J. Algebra Comb. Discrete Appl.
1(1) • 13-17
Received: 31 May 2014; Accepted: 3 August 2014
DOI 10.13069/jacodesmath.25090

Journal of Algebra Combinatorics Discrete Structures and Applications

# The existence of optimal quaternary $[28, 20, 6]$ and quantum $[[28, 12, 6]]$ codes

Research Article

**Vladimir D. Tonchev** *

Michigan Technological University, Houghton, Michigan 49931-1295, USA

**Abstract:** The existence of a quantum $[[28, 12, 6]]$ code was one of the few cases for codes of length $n \leq 30$ that was left open in the seminal paper by Calderbank, Rains, Shor, and Sloane [2]. The main result of this paper is the construction of the first optimal linear quaternary $[28, 20, 6]$ code which contains its Hermitian dual code and yields the first optimal quantum $[[28, 12, 6]]$ code.

**2010 MSC:** 94B05, 94B65, 81-99

**Keywords:** Quantum code, Optimal code

## 1. Introduction

We assume familiarity with the basics of classical and quantum error-correcting codes [2], [5].

The *Hermitian* inner product in $GF(4)^n$ is defined as

$$(x, y)_H = \sum_{i=1}^{n} x_i y_i^2, \tag{1}$$

while the *trace* inner product in $GF(4)^n$ is defined as

$$(x, y)_T = \sum_{i=1}^{n} (x_i y_i^2 + x_i^2 y_i). \tag{2}$$

A code $C$ is *self-orthogonal* if $C \subseteq C^{\perp}$, and *self-dual* if $C = C^{\perp}$. A linear code $C \subseteq GF(4)^n$ is self-orthogonal with respect to the trace product (2) if and only if it is self-orthogonal with respect to the Hermitian product (1) [2].

* *E-mail: tonchev@mtu.edu*

An *additive* $(n, 2^k)$ code $C$ over $GF(4)$ is a subset of $GF(4)^n$ consisting of $2^k$ vectors which is closed under addition. An additive code is *even* if the weight of every codeword is even, and otherwise *odd*. Note that an even additive code is trace self-orthogonal, and a linear self-orthogonal code is even [2]. If $C$ is an $(n, 2^k)$ additive code with weight enumerator

$$W(x, y) = \sum_{j=0}^{n} A_j x^{n-j} y^j, \tag{3}$$

the weight enumerator of the trace-dual code $C^\perp$ is given by

$$W^\perp = 2^{-k} W(x + 3y, x - y) \tag{4}$$

In their seminal paper [2], Calderbank, Rains, Shor and Sloane described a method for the construction of quantum error-correcting codes from additive codes that are self-orthogonal with respect to the trace product (2).

**Theorem 1.1.** *[2] An additive trace self-orthogonal $(n, 2^{n-k})$ code $C$ such that there are no vectors of weight $< d$ in $C^\perp \setminus C$ yields a quantum code with parameters $[[n, k, d]]$.*

A quantum code associated with an additive code $C$ is *pure* if the minimum distance of $C^\perp$ is $d$; otherwise, the code is called *impure*. A quantum code is called *linear* if the associated additive code $C$ is linear.

A table with lower and upper bounds on the minimum distance $d$ for quantum $[[n, k, d]]$ codes of length $n \leq 30$ is given in the paper by Calderbank, Rains, Shor and Sloane [2]. In particular, according to Table III on page 1382 in [2], the largest minimum distance $d$ of a known quantum $[[28, 12]]$ code is $d = 5$, while the best upper bound is $d \leq 6$. In the next section, we describe a simple construction of quaternary Hermitian self-orthogonal codes with parameters $[2n + 1, k + 1]$ and $[2n + 2, k + 2]$ from a given pair of Hermitian self-orthogonal $[n, k]$ codes. As an application of this construction, we find the first optimal quaternary linear $[28, 20, 6]$ which contains its dual code and hence yields the first optimal $[[28, 12, 6]]$ quantum code.

An extended version of Calderbank-Rains-Shor-Sloane table for quantum codes [2, Table III], as well as tables with bounds on the minimum distance of linear codes, was compiled by Grassl [4].

