Optimal Subcodes and Optimum Distance Profiles of Self-Dual Codes

Finley Freibert
Department of Mathematics
Ohio Dominican University
Columbus, OH 43219, USA
Email: ffreibert@yahoo.com

Jon-Lark Kim*
Department of Mathematics
Sogang University
Seoul 121-742, South Korea
Email: jlkim@sogang.ac.kr

Abstract

Binary optimal codes often contain optimal or near-optimal subcodes. In this paper we show that this is true for the family of self-dual codes. One approach is to compute the optimum distance profiles (ODPs) of linear codes, which was introduced by Luo, et. al. (2010). One of our main results is the development of general algorithms, called the Chain Algorithms, for finding ODPs of linear codes. Then we determine the ODPs for the Type II codes of lengths up to 24 and the extremal Type II codes of length 32, give a partial result of the ODP of the extended quadratic residue code q_{48} of length 48. We also show that there does not exist a $[48, k, 16]$ subcode of q_{48} for $k \geq 17$, and we find a first example of a *doubly-even* self-complementary $[48, 16, 16]$ code.

Key Words: algorithm, self-dual codes, subcodes, optimum distance profiles, optimal codes

AMS subject classification: 94B05, 11T71

*corresponding author

1 Introduction

One of the main problems that has arisen in Coding Theory is the search for optimal codes with the largest size given a minimum distance or optimal codes with the largest minimum distance given a size [12, 22, 18]. There has been extensive work in this direction [8]. Some well-known families of codes, such as the Reed-Muller codes or the cyclic codes, contain notable subcodes. However, comparatively little attention has been paid to the subcodes of an optimal linear code in general. It is a natural concern to determine which linear codes contain optimal (or near-optimal) subcodes. Among linear codes, we suggest self-dual or self-orthogonal codes since their possible non-zero weights jump by 2 or 4. Thus there is a possibility to get subcodes with a large minimum distance.

In fact, self-dual codes have been one of the most active topics in algebraic coding theory since V. Pless [21] started to classify binary self-dual codes in 1972. These codes have interesting connections to groups, t-designs, lattices, and theta series [12, 18, 25]. Furthermore, many extremal self-dual codes often turn out to be the best among the linear codes with the same parameters. Nevertheless, little attention has been paid to the subcodes of self-dual codes.

We plan to construct optimal (self-orthogonal) subcodes of a given linear (self-dual) code. In order to construct finite-state codes, Pollara, Cheung and McEliece [24] constructed the first $[24, 5, 12]$ subcode of the binary Golay $[24, 12, 8]$ code, improving a previously known $[24, 5, 8]$ subcode. Maks and Simonis [19] have shown that there are exactly two inequivalent $[32, 11, 12]$ codes in the binary Reed-Muller code $R(2, 5)$ which contain $R(1, 5)$ and have the weight set $\{0, 12, 16, 20, 32\}$.

We show that in the class of self-dual codes, in many cases, optimal subcodes can be obtained by computing optimum distance profiles (ODPs), a concept introduced by Luo, Han Vinck, and Chen [17]. The authors [17] considered how to construct and then exclude (or include, respectively) the basis codewords one by one while keeping a distance profile as large as possible in a dictionary order (or in an inverse dictionary order, respectively). Thus fault-tolerant capability is improved by selecting subcodes in communications and storage systems. The practical applications are found in WCDMA [10], [27] and address retrieval on optical media [28].

In [4] and [17], the authors give results on the ODPs of the binary Hamming $[7, 4, 3]$ code, the binary and ternary Golay codes, Reed-Solomon codes, the first-order and second order Reed-Muller codes. Recently, Yan, et. al. [30] considered the optimum distance profiles of some quasi-cyclic codes and proposed two algorithms, called the "subcodes traversing algorithm" and "supercodes traversing algorithm". These algorithms enumerate all subcodes of a given code. Hence they are rather inefficient in finding ODPs of linear codes with a relatively large dimension. Their examples have dimension 10 only. Hence we ask the following two questions.

(i) Is there an interesting class of linear codes whose ODPs are not known yet?
(ii) Is there an efficient algorithm to compute ODPs of linear codes?

For question (i), we choose a class of self-dual codes since the structure of these subcodes is surprisingly less known. For question (ii), we propose two full algorithms based on cosets, called the Chain Algorithms and two random algorithms to find ODPs of the codes. These

algorithms look at a chain of subcodes of a given code and consider the equivalence of the codes with the same dimension. Hence they are more efficient than the subcodes and supercodes traversing algorithm [30].

From a theoretical point of view, we give the ODPs of Type II self-dual codes of lengths up to 24 and the five extremal Type II codes of length 32, give a partial result of the ODP of the extended quadratic residue code q_{48} of length 48. Moreover, we show that each of the five Type II $[32, 16, 8]$ codes contains the two optimal $[32, 11, 12]$ codes, which was previously known only for the Reed-Muller code $R(2, 5)$. We also construct a $[48, 14, 16]$ code and an optimal $[48, 9, 20]$ code from the extended quadratic residue code q_{48} of length 48. Both codes are not equivalent to the best known codes of the same parameters in the Magma database [3]. We also show that there does not exist a $[48, k, 16]$ subcode C of q_{48} for $k \geq 17$. We find a first example of a **doubly-even** self-complementary $[48, 16, 16]$ code. Such a code was previously not known to exist. Only one singly-even self-complementary $[48, 16, 16]$ code was found by A. Kohnert [16]. Similarly we construct $[72, 29, 16]$, $[72, 23, 20]$ codes which are not equivalent to the best known codes. Further we construct a new self-orthogonal $[72, 35, 16]$ code with $A_{16} = 129972$. All our computations were done using Magma [3].

2 Preliminaries

We refer to [12] for basic definitions and results related to self-dual codes. All codes in this paper are binary. A *linear* $[n, k, d]$ *code* C *of length* n is a k-dimensional subspace of $GF(2)^n$ with the minimum (Hamming) weight d. Two codes over $GF(2)$ are said to be *equivalent* if they differ only by a permutation of the coordinates. The *dual* of C, denoted by $C^{\perp}$ is the set of vectors orthogonal to every codeword of C under the Euclidean inner product. If $C = C^{\perp}$, C is called *self-dual*. If $C \subset C^{\perp}$, C is called *self-orthogonal*. If C is linear and contains the all-one vector, then C is *self-complementary*. A self-dual code is called *Type II (or doubly-even)* if every codeword has weight divisible by 4, and *Type I (or singly-even)* if there exists a codeword whose weight is congruent to 2 (mod 4).

Let C be a binary self-dual code of length n and minimum distance $d(C)$. Then $d(C)$ satisfies the following [25].

$$d(C) \leq \begin{cases} 4\left[\frac{n}{24}\right] + 4, & \text{if } n \neq 22 \pmod{24}, \\ 4\left[\frac{n}{24}\right] + 6, & \text{if } n = 22 \pmod{24}. \end{cases}$$

A self-dual code meeting one of the above bounds is called *extremal*.

A subcode C' of a linear code C with minimum distance $d' = d(C') > d(C)$ is *maximal* if there is no subcode C'' such that $C' \subsetneq C'' \subsetneq C$ and $d(C'') = d'$. Given $d' > d(C)$ such that $d' \in \{\text{the nonzero weights of } C\}$, the maximum of the dimensions of maximal subcodes C' with $d(C') = d'$ is called the *maximum dimension with respect to* d'. Given n and k, a linear $[n, k, d]$ code is *minimum distance optimal* if d is the largest possible. (Grassl's online table [8] is a good source for reasonable lengths and dimensions for finite fields of order up to 9.) Given n and d, a linear $[n, k, d]$ code is *dimension optimal* if k is the largest possible [12, p. 53]. We raise the following natural question. Given a binary self-dual code C and any non-zero weight $d' > d(C)$, how do we find a subcode with maximum dimension with respect

to d'? In general, this question seems very difficult since theoretically we should know all subcodes. On the other hand, there has been another approach related to this problem, as described below.

Let C be a binary $[n, k]$ code and let $C_0 = C$. A sequence of linear subcodes of C, $C_0 \supset C_1 \supset \cdots \supset C_{k-1}$ is called a *subcode chain*, where the dimension of C_i is $k - i$ for $i = 0, \ldots k - 1$. (If we let $C_k = \{\mathbf{0}\}$ and $V_i = C_{k-i} (i = 0, \cdots, k)$, then $\{\mathbf{0}\} = V_0 \subset V_1 \subset \cdots \subset V_k = C$ is known as a *complete flag* [20].)

