Finite Fields and Their Applications 54 (2018) 297–314

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Self-dual codes and orthogonal matrices over large finite fields ☆

Minjia Shi [a,b], Lin Sok [b,c,*], Patrick Solé [d], Selda Çalkavur [e]

[a] *Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, Anhui University, No. 3 Feixi Road, Hefei, Anhui, 230039, China*
[b] *School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China*
[c] *Department of Mathematics, Royal University of Phnom Penh, 12156 Phnom Penh, Cambodia*
[d] *CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France*
[e] *Mathematics Department, Kocaeli University, Kocaeli, Turkey*

ARTICLE INFO

Article history:
Received 16 May 2018
Received in revised form 21 August 2018
Accepted 22 August 2018
Available online xxxx
Communicated by Dieter Jungnickel

MSC:
94B05
94B15

Keywords:
Orthogonal matrices
Self-dual codes
Optimal codes
Almost MDS codes
MDS codes

ABSTRACT

In this paper, we give algorithms and methods of construction of self-dual codes over finite fields using orthogonal matrices. Randomization in the orthogonal group, code extension and projection over a self-dual basis are the main tools. Some optimal, almost MDS, and MDS self-dual codes over both small and large finite fields are constructed. Moreover, over fifty MDS codes with new parameters are constructed. Comparisons with classical constructions are made.

☆ This work was partly presented at the 3rd Sino–Korea International Conference on Coding Theory and Related Topics, August 12–16, 2016, Beijing, China.

* Corresponding author.
E-mail addresses: smjwcl.good@163.com (M. Shi), sok.lin@rupp.edu.kh (L. Sok), sole@math.univ-paris13.fr (P. Solé), selda.calkavur@kocaeli.edu.tr (S. Çalkavur).

https://doi.org/10.1016/j.ffa.2018.08.011
1071-5797/

1. Introduction

Self-dual codes are one of the most interesting classes of linear codes. They have close connections with group theory, lattice theory, design theory, and modular forms. It is well known that self-dual codes are asymptotically good [20]. Being optimal codes, MDS self-dual codes have been of much interest from many researchers. Some classical constructions of self-dual codes over large finite fields use combinatorial matrices [3,7]. Optimal self-dual codes over small finite fields were constructed in [9]. Betsumiya et al. [4] constructed some MDS and almost MDS self-dual codes of length up to 20 over prime fields $\mathbb{F}_q, 11 \leq q \leq 29$. Georgiou et al. [10] gave constructions over some larger prime fields up to length 14. Grassl et al. [11] proved existence of MDS codes of all lengths over $\mathbb{F}_{2^m}$ and of all highest length over finite fields of odd characteristics. Kim et al. [18] studied MDS self-dual codes over Galois rings. Guenda [12] constructed MDS Euclidean and Hermitian self-dual codes over larger fields. Jin et al. [16] proved existence of MDS self-codes $\mathbb{F}_q$ in odd characteristic for $q \equiv 1 \pmod 4$ and for q being a square of prime with restricted lengths.

Recently in the classification of extremal binary self-dual codes of length 38 [2], all nonequivalent extremal codes of shorter lengths were reconstructed from the so-called orthogonal matrices and from the method [1].

In this paper we generalize the constructions of [1] from the binary field to arbitrary finite fields. Three main types of constructions are given: random sampling from the orthogonal group, code extension by two or four symbols and projection over a self-dual basis. For large finite fields, we consider the fields of size up to 109, and lengths up to 22. Over fifty MDS codes with new parameters are constructed. For small finite fields, specifically $\mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5$, we consider length up to 32. Generator matrices and weight enumerators are archived in http://math.ahu.edu.cn/web/user.asp?id=25.

It should be noted that in a companion paper by Sok et al. [22], we have explored similar constructions for LCD codes over large finite fields. We correct some of the formulas there: see preliminaries.

The paper is organized as follows: Section 2 gives preliminaries and background for self-dual codes. Section 3 gives method to construct and to extend a self-dual code. In Section 4 we present numerical results of some optimal codes, almost MDS and MDS self-dual codes over different large fields, and compare them with classical constructions.

2. Preliminaries

We refer to [14] for basic definitions and results related to self-dual codes. A *linear* $[n, k]_{\mathbb{F}_q}$ *code* C *of length* n over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. An element in C is called a *codeword*. The (Hamming) weight $\mathrm{wt}(\mathbf{x})$ of a vector $\mathbf{x} = (x_1, \ldots, x_n)$ is the number of non-zero coordinates in it. The *minimum distance (*or *minimum weight)* $d(C)$ of C is $d(C) := \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$. The *Euclidean inner product* of $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ in $\mathbb{F}_q^n$ is $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i$. The *dual* of C, denoted