## 2. A doubling construction

**Lemma 2.1.** *Suppose that $C_i$ $(i = 1, 2)$ is a linear Hermitian self-orthogonal $[n, k]$ code over $GF(4)$ with generator matrix $G_i$, and $x^{(i)} \in C_i^\perp$ is a vector of odd weight.*

*(a) The code $C'$ with generator matrix*

$$G' = \left( \begin{array}{c|c|c} G_1 & G_2 & \begin{array}{c} 0 \\ \dots \\ 0 \end{array} \\ \hline x^{(1)} & 0 \ \dots \ 0 & 1 \end{array} \right) \tag{5}$$

*is a Hermitian self-orthogonal $[2n + 1, k + 1]$ code with dual distance*

$$d(C')^\perp \leq \min(d(C_{11}^\perp), d(C_2^\perp)), \tag{6}$$

*where $C_{11}$ is the code spanned by the rows of $G_{11}$ given by (7):*

$$G_{11} = \left( \begin{array}{c|c} G_1 & \begin{array}{c} 0 \\ \dots \\ 0 \end{array} \\ \hline x^{(1)} & 1 \end{array} \right). \tag{7}$$

*(b) The code $C''$ with generator matrix*

$$G'' = \left(\begin{array}{c|c|cc} & & 0 & 0 \\ G_1 & G_2 & \ldots & \\ & & 0 & 0 \\ \hline x^{(1)} & 0 \ \ldots \ 0 & 1 & 0 \\ \hline 0 \ \ldots \ 0 & x^{(2)} & 0 & 1 \end{array}\right) \tag{8}$$

*is a Hermitian self-orthogonal $[2n+2, k+2]$ code with dual distance*

$$d(C'')^{\perp} \le \min(d(C_{11}^{\perp}), d(C_{22}^{\perp})), \tag{9}$$

*where $C_{22}$ is the code spanned by the rows of $G_{22}$ given by (10):*

$$G_{22} = \left(\begin{array}{c|c} & 0 \\ G_2 & \ldots \\ & 0 \\ \hline x^{(2)} & 1 \end{array}\right). \tag{10}$$

**Proof**. The self-orthogonality of $C'$ and $C''$ follows from the fact that all rows of $G'$ and $G''$ have even weights, and every pair of rows of $G'$, as well as every pair of rows of $G''$, are pairwise orthogonal. Since the weight of $x^{(1)}$ (resp. $x^{(2)}$) is odd, $x^{(1)}$ does not belong to $C_1$, and $x^{(2)}$ does not belong to $C_2$, and that implies the dimensions of $C'$ and $C''$. The bounds (6), (9) on the dual distance follow trivially by the observation that every codeword of $C_{11}^{\perp}$ (resp. $C_{22}^{\perp}$) extends to a codeword of $(C')^{\perp}$ (resp $(C'')^{\perp}$) by filling in all remaining coordinates with zeros. □

It is worth mentioning that since $C_1$ and $C_2$ are self-orthogonal, their minimum distances are trivial upper bounds on the minimum dual distances $d(C')^{\perp}$ and $d(C'')^{\perp}$. For example, if $d(C_1) = 2$ then $d(C')^{\perp} \le 2$.

We note also that using codes $C_1$, $C_2$ with large minimum distances is a necessary, but not always sufficient condition for large dual distances $d(C')^{\perp}$ and $d(C'')^{\perp}$. For example, if $G_1 = G_2$ and $x^{(1)}$ is the all-one vector, then for every $1 \le i \le n$, the columns of (5) with indices $i$, $i+n$ and $2n+1$ determine a codeword of weight 3 in $(C')^{\perp}$.

These simple observations illustrate that one cannot expect a good general lower bound on $d(C')^{\perp}$ or $d(C'')^{\perp}$, and finding codes $C_1$, $C_2$ with appropriate generator matrices $G_1$, $G_2$ and vectors $x^{(1)}$, $x^{(2)}$ which lead to optimal dual distances $d(C')^{\perp}$ and $d(C'')^{\perp}$ is not a trivial task.

Using the connection to quantum codes described in Theorem 1.1, Lemma 2.1 implies the following.

**Corollary 2.2.** *The existence of quaternary Hermitian self-orthogonal $[n, k]$ codes $C_i$ ($i = 1, 2$) satisfying the assumptions of Lemma 2.1 implies the existence of a pure quantum linear $[[2n+1, 2n-2k-1, d']]$ code with $d' \le \min(d(C_{11}^{\perp}), d(C_2^{\perp}))$, and a pure quantum linear $[[2n+2, 2n-2k-2, d'']]$ code with $d'' \le \min(d(C_{11}^{\perp}), d(C_{22}^{\perp}))$.*

We will apply Lemma 2.1 and Corollary 2.2 to some self-orthogonal codes of length $n = 2k+1$ being shortened codes of extremal self-dual $[2k+2, k+1]$ codes, that is, self-dual codes having maximum possible minimum distance for the given code length.

