10, 11)
63	(6, 12, 13, 10, 11, 8, 15)	64	(6, 9, 13, 11, 10, 14, 15)
65	(6, 9, 15, 13, 14)	66	(6, 9, 11, 10, 14, 15, 13)
67	(6, 9)(7, 10, 11, 12, 14, 15, 13)	68	(6, 9)(7, 10)(11, 14)(13,15)
69	(6, 15, 7, 10, 11, 12, 14, 9)	70	(6, 15, 7, 10, 13, 9)(11, 14)
71	(5, 10, 11, 6, 9)(7, 12, 14, 15)	72	(5, 10, 11, 6, 15, 13, 7, 12, 14, 9)
73	(5, 10, 6, 15, 12, 7, 8, 9)(11, 14, 13)		

Table 2: The Codes $C_{53,\alpha}$

Code	α	Code	α
1	(8, 14, 10, 13, 9, 15, 12)	2	(8, 14)(9, 10, 13)(12, 15)
3	(8, 14, 10, 13, 9, 12)	4	(7, 13, 14, 10, 9, 15, 12)
5	(7, 12, 8, 14, 10, 9, 13, 15, 11)	6	(6, 15, 9, 11, 10, 13, 12, 8)
7	(6, 12, 8, 13, 9, 14, 10, 15)		

Table 3: The Codes $C_{54,\alpha}$

Code	α	Code	α
1	(7, 9)(8, 12)(10, 15 ,14, 11)	2	(6, 8, 15, 10, 9)(11, 13, 14, 12)
3	(6, 8, 15, 10, 9, 14, 12, 11, 13)	4	(6, 8, 15, 9, 14, 12, 11, 13)
5	(6, 8, 9, 13, 14,11, 10)(12, 15)		

Table 4: The Codes $C_{55,\alpha}$

Code	α	Code	α
1	(7, 12, 15)(8, 11, 14, 10)	2	(7, 11, 9, 13, 10)(8, 14)(12, 15)
3	(7,11)(8, 14)(9, 15, 12, 13, 10)	4	(7, 11, 9)(8, 14)(10, 13)(12, 15)
5	(7, 8, 11)(9, 13, 12)(10, 15, 14)	6	(7, 8, 13, 11, 9, 14, 10)(12, 15)
7	(7, 10, 15, 11)(8, 14, 12, 9, 13)	8	(7, 15, 8, 11, 14, 12, 9, 13)
9	(7, 14, 8, 11, 12, 15)(9, 10)	10	(7, 14, 8, 10, 12, 13, 11, 15)
11	(6, 11, 9, 10, 14, 8, 15, 12, 13)	12	(6, 11, 9, 10, 12, 13, 14, 15)
13	(6, 11, 15, 7, 12, 14, 10)	14	(6, 12, 13, 14, 10)(7, 11, 15)
15	(6, 10)(8, 11)(12, 13)(14,15)	16	(5, 15, 12, 7, 9, 14, 10, 11, 8)
17	(5, 15, 14, 10)(8, 13, 11)(9,12)		