Finite Fields and Their Applications 25 (2014) 146–164

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Optimal subcodes and optimum distance profiles of self-dual codes

Finley Freibert [a], Jon-Lark Kim [b,*,1]

[a] Department of Mathematics, Ohio Dominican University, Columbus, OH 43219, USA
[b] Department of Mathematics, Sogang University, Seoul 121-742, South Korea

ARTICLE INFO

Article history:
Received 14 February 2013
Received in revised form 10 July 2013
Accepted 8 September 2013
Available online 5 October 2013
Communicated by W. Cary Huffman

MSC:
94B05
11T71

Keywords:
Algorithm
Self-dual codes
Subcodes
Optimum distance profiles
Optimal codes

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 $k \geqslant 17$, and we find a first example of a *doubly-even* self-complementary $[48, 16, 16]$ code.

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 [11,20,16]. 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

* Corresponding author.
E-mail addresses: ffreibert@yahoo.com (F. Freibert), jlkim@sogang.ac.kr (J.-L. Kim).

[1] J.-L. Kim was supported by Basic Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2005172) and by the Sogang University Research Grant of 201210058.01.

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.09.002

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 [19] started to classify binary self-dual codes in 1972. These codes have interesting connections to groups, t-designs, lattices, and theta series [11,16,23]. 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 [22] 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 [17] 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 [15]. The authors [15] 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 [9,24] and address retrieval on optical media [25].

In [4] and [15], 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. [27] 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 [27].

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, and 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 $k \geqslant 17$. 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 [14]. 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 $A_{16} = 129\,972$. All our computations were done using Magma [3].

2. Preliminaries

We refer to [11] 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