

An Enumeration of Binary Self-Dual Codes of Length 32

R. T. Bilous

Department of Computer Science, University of Manitoba
Winnipeg, Manitoba R3T 2N2, Canada
umbilou1@cs.umanitoba.ca

G. H. J. van Rees *

Department of Computer Science, University of Manitoba
Winnipeg, Manitoba, R3T 2N2, Canada
vanrees@cs.umanitoba.ca

SHORT RUNNING HEAD: *Enumeration of Self-Dual Codes*

Dedicated to Ron Mullin on the Occasion of his 65th Birthday

*Research supported in part by NSERC Grant OGP0003558

Abstract

A binary self-dual code of length $2k$ is a $(2k, k)$ binary linear code C with the property that every pair of codewords in C are orthogonal. Two self-dual codes, C_1 and C_2 , are equivalent if and only if there is a permutation of the coordinates of C_1 that takes C_1 into C_2 . The automorphism group of a binary code C is the set of all permutations of the coordinates of C that takes C into itself.

The main topic of this paper is the enumeration of inequivalent binary self-dual codes. We have developed algorithms that will take lists of inequivalent small codes and produce lists of larger codes where each inequivalent code occurs only a few times. We have defined a canonical form for codes that allowed us to eliminate the overenumeration. So we have lists of inequivalent binary self-dual codes of length up to 32. The enumeration of the length 32 codes is new. Our algorithm also finds the size of the automorphism group so that we can compute the number of distinct binary self-dual codes for a specific length. This number can also be found by counting and matches our total.

Keywords:

enumeration, recursive, algorithm, binary code, self-dual, linear code, equivalence, algorithm, orthogonal, automorphism group, canonical form, weight distribution

Communicating Author:

G. H. J. van Rees

Dept. of Computer Science

University of Manitoba

Winnipeg, Manitoba

Canada R3T 2N2

1 Introduction

Undefined coding theory terms and examples can be found in MacWilliams and Sloane [6]. Let $V_n(m)$ denote the vector space of all vectors of length n over the field $GF(m)$. An (n, k) linear code over $GF(m)$ is a k dimensional subspace C of $V_n(m)$. The vectors will be referred to as *codewords*. The integers n and k will be referred to as the *length* of the code and the *dimension* of the code. In this paper, we consider only linear codes over $GF(2)$. The *dual code* C^\perp , of a code C , is the orthogonal complement subspace of the original subspace (under the usual dot product), i.e. the dot product of any codeword with any dual codeword is 0. The dual of a (n, k) code is a $(n, n-k)$ code. A code is *self-dual* when $C = C^\perp$. Let C and C' be any two (n, k) codes. As in Pless [7], C and C' are said to be *equivalent* if there exists a permutation, Π , of the coordinates that sends one code into the other, i.e. $C^\Pi = C'$. Two codes that are not equivalent are said to be *inequivalent*. If $C^\Pi = C$ then Π is said to be an *automorphism* of the code. The set of all automorphisms of a code is called the *automorphism group* of the code. For convenience, a code of length 0 with no codewords is considered to be a self-dual code.

The following theorem is well-known, see [7], and will be useful as a check on our results.

Theorem 1.1 The number of $(2k, k)$ self-dual codes in $V_{2k}(2)$ is $\prod_{i=1}^{k-1} (2^i + 1)$.

In this paper, we enumerate the inequivalent $(32, 16)$ self-dual codes. This continues a long line of research conducted by Pless and her associates. Specifically, Pless [7] enumerated the inequivalent self dual codes of length up to 20, then Pless and Sloane [8] enumerated the inequivalent self-dual codes of length 22 and 24. More recently Conway and Pless [3], and Conway, Pless and Sloane [5] enumerated all inequivalent self-dual codes of length up to 30.

This previous research was carried on in an essentially ad hoc fashion. In [3] they obtained, by hook or crook, all inequivalent $(32, 16)$ self-dual codes in which the number of ones in any codeword was a multiple of four, so called *doubly-even length* codes. From that list, they “easily read off” the list of all inequivalent self-dual codes of lengths 26, 28 and 30. To continue in this fashion one would need the list of all inequivalent doubly-even self-dual codes of length 40. This is extremely hard to come by and closed this approach to the enumeration problem for some time. Before we show you how to get around this problem we will first need to define some more terminology.

One can describe an arbitrary code in many ways. We are going to describe codes using their generator matrices. A *generator matrix* of a code C is a $k \times n$ matrix G whose rows

form a basis for C . It is important to note that if G and G' are two generator matrices for a code C , then G' can be produced from G by elementary row operations. So clearly we can use elementary row operations to produce for any $(2k, k)$ self-dual code, a generator matrix in row reduced echelon form, i.e. there is a k by k identity matrix occupying some set of k columns of the generator matrix. Further, since we are interested in inequivalent codes, we can represent the codes of a particular equivalence class with a generator matrix that has an identity matrix on the left and a square matrix A on the right, i.e. $G = [I_k|A]$. It is possible to go from one generator matrix in this form to another generator matrix in this form of an equivalent code by 1) interchanging columns in A , 2) interchanging rows in A and the corresponding columns in I_k and 3) interchanging column i of A with a column j of I_k and zeroing out column j to restore I_k .

The properties of a code that we are interested in will now be defined. The *weight* of a vector is the number of non-zero entries in it. In binary codes this is the number of ones in the vector. The *distance* between two vectors is the number of positions they disagree in. So the weight of $x + y$ is the distance between x and y , where x and y are binary vectors. The *distance of a linear code* is the least weight of any non-zero codeword in the code. An (n, k, d) *linear code* is an (n, k) linear code with distance d . The number of codewords of weight i in a code will be denoted by A_i . The *weight distribution* of a code, C , is a sequence (A_0, A_1, \dots, A_n) .

Our approach to enumerating binary self-dual codes is to use a systematic method to produce a complete list of inequivalent $(2k, k)$ self-dual codes. This will be done recursively. First, it is very easy to get the $(2k, k, 2)$ self-dual codes from the $(2j, j)$ self-dual codes where $j \leq k - 1$. Our second algorithm will take the lists of inequivalent $(2j, j, d \geq 4)$ self-dual codes, where $j \leq k - 2$, and produce a list of all inequivalent $(2k, k, 4)$ self-dual codes. Then a subset of the inequivalent $(2k, k, 4)$ self-dual codes just produced will be used by our third algorithm to produce a list of inequivalent $(2k, k, d)$ self-dual codes where $d \geq 6$. In this way, the algorithms can be used to systematically produce the required list of self-dual codes. Since our algorithms also produce the size of the automorphism group of the codes, we can check that our list has the correct number of codes. In the last section we list the weight enumerators and the size of the automorphism group for each inequivalent code.

With our enumeration, we can prove the following theorem that was conjectured by Conway and Sloane [4]:

Theorem 1.2 The smallest possible length for a binary self-dual code whose full automorphism group has size 1 is 34.

2 Long Codes from Short Codes

In this section we will enumerate all $(2k, k)$ self-dual codes. We will represent our $(2k, k, d)$ self-dual code, C , with a generator matrix that has been row-reduced. All codes with distance $d = 2$ and 4 will be constructed from the smaller codes by Theorem 2.3 and Theorem 2.8 respectively. Finally, Theorem 2.14 will construct the remaining codes whose distances are greater than 4 by starting from a special class of the distance 4 codes with no intersecting weight 4 words.

The following general theorem is quite useful. Since its proof is quite standard, it will not be given.

Theorem 2.1 Let C be a (n, k, d) linear code generated by $G = [I_k|A]$. Let w be any weight d codeword of C . Then there exists a code C' , equivalent to C , generated by $G' = [I_k|A']$ such that w' , the codeword in C' corresponding to w , is a row of G' .

We specialize the above theorem to binary self-dual codes.

Corollary 2.2 For any $(2k, k, d)$ self-dual code, there exists an equivalent code C , generated by $G = [I_k|A]$, such that G contains a row with weight d .

Next we will partition the problem into three parts. The first part is to enumerate all $(2k, k, 2)$ codes and the sizes of their automorphism groups. This is quite easy.

Theorem 2.3 In each equivalence class of $(2k, k, 2)$ self-dual codes, there is a code which has a generator matrix of the form $[I_k|A]$ where $A = I_k$ or A is a direct sum of I_{k-i} and A_i where $G_i = [I_i|A_i]$ generates a $(2i, i, d \geq 4)$ self-dual code C_i , $i < k$, i.e.

$$A = \begin{bmatrix} I_{k-i} & 0 \\ 0 & A_i \end{bmatrix}$$

Further, the size of the automorphism group is $2^k k!$ when $A = I$ and otherwise it is $2^{k-i}(k-i)!$ where s is the size of the automorphism group of C_i .

Proof Since this is a self-dual code, all weight two codewords are disjoint, i.e. there is at most one weight two codeword with a 1 in any coordinate position. This means the weight two codewords are independent as vectors. Then, from linear algebra, we know that there is a generator matrix, G , that has all these weight two codewords as rows. We may assume

that these weight two rows are the first $k - i$ rows of G . Further, since we are considering equivalent codes, we may assume the first row has its 1's in columns 1 and $k + 1$, the second row in columns 2 and $k + 2$, etc. Since this is a self-dual code any row of G must have 00 or 11 in columns j and $k + j$, for $j \leq k - i$. So row j where $j \leq k - i$ can be used to zero out columns j and $k + j$.