Definition 2.1. Let $d_i = d(C_i)$ be the minimum distance of C_i. Then the sequence $d_0 \leq d_1 \leq \cdots \leq d_{k-1}$ is called a *distance profile* of C (see [4], [17] for details). A generator matrix such that its first $k - i$ rows (i.e., the remaining rows after removing its i rows from the bottom) form a generator matrix of C_i for $0 \leq i \leq k - 1$, is called a *generator matrix with respect to the distance profile*.

Definition 2.2. For any two integer sequences of length k, $a = a_0, \ldots, a_{k-1}$ and $b = b_0, \ldots, b_{k-1}$, a is called an *upper bound on b in the dictionary order* if a is equal to b or there is an integer t such that

$$a_i = b_i \text{ for } 0 \leq i \leq t - 1, \text{ and } a_t > b_t.$$

On the other hand, a is called an *upper bound on b in the inverse dictionary order* if a is equal to b or there is an integer t such that

$$a_i = b_i \text{ for } t + 1 \leq i \leq k - 1, \text{ and } a_t > b_t.$$

Definition 2.3. A distance profile of the linear block code is called the *optimum distance profile* (or *ODP* for short) *in the dictionary order*, which is denoted by $\mathrm{ODP}^{dic}[C](0)$, $\mathrm{ODP}^{dic}[C](1), \ldots, \mathrm{ODP}^{dic}[C](k-1)$ if it is an upper bound on any distance profile of C in the dictionary order. Similarly, a distance profile of the linear block code is called the *optimum distance profile* (or *ODP* for short) *in the inverse dictionary order*, which is denoted by $\mathrm{ODP}^{inv}[C](0)$, $\mathrm{ODP}^{inv}[C](1), \ldots, \mathrm{ODP}^{inv}[C](k-1)$ if it is an upper bound on any distance profile of C in the inverse dictionary order.

To simplify notations, for a given $[n, k]$ code C we may use $\mathrm{ODP}^{dic}[C]_i = \mathrm{ODP}^{dic}[C](k-i)$ (resp. $\mathrm{ODP}^{inv}[C]_i = \mathrm{ODP}^{inv}[C](k-i)$) so that we may easily interpret the corresponding subcode parameters: $[n, i, \mathrm{ODP}^{dic}[C]_i]$ (resp. $[n, i, \mathrm{ODP}^{inv}[C]_i]$). We also use $\mathrm{ODP}[C]$ to denote the optimum minimum distance profile in both orders. Note that for a given $[n, k]$ code C over $GF(q)$, the number of its subcode chains [17] is

$$\prod_{t=2}^{k} Q[t, t-1] = \prod_{t=2}^{k} \frac{q^t - 1}{q - 1},$$

where $Q[t, r]$ is the q-ary Gaussian binomial coefficient $\prod_{j=0}^{r-1} \frac{q^{t-j}-1}{q^{r-j}-1}$. Hence for large dimensions it will be very difficult to determine ODP of a linear code by a brute-force search.

3 Relation between ODP and the maximum dimension

The ODP of a code and the maximum dimension with respect to a minimum distance are related concepts. Note that the first minimum distance d' to appear in the ODP in dictionary order corresponds to a maximal subcode with maximum dimension corresponding to d'. However, after this term, maximal subcodes in the subcode chain do not necessarily imply the maximum dimension. This is an observation which follows from the definition of a maximal subcode and the definition of ODP; we formalize the theory in the following results. However, note that given a dimension $k' \leq k$ there may be multiple minimum distances d' with respect to which k' is the maximum dimension. Therefore for the first proposition we define $d_{k'}$ to be the maximum of such minimum distances.

Proposition 3.1. *Let C be an $[n,k]$ code. Let $k' \leq k$ be given. Define $d_{k'} = \max(\{d' : k' \text{ is the maximum dimension in } C \text{ with respect to } d'\})$ and define d_{opt} to be the optimal minimum distance attained among all $[n,k']$ codes (many values available at [8]), then*

$$d_{opt} \geq d_{k'} \geq \max(\{ODP^{dic}[C]_{k'}, ODP^{inv}[C]_{k'}\}).$$

Proof. The claim $d_{opt} \geq d_{k'}$ is clear since d_{opt} is the maximum minimum distance possible among all $[n,k']$ codes. By the definition of $d_{k'}$, if C contains an $[n,k',d']$ subcode, then $d_{k'} \geq d'$. Since $\mathrm{ODP}^{dic}[C]_{k_i}$ (respectively $\mathrm{ODP}^{inv}[C]_{k_i}$) corresponds to a dimension k_i subcode in the subcode chain having minimum distance $\mathrm{ODP}^{dic}[C]_{k_i}$ (respectively $\mathrm{ODP}^{inv}[C]_{k_i}$), the preceding claim proves the proposition. □

Corollary 3.2. *Let C be an $[n,k]$ code. Let $k' \leq k$ be given. Define $d_{k'}$ and d_{opt} as above. If $ODP^{dic}[C]_{k'} = d_{opt}$ or $ODP^{inv}[C]_{k'} = d_{opt}$, then*

$$d_{opt} = d_{k'} = \max(\{ODP^{dic}[C]_{k'}, ODP^{inv}[C]_{k'}\}).$$

The necessity of defining $d_{k'}$, in Proposition 3.1, as a maximum is due to the fact that there may be multiple minimum distances yielding the same maximum dimension. An example where this occurs is the following:

Example 3.3. Let C be the [6,3,1] code with the following generator matrix:

$$G = \begin{bmatrix} 11 & 11 & 00 \\ 11 & 00 & 11 \\ 10 & 00 & 00 \end{bmatrix}$$

The maximum dimension with respect to $d_1 = 4$ is 2, due to the fact that the first two rows of G generate a [6,2,4] subcode of C with the following generator matrix:

$$G_1 = \begin{bmatrix} 11 & 11 & 00 \\ 11 & 00 & 11 \end{bmatrix}.$$

Similarly, the maximum dimension with respect to $d_2 = 3$ is 2; this is obtained by adding the third row of G to each row in G_1 which yields a $[6,2,3]$ subcode of C with the following generator matrix:

$$G_2 = \begin{bmatrix} 01 & 11 & 00 \\ 01 & 00 & 11 \end{bmatrix}$$

Notice that in Proposition 3.1 we fix the dimension k'; a dual statement where we instead fix the minimum distance is the following.

Proposition 3.4. *Let C be an $[n,k]$ code and let $0 \leq j \leq k-1$. Suppose d_j is a minimum distance appearing as $ODP^{dic}[C]_j$ or $ODP^{inv}[C]_j$. Define k_j to be the maximum dimension with respect to d_j, then $k_j \geq j$.*

Proof. The proof follows directly from the definition of maximal dimension with respect to d_j, since a subcode with this maximal dimension will have dimension k_j which is an upper bound on the dimension of any $[n, j, d_j]$ subcode. □

The following proposition is a special case of Proposition 3.4; this proposition states that in fact the first minimum distance in the dictionary order ODP corresponds to a maximal subcode with respect to that minimum distance.

