Finite Fields and Their Applications 55 (2019) 64–77

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Constructing self-orthogonal and Hermitian self-orthogonal codes via weighing matrices and orbit matrices

Dean Crnković, Ronan Egan, Andrea Švob *

Department of Mathematics, University of Rijeka, Radmile Matejčić 2, 51000 Rijeka, Croatia

A R T I C L E   I N F O

Article history:
Received 6 March 2018
Received in revised form 4 September 2018
Accepted 7 September 2018
Available online xxxx
Communicated by Dieter Jungnickel

MSC:
05B20
05B30
94B05
12E20

Keywords:
Weighing matrix
Orbit matrix
Hermitian self-orthogonal code

A B S T R A C T

We define the notion of an orbit matrix with respect to standard weighing matrices, and with respect to types of weighing matrices with entries in a finite field. In the latter case we primarily restrict our attention the fields of order 2, 3 and 4. We construct self-orthogonal and Hermitian self-orthogonal linear codes over finite fields from these types of weighing matrices and their orbit matrices respectively. We demonstrate that this approach applies to several combinatorial structures such as Hadamard matrices and balanced generalized weighing matrices. As a case study we construct self-orthogonal codes from some weighing matrices belonging to some well known infinite families, such as the Paley conference matrices, and weighing matrices constructed from ternary periodic Golay pairs.

* Corresponding author.

E-mail addresses: deanc@math.uniri.hr (D. Crnković), ronan.egan@math.uniri.hr (R. Egan), asvob@math.uniri.hr (A. Švob).

https://doi.org/10.1016/j.ffa.2018.09.002
1071-5797/

1. Introduction

In this paper we are concerned with constructing self-orthogonal codes from weighing matrices, and self-orthogonal or Hermitian self-orthogonal codes from types of weighing matrices with entries in $\mathbb{F}_q$ which we will call $\mathbb{F}_q$-weighing matrices. These generalize weighing matrices in that the entries are in any finite field $\mathbb{F}_q$, with the understanding that a weighing matrix with non-zero entries in $\{\pm 1\}$ can be considered an $\mathbb{F}_3$-weighing matrix under our convention. The conditions for existence are less restrictive than for generalized weighing matrices with non-zero entries in the multiplicative group of $\mathbb{F}_q$, but are sufficient for our construction of Hermitian self-orthogonal codes over $\mathbb{F}_q$ where $q \in \{2, 3, 4\}$. We then define and construct orbit matrices from these structures, which in turn leads to further self-orthogonal and Hermitian self-orthogonal codes. The introduction of $\mathbb{F}_q$-weighing matrices and use of orbit matrices in this manuscript are our main contributions, which build on the earlier work of Tonchev [19] where generalized weighing matrices are used to construct codes. We also present a construction of $\mathbb{F}_q$-weighing matrices based on ternary periodic Golay sequences, and in doing so we establish a link between the theory of orbit matrices, and compression of complementary sequences, discussed by Đoković and Kotsireas in [7].

It is well known that self-orthogonal codes have wide applications in communications (see e.g., [16]), including, for example, in secret sharing [4]. This is one of the key reasons why our interest is constructing Hermitian self-orthogonal codes, and not just in the minimum distance and error correcting properties of the codes constructed, as is often the primary motivation in coding theory. Where $q = 4$, we are particularly motivated by the construction of quantum-error-correcting codes (first discovered by Shor [18]) from Hermitian self-orthogonal linear $\mathbb{F}_4$ codes due to Calderbank et al. [3]. In particular, given a Hermitian self-orthogonal $[n, k]_4$ code C such that no codeword in $C^\perp \setminus C$ has weight less than d, one can construct a quantum $[[n, n-2k, d]]$ code, (see [3, Theorems 2, 3]). An outline of some applications to quantum codes is also presented in [19, Section 4]. Self-orthogonal and Hermitian self-orthogonal codes of length up to 29 and dimension up to 6 over $\mathbb{F}_3$ and $\mathbb{F}_4$ respectively, with the largest possible minimum distance, were classified in [2], and Hermitian self-dual [18, 9] codes over $\mathbb{F}_4$ for lengths up to 18, were classified in [10].

The paper is outlined as follows. In the next section we provide the relevant background information. In Section 3 we formally define $\mathbb{F}_q$-weighing matrices and demonstrate their usefulness for constructing self-orthogonal codes where $q \in \{2, 3, 4\}$. Following this we describe our construction using orbit matrices of weighing matrices (Section 4) and then generalize to $\mathbb{F}_q$-weighing matrices (Section 5), giving examples to demonstrate the construction in each case. We conclude with our construction of $\mathbb{F}_q$-weighing matrices via complementary sequences.

The codes constructed in this paper have been constructed and examined using Magma [1]. Minimum distances are compared to known codes and bounds at [9].