So the generator matrix has an identity matrix of size $k - i$ and an i by $k - i$ matrix of 0's in columns 1 to $k - i$ and also columns $k + 1$ to $2k - i$. Rows 1 to $k - i$ of the generator matrix contains the two identity matrices and two $k - i$ by i matrices of 0's. The rest of the matrix consists of two i by i matrices, say R_1 and R_2 . Let R be the concatenation of R_1 and R_2 . Clearly the rows of R must be orthogonal and have rank i and there are $2i$ columns. So R must generate a $(2i, i, d \geq 4)$ self-dual code. So R may be row reduced to $[I_i|A_i]$, where the identity matrix occupies some set of i columns not necessarily the left-most. Now this row reduction can occur in the big generator matrix without affecting the other parts of it. Further, since we are dealing with equivalent codes, the identity matrix of size i in R can be put in columns $k - i + 1$ to k . This leaves the generator matrix in the required form.

Let us now consider the automorphism group of our code. Clearly we have two choices for which one of the two ones in a weight two codeword to put in the left half of the generator matrix. Also, the $k - i$ weight 2 codewords in C can be permuted amongst one another in $(k - i)!$ ways. This is independent of the automorphism group of size s acting on $[I_i|A_i]$ in A . This gives us the size of the automorphism group as $2^{k-i}(k - i)!s$. \square

Using the preceding theorem, it is easy to develop the following efficient recursive algorithm for finding self-dual codes with distance two. Since only one representative code is needed from each equivalence class, our algorithm will assume that the identity matrix is on the left and will not explicitly produce it. The algorithm works exclusively with the A matrix which is the right half of the generator matrix $G = [I_k|A]$.

Algorithm 2.4 :

- Input: a list L_0 of $j \times j$ matrices A_0 , where $j \leq k - 1$ and $G_0 = [I_j|A_0]$ generates a $(2j, j)$ self-dual code C_0 such that C_0 is the unique representative of its equivalence class.
- Output: a list L of $k \times k$ matrices A , where $G = [I_k|A]$ generates a $(2k, k, 2)$ self-dual code C_0 such that C_0 is the unique representative of its equivalence class.

begin

Theorem 2.7 The self-dual extension of a $(2k - 4, k - 2)$ self-dual code, C , is a $(2k, k)$ self-dual code C' .

Proof Without loss of generality, let C have a generator matrix $G = [I_{k-2} | A_{k-2}]$ and an extension as shown in Figure 1. By construction, the first two rows of G' are orthogonal. By the way F and v were constructed, the first two rows of G' are orthogonal to all the other rows of G' . Finally, since the rows of G are orthogonal and the rows of F are either 00 or 11, the last $k - 2$ rows of G' are orthogonal. Clearly, G' generates a $(2k, k)$ self-dual code. \square

We will now examine the converse of Theorem 2.7. Since the sum of the first two rows of a self-dual extension has weight four, the converse is not true for self-dual codes of distance greater than four. But if we restrict ourselves to codes of distance four, the converse of Theorem 2.7 is true.

Theorem 2.8 Any $(2k, k, 4)$ self-dual code, C' , is a self-dual extension of a $(2k - 4, k - 2)$ self-dual code, C .

Proof Since $d = 4$, there must be a codeword of weight four in the code. For convenience, let the positions containing 1 in this codeword be in the left-most positions 1,2,3 and 4. It is well-known [6] that either half the codewords contain a 1 in a particular position and the other half of the codewords contain a 0 or all the codewords contain a 0 in that particular position. So our code must contain another codeword with a 1 in at least one of the first four positions. To ensure even intersection, the second codeword must contain either two 1's or four 1's in the first four positions. Now not all codewords can have four 1's in the first four positions, so there is another codeword which has exactly two 1's in the first four positions since the dimension is maximal.

We know from linear algebra that these two codewords can be extended to a full basis. So let $v_1 = (1, 1, 1, 1, 0, \dots, 0)$ and $v_2 = (1, 1, 0, 0, a)$, where the weight of a is even and positive. So let us consider v_2 and v_1 as the first two rows of our generator matrix for C' . If we add the first row to the second row we get the first two rows to be:

$$\begin{array}{cccccc} 1 & 1 & 0 & 0 & a \\ 0 & 0 & 1 & 1 & a \end{array}$$

Let us split the columns into the first k columns and the last k columns of the generator matrix where (a_1, a_2) is a permutation of a .

$$\begin{array}{ccc|cc} 1 & 0 & a_1 & 1 & 0 & a_2 \\ 0 & 1 & a_1 & 0 & 1 & a_2 \end{array}$$

Use row 1 to zero out column 1 and row 2 to zero out column 2 of our generator matrix. Then in columns $k + 1$ and $k + 2$ we have 00 or 11 in rows 3 to k as the dot product of any such row with the weight four word must be even. Since row operations and column permutations do not affect orthogonality, the rows of the new generator matrix must be orthogonal. The dot product of any two rows from rows 3 to k is even in the four columns 1, 2, $k + 1$ and $k + 2$, so the dot product of any two rows from rows 3 to k in the remaining $2k - 4$ columns must also be even. Then the submatrix, R , consisting of the rows 3 to k and the columns 3 to k and $k + 3$ to $2k$ must be a $(2k - 4, k - 2)$ self-dual code. So, as in the proof of Theorem 2.3, there is a generator matrix $R' = [I_{k-2}|A_{k-2}]$ that can be produced from R using only the three basic operations as described in Section 1. If this is applied to the generator matrix of the longer code, we obtain an identity matrix in rows 3 to k and columns 3 to k and a matrix A_{k-2} in the last $k - 2$ columns of the last $k - 2$ rows. Columns 1, 2, $k + 1$ and $k + 2$ are not affected. In rows 1 and 2 of the big generator matrix, 0's are produced when columns 3 to k are zeroed out and the last $k - 2$ columns, which contain a , are changed to v . Since the code has distance 4, the weight of v is even and positive. The generator matrix, G' , now looks like the one in Figure 1.

Since only row operations and column permutations were used, G' generates a $(2k, k)$ self-dual code. Now the inverse of the product of all column permutations used can be applied to G' to obtain a generator matrix of the proper form for the original code. \square

So we have proved that any $(2k, k)$ self-dual code of distance four contains a shorter self-dual code. If we have a list of all shorter self-dual codes then we just need to self-dual extend each of them to get a list of the $(2k, k)$ self-dual codes. However, if our list of shorter codes contains only one representative, C , of each equivalence class of codes, then we must prove that C can be self-dual extended to any $(2k, k)$ self-dual code that was self-dual extended from any code in the equivalence class containing C . The following theorem does this.

Theorem 2.9 Let C' be a $(2k, k)$ self-dual code generated by $G' = [I_k|\mathcal{A}(A_{k-2}, v)]$, where $G = [I_{k-2}|A_{k-2}]$ generates a $(2k - 4, k - 2)$ self-dual code C . Then for any $(2k - 4, k - 2)$ self-dual code C_0 , equivalent to C , generated by $G_0 = [I_{k-2}|A_{0,k-2}]$ there exists a vector v' such that $G'_0 = [I_k|\mathcal{A}(A_{0,k-2}, v')]$ generates a code C'_0 equivalent to C' .

Proof C' is generated by the matrix $G' = [I_k|\mathcal{A}(A_0, v)]$ as is shown in Figure 1. Recall that by using three types of operations, a generator matrix of a self-dual code may be transformed into a generator matrix of any equivalent self-dual code. Apply the set of operations that take G into G_0 , to G' . In doing so, we change A_{k-2} to $A_{0,k-2}$ and transform some rows in

F to 00 from 11 or vice versa and v to say v' but the rest stays the same. So we obtain a matrix $G'_0 = [I_k | \mathcal{A}(A_0, v')]$. Since these operations only use row operations and column permutations, G' and G'_0 are equivalent. \square

We can now state our algorithm for enumerating the $(2k, k, 4)$ self-dual codes. Again, the algorithm assumes that there is an identity matrix on the left and only works with the A matrix.