Proposition 3.5. *Let C be an $[n,k,d]$ code. Suppose that for some j, $ODP^{dic}[C]_j$ is the first term in ODP greater than d. Then j is the maximum dimension with respect to $ODP^{dic}[C]_j$.*

Proof. If $\mathrm{ODP}^{dic}[C]_j$ is the first term in ODP greater than d, then $\mathrm{ODP}^{dic}[C]_{j+1} = d$ where $0 < j < k$. Suppose to the contrary that the maximum dimension with respect to $\mathrm{ODP}^{dic}[C]_j$ is greater than j, then there must exist an $[n, j+1]$ subcode with minimum distance $\mathrm{ODP}^{dic}[C]_j$. This implies $\mathrm{ODP}^{dic}[C]_{j+1} = \mathrm{ODP}^{dic}[C]_j$ by definition of the dictionary order. Compiling this information we obtain the contradiction: $d = \mathrm{ODP}^{dic}[C]_{j+1} = \mathrm{ODP}^{dic}[C]_j > d$. □

Propositions 3.1, 3.4, and 3.5 give insight into the relation between maximum dimension subcodes and optimum distance profiles. If a code contains an optimal subcode (minimum distance optimal, dimension optimal, or both) there are many cases where this subcode appears in the subcode chain involved in an optimum distance profile. However, this is not always the case as in the following example:

Example 3.6. Let C be the [6,5,1] code with the following generator matrix:

$$G = \begin{bmatrix} 11 & 11 & 00 \\ 11 & 00 & 11 \\ 10 & 10 & 10 \\ 10 & 10 & 00 \\ 10 & 00 & 00 \end{bmatrix}$$

By expurgating weight 1 vectors from C we may obtain $[6,4,2]$ subcodes of C. Since there does not exist a $[6,4,3]$ code (see [8]), we may conclude that $\mathrm{ODP}^{dic}[C]_4 = 2$. By examining all $[6,4,2]$ subcodes of C it can be determined that none contain a $[6,3,3]$ subcode, and since no $[6,3,4]$ code exists we obtain $\mathrm{ODP}^{dic}[C]_3 = 2$. Finally, there is a unique $[6,2,4]$ code (which has a single non-zero weight of 4); as this code is a subcode of at least one $[6,4,2]$ subcode of C, and since there does not exist a $[6,2,5]$ code we may conclude $\mathrm{ODP}^{dic}[C]_2 = 4$ and $\mathrm{ODP}^{dic}[C]_1 = 4$. Therefore the optimum distance profile in dictionary order is $\mathrm{ODP}^{dic}[C] = [1,2,2,4,4]$.

Using similar arguments the ODP in inverse dictionary order is obtained as $\mathrm{ODP}^{inv}[C] = [1, 2, 2, 3, 5]$. Notice that the first three rows of G generate an optimal [6,3,3] code (both minimum distance optimal and dimension optimal). Therefore the maximum dimension with respect to minimum distance $d' = 3$ is $k' = 3$. However, the subcodes of dimension 3 appearing in both ODP orders have minimum distance 2. An explanation for this phenomenon is that all supercodes of the [6,3,3] code in C have minimum distance 1. This is an example where equality is not possible in Proposition 3.1 and in Proposition 3.4.

4 ODP of Type II self-dual codes

Using the algorithms in the appendix, we determine the ODP of binary Type II codes of lengths up to 24 and the extremal Type II codes of length 32. The classification of self-dual codes of lengths up to 32 can be found in [5, 6, 21, 23]. The generator matrices for each profile in this section are from the algorithms.

4.1 $n = 8$

For length $n = 8$, there is a unique binary Hamming $[8, 4, 4]$ code e_8. It has two non-zero weights 4 and 8. It is clear that there is a unique subcode $\langle \mathbf{1} \rangle$ of e_8 with $d_4 = 8$. Hence

$$\mathrm{ODP}[e_8] = [4, 4, 4, 8].$$

One generator matrix with respect to the ODP in the dictionary order is

$$G(e_8) = \left[\begin{array}{cccc} 11 & 11 & 11 & 11 \\ \hline 00 & 00 & 11 & 11 \\ 00 & 11 & 00 & 11 \\ 01 & 01 & 01 & 01 \end{array}\right].$$

4.2 $n = 16$

Next let us consider $n = 16$. There are two Type II $[16, 8, 4]$ codes, denoted by d_{16} and $2e_8$ [5] (blank represents 0):

$$G(d_{16}) = \left[\begin{array}{cccccccc} 11 & 11 & & & & & & \\ 11 & & 11 & & & & & \\ 11 & & & 11 & & & & \\ 11 & & & & 11 & & & \\ 11 & & & & & 11 & & \\ 11 & & & & & & 11 & \\ 11 & & & & & & & 11 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

$$\text{and } G(2e_8) = \left[\begin{array}{cccccccc} 11 & 11 & 11 & 11 & & & & \\ 00 & 00 & 11 & 11 & & & & \\ 00 & 11 & 00 & 11 & & & & \\ 01 & 01 & 01 & 01 & & & & \\ & & & & 11 & 11 & 11 & 11 \\ & & & & 00 & 00 & 11 & 11 \\ & & & & 00 & 11 & 00 & 11 \\ & & & & 01 & 01 & 01 & 01 \end{array}\right].$$

The next higher weight in d_{16} is 8. We have constructed a $[16, 5, 8]$ subcode of d_{16}. This subcode is equivalent to the first order Reed-Muller code $R(1, 4)$ and hence is unique up to equivalence [29]. As there is no $[16, 6, 8]$ code [8], we know that $k = 5$ is the maximum dimension with respect to $d = 8$. Since $R(1, 4)$ contains the all-one vector, we have

$$\text{ODP}[d_{16}] = [4, 4, 4, 8, 8, 8, 8, 16].$$

Considering some linear combinations of the rows of $G(d_{16})$, we give below one generator matrix with respect to the ODP in the dictionary order.

$$G'(d_{16}) = \left[\begin{array}{cccccccc} 11 & 11 & 11 & 11 & 11 & 11 & 11 & 11 \\ \hline 11 & 11 & 11 & 11 & & & & \\ 11 & 11 & & & 11 & 11 & & \\ 11 & & 11 & & 11 & & 11 & \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 11 & & & 11 & & & & \\ 11 & & & & & 11 & & \\ 11 & & & & & & & 11 \end{array}\right]$$

In a similar manner, we have verified that $2e_8$ has a maximal $[16, 5, 8]$ subcode, which is generated by the first five rows of $G'(d_{16})$. Hence we have

$$\text{ODP}[2e_8] = [4, 4, 4, 8, 8, 8, 8, 16].$$

We give below one generator matrix with respect to the ODP in the dictionary order.

$$G(2e_8) = \left[\begin{array}{cccccccc} 11 & 11 & 11 & 11 & 11 & 11 & 11 & 11 \\ \hline 11 & 11 & 11 & 11 & & & & \\ 11 & 11 & & & 11 & 11 & & \\ 11 & & 11 & & 11 & & 11 & \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline & & & & 11 & 11 & & \\ & & & & 11 & & 11 & \\ & & & & 1 & 1 & 1 & 1 \end{array}\right]$$

As a summary, we have

Theorem 4.1.

$$ODP[d_{16}] = ODP[2e_8] = [4, 4, 4, 8, 8, 8, 8, 16].$$

4.3 $n = 24$

Consider $n = 24$. There are exactly nine Type II self-dual codes of length 24. These are denoted by $A24(2d_{12}), B24(d_{10}+2e_7), C24(3d_8), D24(4d_6), E24(d_{24}), F24(6d_4), G24(g_{24}), d_{16}+e_8$, and $3e_8$ in the notations of [5], [23]. The first seven codes are indecomposable and the rest are decomposable. Note that $G24(g_{24})$ represents the binary Golay $[24, 12, 8]$ code.

Pollara, et. al. [24] constructed the first $[24, 5, 12]$ subcode $C_{24}^{5,12}$ of g_{24}, improving a previously known $[24, 5, 8]$ subcode. Note that $C_{24}^{5,12}$ is unique [29], has only two non-zero weights 12 and 16, and has a $[24, 2, 16]$ subcode $C_{24}^{2,16}$. As $C_{24}^{2,16}$ satisfies the Griesmer bound, it has a generator matrix of which each row has weight 16 [29], [12]. Hence it is easy to see that $C_{24}^{2,16}$ is unique.

Using this information, Luo, et. al. [17] have determined

$$\begin{aligned} \mathrm{ODP}^{dic}[g_{24}] &= [8,8,8,8,8,8,8,12,12,12,16,16] \\ \mathrm{ODP}^{inv}[g_{24}] &= [8,8,8,8,8,8,8,8,12,12,12,24]. \end{aligned}$$

However, less is known of the subcodes of the other Type II self-dual codes of length 24. We have checked that the unique $[24, 5, 12]$ code is contained in any of the nine Type II codes of length 24.

Using (Subcodes) Chain Algorithm I we obtain inequivalent maximal $[24, k', 8]$ subcodes of each Type II code of length 24 (with minimum distance 4). Then applying (Supercodes) Chain Algorithm II to the unique $[24, 5, 12]$ code for each Type II code of length 24 (with minimum distance 4) we obtain a $[24, k', 8]$ code equivalent to one of the maximal subcodes. Therefore we determine the ODP in the dictionary order of the Type II $[24, 12, 4]$ codes as follows. The generator matrices with respect to the ODP in the dictionary order are posted on the website [15].

