Finite Fields and Their Applications 42 (2016) 57–66

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the classification of self-dual $[20, 10, 9]$ codes over $\mathrm{GF}(7)$

Masaaki Harada *, Akihiro Munemasa

Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan

ARTICLE INFO

Article history:
Received 1 February 2016
Received in revised form 6 June 2016
Accepted 10 July 2016
Available online 22 July 2016
Communicated by Chaoping Xing

In memory of Yutaka Hiramine

MSC:
94B05

Keywords:
Self-dual code
Skew-Hadamard matrix
Unimodular lattice

ABSTRACT

It is shown that the extended quadratic residue code of length 20 over $\mathrm{GF}(7)$ is a unique self-dual $[20, 10, 9]$ code C such that the lattice obtained from C by Construction A is isomorphic to the 20-dimensional unimodular lattice D_{20}^{+}, up to equivalence. This is done by converting the classification of such self-dual codes to that of skew-Hadamard matrices of order 20.

1. Introduction

Let $\mathrm{GF}(p)$ be the finite field of order p, where p is prime. As described in [16], self-dual codes are an important class of linear codes for both theoretical and practical reasons. For $p \equiv 1 \pmod 4$, a self-dual code of length n over $\mathrm{GF}(p)$ exists if and only if n is even, and for $p \equiv 3 \pmod 4$, a self-dual code of length n over $\mathrm{GF}(p)$ exists if and only

* Corresponding author.
E-mail addresses: mharada@m.tohoku.ac.jp (M. Harada), munemasa@math.is.tohoku.ac.jp (A. Munemasa).

http://dx.doi.org/10.1016/j.ffa.2016.07.004
1071-5797/

if $n \equiv 0 \pmod 4$. It is a fundamental problem to classify self-dual codes over GF(p) and determine the largest minimum weight among self-dual codes over GF(p) for a fixed length. Much work has been done towards classifying self-dual codes over GF(p) and determining the largest minimum weight among self-dual codes of a given length over GF(p) for $p = 2$ and 3 (see [16]).

Self-dual codes over GF(7) have been classified for lengths up to 12 (see [9]), and the largest minimum weight $d_7(n)$ among self-dual codes of length n over GF(7) has been determined for $n \leq 28$ (see [7, Table 2]). For example, it is known that $d_7(20) = 9$ and the extended quadratic residue code QR_{20} of length 20 over GF(7) is a self-dual $[20, 10, 9]$ code (see [5]).

There are 12 nonisomorphic 20-dimensional unimodular lattices having minimum norm 2 (see [3, Table 16.7]), and one of them is D_{20}^+. Let $A_7(C)$ denote the unimodular lattice obtained from a self-dual code C over GF(7) by Construction A.

In this paper, we convert the classification of self-dual $[20, 10, 9]$ codes C over GF(7) such that $A_7(C)$ is isomorphic to D_{20}^+ to that of skew-Hadamard matrices of order 20. The main aim of this paper is to give the following partial classification of self-dual $[20, 10, 9]$ codes over GF(7).

Theorem 1. *Up to equivalence, the extended quadratic residue code of length* 20 *over* GF(7) *is a unique self-dual* $[20, 10, 9]$ *code* C *over* GF(7) *such that* $A_7(C)$ *is isomorphic to* D_{20}^+.

All computer calculations in this paper were done with the help of Magma [1].

2. Preliminaries

In this section, we give definitions and notions on self-dual codes, unimodular lattices and skew-Hadamard matrices. Some basic facts on these subjects are also provided.

2.1. Self-dual codes

An $[n, k]$ *code* C over GF(p) is a k-dimensional subspace of GF$(p)^n$. The value n is called the *length* of C. The *weight* $\mathrm{wt}(x)$ of a vector $x \in \mathrm{GF}(p)^n$ is the number of non-zero components of x. A vector of C is called a *codeword* of C. The minimum non-zero weight of all codewords in C is called the *minimum weight* of C and an $[n, k]$ code with minimum weight d is called an $[n, k, d]$ code. The *weight enumerator* $W(C)$ of C is given by $W(C) = \sum_{i=0}^{n} A_i y^i$, where A_i is the number of codewords of weight i in C. The *dual code* $C^\perp$ of C is defined as

$$C^\perp = \{x \in \mathrm{GF}(p)^n \mid x \cdot y = 0 \text{ for all } y \in C\},$$