Algorithm 2.10 :

- Input: a list L_0 of $(k-2) \times (k-2)$ matrices A_0 , where the corresponding $G_0 = [I_{k-2} | A_0]$ matrices generate all inequivalent $(2k-4, k-2)$ self-dual codes.
- Output: a list L of $k \times k$ matrices A , where the corresponding $G = [I_k | A]$ matrices generate at least one $(2k, k, 4)$ self-dual code for each equivalence class of such codes.

begin

for each $A_0 \in L_0$ **do**

for each $(k-2)$ -vector v such that $w(v) \equiv 0 \pmod{2}$, $w(v) \geq 2$ **do**

Set $A = \mathcal{A}(A_0, v)$.

if $G = [I_k | A]$ generates a code with distance four **then**

if $A \notin L$ **then**

Insert A into L .

end

Finally, we come to the most difficult of the three parts that we have subdivided the problem into, i.e. enumeration of the $(2k, k, d \geq 6)$ self-dual codes. We saw that Theorem 2.7's converse was true when the distance of the code was four. However, the converse is false when the distance is greater than 4. So we will examine what happens when a $(2k, k, d \geq 6)$ self-dual code is self-dual extended. It would be nicest if the resulting code has only one codeword of weight four. Codes with exactly one codeword of weight four are rare but still have to be the self-dual extension of some $(2k-4, k-2)$ self-dual code. The next theorem shows that if v is chosen wisely, then the extension of a $(2k, k, d \geq 6)$ self-dual code contains only one codeword of weight four. First we define the special case when we self-dual extend a $(2k, k, d \geq 6)$ self-dual code in which the first row of the generator matrix has weight d . Theorem 2.1 allows us to assume that the first row has weight d .

components added to the zero codeword in C all have value 0, the corresponding codeword in C' is also the zero codeword. Further, since the non-zero codewords in C' all have weight that is greater than or equal to $d \geq 6$, S_A does not contain any weight 2 or weight 4 codewords.

Let us now consider the set of codewords S_B . Since $w_1 \oplus w_2 = (1100 \dots 01100 \dots 0)$, the codewords of S_B are the codewords of C with four extra coordinate positions added to them. Since the non-zero codewords in C have weight that is greater than or equal to $d \geq 6$, all of the corresponding codewords in S_B have weight that is greater than four. The codeword in S_B that corresponds to the zero codeword of C has weight four, so S_B has no weight 2 words and only one weight 4 word, namely $w_1 \oplus w_2$.

Let us now consider the set of codewords $S_C = r \oplus w_1$, where r is an element of S_A . By the definition of special self-dual extension, we know there are four different ways in which r can intersect w_1 and w_3 (which is a codeword in S_A). Table 1 sets up these possibilities.

	a_1	a_2	c_1	c_2	e_1	$e_2 \dots e_{d-2}$	e_{d-1}	e_d	b_1	$e_{d+1} \dots e_k$	$b_2 \dots b_k$
w_1	1	0	1	0	1	1^{d-3}	0	0	0		0^*
w_3	0	0	1	1	0	1^{d-3}	1	1	1		0^*
Case 1	0	0	1	1	1	1^{2f}				1^{2x+1}	
Case 2	0	0	1	1	0	1^{2f+1}				1^{2x+1}	
Case 3	0	0	0	0	1	1^{2f+1}				1^{2x}	
Case 4	0	0	0	0	0	1^{2f}				1^{2x}	

Table 1: The four different ways r can intersect w_1 and w_3 .

Note that since, in all four cases, either $2f \leq d - 3$ or $2f + 1 \leq d - 3$, and since the distance d must be even, we know $d - 2f$ must always be greater than or equal to 4. Further, in Cases 1, 2, and 3, since our smaller code C has distance d , we must have $2x + 2f + 2 \geq d$ which implies $2x$ is at least 2. Similarly, in Case 4, we must have $2x \geq 4$.

Let us first consider Case 1. In this case, the weight of $r + w_1$ is $2 + d - 3 - 2f + 2x + 1 = d - 2f + 2x \geq 4 + 2x \geq 6$. Similarly, in Case 2, the weight of $r + w_1$ is $3 + d - 3 - 2f - 1 + 2x + 1 = d - 2f + 2x \geq 6$. In Case 3, the weight of $r + w_1$ is $2 + d - 3 - 2f - 1 + 2x = d - 2f + 2x - 2 \geq 2 + 2x \geq 4$. The only way the weight of $r + w_1$ can be exactly 4 is if $2x = 2$ and $d - 2f = 4$, which implies $2f + 1 = d - 3$. Since r and w_3 must be orthogonal, and $2x = 2$, r must have a value of 1 in one and only one of the three coordinates e_{d-1}, e_d, b_1 . However, if this were the case then the codeword in C , that is equal to $r + w_3$ with coordinates a_1, a_2, c_1, c_2 deleted, would have weight 4 which contracts the distance of C being greater than or equal

to 6. Therefore, in Case 3, the weight of $r + w_1$ must be greater than or equal to 6. Finally, in Case 4, the weight of $r + w_1$ is $3 + d - 3 - 2f + 2x = d - 2f + 2x \geq 4 + 2x \geq 8$. Thus, the codewords in S_C all have weight greater than or equal to 6.

Using the same method, it can be shown that S_D does not contain any weight 2 or weight 4 codewords. This completes all cases.

Therefore, C does not contain any weight 2 words and the only weight 4 word in C is $w_1 \oplus w_2$. □

So we have found that a $(2k, k, d \geq 6)$ self-dual code can be extended to a $(2k+4, 2k+2, 4)$ self-dual code containing exactly one weight four word. We are now going to see which $(2k, k)$ self-dual codes extend to such a $(2k+4, 2k+2, 4)$ self-dual code. The next theorem will tell us how many.

Theorem 2.13 A $(2k+4, k+2, 4)$ self-dual code with exactly one weight 4 word is the self-dual extension of at most three inequivalent $(2k, k)$ self-dual codes.

Proof Recall, by Theorem 2.8, that any $(2k+4, k+2, 4)$ self-dual code C' is generated by $G' = [I_{k+2} | \mathcal{A}(A'_k, v')]$, where the first two rows of G' sum to some weight 4 word w , (see Figure 1).

Since C' has exactly one weight 4 codeword, w , the four extension columns of G' , labelled by c_1, c_2, c_3, c_4 in Figure 1, correspond to the four columns of C' in which the weight 4 word w has a value of one. The matrix $G = [I_k | A'_k]$ generates a $(2k, k)$ self-dual code C . The k -vector v' has positive even weight. The $k \times 2$ matrix F is determined by A'_k and v' as follows: If a row in A'_k intersects v' in an even number of positions then the corresponding row in F is 00, and if a row in A'_k intersects v' in an odd number of positions then the corresponding row in F is 11.

Since C has exactly one weight 4 word, there are only 6 ways to choose which two of the four columns, c_1, c_2, c_3, c_4 , will go into the identity part of the generator matrix. However, the column permutation $(c_1, c_3)(c_2, c_4)$ is an automorphism of G' , so there are at most three $(2k, k)$ self-dual codes that extend to G' . Let us examine them more closely.

In $\mathcal{A}(A'_k, v')$ every column must have weight at least three, implying that there is a row, i , in F that is 11. This implies that row i in A'_k intersects v' in an odd number. Since v' has even positive weight, there must be a column in row i of A'_k where row i has a 0 and v' has a 1. Call this column c and let i be the first row of $\mathcal{A}(A'_k, v')$. We now have the following

generator matrix, $G' = [I_{k+2} | \mathcal{A}(A'_k, v')]$, where $v' = 1v$, for any $(2k+4, k+2, 4)$ self-dual code with exactly one weight 4 codeword:

$$\mathcal{A}(A'_k, v') = \left[\begin{array}{cc|c} c_3 & c_4 & c \\ \hline 1 & 0 & 1 \\ 0 & 1 & 1 \\ \hline 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{array} \begin{array}{l} v \\ v \\ u \\ X_0 \\ X_1 \\ X_2 \\ X_3 \end{array} \right] \begin{array}{l} \text{weight}(v) \equiv 1 \pmod{2} \\ u \bullet v \equiv 1 \pmod{2} \\ \text{for any } x_0 \in X_0, x_0 \bullet v \equiv 0 \pmod{2} \\ \text{for any } x_1 \in X_1, x_1 \bullet v \equiv 1 \pmod{2} \\ \text{for any } x_2 \in X_2, x_2 \bullet v \equiv 1 \pmod{2} \\ \text{for any } x_3 \in X_3, x_3 \bullet v \equiv 0 \pmod{2} \end{array}$$

To find the next code that self-dual extends to C' we will put columns c_1 and c_4 into the identity matrix. This will be done by first using row 2 to zero out column c_4 and then restoring I_{k+2} by interchanging column c_4 with columns c_2 (i.e. the second column in I_{k+2}) giving us $G'' = [I_{k+2} | \mathcal{A}(A''_k, v'')]$, where $v'' = 1v$ and:

$$\mathcal{A}(A''_k, v'') = \left[\begin{array}{cc|c} c_3 & c_2 & c \\ \hline 1 & 0 & 1 \\ 0 & 1 & 1 \\ \hline 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{array} \begin{array}{l} v \\ v \\ u \oplus v \\ X_0 \oplus v \\ X_1 \oplus v \\ X_2 \\ X_3 \end{array} \right]$$

To obtain the last of the three codes that self-dual extend to C' , put c_1 and c_3 into the identity matrix by the following procedure. Use row 3 of G'' to zero out column c_3 and then interchange column c_3 with column 3 of G'' . Then use row 2 to zero out column c and then interchange columns c and c_2 . Finally, interchange rows 2 and 3 and columns $k+1$ and $k+3$. We are left with $G''' = [I_{k+2} | \mathcal{A}(A'''_k, v''')]$, where $v''' = 1u$ and:

$$\mathcal{A}(A'''_k, v''') = \left[\begin{array}{cc|c} c_2 & c_4 & \\ \hline 1 & 0 & 1 \\ 0 & 1 & 1 \\ \hline 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{array} \begin{array}{l} u \\ u \\ v \\ X_0 \oplus v \oplus u \\ X_1 \oplus u \\ X_2 \oplus v \\ X_3 \end{array} \right]$$

□

We will now combine and expand the previous two theorems.