Theorem 4.2.

$$\begin{aligned} ODP^{dic}[2d_{12}] &= ODP^{dic}[d_{10}+2e_7] \\ &= ODP^{dic}[d_{16}+e_8] \\ &= ODP^{dic}[3e_8] \\ &= [4,4,4,8,8,8,8,12,12,12,16,16] \\ \\ ODP^{dic}[3d_8] &= ODP^{dic}[4d_6] \\ &= [4,4,8,8,8,8,8,12,12,12,16,16] \\ \\ ODP^{dic}[d_{24}] &= [4,4,4,4,8,8,8,12,12,12,16,16] \\ ODP^{dic}[6d_4] &= [4,8,8,8,8,8,8,12,12,12,16,16] \end{aligned}$$

For each Type II $[24, 12, 4]$ code we apply (Subcodes) Chain Algorithm I to the maximal $[24, k', 8]$ subcodes (containing the all one vector) to obtain a $[24, 4, 12]$ subcode (containing the all one vector). Therefore we may determine the ODP in the inverse dictionary order of the Type II $[24, 12, 4]$ codes as follows. The generator matrices with respect to the ODP in the inverse dictionary order are posted on the website [15].

Theorem 4.3.

$$\begin{aligned}
ODP^{inv}[2d_{12}] &= ODP^{inv}[d_{10}+2e_7] \\
&= ODP^{inv}[d_{16}+e_8] \\
&= ODP^{inv}[3e_8] \\
&= [4,4,4,8,8,8,8,8,12,12,12,24] \\
\\
ODP^{inv}[3d_8] &= ODP^{inv}[4d_6] \\
&= [4,4,8,8,8,8,8,8,12,12,12,24] \\
\\
ODP^{inv}[d_{24}] &= [4,4,4,4,8,8,8,8,12,12,12,24] \\
ODP^{inv}[6d_4] &= [4,8,8,8,8,8,8,8,12,12,12,24]
\end{aligned}$$

Table 1 gives the maximum dimension with respect to minimum distance d for the Type II length 24 codes.

Corollary 4.4. *For each Type II length 24 code, there are maximum dimension subcodes with respect to* $d = 8, 12, 16, 24$ *(except* 20*) that are involved in the subcode chain for the ODP in dictionary order or the inverse order. Furthermore, each Type II length 24 code contains dimension optimal (and minimum distance optimal) subcodes with parameters* $[24,5,12], [24,2,16], [24,1,24]$.

Table 1: Subcodes of All Type II codes of $n = 24$

Codes	max. dim. with $d = 8$	max. dim. with $d = 12$
$2d_{12}$	9	5
$d_{10} + 2e_7$	9	5
$3d_8$	10	5
$4d_6$	10	5
d_{24}	8	5
$6d_4$	11	5
$d_{16} + e_8$	9	5
$3e_8$	9	5
g_{24}	12	5

4.4 $n = 32$

As there are 85 Type II self-dual codes of length 32, we focus on extremal Type II self-dual $[32,16,8]$ codes. There are exactly five Type II self-dual $[32,16,8]$ codes, denoted by $C81$ (or q_{32}), $C82$ (or r_{32}, $R(2,5)$), $C83$ (or $2g_{16}$), $C84$ (or $8f_4$), $C85$ ($16f_2$) in the notation of [5], [6]. Using symplectic geometric approach, Maks and Simonis [19] show that the second order Reed-Muller code r_{32} contains exactly two inequivalent $[32,11,12]$ codes, each of which

further contains the first order Reed-Muller $[32, 6, 16]$ code $R(1, 5)$. Note that any $[32, 6, 16]$ code is equivalent to $R(1, 5)$. Furthermore, Jaffe [13] proved using his language `Split` that there exist exactly two $[32, 11, 12]$ codes. These subcodes have optimal dimensions for each minimum distance. Hence Chen and Han Vinck [4] have determined the ODP in the dictionary order for r_{32} as follows:

$$\mathrm{ODP}[r_{32}] = [8, 8, 8, 8, 8, 12, 12, 12, 12, 12, 16, 16, 16, 16, 16, 32].$$

On the other hand, little was known of the subcodes of the other four extremal Type II $[32, 16, 8]$ codes. We show that they also have the same optimum distance profiles as r_{32} does.

Using (Supercodes) Chain Algorithm II with $C_{k',d'} = \{R(1, 5)\}$, we independently construct two inequivalent $[32, 11, 12]$ codes in r_{32} containing $R(1, 5)$, denoted by RC_1 and RC_2. We note that $\dim(RC_1 \cap RC_2) = 10$. Using (Supercodes) Chain Algorithm II, we have checked that each of RC_1 and RC_2 is a subcode of any of the five Type II $[32, 16, 8]$ codes. We denote the five codes based on RC_1 (RC_2, respectively) by $C81^1, \ldots, C85^1$ ($C81^2, \ldots, C85^2$, respectively).

Hence we obtain:

Theorem 4.5. *Each code C of the five Type II $[32, 16, 8]$ codes has*

$$\mathit{ODP}[C] = [8, 8, 8, 8, 8, 12, 12, 12, 12, 12, 16, 16, 16, 16, 16, 32].$$

One generator matrix for each Type II $[32, 16, 8]$ code with respect to the ODP in the dictionary order is given in Table 2 of the appendix the appendix.

$$RC_1 = \left[\begin{array}{c} 11111111111111111111111111111111 \\ \hline 00000000000000001111111111111111 \\ 00000000111111110000000011111111 \\ 00001111000011110000111100001111 \\ 00110011001100110011001100110011 \\ 01010101010101010101010101010101 \\ \hline 10000001000101110100110100100100 \\ 01000001000101000010011110001101 \\ 00100001010001110111010000010010 \\ 00001001000010010101110010100011 \\ 00100001000100100001110111010001 \end{array}\right], \quad RC_2 = \left[\begin{array}{c} 11111111111111111111111111111111 \\ \hline 00000000000000001111111111111111 \\ 00000000111111110000000011111111 \\ 00001111000011110000111100001111 \\ 00110011001100110011001100110011 \\ 01010101010101010101010101010101 \\ \hline 10000001000101110100110100100100 \\ 01000001000101000010011110001101 \\ 00100001010001110111010000010010 \\ 00001001000010010101110010100011 \\ 00100001000100100111101101001000 \end{array}\right]$$

Corollary 4.6. *For each extremal Type II length 32 code, there are maximum dimension subcodes with respect to $d = 12, 16, 32$ that are involved in the subcode chain for the ODP in dictionary order or the inverse order. Furthermore, each extremal Type II length 32 code contains dimension optimal (and minimum distance optimal) subcodes with parameters $[32, 11, 12], [32, 6, 16], [32, 1, 32]$.*

4.5 $n = 48$

Since there are two many type II $[40, 20, 8]$ codes (there are exactly 16470 such codes by [1]) and $d = 8$ is not optimal for a linear $[40, 20]$ code, we investigate the extended QR code q_{48}. Note that q_{48} is a unique $[48, 24, 12]$ self-dual code [11]. Using Random (Subcodes) Algorithm I, we find that for $d' = 16$, there is a maximal $[48, 14, 16]$ subcode of q_{48}. The best known minimum distance optimal $[48, 14]$ code has $d = 16$. (Note that 17 is the upper bound.) One code is given in Magma. We have checked that our code is not equivalent to this code. Similarly, for $d' = 20$, there is a maximal $[48, 9, 20]$ subcode of q_{48}. This is minimum distance optimal. One $[48, 9, 20]$ code is given in Magma. We have checked that our $[48, 9, 20]$ code is not equivalent to this code. For $d' = 24$, there is a maximal $[48, 6, 24]$ subcode of q_{48}, which is in fact a unique code by [29]. This is minimum distance optimal. One code is given in Magma. We have checked that our code is equivalent to this code.

With respect to the inverse dictionary order we have examined some self-complementary subcodes of q_{48}. There is a $[48, 5, 24]$ self-complementary subcode (note that $k = 5$ is the maximum dimension of a $[48, k, 24]$ self-complementary subcode since the unique $[48, 6, 24]$ code does not contain the all-one vector). There is a maximal $[48, 9, 20]$ self-complementary subcode containing the $[48, 5, 24]$ code (note that $k = 10$ is the maximum dimension of a $[48, k, 20]$ self-complementary subcode).

