A doubling construction for self-orthogonal codes

Vladimir D. Tonchev
Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan 49931, USA, tonchev@mtu.edu

Abstract
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 self-orthogonal \([n, k]\) codes, and its link to quantum codes is considered. As an application, an optimal quaternary linear \([28, 12, 6]\) dual containing code is found that yields a new optimal \([[28, 12, 6]]\) quantum code.

Key words: hermitian self-orthogonal code, quantum code
1991 MSC: 94B.

1 Introduction

We assume familiarity with the basics of classical error-correcting codes [1].

The hermitian inner product in \(GF(4)^n\) is defined as

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

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

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

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].
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 \textit{even} if the weight of every codeword is even, and otherwise \textit{odd}. Note that an even additive code is trace self-orthogonal, and a linear self-orthogonal code is even \cite{2}. If \(C\) is an \((n, 2^k)\) additive code with weight enumerator

\[ W(x, y) = \sum_{j=0}^{n} A_j x^{n-j} y^j, \]  

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

\[ W^\perp = 2^{-k} W(x + 3y, x - y) \]  

In \cite{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 \cite{2}.

**Theorem 1** \cite{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 \textit{pure} if there are no vectors of weight \(< d\) in \(C^\perp\); otherwise, the code is called \textit{impure}. A quantum code is called \textit{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 \cite{2}. An extended version of this table was compiled by Grassl \cite{3}. Bounds on the minimum distance of linear codes are available online at [http://www.codetables.de](http://www.codetables.de).

## 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

$$G' = \begin{pmatrix} G_1 & G_2 & \ldots \\ 0 & 0 & \ldots \\ x^{(1)} & 0 & \ldots & 0 & 1 \end{pmatrix}$$

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

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

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

$$G_{11} = \begin{pmatrix} 0 \\ G_1 & \ldots \\ 0 \\ x^{(1)} \end{pmatrix}.$$

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

$$G'' = \begin{pmatrix} G_1 & G_2 & \ldots \\ 0 & 0 & \ldots \\ x^{(1)} & 0 & \ldots & 0 & 1 & 0 \\ 0 & \ldots & 0 & x^{(2)} & 0 & 1 \end{pmatrix}$$

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

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

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

$$G_{22} = \begin{pmatrix} 0 \\ G_2 & \ldots \\ 0 \\ x^{(2)} \end{pmatrix}.$$

**Proof.** The self-orthogonality of $C'$ and $C''$ follows from the fact that all rows of $G'$ and $G''$ have even weights, and every two rows of $G'$, as well as every two
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 $C_1^\perp$ (resp. $C_2^\perp$) extends to a codeword of $(C')^\perp$ (resp $(C'')^\perp$) by filling in all remaining coordinates with zeros. □

Using the connection to quantum codes described in Theorem 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 $d' \leq \min(d(C_1^\perp), d(C_2^\perp))$, and a pure quantum linear $[[2n + 2, 2n - 2k - 2, d'']]$ code with $d'' \leq \min(d(C_1^\perp), d(C_2^\perp))$.

We will apply Lemma 2.1 and its Corollary 2.2 to some self-orthogonal codes of length $n = 2k + 1$ being shortened codes of self-dual $[2k + 2, k + 1]$ codes.

For example, the matrix

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

is the generator matrix of a self-orthogonal $[5, 2, 4]$ code $C_1$ over $GF(4) = \{0, 1, \alpha, \alpha^2\}$. 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 give optimal quantum $[[11, 5, 3]]$ and $[[12, 4, 4]]$ codes respectively via Corollary 2.2.

Similarly, 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.

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 $q_{14}$ [5, 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:

\[
G_1 = \begin{pmatrix}
0000100210233 \\
3000010021023 \\
3300010021023 \\
2330001002102 \\
023300010021 \\
102330001002 \\
\end{pmatrix}, \quad
G_2 = \begin{pmatrix}
0000113023002 \\
200001130230 \\
020000113023 \\
300200011302 \\
230020001130 \\
230020001130 \\
\end{pmatrix},
\]

where for convenience, the elements $\alpha$ and $\alpha^2$ 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 $G'$ of a self-orthogonal $[27, 7]$ code $C'$ with dual distance 5, and the generator matrix $G''$ of a self-orthogonal $[28, 8]$ code with dual distance 6. The matrix $G''$ is available on line at

\protect\texttt{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 [6]. To the best of our knowledge, the quantum code with the second parameters, $[[28, 12, 6]]$, is new (a quantum $[[28, 12, 5]]$ code was listed in [2]).

The weight distribution of the $[28, 8]$ code $C''$ is given in Table 2.3

\begin{table}[h]
\centering
\caption{Weight distribution of the $[28, 8]$ code $C''$}
\begin{tabular}{c c c c}
\hline
Weight & Frequency \\
\hline
0 & 1 \\
1 & 28 \\
2 & 70 \\
3 & 126 \\
4 & 156 \\
5 & 105 \\
6 & 42 \\
7 & 12 \\
8 & 2 \\
\hline
\end{tabular}
\end{table}
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 $[28, 8, 6]$ quaternary code: 6 is the largest possible minimum distance of a quaternary linear $[28, 8]$ code [3].

3 Acknowledgments

Magma [1] was used for some of the computations. The author wishes to thank the unknown referee for noticing some typos and discrepancies that were subsequently corrected.

References

[1] Bosma, W., 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 (1998), 1369-1387.

[3] M. Grassl, http://www.codetables.de

[4] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam 1977.
[5] G. Nebe, E. M. Rains, N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, Springer, Berlin, 2006.

[6] V.D. Tonchev, Quantum codes from caps, *Discrete Math.*, **308** (2008), 6368-6372.