Theorem 2.14 Let C' be a $(2k + 4, k + 2, 4)$ self-dual code that is obtained by the special self-dual extension of a $(2k, k, d \geq 6)$ self-dual code, C_1 . Then C' is the self-dual extension of at most three inequivalent $(2k, k)$ self-dual codes; namely, C_1 , the original $(2k, k, d \geq 6)$ self-dual code; C_2 , a $(2k, k, 4)$ self-dual code with no intersecting weight 4 words; and C_3 , a $(2k, k, 4 \leq d' \leq d - 2)$ self-dual code.

Proof By Theorem 2.12 and Theorem 2.13 we know that there are at most three $(2k, k)$ self-dual codes that self-dual extend to C' . Since the extension vector is equal to $(11^{d-3}000^*)$ where the special row of the generator matrix is $0u = (01^{d-3}110^*)$ as depicted in the proof of Theorem 2.12, let the first figure in the proof of Theorem 2.13 be the original code. The next two figures represent the other two codes. Since C' contains one and only one weight 4 word, neither of these codes have distance 2 (for if either did contain a weight 2 codeword, then C' would either contain a weight 2 codeword or a second weight 4 codeword). Therefore, the second and third codes have distance at least 4. The second code has distance 4 as can be seen from its top row and the third code has distance at most $d - 2$ as can be seen from its top row. Now we only have to prove that no weight 4 codewords overlap in the second code.

Let us assume that the second code contains two weight 4 codewords that intersect. This intersection must be of size 2. Let the codewords be $c_a = 1111000^*$ and $c_b = 1100110^*$. Let G_2 denote the generator matrix for C_2 and let R_a and R_b denote the rows of G_2 that sum to c_a and c_b , respectively. In C'' , i.e. the code equivalent to C' that C_2 extends to, the unique weight 4 codeword has 1's in the four new columns used for self-dual extension. Let R_a'' and R_b'' denote the rows of G'' that correspond to R_a and R_b in G_2 of C_2 . The 2 codewords generated by R_a'' and R_b'' are equal to c_a and c_b with four extra components adjoined to them. The two components in the identity matrix will be 00. The other two components in F will be 00 or 11. If either c_a or c_b have 00 then they would be a weight 4 codeword of C'' that is not the sum of the first two rows of G'' . This is a contradiction so the columns must be 11 in both cases. But then the sum of R_a'' and R_b'' would be a weight 4 codeword that is not the sum of the first two rows of G'' . Hence C_2 has no overlapping weight 4 codewords. □

Given one of the generator matrices G_1 , G_2 or G_3 along with the extension vector v , it is easy to directly determine the other two generator matrices. We will use the functions $R(A_2, v)$ and $S(A_2, v)$ to indicate the A part of the generator matrix of the self-dual codes G_1

and G_3 that one gets from A_2 in G_2 . One should note that it is not clear whether $R(A_2, v)$ is G_1 or G_3 . Nevertheless this allows us to develop an algorithm to find $(2k, k, d \geq 6)$ self-dual codes from $(2k, k, 4)$ self-dual codes with no overlapping weight 4 codewords. We will refer to the $(2k, k, 4)$ self-dual code C_2 as an *extension mate* of the $(2k, k, d \geq 6)$ self-dual code C_1 .

Algorithm 2.15 :

- Input: a list L_0 of $k \times k$ matrices A_0 , where the corresponding $G_0 = [I_k | A_0]$ matrices generate one inequivalent $(2k, k)$ self-dual code with no overlapping weight 4 codewords for each equivalence class of such codes.
- Output: a list L of $k \times k$ matrices A , where the corresponding $G = [I_k | A]$ matrices generate at least one $(2k, k, d \geq 6)$ self-dual code for each equivalence class of such codes.

begin

for each $A_0 \in L_0$ **do**

for each k -vector v such that $w(v) \equiv 0 \pmod{2}$, $w(v) \geq 2$ **do**

if $G = [I_{k+2} | \mathcal{A}(A_0, v)]$ generates a code with exactly one weight 4 codeword **then**

Set $A_r = R(A_0, v)$.

Set $A_s = S(A_0, v)$.

Let $d_r =$ distance of code generated by $G_r = [I_k | A_r]$

Let $d_s =$ distance of code generated by $G_s = [I_k | A_s]$

if $d_r > d_s$ **then**

Set $A = A_r$.

else if $d_s > d_r$ **then**

Set $A = A_s$.

if $A \notin L$ **then**

Insert A into L .

end

So, we have developed three algorithms that will produce at least one representative of each equivalence class of $(2k, k)$ self-dual codes. The problem is these algorithms produce many, many representatives for each equivalence class. If these algorithms were implemented straightforwardly, they would be impractical for $n > 28$.

To become practical several improvements were implemented. The extension vectors were reduced to those that actually gave the target code and many vectors that gave equivalent

codes were eliminated. As in Pless et al. [7], [8], [3] and [5], we found it beneficial to study the collection of weight four words in a self-dual code. We specialized our algorithms depending on which collections of weight four codewords were contained in the code. These changes greatly increased the efficiency of our programs.

Also, our algorithms counted the number of times a canonical form was produced so that the size of the automorphism group of the code could be calculated. This allowed us calculate the number of distinct codes and check it with Theorem 1.1.

To describe all these improvements to the basic algorithms would take up too many pages, however the reader can consult the thesis of Bilous [1] for the details. These details will also appear in a subsequent paper which enumerates the self-dual codes of length 34.

3 Conclusion

All our algorithms were written in C and run on a Sun ULTRASPARC 1/140. The first conclusion is that our algorithms are fast enough to compute all inequivalent $(2k, k)$ self-dual codes for $k \leq 16$. Secondly, we find that number of distinct $(2k, k)$ self-dual codes for $k = 2, 3, \dots, 16$ that our programs found equals the number in Theorem 1.1. This is excellent evidence our programs are correct. Thirdly, we have checked the literature, specifically, [7], [8], [3], and [5], and found that when we could compare results, the results in the literature agreed with our results except for one typographical error. In [5] in Table F, which lists the weight distributions for the $(2k, k, d \geq 6)$ self-dual codes for $2k=26, 28$ and 30 , the number of weight 14 words in the codes B_{28} and C_{28} should be 4860 not 4680.

We now give a summary of our results in Table 2 which contains the following information:

- $2k$: the length of the codes, $1 \leq k \leq 16$.
- Self-Dual Codes: the number of inequivalent $(2k, k, d)$ self-dual codes, for $d = 2, 4, 6, 8$. For $k \leq 16$, there are no $(2k, k, d \geq 10)$ self-dual codes.
- Indecomposable: the number of inequivalent indecomposable $(2k, k, d)$ self-dual codes, for $d = 4, 6, 8$. The only indecomposable self-dual code with distance 2 is the trivial $(2, 1, 2)$ self-dual code.
- Doubly-Even: the number of inequivalent doubly-even $(2k, k)$ self-dual codes, for $d = 4, 8$. Note that a $(2k, k)$ self-dual code C is doubly-even if and only if the weight of every codeword in C is divisible by 4.

- Total: the total number of inequivalent $(2k, k)$ self-dual codes.

The number of inequivalent decomposable $(2k, k, d)$ self-dual codes can be found by subtracting the number of inequivalent indecomposable $(2k, k, d)$ self-dual codes from the total number of inequivalent $(2k, k, d)$ self-dual codes. The newly discovered information in Table 2 (indicated by the boldface entries) is the number of inequivalent $(32, 16, d \geq 4)$ self-dual codes and the total number of inequivalent $(32, 16)$ self-dual codes.

$2k$	Self-Dual Codes				Indecomposable			Doubly-Even		Total
	$d = 2$	$d = 4$	$d = 6$	$d = 8$	$d = 4$	$d = 6$	$d = 8$	$d = 4$	$d = 8$	
2	1	0	0	0	0	0	0	0	0	1
4	1	0	0	0	0	0	0	0	0	1
6	1	0	0	0	0	0	0	0	0	1
8	1	1	0	0	1	0	0	1	0	2
10	2	0	0	0	0	0	0	0	0	2
12	2	1	0	0	1	0	0	0	0	3
14	3	1	0	0	1	0	0	0	0	4
16	4	3	0	0	2	0	0	2	0	7
18	7	2	0	0	2	0	0	0	0	9
20	9	7	0	0	6	0	0	0	0	16
22	16	8	1	0	7	1	0	0	0	25
24	25	28	1	1	24	1	1	8	1	55
26	55	47	1	0	44	1	0	0	0	103
28	103	155	3	0	145	3	0	0	0	261
30	261	457	13	0	444	13	0	0	0	731
32	731	2482	74	8	2441	74	8	80	5	3295

Table 2: The total number of inequivalent codes in various classes of $(2k, k)$ self-dual codes, for $2k \leq 32$.