Lemma 4.7. ([18, the MacWilliams Identities, p. 129]) *Let C be an $[n, k]$ code and denote A_w and $A_w^\perp$ to be the number of codewords of weight w in the code C and $C^\perp$ respectively. Then*

$$\sum_{i=0}^{n} A_i P_w(n, i) = 2^k A_w^\perp, \quad \textit{for} \;\; 0 \le w \le n,$$

where $P_w(n, i) = \sum_{j=0}^{w} (-1)^j \begin{pmatrix} i \\ j \end{pmatrix} \begin{pmatrix} n-i \\ w-j \end{pmatrix}$ is a Krawtchouk polynomial.

Let C be an $[n, k, d]$ code over $\mathbb{F}_q$. Let T be a set of t coordinates. Let $C(T)$ be the set of codewords of C which are $\mathbf{0}$ on T. We puncture $C(T)$ on T to get a linear code of length $n - t$ called the *code shortened on T* and denoted by C_T [12].

Lemma 4.8. ([12, Theorem 1.5.7 (iii)]) *Let C be an $[n, k, d]$ code over $\mathbb{F}_q$. Let T be a set of t coordinates. If $t = d$ and T is the set of coordinates where a minimum weight codeword is non-zero, then $(C^\perp)_T$ has dimension $n - d - k + 1$.*

Both Lemma 4.7 and Lemma 4.8 are useful in determining the non-existence of codes with particular parameters and restricted weight distributions. These lemmas are invoked to prove the non-existence of particular subcodes of the extended quadratic residue code: q_{48}. Lemma 4.7 is also applied to determine the possible weight distribution of a putative subcode.

In what follows, we classify all possible weight distributions of a supposed $[48, 10, 20]$ self-complementary subcode of q_{48}.

Lemma 4.9. *If C is a self-complementary [48,10,20] subcode of q_{48}, then the non-zero codewords of C have weights 20,24,28,48.*

Proof. Suppose to the contrary that C has non-zero weights 20,28,48. Then clearly $A_{20} := 2^9-1$. Using the MacWilliams Identities (Lemma 4.7) we obtain the equation $2256+16A_{20} = 2^{10}A_2^\perp$. Hence $A_2^\perp = \frac{163}{16}$, a contradiction. □

Lemma 4.10. *If C is a self-complementary [48,10,20] subcode of q_{48}, then $d^\perp(C) \neq 2$.*

Proof. Suppose to the contrary that $d^\perp(C) = 2$. Shortening C on a minimum weight codeword x_2 of $C^\perp$ yields a [46,9,20] code C_{46} with possible non-zero weights 20,24,28 by Lemma 4.8 (here we switched the role of C and $C^\perp$).

Define the following matrices:

$$\begin{array}{rcl} B & = & [A_0^\perp(C_{46}) \quad A_1^\perp(C_{46}) \quad A_2^\perp(C_{46}) \quad A_3^\perp(C_{46})]^T, \\ A & = & [A_0(C_{46}) \quad A_{20}(C_{46}) \quad A_{24}(C_{46}) \quad A_{28}(C_{46})]^T. \end{array}$$

Then the MacWilliams Identities yield the matrix equation $2^9B = PA$, where

$$P = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 46 & 6 & -2 & -10 \\ 1035 & -5 & -21 & 27 \\ 15180 & -100 & 44 & 60 \end{bmatrix}.$$

By Grassl's table [8] there (respectively) does not exist a [45,9,20] linear code and there does not exist a [44,8,20] linear code, therefore respectively we have $A_1^\perp(C_{46}) = 0$ and $A_2^\perp(C_{46}) = 0$. Combined with the fact that $A_0^\perp(C_{46}) = 1$ the above matrix equation yields a unique solution of:

$$A = [1 \quad 243 \quad 147 \quad 121]^T. \tag{1}$$

The possible weight distribution of C_{46} and $C_{46}^\perp$ follows from (1). In particular, $d(C_{46}^\perp) = 3$ which by shortening C_{46} on a minimum weight codeword of $C_{46}^\perp$ using Lemma 4.8 implies the existence of a $[43, 7, 20]$ code with non-zero weights 20,24,28. This is a contradiction to the classification of [43,7,20] due to Bouyuklieva and Jaffe [2], where it is proved that there are exactly seven $[43, 7, 20]$ codes, which must have a codeword of weight 32 or 36. □

Lemma 4.11. *If C is a self-complementary [48,10,20] subcode of q_{48}, then there is one possible weight distribution of C:*

$$A_0 = 1 \quad A_{20} = 348 \quad A_{24} = 326 \quad A_{28} = 348 \quad A_{48} = 1.$$

Proof. Define the following matrices:

$$\begin{array}{rcl} B & = & [A_0^\perp \quad A_2^\perp \quad A_4^\perp]^T, \\ A & = & [A_0 \quad A_{20} \quad A_{24}]^T. \end{array}$$

Then the MacWilliams Identities along with the fact that C is self-complementary yield the matrix equation $2^{10}B = PA$, where

$$P = \begin{bmatrix} 2 & 2 & 1 \\ 2256 & 16 & -24 \\ 389160 & -600 & 276 \end{bmatrix}.$$

By the previous lemma $A_2^\perp = 0$, combined with the fact that $A_0 = A_0^\perp = 1$ the above matrix equation yields a unique solution of:

$$A = [1 \quad 348 \quad 326]^T.$$

□

Lemma 4.12. *There does not exist a self-complementary [48,k,16] subcode C of q_{48} for $k \geq 17$.*

Proof. Suppose a [48,17,16] self-complementary subcode C exists. The possible non-zero weights of C are 16,20,24,28,32,48. Define the following matrices:

$$\begin{aligned} B &= [A_0^\perp \quad A_2^\perp \quad A_4^\perp \quad A_6^\perp]^T, \\ A &= [A_0 \quad A_{16} \quad A_{20} \quad A_{24}]^T. \end{aligned}$$

Then the MacWilliams Identities along with the fact that C is self-complementary yield the matrix equation $2^{17}B = PA$, where

$$P = \begin{bmatrix} 2 & 2 & 2 & 1 \\ 2256 & 208 & 16 & -24 \\ 389160 & 40 & -600 & 276 \\ 24543024 & -14544 & 5616 & -2024 \end{bmatrix}.$$

Isolating the matrix A yields the matrix equation $2^{17}P^{-1}B = A$ where

$$2^{17}P^{-1} = \begin{bmatrix} 17/14 & 65/224 & 3/56 & 1/224 \\ 9729/2 & 17457/32 & 211/8 & -15/32 \\ 207552/7 & -1012/7 & -752/7 & 12/7 \\ 62040 & -1605/2 & 162 & -5/2 \end{bmatrix}.$$

The first row of $2^{17}P^{-1}$ implies

$$\frac{65}{224}A_2^\perp + \frac{3}{56}A_4^\perp + \frac{1}{224}A_6^\perp = -\frac{3}{14},$$

which is impossible as $A_i^\perp \geq 0$ for all i. Hence no such code C can exist. □

The previous lemmas and example from this section yield the following theorem towards the inverse dictionary order ODP for q_{48}.

Theorem 4.13.

$$ODP^{inv}[q_{48}] = [12, 12, 12, 12, 12, 12, 12, 12, a_1, a_2, a_3, a_4, a_5, a_6, b, 20, 20, 20, 20, 24, 24, 24, 24, 48]$$

where $a_i \in \{12, 16\}$ and $b \in \{12, 16, 20\}$.

