Finite Fields and Their Applications 52 (2018) 261–280

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Quasi-cyclic constructions of quantum codes ☆

Carlos Galindo [a], Fernando Hernando [a,*], Ryutaroh Matsumoto [b]

[a] *Instituto Universitario de Matemáticas y Aplicaciones de Castellón and Departamento de Matemáticas, Universitat Jaume I, Campus de Riu Sec., 12071 Castelló, Spain*

[b] *Department of Information and Communication Engineering, Nagoya University, Nagoya 464-8603, Japan*

A R T I C L E I N F O

Article history:
Received 20 December 2017
Received in revised form 16 April 2018
Accepted 17 April 2018
Available online 2 May 2018
Communicated by Arne Winterhof

MSC:
94B65
94B15
81P70

Keywords:
Quasi-cyclic codes
Trace
Symplectic
Hermitian and Euclidean duality
Quantum codes

A B S T R A C T

We give sufficient conditions for self-orthogonality with respect to symplectic, Euclidean and Hermitian inner products of a wide family of quasi-cyclic codes of index two. We provide lower bounds for the symplectic weight and the minimum distance of the involved codes. Supported in the previous results, we show algebraic constructions of good quantum codes and determine their parameters.

☆ Supported by the Spanish Ministry of Economy/FEDER: grants MTM2015-65764-C3-2-P and MTM2015-69138-REDT, the Universitat Jaume I: grant PB1-1B2015-02, and the JSPS grant: 26289116.

* Corresponding author.

E-mail addresses: galindo@uji.es (C. Galindo), carrillf@uji.es (F. Hernando), ryutaroh.matsumoto@nagoya-u.jp (R. Matsumoto).

https://doi.org/10.1016/j.ffa.2018.04.010

Introduction

Attention to quantum information processing, especially quantum computing, is rapidly growing, as several companies seem to be building quantum computers with many qubits [6]. One of the important theoretical techniques to realize quantum computation is the quantum error correction, which protects quantum memory and quantum computational process from noise.

Quantum error correction was proposed by Shor [22]. Its connection to classical error correction was mainly described in [5,3,4,10,24]. Afterwards that connection was generalized to the non-binary case (see [20,2,1]). Since then, the use of classical (error-correcting) codes has become one of standard methods for constructing quantum codes, see [15] for a survey.

Quasi-cyclic codes (QC codes) are a generalization of classical cyclic codes. It is well-known that there are asymptotically good codes attaining the Gilbert–Varshamov bound among QC codes [14,19], so it is natural to use QC codes to construct good quantum codes. Hagiwara et al. [12,13] studied constructions of quantum codes by QC LDPC codes. They focused on long codes and probabilistic constructions.

In this paper, we consider a wide class of QC codes of index 2 (see Subsections 1.2 and 1.3) and give sufficient conditions for their self-orthogonality with respect to symplectic, Euclidean and Hermitian inner products. Sections 2, 3 and 4 are devoted to the symplectic, Euclidean and Hermitian cases, respectively. In addition, we get lower bounds for the symplectic weight and the minimum distance of the involved codes. As a consequence, we provide an algebraic construction of short stabilizer quantum codes coming from the previously introduced QC codes (see Theorems 5, 13 and 16). To testify the interest of our construction, we complete this paper by showing several examples of quantum codes with good parameters. Indeed, we get quantum codes exceeding the Gilbert–Varshamov bounds [8,9,20] and/or improving the parameters of those codes which could be obtained by the CSS procedure from the best known linear codes under the assumption of being self-orthogonal.

1. Preliminaries

Throughout the paper, $\mathbb{F}_q$ will denote the finite field with q elements, q being a positive power p^r of a prime number p. Recall than an $[n, k, d]_q$ classical code is a linear space $C \subset \mathbb{F}_q^n$ of dimension k and minimum (Hamming) distance d. For a set $S \subset \mathbb{F}_q^n$, $w(S)$ will denote the minimum of the Hamming weights of those vectors in S.

In this section we review the existing connections between stabilizer quantum codes and classical codes, and the concept of quasi-cyclic (QC) code. We also introduce the class of QC codes we will use. Let us start explaining the mentioned connections.