Table 3 contains the weight distributions and sizes of automorphism group of the individual codes. The individual codes are not given in this paper because of their size. However, this information can be found at the following web site [2].

Finally, Table 3 shows that no $(2k, k)$ self-dual code for $k \leq 16$, has full automorphism group size of 1, proving Conjecture 1.1 as Conway and Sloane [4] had already found a rigid $(34,17)$ self-dual code.

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
0	0	364	2048	6720	14336	18598	0, 294912, 2064384
0	0	620	0	13888	0	36518	14880, 23040, 86016, 10321920, 319979520
0	8	348	2024	6784	14352	18502	384, 1536, 6144
0	12	340	2012	6816	14360	18454	60, 64, 144(2)
0	16	332	2000	6848	14368	18406	8, 16, 32(2), 48, 64, 128, 768, 1024(2), 6144
0	20	324	1988	6880	14376	18358	4, 6, 8, 12, 16(2), 48, 96
0	24	316	1976	6912	14384	18310	4(2), 8(4), 12, 24(2), 32(3), 96(2), 192, 384, 512, 1152, 6144, 18432
0	28	308	1964	6944	14392	18262	2, 4(2), 8, 12, 16(2), 48, 1344
0	32	300	1952	6976	14400	18214	4, 12(2), 16, 20, 24, 32(2), 64(2), 120, 192(3), 1440, 1536, 2048, 23040, 368640
1	0	630	0	13839	0	36594	5376
1	8	358	2024	6735	14352	18578	384
1	12	350	2012	6767	14360	18530	64, 192, 864, 1536
1	16	342	2000	6799	14368	18482	32, 48(3), 64(2), 144, 192, 256, 288, 576
1	20	334	1988	6831	14376	18434	8, 16(3), 32(2), 48(3), 64, 96, 128, 192(2), 512, 768
1	24	326	1976	6863	14384	18386	8(3), 16(5), 32(3), 48, 64(3), 96, 192
1	28	318	1964	6895	14392	18338	8(4), 16(5), 24, 32(5), 48, 64, 72, 96, 128, 144, 192(2), 384, 768
1	32	310	1952	6927	14400	18290	8(5), 16(4), 32, 48, 64, 96, 192
1	36	302	1940	6959	14408	18242	16(4), 32(3), 48, 64, 128(2), 192, 256, 384, 512
2	0	384	2048	6622	14336	18750	98304
2	0	640	0	13790	0	36670	9216, 18432, 294912
2	8	368	2024	6686	14352	18654	1024, 3072, 4096, 18432, 122880
2	12	360	2012	6718	14360	18606	192, 768
2	16	352	2000	6750	14368	18558	64, 128, 192, 256(4), 384, 512, 768, 1152, 2048(2), 3072(3), 8192, 9216, 18432, 24576, 73728
2	20	344	1988	6782	14376	18510	32(3), 64(4), 128, 192, 256, 576, 768
2	24	336	1976	6814	14384	18462	16, 32(3), 64(7), 128(4), 192, 256(7), 512(2), 768(2), 1024(2), 2048(2), 2304, 3072(2), 4096(2), 8192, 49152
2	28	328	1964	6846	14392	18414	16(2), 32(6), 64(6), 96(3), 128, 192(3), 256, 384
2	32	320	1952	6878	14400	18366	16(2), 32(5), 64(7), 96, 128(9), 256(8), 384, 512(2), 1024(2), 2048(2), 4096
2	36	312	1940	6910	14408	18318	16, 32(7), 64(5), 128, 192

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
2	40	304	1928	6942	14416	18270	32, 64(3), 128(2), 192(2), 256(7), 384, 512(3), 1024(2), 1536, 4608, 6144, 8192, 16384, 49152
3	0	650	0	13741	0	36746	9216, 269568
3	8	378	2024	6637	14352	18730	3072(2)
3	12	370	2012	6669	14360	18682	384, 10368, 138240
3	16	362	2000	6701	14368	18634	256(2), 512, 768(2), 1024, 1536, 2304(2)
3	20	354	1988	6733	14376	18586	128(4), 256(4), 768, 1024, 1728, 13824
3	24	346	1976	6765	14384	18538	64, 128(7), 256(6), 288, 384(3), 512(3), 768, 1152, 1728, 5184, 10368
3	28	338	1964	6797	14392	18490	64(3), 128(8), 192, 256(7), 384(2), 512, 768(2), 1024(3), 4608
3	32	330	1952	6829	14400	18442	64(4), 128(10), 192, 256(4), 288(2), 384, 512(2), 576, 768, 5184
3	36	322	1940	6861	14408	18394	64(2), 128(10), 256(10), 288(2), 384(4), 512(3), 1536, 3072
3	40	314	1928	6893	14416	18346	64(4), 128(5), 256(2), 288, 384, 512, 576
3	44	306	1916	6925	14424	18298	128, 256(6), 768, 1024(3), 1152(2), 1536, 2304(2), 6144
4	0	404	2048	6524	14336	18902	262144
4	0	660	0	13692	0	36822	16384, 110592, 786432
4	8	388	2024	6588	14352	18806	4096, 18432, 55296, 98304, 3870720
4	12	380	2012	6620	14360	18758	2048, 12288
4	16	372	2000	6652	14368	18710	768, 1024(2), 2048(2), 2304, 8192(2), 10368, 12288(3), 32768, 55296, 98304, 368640, 589824
4	20	364	1988	6684	14376	18662	256, 512(3), 1024(3), 1152, 2048, 3456
4	24	356	1976	6716	14384	18614	256, 512(5), 576, 768(3), 1024(6), 1152, 1536(2), 2048(5), 2304, 3072, 4096(4), 6144, 8192, 16384, 18432, 110592, 184320
4	28	348	1964	6748	14392	18566	192, 256(4), 384, 512(7), 576(2), 1024(3), 1152, 3072, 9216, 10368, 36864
4	32	340	1952	6780	14400	18518	192, 256(4), 384(3), 512(7), 768(2), 1024(6), 1152, 1536(3), 2048(7), 2304, 3072(2), 4096(7), 8192, 16384(2), 18432(2), 24576, 32768, 196608(2)
4	36	332	1940	6812	14408	18470	192(2), 256(7), 384(2), 512(6), 1024(2), 1152, 1536
4	40	324	1928	6844	14416	18422	192, 256(3), 384, 512(5), 768(5), 1024(9), 1152, 1536(3), 2048(4), 2304(2), 3072, 4096(2), 6144(2), 6912, 9216, 12288(2), 16384(2)

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
4	44	316	1916	6876	14424	18374	256(4), 384(2), 512(3), 576, 1024(2), 2048, 3456
4	48	308	1904	6908	14432	18326	512(2), 1024(3), 1536, 2048(3), 2304, 3072, 3456, 4096(5), 8192, 12288, 18432, 24576, 49152, 65536
5	0	670	0	13643	0	36898	61440, 82944, 147456
5	8	398	2024	6539	14352	18882	8192
5	12	390	2012	6571	14360	18834	10240
5	16	382	2000	6603	14368	18786	2048, 3072, 4096, 4608, 8192, 12288, 13824, 27648, 49152
5	20	374	1988	6635	14376	18738	1536, 2048(3), 4096, 8192, 12288
5	24	366	1976	6667	14384	18690	768(2), 1024, 1536(3), 2048(5), 3072(2), 4096(3), 9216
5	28	358	1964	6699	14392	18642	384, 768(3), 1024, 1536(3), 2048(8), 3072, 4096, 4608(2), 6144
5	32	350	1952	6731	14400	18594	384, 768(5), 1024(3), 1536(3), 2048(6), 3072, 4096(2)
5	36	342	1940	6763	14408	18546	384, 768(6), 1024(2), 1536(4), 2048(6), 3072(2), 4096(5), 6144, 32768
5	40	334	1928	6795	14416	18498	384(2), 768(5), 1024(5), 2048(3), 2304, 3072, 4096, 4608(2), 6144
5	44	326	1916	6827	14424	18450	768(4), 1024, 1536(6), 2048(7), 3072, 4096(3)
5	48	318	1904	6859	14432	18402	768(3), 1024(3), 1536, 2048, 4096, 8192
5	52	310	1892	6891	14440	18354	2048, 3072, 4096(3), 4608, 6144, 8192, 9216, 12288(3), 18432, 20480, 32768
6	0	424	2048	6426	14336	19054	786432, 4423680, 26542080
6	0	680	0	13594	0	36974	73728, 196608, 786432, 4423680, 26542080
6	8	408	2024	6490	14352	18958	24576, 32768, 131072, 170311680
6	12	400	2012	6522	14360	18910	9216
6	16	392	2000	6554	14368	18862	6144, 8192, 16384, 24576, 36864, 49152, 65536, 131072(2), 147456, 393216
6	20	384	1988	6586	14376	18814	3072, 6144, 18432
6	24	376	1976	6618	14384	18766	1536, 3072(2), 6144(8), 8192(2), 12288, 13824, 16384(5), 18432(2), 24576, 32768, 49152, 55296, 65536, 73728, 110592, 131072(2), 147456, 26542080
6	28	368	1964	6650	14392	18718	1536(5), 3072(3), 6144, 18432
6	32	360	1952	6682	14400	18670	1536(4), 3072(3), 4096, 6144(11), 6912, 8192(3), 9216(2), 12288, 13824, 16384(5), 18432(3), 24576, 32768, 65536, 131072(3), 221184, 294912