Proof. Since q_{48} contains the all-one vector, the repetition code $[48, 1, 48]$ must be the one dimensional subcode first appearing in the subcode chain. By [29] there is a unique $[48, 6, 24]$ code with non-zero weights $24, 32$; since this code does not contain the all-one vector it cannot be involved in the inverse dictionary order subcode chain. Hence $k \leq 5$ for a $[48, k, 24]$ code involved in the subcode chain. Applying Random (Supercode) Algorithm II to the $[48, 1, 48]$ subcode of q_{48} we obtained a subcode chain involving a $[48, 5, 24]$ code contained in a $[48, 9, 20]$ subcode of q_{48}. Therefore $\mathrm{ODP}^{inv}[q_{48}]_i = 24$ for $2 \leq i \leq 5$, and $\mathrm{ODP}^{inv}[q_{48}]_j = 20$ for $6 \leq i \leq 9$. The maximum dimension for a $[48, k, 20]$ code is $k = 10$ by Grassl's table [8], hence $\mathrm{ODP}^{inv}[q_{48}]_{10} = b$ for $b \in \{12, 16, 20\}$ and also $\mathrm{ODP}^{inv}[q_{48}]_j = a_i$ for $11 \leq j \leq 16$ and $a_i \in \{12, 16\}$. Finally, $\mathrm{ODP}^{inv}[q_{48}]_i = 12$ for $17 \leq i \leq 24$ by Lemma 4.12. □

Lemma 4.14. *There does not exist a [48,k,16] subcode C of q_{48} for $k \geq 17$.*

Proof. Suppose a [48,17,16] subcode of C exists. Since the self-complementary case is already considered in Lemma 4.12, we only need to examine the case where the maximum weight in C is 36 since the non-zero weights in q_{48} are 12, 16, 20, 24, 28, 32, 36, 48. Hence the possible non-zero weights of C are 16,20,24,28,32,36. Define the following matrices:

$$\begin{aligned} B &= [A_0^\perp \quad A_1^\perp \quad A_2^\perp \quad A_3^\perp \quad A_4^\perp \quad A_5^\perp \quad A_6^\perp]^T, \\ A &= [A_0 \quad A_{16} \quad A_{20} \quad A_{24} \quad A_{28} \quad A_{32} \quad A_{36}]^T. \end{aligned}$$

Then the MacWilliams Identities yield the matrix equation $2^{17}B = PA$, where

$$P = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 48 & 16 & 8 & 0 & -8 & -16 & -24 \\ 1128 & 104 & 8 & -24 & 8 & 104 & 264 \\ 17296 & 304 & -104 & 0 & 104 & -304 & -1736 \\ 194580 & 20 & -300 & 276 & -300 & 20 & 7380 \\ 1712304 & -2672 & 456 & 0 & -456 & 2672 & -19800 \\ 12271512 & -7272 & 2808 & -2024 & 2808 & -7272 & 25080 \end{bmatrix}.$$

Isolating the matrix A yields the matrix equation $2^{17}P^{-1}B = A$ where

$$2^{17}P^{-1} = \begin{bmatrix} 34/21 & 17/21 & 65/168 & 1/6 & 1/14 & 1/42 & 1/168 \\ 4788 & 1698 & 2109/4 & 135 & 23 & 1 & -3/4 \\ 30000 & 4592 & -61 & -312 & -92 & -8 & 3 \\ 61360 & 680 & -965 & 140 & 132 & 20 & -5 \\ 212448/7 & -39488/7 & 158/7 & 96 & -536/7 & -160/7 & 30/7 \\ 4482 & -1239 & 3633/8 & -81/2 & 19/2 & 25/2 & -15/8 \\ 272/3 & -272/3 & 65/3 & -56/3 & 4 & -8/3 & 1/3 \end{bmatrix}.$$

The first row of $2^{17}P^{-1}$ implies

$$\frac{17}{21}A_1^\perp + \frac{65}{168}A_2^\perp + \frac{1}{6}A_3^\perp + \frac{1}{14}A_4^\perp + \frac{1}{42}A_5^\perp + \frac{1}{168}A_6^\perp = -\frac{13}{21},$$

which is impossible as $A_i^\perp \geq 0$ for all i. Hence no such code C can exist.

□

Remark 4.15. We note that determining $\mathrm{ODP}^{dic}[q_{48}]$ completely is quite difficult. So we only display our partial result with the help of Lemma 4.14. Interested readers can find more.

$\mathrm{ODP}^{dic}[q_{48}] = [12, 12, 12, 12, 12, 12, 12, 12, a_1, a_2, 16, 16, 16, 16, b_1, b_2, b_3, b_3, c_1, c_2, c_3, c_4, d, e]$ where $a_i \in \{12, 16\}$, $b_k \in \{16, 20\}$, $c_l \in \{16, 20, 24\}$, $d \in \{16, 20, 24, 28, 32\}$, and $e \in \{20, 24, 28, 32, 36, 48\}$.

On the other hand, we were able to find a doubly-even self-complementary $[48, 16, 16]$ code with generator matrix $G_{[48,16,16]}$. Such a code was previously not known to exist. Only one singly-even self-complementary $[48, 16, 16]$ code was found by A. Kohnert [16].

The dual code has minimum distance $d = 4$. The generator matrix for this doubly-even self-complementary $[48, 16, 16]$ code is the following:

$$G_{[48,16,16]} = \begin{bmatrix}
100100000000001000110001001011100011100100010100 \\
010100000000000001111000001001001100110010110100 \\
001100000000001000101111000010101001010111011110 \\
000010000000001000101000111100101110101111000111 \\
000001000000000000011110010000101010101010110101 \\
000000100000001001001110101100000101100100001101 \\
000000010000000001111111110010100000011110000000 \\
000000001000000001100001101101000111111110000000 \\
000000000100000000110011100111100100110111111100 \\
000000000010000001001101100111100011001111111010 \\
000000000001001001110011111110000010100000101000 \\
000000000000101000010100011110000011000111001110 \\
000000000000011001111001100000000110000110011110 \\
000000000000000100001101011001101101011010011000 \\
000000000000000010010010111001101101000011100110 \\
000000000000000000000000000000011111111111111110
\end{bmatrix}$$

Open Problem 1: Determine if the code with generator matrix $G_{[48,16,16]}$ is equivalent to a subcode of q_{48}.

4.6 $n = 72$

Note that q_{72} (the extended quadratic residue code of length 72) is a Type II $[72, 36, 12]$ code. Due to the complexity, we use Random (Subcodes) Algorithm I. For $d' = 16$, there is a maximal $[72, 29, 16]$ subcode of q_{72} with $A_{16} = 2160$. The best known minimum distance optimal $[72, 29]$ code has $d = 16$ (and at most $d \leq 21$) with $A_{16} = 28417$, given in Magma. Hence our code is not equivalent to this code. For $d' = 20$, there is a maximal $[72, 23, 20]$ subcode with $A_{20} = 3046$. The best known minimum distance optimal $[72, 23]$ code has $d = 20$ (and at most ≤ 24) with $A_{20} = 7120$ given in Magma. Hence our code is not equivalent to this code.

We start from a best known linear $[72, 31, 20]$ code, given in Magma. Let C_1 be this code and let $d' = 16 < d = 20$. Using Random (Supercode) Algorithm II, we have constructed in a few seconds a *doubly-even self-orthogonal* $[72, 35, 16]$ *code* C' containing C_1 with $A_{16} =$

129972. It is known from Magma that there is a best known minimum distance code with parameters $[72, 35, 16]$. This is a doubly-even self-orthogonal code with $A_{16} = 136116$. Hence our code *is not equivalent* to the known code. We do not know how many doubly-even self-orthogonal $[72, 35, 16]$ codes exist.

5 Conclusion

The optimum distance profile for a linear code (and any code in general) is a relatively new concept developed in [4] and [17]. This area is particularly interesting due to its practical applications. In this paper we relate the optimum distance profile of a code to the concept of maximal subcodes of high minimum distance. We develop four algorithms which are highly efficient in comparison to a brute force examination of all subcodes.

The classification of self-dual codes continues to be an extremely active area in coding theory. A particularly interesting class of self-dual codes is those of Type II which have high minimum distance (called extremal or near-extremal). It is notable that this class of codes contains famous unique codes: the extended Hamming $[8, 4, 4]$ code, the extended Golay $[24, 12, 8]$ code, and the extended quadratic residue $[48, 24, 12]$ code. A long standing open problem in coding theory is to prove the existence or non-existence of a Type II $[72, 36, 16]$ code. The aim of this paper is to shed light on the structure of this interesting class of codes. We examine the maximal subcodes and ODPs of Type II codes for lengths up to 32. Of recent significance is the classification of length 40 Type II codes [1]. The examination of these codes would be extensive work as there are 16470 Type II $[40, 20, 8]$ codes (the highest minimum distance in this case is 8 which is not minimum distance optimal by [8]). Therefore we examined a more interesting case, the unique Type II code q_{48} of length 48, with some interesting results.

Acknowledgement

J.-L. Kim would like to mention that this work was supported by the Sogang University Research Grant of 201210058.01. J.-L. Kim would like to thank Prof. Vera Pless for discussing the concept of optimal subcodes when she visited University of Louisville in 2006.

