Finite Fields and Their Applications 36 (2015) 98–120

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

New quantum codes from evaluation and matrix-product codes ☆

Carlos Galindo [a], Fernando Hernando [a,*], Diego Ruano [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 Mathematical Sciences, Aalborg University, Fredrik Bajers Vej 7G, 9220 Aalborg East, Denmark*

ARTICLE INFO

Article history:
Received 18 March 2015
Received in revised form 6 July 2015
Accepted 10 July 2015
Available online 4 August 2015
Communicated by Chaoping Xing

MSC:
94B27
81Q99
14R99

Keywords:
Quantum codes
Steane's enlargement
Affine variety codes
Subfield-subcodes
Matrix-product codes

ABSTRACT

Stabilizer codes obtained via the CSS code construction and the Steane's enlargement of subfield-subcodes and matrix-product codes coming from generalized Reed–Muller, hyperbolic and affine variety codes are studied. Stabilizer codes with good quantum parameters are supplied; in particular, some binary codes of lengths 127 and 128 improve the parameters of the codes in http://www.codetables.de. Moreover, non-binary codes are presented either with parameters better than or equal to the quantum codes obtained from BCH codes by La Guardia or with lengths that cannot be reached by them.

☆ Supported by the Spanish Ministry of Economy: grant MTM2012-36917-C03-03, the University Jaume I: grant PB1-1B2012-04 and the Danish Council for Independent Research: grant DFF-4002-00367.

* Corresponding author.
E-mail addresses: galindo@uji.es (C. Galindo), carrillf@uji.es (F. Hernando), diego@math.aau.dk (D. Ruano).

http://dx.doi.org/10.1016/j.ffa.2015.07.003
1071-5797/

1. Introduction

Quantum computers are based on the principles of quantum mechanics and use subatomic particles (qubits) to hold memory. The construction of efficient devices of this type would have important consequences as the breaking of some well-known cryptographical schemes [41]. Information on a recent attempt to built a quantum computer can be found in [2,43].

Despite quantum mechanical systems are very sensitive to disturbances and arbitrary quantum states cannot be replicated, error correction is possible [42]. In this paper we are concerned with stabilizer codes which are a class of quantum error-correcting codes. Parameters of our codes will be expressed as $[[n,k,d]]_q$, where q is a power p^r of a prime number p and r a positive integer. That means that our codes are q^k-dimensional linear subspaces of $\mathbb{C}^{q^n}$, $\mathbb{C}$ being the complex field, and d its minimum distance, which determines detection and correction of errors. A stabilizer code is called to be pure to a positive integer t whenever its stabilizer group does not contain non-scalar matrices with weight less than t (see, for instance, [30,29] for details).

Stabilizer codes can be derived from classical ones with respect to Symplectic or Hermitian inner product [7,3,1,29], although this can also be done with respect to Euclidean inner product by using the so-called CSS code construction [8,44]. The following results [29, Lemma 20 and Corollary 21] show the parameters of the stabilizer codes that one gets by using the above mentioned code construction. The reader can consult [29, Theorem 13] to see how stabilizer codes are obtained from classical ones.

Theorem 1. *Let C_1 and C_2 be two linear error-correcting block codes with parameters $[n,k_1,d_1]$ and $[n,k_2,d_2]$ over the field $\mathbb{F}_q$ and such that $C_2^\perp \subset C_1$, where $C_2^\perp$ stands for the dual code of C_2. Then, there exists an $[[n,k_1+k_2-n,d]]_q$ stabilizer code with minimum distance*

$$d = \min\left\{\mathrm{w}(c) \mid c \in (C_1 \setminus C_2^\perp) \cup (C_2 \setminus C_1^\perp)\right\},$$

which is pure to $\min\{d_1,d_2\}$, where $\mathrm{w}(c)$ denotes the weight of a word c.

Corollary 1. *Let C be a linear $[n,k,d]$ error-correcting block code over $\mathbb{F}_q$ such that $C^\perp \subset C$. Then, there exists an $[[n,2k-n,\geq d]]_q$ stabilizer code which is pure to d.*

Note that we use the symbol $\subset$ to indicate a subset, in particular $C \subset C$ holds. Next, we state the Hamada's generalization of the Steane's enlargement procedure [46] because it will be used in the paper. Given two suitable codes C and C', the code obtained by applying this procedure will be called their Steane's enlargement and denoted by $\mathrm{SE}(C,C')$.

Corollary 2. *(See [20].) Let C be an $[n,k]$ linear code over the field $\mathbb{F}_q$ such that $C^\perp \subset C$. Assume that C can be enlarged to an $[n,k']$ linear code C', where $k' \geq k+2$. Then, there*