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
6	36	352	1940	6714	14408	18622	1536(6), 3072(5), 6144, 6912, 9216
6	40	344	1928	6746	14416	18574	1536(4), 3072(4), 4096, 4608, 6144(6), 8192(4), 9216, 12288(5), 16384(3), 18432, 24576, 32768(4), 49152, 65536(2), 73728, 737280
6	44	336	1916	6778	14424	18526	1536(7), 3072(3), 6144, 6912
6	48	328	1904	6810	14432	18478	1536, 3072(4), 4096, 6144(12), 8192(4), 9216, 12288, 16384(2), 18432(2), 27648, 49152(2), 110592, 131072, 196608
6	52	320	1892	6842	14440	18430	1536(2), 3072(3)
6	56	312	1880	6874	14448	18382	6144, 12288(2), 16384(2), 18432, 24576(2), 32768(4), 65536(2), 110592, 147456, 221184, 589824, 786432, 2211840
7	0	690	0	13545	0	37050	98304
7	8	418	2024	6441	14352	19034	49152
7	16	402	2000	6505	14368	18938	12288(2), 36864, 98304, 221184
7	20	394	1988	6537	14376	18890	12288(2), 36864
7	24	386	1976	6569	14384	18842	6144, 12288(7), 24576, 36864(2), 73728
7	28	378	1964	6601	14392	18794	4608, 6144(3), 9216, 12288(4), 13824, 24576(2), 27648, 36864, 20321280
7	32	370	1952	6633	14400	18746	4608, 6144(6), 9216, 12288(6), 24576
7	36	362	1940	6665	14408	18698	4608(2), 6144(4), 9216(3), 12288(6), 24576(3), 36864
7	40	354	1928	6697	14416	18650	2304, 6144(6), 9216, 12288(6), 18432, 24576, 36864, 72576
7	44	346	1916	6729	14424	18602	4608(2), 6144(5), 9216(2), 12288(7), 18432, 24576, 49152
7	48	338	1904	6761	14432	18554	2304, 6144(6), 12288(5)
7	52	330	1892	6793	14440	18506	6144(2), 9216(2), 12288(5), 18432, 24576, 27648(2), 73728, 193536
7	56	322	1880	6825	14448	18458	6144, 12288(5)
7	60	314	1868	6857	14456	18410	12288, 24576(3), 49152
8	0	444	2048	6328	14336	19206	8388608, 25165824
8	0	700	0	13496	0	37126	294912, 442368, 3538944, 22020096, 75497472, 81285120, 528482304
8	8	428	2024	6392	14352	19110	98304
8	16	412	2000	6456	14368	19014	36864, 49152, 98304(2), 147456, 442368, 589824(2), 786432, 1048576, 1769472, 3870720
8	20	404	1988	6488	14376	18966	36864
8	24	396	1976	6520	14384	18918	18432, 24576, 36864(4), 49152(7), 73728, 98304(2), 147456, 196608, 294912

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
8	28	388	1964	6552	14392	18870	9216(2), 18432, 36864(2)
8	32	380	1952	6584	14400	18822	9216(2), 24576(5), 36864(3), 49152(5), 73728(2), 98304(2), 147456(2), 196608(2), 393216(3), 524288(2), 1048576
8	36	372	1940	6616	14408	18774	9216(4), 18432(2), 36864
8	40	364	1928	6648	14416	18726	6144, 9216, 18432(4), 24576(5), 36864(3), 48384, 49152(7), 73728(4), 98304(3), 129024, 294912
8	44	356	1916	6680	14424	18678	9216(5), 18432, 36864
8	48	348	1904	6712	14432	18630	9216(3), 12288(2), 18432, 24576(2), 36864(4), 49152(9), 98304, 196608(2), 262144, 294912, 393216(2), 1048576, 3145728
8	52	340	1892	6744	14440	18582	9216(2), 18432, 36864, 72576
8	56	332	1880	6776	14448	18534	18432(2), 24576(5), 36864(3), 49152(3), 73728, 98304
8	60	324	1868	6808	14456	18486	18432(2)
8	64	316	1856	6840	14464	18438	49152(2), 98304, 147456, 196608(2), 221184, 589824(2), 786432(2), 1048576, 2580480, 12582912
9	0	710	0	13447	0	37202	442368
9	8	438	2024	6343	14352	19186	442368
9	12	430	2012	6375	14360	19138	221184
9	16	422	2000	6407	14368	19090	73728
9	20	414	1988	6439	14376	19042	73728
9	24	406	1976	6471	14384	18994	36864(2), 73728(3), 147456
9	28	398	1964	6503	14392	18946	24576, 36864(2), 73728(3)
9	32	390	1952	6535	14400	18898	36864(8), 73728(2), 147456
9	36	382	1940	6567	14408	18850	12288, 24576, 36864(3), 49152, 73728(5), 147456, 221184, 294912
9	40	374	1928	6599	14416	18802	27648, 32256, 36864(7), 73728(2), 147456
9	44	366	1916	6631	14424	18754	12288, 36864(3), 49152(2), 55296, 73728(7)
9	48	358	1904	6663	14432	18706	36864(6), 73728, 82944, 110592, 147456
9	52	350	1892	6695	14440	18658	12288, 24576, 43008, 55296, 73728(11), 147456
9	56	342	1880	6727	14448	18610	36864(5), 73728(2), 221184
9	60	334	1868	6759	14456	18562	36864(2), 49152(2), 73728(3), 147456
9	64	326	1856	6791	14464	18514	36864, 73728
9	68	318	1844	6823	14472	18466	147456, 442368, 884736
10	0	464	2048	6230	14336	19358	4718592

Weight Distributions							Automorphism
4	6	8	10	12	14	16	Group Sizes
10	0	720	0	13398	0	37278	1179648, 2359296, 4718592, 1703116800
10	8	448	2024	6294	14352	19262	294912, 1179648(2), 2359296
10	16	432	2000	6358	14368	19166	294912, 1179648, 2359296(2), 3538944, 7077888
10	24	416	1976	6422	14384	19070	147456(2), 196608, 294912(4), 589824(2), 1179648
10	28	408	1964	6454	14392	19022	55296, 110592, 165888, 1161216
10	32	400	1952	6486	14400	18974	73728, 98304(3), 110592(2), 147456(2), 196608(2), 221184, 294912(3), 589824, 786432(2), 1179648(3), 2359296, 7372800
10	36	392	1940	6518	14408	18926	55296(2), 110592
10	40	384	1928	6550	14416	18878	55296, 64512, 73728(2), 86016, 98304(3), 110592(3), 147456(3), 196608(4), 294912(3), 393216, 589824(2), 774144, 786432, 1179648, 2211840, 3538944
10	44	376	1916	6582	14424	18830	55296, 110592
10	48	368	1904	6614	14432	18782	36864, 98304(2), 110592, 147456(3), 196608(3), 221184, 294912(3), 663552, 786432, 1179648, 2359296
10	52	360	1892	6646	14440	18734	43008, 55296, 110592
10	56	352	1880	6678	14448	18686	55296, 73728, 98304(3), 110592, 147456, 196608(2), 294912(6), 393216, 442368, 589824(5), 1105920, 1179648
10	60	344	1868	6710	14456	18638	55296
10	64	336	1856	6742	14464	18590	98304, 110592, 147456(3), 196608, 258048, 294912(2), 331776, 786432
10	72	320	1832	6806	14480	18494	294912, 589824(3), 1572864, 2359296, 77414400
11	0	730	0	13349	0	37354	1327104, 18579456
11	16	442	2000	6309	14368	19242	221184, 442368, 2064384
11	24	426	1976	6373	14384	19146	221184, 442368(3)
11	28	418	1964	6405	14392	19098	147456, 221184, 442368
11	32	410	1952	6437	14400	19050	221184(3), 442368(4)
11	36	402	1940	6469	14408	19002	73728(2), 147456(2), 221184, 442368(2)
11	40	394	1928	6501	14416	18954	86016, 221184(4), 344064, 442368(3)
11	44	386	1916	6533	14424	18906	73728(3), 221184(2), 442368(2), 884736
11	48	378	1904	6565	14432	18858	221184(4), 442368(3)
11	52	370	1892	6597	14440	18810	73728, 147456(2), 172032, 193536, 221184(4), 258048, 276480
11	56	362	1880	6629	14448	18762	221184(3), 442368(2)
11	60	354	1868	6661	14456	18714	73728(2), 221184(2), 442368(2)
11	64	346	1856	6693	14464	18666	221184(2), 258048