Appendix

Algorithms based on cosets

Given an $[n, k, d]$ code C which has small length and dimension it may be relatively easy to examine its subcode structure by a brute force generation of all possible subcodes. However, as length and dimension increase this method becomes very time consuming; this is why we propose four algorithms based on cosets which are relatively efficient in comparison to the brute force search. The first two algorithms, called the *Chain Algorithms* are useful in the classfication in the sense that when applying them we obtain a complete list of inequivalent subcodes (respectively supercodes), with prescribed minimum distance, contained in (respectively containing) the given code C; in this way, the redundant cases

considered in a brute force search are eliminated. The remaining two *Random Algorithms* are random versions of the Chain Algorithms, and especially useful for very large length and dimension, where the exhaustive search is infeasible. The Random Algorithms can also give results much faster than the Chain Algorithms since not all cases are considered.

(Subcodes) Chain Algorithm I: An algorithm to produce all maximal subcodes with maximum dimension k' and minimum distance $d' \geq d$.

(i) Input: Begin with a binary $[n, k, d]$ code D and a positive integer $d' \geq d$ (such that there exists a codeword of weight d' in D).

(ii) Output: Produce the maximum dimension k' among all maximal subcodes with minimum distance d' and a list of inequivalent maximal subcodes of this dimension and minimum distance d'.

(a) Initialize the set $\mathbf{B}_1 = \{D^{\perp}\}$. Begin with $i = 1$.

(b) Build a set $\mathbf{B}_{i+1}$ of all inequivalent supercodes of dimension 1 higher of C for all $C \in \mathbf{B}_i$. In order to do this we add coset representatives from $\mathbb{F}_q^n/C$ to each code C in $\mathbf{B}_i$.

(c) Check if $d(C^{\perp}) = d'$ for any code $C \in \mathbf{B}_{i+1}$. If "No" for all $C \in \mathbf{B}_{i+1}$, then repeat step (ii) by increasing i to $i + 1$. If "Yes" for some C, then output the maximum dimension $k' = k - i + 1$ and the set of $[n, k - i + 1, d']$ subcodes of D.

(Supercodes) Chain Algorithm II: An algorithm to find all $[n, k, d]$ supercodes containing an $[n, k', d']$ code with $d' \geq d$ and $k \geq k'$.

(i) Input: Begin with a set $\mathbf{C}_{k',d'}$ of inequivalent $[n, k', d']$ codes (respectively self-orthogonal codes) with $k \geq k'$ and $d' \geq d$.

(ii) Output: For each code C in $\mathbf{C}_{k',d'}$, produce all $[n, k, d]$ codes (respectively self-orthogonal codes) containing C.

(a) Begin by building a set of all inequivalent supercodes (respectively self-orthogonal supercodes) of dimension 1 higher of each code C in $\mathbf{C}_{k',d'}$ with minimum distance greater than or equal to d. In order to do this we add coset representatives from $\mathbb{F}_q^n/C$ (respectively $C^{\perp}/C$ if C is self-orthogonal) to each code C in $\mathbf{C}_{k',d'}$ and keep a set of inequivalent supercodes $\mathbf{C}_{k'+1}$ generated in this way.

(b) Repeat the first step, by replacing $\mathbf{C}_{k',d'}$ with $\mathbf{C}_{k'+1}$ until the set of inequivalent codes which are generated have dimension k.

(c) Stop once dimension k is reached. For each code C in $\mathbf{C}_{k',d'}$ output all $[n, k, d]$ supercodes of C.

Analysis and comparison of our algorithms:

Given an $[n, k]$ code C, the search for subcodes of dimension k' may be conceptualized as a search tree with root C and each node of branch distance b from C given by a $[n, k-b]$ subcode. A brute-force search of the subcodes of dimension k' for an $[n, k]$ code searches through all branches of the search tree up to distance $k - k'$; this search has complexity given by the Gaussian binomial coefficient $\begin{bmatrix} k \\ k' \end{bmatrix}_2$. The Chain Algorithms greatly reduce this search by "pruning" the search tree in two manners. First, we keep only inequivalent subcodes (resp. supercodes) at each branch level (in addition this keeps the search efficient memory-wise). Second, branches can only extend from subcodes that were preserved in the previous step creating a *chain of subcodes*. In comparison, the algorithms given in Yan, et. al. [30] construct all subcodes of the same dimension not necessarily in chains of codes; this method corresponds to searching all nodes at a given branch distance (many of which are redundant).

For example, a brute-force search of the subcodes of dimension k' for an $[n, k]$ code has complexity given by the Gaussian binomial coefficient $\begin{bmatrix} k \\ k' \end{bmatrix}_2$. In Section 4.4 for some $[32, 16, 8]$ codes we determine the maximum dimension subcode with respect to $d = 12$ to have dimension 11. A brute-force subcode search (such as the subcodes traversing algorithm in [30]) would have to enumerate $\begin{bmatrix} 16 \\ 11 \end{bmatrix}_2 = 120,843,139,740,969,555$ subcodes; this task is not feasible.

Example 5.1. As a more concrete example, we determine the ODPs for the four optimal $[28, 7, 12]$ self-complementary codes classified in [7]. These codes are doubly-even with non-zero weights 12,16,28. We begin with a $[28, 3, 16]$ constant weight code (meaning the only non-zero weight is 16). There is only one such code due to the fact that all non-zero codewords must intersect in exactly 8 positions; if the first two basis vectors are fixed, then there is only one possibility (up to coordinate permutation) for the third basis vector. By adding the all-one vector to the constant weight code we obtain a $[28, 4, 12]$ code with the following generator matrix:

$$G_{[28,4,16]} = \begin{bmatrix} 1111 & 0000 & 0000 & 1111 & 0000 & 1111 & 1111 \\ 0000 & 1111 & 0000 & 1111 & 1111 & 0000 & 1111 \\ 0000 & 0000 & 1111 & 1111 & 1111 & 1111 & 0000 \\ 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \end{bmatrix}$$

Applying (Supercodes) Chain Algorithm II to this generator matrix (and only keeping doubly-even supercodes) we obtain all four self-complementary $[28, 7, 12]$ codes with the following generator matrices:

$$\begin{bmatrix} G_{[28,4,16]} \\ 0100010001011010010010111001 \\ 0010011101110111001111001100 \\ 0001000100011110010101010011 \end{bmatrix}, \begin{bmatrix} G_{[28,4,16]} \\ 0100010001001101001110101010 \\ 0010011101110111001111001100 \\ 0001000100011110010101010011 \end{bmatrix},$$

$$\left[\begin{array}{c} G_{[28,4,16]} \\ 0100010001001011010100110110 \\ 0010011101110111001111001100 \\ 0001000100011110010101010011 \end{array}\right], \left[\begin{array}{c} G_{[28,4,16]} \\ 0101001100111010000010011010 \\ 0011000000110011001100110011 \\ 0000011001011010010110101100 \end{array}\right].$$

Let C be any $[28, 7, 12]$ self-complementary code. Since the $[28, 3, 16]$ subcode is optimal, in light of Proposition 3.5, we determine $\mathrm{ODP}^{dic}[C]_3 = 16$. As a [28,3,16] subcode cannot contain the all-one vector, we determine the ODP in dictionary order:

$$\mathrm{ODP}^{dic}[C] = [12, 12, 12, 12, 16, 16, 16].$$

The ODP in inverse order is clear since any supercode of the repetition code, containing a weight 16 vector, must also contain a weight 12 vector. Hence

$$\mathrm{ODP}^{inv}[C] = [12, 12, 12, 12, 12, 12, 28].$$

We now introduce the random algorithms which are random versions of the above coset algorithms:

Random (Subcodes) Algorithm I: An algorithm to search for maximal subcodes

(i) Input: A linear code C with parameters $[n, k, d]$ and $d' > d$ where $A_{d'}$ is non-zero.

(ii) Output: A maximal subcode C' of C with d'.

(a) Take any codeword x from C such that $\mathrm{wt}(x) \geq d'$. Let $C_1 = \langle x \rangle$.

(b) Choose any coset representative y of C/C_1. Let $C_1 := \langle y \rangle + C_1$. Repeat this until $d(C_1) = d'$.

(c) Repeat (b) until there is no coset representative such that $d(C_1) = d'$. Let $C' := C_1$.

The below algorithm is somewhat opposite to Random Algorithm I.
Random (Supercode) Algorithm II: An algorithm to search for codes containing good codes

(i) Input: A (best known) linear code C_1 with parameters $[n, k, d]$ and $d' < d$.

(ii) Output: A code C' containing C_1 with d' and $k' > k$ (if such a C' exists).