**Example 2.3.** The matrix

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & \omega & \omega \\ 0 & 1 & \omega & \omega & 1 \end{pmatrix}$$

is the generator matrix of a self-orthogonal $[5, 2, 4]$ code $C_1$ over $GF(4) = \{0, 1, \omega, \omega^2\}$. The code $C_1$ is a shortened code of the unique (up to equivalence) self-dual $[6, 3, 4]$ code. Applying Lemma 2.1 with

$C_2 = C_1$, $G_2 = G_1$, and $x^{(1)} = x^{(2)}$ being the all-one vector of length 5, gives a self-orthogonal [11, 3] code $C'$ with dual distance 3 and a self-orthogonal [12, 4] code $C''$ with dual distance 4, which gives optimal quantum [[11, 5, 3]] and [[12, 4, 4]] codes respectively via Corollary 2.2.

**Example 2.4.** A pair of self-orthogonal [7, 3] codes obtained as shortened codes of the unique (up to equivalence) self-dual [8, 4, 4] code can be used to obtain optimal quantum [[15, 7, 3]] and [[16, 6, 4]] codes.

## 3. An optimal quantum [[28, 12, 6]] code

The smallest parameters of a self-dual quaternary linear code that yields a quantum code with minimum distance $d \geq 5$ via Corollary 2.2 are [14, 7, 6]. The only such code, up to equivalence, is the quaternary extended quadratic residue code $q_{14}$ [6, page 340]. We apply Lemma 2.1 using the pair of self-orthogonal [13, 6] codes $C_1$, $C_2$ generated by the following matrices:

$$G_1 = \begin{pmatrix} 0000100210233 \\ 3000010021023 \\ 3300001002102 \\ 2330000100210 \\ 0233000010021 \\ 1023300001002 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 0000113023002 \\ 2000011302300 \\ 0200001130230 \\ 0020000113023 \\ 3002000011302 \\ 2300200001130 \end{pmatrix},$$

where for convenience, the elements $\omega$ and $\omega^2$ of $GF(4)$ are written as 2 and 3 respectively. The matrices $G_1$, $G_2$ are circulant. The codes $C_1$, $C_2$ are cyclic and equivalent to a shortened code of $q_{14}$.

Choosing $x^{(1)} = x^{(2)}$ to be the all-one vector of length 13, we obtain the generator matrix $G'$ (5) of a self-orthogonal [27, 7] code $C'$ with dual distance 5, and the generator matrix $G''$ (8) of a self-orthogonal [28, 8] code with dual distance 6. The matrix $G''$ is available on line at

http://www.math.mtu.edu/~tonchev/gm28-8.html

By Corollary 2.2, $C'$ gives a pure optimal quantum [[27, 13, 5]] code, while $C''$ gives a pure optimal quantum [[28, 12, 6]] code.

An alternative geometric construction of a quantum code with the first parameters, [[27, 13, 5]], was given by the author in [7]. To the best of our knowledge, the quantum code with the second parameters, [[28, 12, 6]], is the first known quantum code with these parameters (a quantum [[28, 12, 5]] code was listed in [2]).

The weight distribution of the [28, 8] code $C''$ is given in Table 1.

The weight enumerator of the dual [28, 20] code $(C'')^{\perp}$ is

$$1 + 6240y^6 + 37128y^7 + 314223y^8 + 2044848y^9 + 11883768y^{10} + \ldots$$

We note that the code $(C'')^{\perp}$ is an optimal linear [28, 20, 6] quaternary code: 6 is the best theoretical upper bound on the minimum distance of a quaternary linear [28, 20] code. The largest minimum distance of any previously known [28, 20] code was 5 [3], [4].

## Acknowledgments

Magma [1] was used for some of the computations. This research was partially supported by NSA Grant H98230-12-0213. The author wishes to thank the unknown reviewers for noticing some typos and suggesting several improvements of the text layout and notation.

**Table 1.**

| $w$ | $A_w$ |
|---|---|
| 12 | 39 |
| 14 | 6 |
| 16 | 3198 |
| 18 | 9204 |
| 20 | 18213 |
| 22 | 22854 |
| 24 | 10569 |
| 26 | 1248 |
| 28 | 204 |

## References

[1] W. Bosma, J. Cannon, J, *Handbook of Magma Functions*, Department of Mathematics, University of Sydney, 1994.
[2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum error correction via codes over* $GF(4)$, IEEE Trans. Information Theory, 44(4), 1369-1387, 1998.
[3] A. E. Brouwer, *Tables of linear codes*, http://www.win.tue.nl/ aeb/.
[4] M. Grassl, http://www.codetables.de.
[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam 1977.
[6] G. Nebe, E. M. Rains, N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, Springer, Berlin, 2006.
[7] V. D. Tonchev, *Quantum codes from caps*, Discrete Math., 308, 6368-6372, 2008.