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
11	68	338	1844	6725	14472	18618	221184(2), 294912
11	72	330	1832	6757	14480	18570	442368(2)
11	76	322	1820	6789	14488	18522	884736, 2654208
12	0	484	2048	6132	14336	19510	37748736
12	0	740	0	13300	0	37430	3538944, 5308416, 15925248, 37748736
12	8	468	2024	6196	14352	19414	3538944, 5308416
12	12	460	2012	6228	14360	19366	7962624
12	16	452	2000	6260	14368	19318	1179648, 1769472, 2654208, 3145728, 94371840
12	20	444	1988	6292	14376	19270	1327104
12	24	436	1976	6324	14384	19222	589824(2), 884736, 1179648, 1327104, 1769472(4), 15925248
12	28	428	1964	6356	14392	19174	2654208
12	32	420	1952	6388	14400	19126	294912, 589824(5), 663552, 1572864, 3538944, 6291456(2), 15925248, 18874368
12	36	412	1940	6420	14408	19078	663552
12	40	404	1928	6452	14416	19030	258048(2), 294912(4), 344064, 442368, 589824(4), 663552, 737280, 884736, 1769472(3), 4128768
12	48	388	1904	6516	14432	18934	245760, 294912(3), 442368, 589824(5), 663552, 884736, 1179648, 1572864, 3145728, 3538944(2), 4718592, 6291456, 37748736
12	52	380	1892	6548	14440	18886	129024, 663552
12	56	372	1880	6580	14448	18838	294912(3), 589824(2), 663552, 884736, 1327104, 1769472(2)
12	60	364	1868	6612	14456	18790	1990656
12	64	356	1856	6644	14464	18742	294912, 491520, 589824(6), 663552, 688128, 884736(2), 1179648, 1572864, 2752512, 3145728
12	72	340	1832	6708	14480	18646	589824(2), 1769472
12	76	332	1820	6740	14488	18598	2654208
12	80	324	1808	6772	14496	18550	3538944(3), 6291456, 10616832, 12582912, 37748736
13	0	750	0	13251	0	37506	10616832
13	8	478	2024	6147	14352	19490	5308416
13	16	462	2000	6211	14368	19394	31850496
13	20	454	1988	6243	14376	19346	10616832
13	24	446	1976	6275	14384	19298	1327104, 2654208
13	28	438	1964	6307	14392	19250	442368, 1548288
13	32	430	1952	6339	14400	19202	1327104(2), 2654208
13	36	422	1940	6371	14408	19154	442368(2), 737280, 2654208(2)

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
13	40	414	1928	6403	14416	19106	516096(2), 774144, 1327104, 2654208(2)
13	44	406	1916	6435	14424	19058	442368(2), 491520, 884736, 1327104, 2654208
13	48	398	1904	6467	14432	19010	1327104, 2654208
13	52	390	1892	6499	14440	18962	442368(3), 516096(2), 884736, 1032192, 1327104, 5308416
13	56	382	1880	6531	14448	18914	1327104, 2654208
13	60	374	1868	6563	14456	18866	245760, 442368(2), 1327104, 2654208
13	64	366	1856	6595	14464	18818	258048, 1327104, 7962624
13	68	358	1844	6627	14472	18770	442368, 2654208
13	72	350	1832	6659	14480	18722	1327104
13	76	342	1820	6691	14488	18674	2654208(2), 3096576, 4423680
13	80	334	1808	6723	14496	18626	10616832
13	84	326	1796	6755	14504	18578	10616832
14	0	504	2048	6034	14336	19662	84934656
14	0	760	0	13202	0	37582	7077888, 24772608, 70778880, 254803968, 329042165760
14	16	472	2000	6162	14368	19470	3538944, 7077888, 8257536
14	24	456	1976	6226	14384	19374	3538944(3), 5898240, 7077888, 21233664
14	32	440	1952	6290	14400	19278	1769472(4), 3538944(3), 4718592, 7077888(2), 7864320
14	40	424	1928	6354	14416	19182	1179648, 1769472(5), 1966080, 2064384(2), 3538944(3), 4128768, 7077888, 21233664
14	48	408	1904	6418	14432	19086	1179648, 1769472(2), 1966080, 2359296, 3538944(3), 7077888
14	52	400	1892	6450	14440	19038	387072
14	56	392	1880	6482	14448	18990	737280, 983040, 1769472(5), 1966080, 2359296, 3538944, 7077888
14	64	376	1856	6546	14464	18894	1032192, 1548288, 1769472(3), 2359296(2), 3538944(2), 11796480, 185794560
14	72	360	1832	6610	14480	18798	1769472, 1966080, 3538944(4), 7077888(2), 42467328
14	80	344	1808	6674	14496	18702	1769472, 3538944(2)
14	88	328	1784	6738	14512	18606	14155776, 24772608
15	0	770	0	13153	0	37658	79626240
15	24	466	1976	6177	14384	19450	15925248, 47775744
15	36	442	1940	6273	14408	19306	2654208(2)
15	40	434	1928	6305	14416	19258	1548288(3), 3096576
15	44	426	1916	6337	14424	19210	737280, 2654208(2), 5308416
15	48	418	1904	6369	14432	19162	15925248

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
15	52	410	1892	6401	14440	19114	737280, 1548288, 2064384, 2654208, 3096576
15	56	402	1880	6433	14448	19066	15925248
15	60	394	1868	6465	14456	19018	2654208, 15925248
15	64	386	1856	6497	14464	18970	1548288, 3096576
15	68	378	1844	6529	14472	18922	1474560, 5308416
15	76	362	1820	6593	14488	18826	2654208, 3096576
15	80	354	1808	6625	14496	18778	15925248
15	92	330	1772	6721	14520	18634	31850496
16	0	524	2048	5936	14336	19814	150994944
16	0	780	0	13104	0	37734	21233664, 150994944
16	8	508	2024	6000	14352	19718	10616832, 21233664
16	16	492	2000	6064	14368	19622	21233664, 37748736
16	24	476	1976	6128	14384	19526	21233664(2), 63700992
16	28	468	1964	6160	14392	19478	13934592
16	32	460	1952	6192	14400	19430	5898240, 7077888, 9437184, 10616832(2), 21233664, 37748736, 75497472
16	40	444	1928	6256	14416	19334	2949120, 3538944(2), 4128768, 4423680, 4644864, 6193152, 10616832, 13934592, 21233664(3)
16	48	428	1904	6320	14432	19238	2949120, 3538944, 5898240(2), 7077888(2), 9437184, 10616832(2), 18874368
16	52	420	1892	6352	14440	19190	4644864
16	56	412	1880	6384	14448	19142	3538944, 10616832, 21233664(2)
16	64	396	1856	6448	14464	19046	2949120, 3538944, 4128768, 17694720, 18874368, 21233664(3), 24772608(2), 75497472(2)
16	72	380	1832	6512	14480	18950	3538944, 10616832(2), 21233664
16	80	364	1808	6576	14496	18854	5898240(2), 10616832(2), 11796480, 14155776, 18874368(2)
16	88	348	1784	6640	14512	18758	21233664
16	96	332	1760	6704	14528	18662	21233664, 75497472
17	0	790	0	13055	0	37810	55738368
17	16	502	2000	6015	14368	19698	18579456
17	36	462	1940	6175	14408	19458	8847360
17	40	454	1928	6207	14416	19410	9289728, 18579456(2)
17	44	446	1916	6239	14424	19362	4423680
17	52	430	1892	6303	14440	19266	3096576, 4423680, 18579456, 21676032, 55738368
17	60	414	1868	6367	14456	19170	4423680
17	64	406	1856	6399	14464	19122	9289728(2)

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
17	68	398	1844	6431	14472	19074	8847360
17	76	382	1820	6495	14488	18978	4423680, 9289728, 18579456
17	88	358	1784	6591	14512	18834	18579456
18	0	544	2048	5838	14336	19966	509607936
18	0	800	0	13006	0	37886	70778880, 84934656, 509607936
18	16	512	2000	5966	14368	19774	35389440, 84934656
18	24	496	1976	6030	14384	19678	17694720, 21233664, 42467328, 382205952
18	32	480	1952	6094	14400	19582	42467328, 70778880, 84934656, 254803968
18	40	464	1928	6158	14416	19486	12386304(3), 17694720, 35389440(2), 115605504
18	48	448	1904	6222	14432	19390	11796480, 17694720, 21233664, 42467328(2), 84934656(3)
18	56	432	1880	6286	14448	19294	11796480, 17694720, 21233664, 35389440(2), 42467328, 127401984
18	64	416	1856	6350	14464	19198	12386304(3), 16515072, 42467328, 84934656
18	72	400	1832	6414	14480	19102	8847360, 17694720(2), 21233664, 23592960, 42467328, 509607936
18	80	384	1808	6478	14496	19006	42467328, 84934656
18	88	368	1784	6542	14512	18910	24772608, 35389440, 42467328
18	104	336	1736	6670	14544	18718	509607936
19	28	498	1964	6013	14392	19706	37158912
19	40	474	1928	6109	14416	19562	55738368
19	44	466	1916	6141	14424	19514	26542080
19	52	450	1892	6205	14440	19418	18579456, 37158912, 53084160
19	60	434	1868	6269	14456	19322	26542080
19	64	426	1856	6301	14464	19274	21676032, 167215104
19	68	418	1844	6333	14472	19226	26542080
19	76	402	1820	6397	14488	19130	18579456, 111476736
19	84	386	1796	6461	14504	19034	53084160
20	0	820	0	12908	0	38038	148635648, 679477248, 2831155200, 11890851840
20	16	532	2000	5868	14368	19926	148635648, 226492416
20	32	500	1952	5996	14400	19734	35389440, 188743680, 226492416(3)
20	40	484	1928	6060	14416	19638	35389440, 74317824(3)
20	48	468	1904	6124	14432	19542	35389440, 188743680, 212336640, 226492416(2)
20	52	460	1892	6156	14440	19494	65028096
20	56	452	1880	6188	14448	19446	17694720, 35389440(2)
20	64	436	1856	6252	14464	19350	17694720, 24772608, 35389440, 41287680, 49545216, 74317824, 148635648, 212336640, 226492416(3), 264241152