(a) Let C:=${C_1}^{\perp}$.

(b) Choose any coset representative y of C/C_1. Let $C_1 := \langle y \rangle + C_1$. Repeat this until $d(C_1) = d'$.

(c) Repeat (b) until there is no coset representative such that $d(C_1) = d'$. Let $C' := C_1$.

Example 5.2. Using their traversing algorithms, the authors [30] have determined ODPs of a quasi-cyclic $[48, 10, 20]$ code C_{48} by finding all k-dimensional subcodes of C which is extensive work. Using the above Random Algorithms, we have also computed ODPs of C_{48} in the *dictionary* and *inverse dictionary* orders *in a minute* as follows:

$$\mathrm{ODP}^{dic}[C_{48}] = [20, 20, 20, 20, 24, 24, 24, 24, 32, 32],$$
$$\mathrm{ODP}^{inv}[C_{48}] = [20, 20, 20, 20, 20, 20, 20, 24, 28, 36].$$

References

[1] K. Betsumiya, M. Harada, A. Munemasa, A complete classification of doubly-even self-dual codes of length 40, Electronic J. Combin. 19 (3) (2012), #P18 (12 pp.)

[2] I. Bouyuklieva and D.B. Jaffe, Optimal binary linear codes of dimension at most seven, Discrete Math 226 (2001) 51–70.

[3] J. Cannon and C. Playoust, An Introduction to Magma, University of Sydney, Sydney, Australia, (1994), version V2.12-19.

[4] Y. Chen and A.J. Han Vinck, A lower bound on the optimum distance profiles of the second-order Reed-Muller codes, IEEE Trans. Inform. Theory 56 (9) (2010) 4309–4320.

[5] J.H. Conway and V. Pless, On the enumeration of self-dual codes, J. Combin. Theory. Ser. A 28 (1) (1980) 26–53.

[6] J.H. Conway, V. Pless, and N.J.A. Sloane, The binary self-dual codes of length up to 32:A revised enumeration, J. Combin. Theory. Ser. A 60 (2) (1992) 183–195.

[7] S.M. Dodunekov, S.B. Encheva and S.N. Kapralov, On the $[28, 7, 12]$ binary self-complementary codes and their residuals, Designs, Codes and Cryptography 4 (1) (1994) 57–67.

[8] M. Grassl, *Bounds on the minimum distance of linear codes*, online available at `http://www.codetables.de`.

[9] T.A. Gulliver and P.R.J. Östergard, Binary optimal linear rate 1/2 codes, Discrete Math 283 (1–3) (2004) 255–261.

[10] H. Holma and A. Toskala, WCDMA for UMTS-HSPA Evolution and LTE, 4th ed. London, U.K.: Wiley, 2007.

[11] 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. Inform. Theory 49 (1) (2003) 53–59.

[12] W.C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, 2003.

[13] D.B. Jaffe, Optimal binary linear codes of length $\leq$ 30, Discrete Math 223 (2000) 135–155.

[14] D.B. Jaffe, *Information about binary linear codes*, online available at `http://www.math.unl.edu/~djaffe2/codes/webcodes/codeform.html`. Accessed 1/24/2013.

[15] J.-L. Kim, `http://maths.sogang.ac.kr/jlkim/preprints.html`.

[16] A. Kohnert, New $[48, 16, 16]$ optimal linear binary block code, Online available at http://arXiv:0912.4107v1. 2009.

[17] Y. Luo, A.J. Han Vinck, Y. Chen, On the optimum distance profiles about linear block codes, IEEE Trans. Inform. Theory 56 (3) (2010) 1007–1014.

[18] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland), 1977.

[19] J. Maks and J. Simonis, Optimal subcodes of second order Reed-Muller codes and maximal linear spaces of bivectors of maximal rank, Des. Codes and Cryptogr. 21 (2000) 165–180.

[20] E. Miller and B. Sturmfels, Combinatorial Commutative Algebra, GTM, Springer, New York, 2005.

[21] V. Pless, A classification of self-orthogonal codes over $GF(2)$, Discrete Math 3 (1972) 215–228.

[22] V. S. Pless, W.C. Huffman, Eds. Handbook of Coding Theory, Amsterdam. The Netherlands: Elsevier, 1998.

[23] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, J. of Combin. Theory 18 (3) (1975) 313–335.

[24] F. Pollara, K.-M. Cheung, and R.J. McEliece, Further results on finite-state codes, TDA Progress Report 42-92, October-Decemeber, (1987) 56–62.

[25] E. M. Rains and N. J. A. Sloane, " Self-dual codes," in Handbook of Coding Theory, ed. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 177–294, 1998.

[26] J. Simonis, The [18, 9, 6] code is unique, Discrete Math. 106-107 (1) (1992) 439–448.

[27] R. Tanner and J. Woodard, WCDMA-Requirements and Practical Design, London, U.K.: Wiley, 2004.

[28] M. van Dijk, S. Baggen, and L. Tolhuizen, Coding for informed decoders, in Proc. IEEE Int. Symp. Inf. Theory, Washington, DC. Ju. (2001) 202.

[29] H. van Tilborg, On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound, Inf. Control. 44 (1980) 16–35.

[30] J. Yan, Z. Zhuang, and Y. Luo, On the optimum distance profiles of some quasi cyclic codes, Proc. of 2011 13th International Conference on Communication Technology (2011) 979–983.

Table 2: $[32, 11, 12]$ Subcodes of the five Type II $[32, 16, 8]$ codes

$$C81^1 = \left[\begin{array}{c} RC_1 \\ \hline 10000000000000010001011000001110 \\ 01000000000000100001010100110001 \\ 00100000000000100011000101001001 \\ 00010000000000010001000011001101 \\ 00001000000100000010010100110010 \end{array}\right] \quad C82^1 = \left[\begin{array}{c} RC_1 \\ \hline 10000000000000010110111000011111 \\ 01000000000000100100000000111011 \\ 00100000000000010110110111010101 \\ 00010000000000010000111001000101 \\ 00001000000000010001101000010011 \end{array}\right]$$

$$C83^1 = \left[\begin{array}{c} RC_1 \\ \hline 10000001000100010011010101100110 \\ 01000001000100100011011001011001 \\ 00100001000100100001001000100001 \\ 00010001000100010010001000100010 \\ 00001001000000000001011100100010 \end{array}\right] \quad C84^1 = \left[\begin{array}{c} RC_1 \\ \hline 10000000000000010001011000001110 \\ 01000000000000100001010100110001 \\ 00100000000000100011000101001001 \\ 00010000000000010000000110110101 \\ 00001000000100000011010001001010 \end{array}\right]$$

$$C85^1 = \left[\begin{array}{c} RC_1 \\ \hline 10000000000000010001011000001110 \\ 01000000000000010101011111011010 \\ 00100000000000010001101000110100 \\ 00010000000000010000000110110101 \\ 00001000000000010000010010011011 \end{array}\right] \quad C81^2 = \left[\begin{array}{c} RC_2 \\ \hline 10000000001000000100101001011100 \\ 01000000001001100100110111011100 \\ 00100000001001100000010100101000 \\ 00010000001000000100011111011111 \\ 00001000000000010001011011101111 \end{array}\right]$$

$$C82^2 = \left[\begin{array}{c} RC_2 \\ \hline 10000001000101110001011101111110 \\ 01000001000101000001010001000001 \\ 00100001000100100001001000100001 \\ 00010001000100010001000100010001 \\ 00001001000001100000011000001001 \end{array}\right] \quad C83^2 = \left[\begin{array}{c} RC_2 \\ \hline 10000001000100010011010101100110 \\ 01000001000100100011011001011001 \\ 00100001000100100001001000100001 \\ 00010001000100010010001000100010 \\ 00001001000000000001011100100010 \end{array}\right]$$

$$C84^2 = \left[\begin{array}{c} RC_2 \\ \hline 10000000000100000010010100101100 \\ 01000000000100110010011011101100 \\ 00100000000100110000001010010100 \\ 00010000001000000110010011010000 \\ 00001000000000010000011101101000 \end{array}\right] \quad C85^2 = \left[\begin{array}{c} RC_2 \\ \hline 10000000000100000010010100101100 \\ 01000000000100000110011111110100 \\ 00100000000100000100001110001100 \\ 00010000000100000010001111101111 \\ 00001000000000010001011011101111 \end{array}\right]$$