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
20	72	420	1832	6316	14480	19254	35389440
20	80	404	1808	6380	14496	19158	35389440(2), 94371840, 113246208
20	88	388	1784	6444	14512	19062	74317824
20	96	372	1760	6508	14528	18966	226492416
20	112	340	1712	6636	14560	18774	1358954496, 2831155200
21	40	494	1928	6011	14416	19714	65028096, 260112384
21	52	470	1892	6107	14440	19570	30965760
21	76	422	1820	6299	14488	19282	130056192
22	0	840	0	12810	0	38190	424673280
22	8	568	2024	5706	14352	20174	424673280
22	32	520	1952	5898	14400	19886	212336640, 424673280
22	40	504	1928	5962	14416	19790	106168320, 123863040, 148635648(2), 212336640, 424673280
22	48	488	1904	6026	14432	19694	53084160, 212336640(2), 235929600
22	56	472	1880	6090	14448	19598	106168320, 212336640, 424673280
22	64	456	1856	6154	14464	19502	49545216, 106168320, 141557760, 148635648, 173408256, 297271296
22	72	440	1832	6218	14480	19406	106168320
22	88	408	1784	6346	14512	19214	106168320, 148635648, 212336640, 424673280
22	104	376	1736	6474	14544	19022	212336640, 424673280
23	0	850	0	12761	0	38266	2341011456
23	52	490	1892	6009	14440	19722	130056192, 185794560
23	76	442	1820	6201	14488	19434	185794560
23	88	418	1784	6297	14512	19290	780337152
23	100	394	1748	6393	14536	19146	371589120
23	124	346	1676	6585	14584	18858	4682022912
24	0	604	2048	5544	14336	20422	5435817984, 10871635968, 32614907904
24	0	860	0	12712	0	38342	1911029760, 10871635968, 32614907904
24	24	556	1976	5736	14384	20134	637009920
24	32	540	1952	5800	14400	20038	2717908992
24	40	524	1928	5864	14416	19942	247726080, 1040449536
24	48	508	1904	5928	14432	19846	283115520, 353894400, 637009920
24	56	492	1880	5992	14448	19750	106168320
24	64	476	1856	6056	14464	19654	148635648, 247726080, 283115520, 353894400, 528482304, 2717908992
24	72	460	1832	6120	14480	19558	637009920
24	80	444	1808	6184	14496	19462	247726080, 637009920
24	96	412	1760	6312	14528	19270	566231040, 637009920, 707788800, 2717908992, 8153726976
24	104	396	1736	6376	14544	19174	1911029760
24	128	348	1664	6568	14592	18886	10871635968

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
25	64	486	1856	6007	14464	19730	910393344
26	0	624	2048	5446	14336	20574	8493465600
26	0	880	0	12614	0	38494	1486356480, 4161798144, 8493465600, 10701766656
26	16	592	2000	5574	14368	20382	1486356480, 4161798144(2), 4246732800
26	40	544	1928	5766	14416	20094	1486356480(2)
26	48	528	1904	5830	14432	19998	1415577600
26	64	496	1856	5958	14464	19806	247726080, 297271296, 371589120, 3567255552
26	80	464	1808	6086	14496	19614	1415577600
26	88	448	1784	6150	14512	19518	1486356480(2), 2080899072
27	76	482	1820	6005	14488	19738	1300561920
28	0	900	0	12516	0	38646	6794772480
28	16	612	2000	5476	14368	20534	3397386240
28	28	588	1964	5572	14392	20390	19118260224
28	32	580	1952	5604	14400	20342	6794772480(2)
28	40	564	1928	5668	14416	20246	2229534720
28	48	548	1904	5732	14432	20150	1486356480, 3397386240
28	64	516	1856	5860	14464	19958	1040449536, 1486356480, 1585446912, 2229534720, 3397386240, 4954521600
28	72	500	1832	5924	14480	19862	1061683200
28	80	484	1808	5988	14496	19766	3397386240
28	96	452	1760	6116	14528	19574	743178240, 6794772480
28	112	420	1712	6244	14560	19382	3397386240, 4459069440
29	0	910	0	12467	0	38722	76473040896
30	0	920	0	12418	0	38798	26754416640, 42467328000
30	32	600	1952	5506	14400	20494	8918138880, 14155776000
30	40	584	1928	5570	14416	20398	5202247680, 20808990720
30	64	536	1856	5762	14464	20110	2972712960
30	80	504	1808	5890	14496	19918	1486356480
31	100	474	1748	6001	14536	19754	18207866880
32	0	940	0	12320	0	38950	31213486080, 57076088832
32	48	588	1904	5536	14432	20454	16986931200
32	64	556	1856	5664	14464	20262	5202247680, 19025362944, 57076088832
32	88	508	1784	5856	14512	19974	7431782400, 31213486080
32	96	492	1760	5920	14528	19878	10569646080
34	48	608	1904	5438	14432	20606	14863564800
34	64	576	1856	5566	14464	20414	10404495360(2), 14566293504, 14863564800
34	80	544	1808	5694	14496	20222	5945425920
36	0	724	2048	4956	14336	21334	203843174400
36	0	980	0	12124	0	39254	203843174400

Weight Distributions							Automorphism Group Sizes
4	6	8	10	12	14	16	
36	48	628	1904	5340	14432	20758	101921587200
36	64	596	1856	5468	14464	20566	15854469120, 23781703680
36	80	564	1808	5596	14496	20374	101921587200
36	144	436	1616	6108	14624	19606	203843174400
38	0	1000	0	12026	0	39406	104044953600, 145662935040
38	16	712	2000	4986	14368	21294	104044953600
40	0	1020	0	11928	0	39558	380507258880
40	32	700	1952	5016	14400	21254	190253629440
40	64	636	1856	5272	14464	20870	266355081216, 380507258880
40	128	508	1664	5784	14592	20102	380507258880(2)
42	96	592	1760	5430	14528	20638	107017666560
42	112	560	1712	5558	14560	20446	291325870080
44	0	1060	0	11732	0	39862	1426902220800
44	64	676	1856	5076	14464	21174	1426902220800
44	96	612	1760	5332	14528	20790	475634073600
46	64	696	1856	4978	14464	21326	374561832960
48	64	716	1856	4880	14464	21478	1331775406080
50	0	1120	0	11438	0	40318	5243865661440
52	96	692	1760	4940	14528	21398	1426902220800
56	0	924	2048	3976	14336	22854	53271016243200
56	0	1180	0	11144	0	40774	18644855685120, 53271016243200, 78308393877504
60	0	1220	0	10948	0	41078	42807066624000
60	32	900	1952	4036	14400	22774	42807066624000
72	96	892	1760	3960	14528	22918	188351093145600
80	0	1420	0	9968	0	42598	1318457652019200
120	0	1820	0	8008	0	45638	685597979049984000

References

- [1] R. T. Bilous, A Recursive Enumeration of the Inequivalent Binary $(2k, k)$ Self-Dual Codes, for $2k \leq 32$, Dept. of Computer Science, University of Manitoba Master's Thesis 1998
- [2] R. T. Bilous, <http://www.cs.umanitoba.ca/~umbilou1/SelfDualCodes/toc.html> (1998)
- [3] J. H. Conway and V. Pless, On the enumeration of self-dual codes, *J. Combin Theory Ser. A* **28** (1980), 26-53.
- [4] J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (Nov 1990), 1319-1333.
- [5] J. H. Conway, V. Pless and N. J. A. Sloane, The binary self-dual codes of length up to 32: a revised enumeration, *IEEE Trans. Inform. Theory* **36** (NOV 1990), 183-195.
- [6] F. J. MacWilliams and N. J. A. Sloane, "The theory of error correcting codes", North-Holland, Amsterdam (1977)
- [7] V. Pless, A classification of self-orthogonal codes over $GF(2)$, *Discrete Math.* **3** (1972), 209-246.
- [8] V. Pless and N. J. A. Sloane, On the classification and enumeration of self-dual codes, *J. Combin. Theory Ser. A* **18** (1975), 313-335.