New quantum codes constructed from some self-dual additive $\mathbb{F}_4$-codes

Masaaki Harada*

June 1, 2018

Abstract

For $(n, d) = (66, 17), (78, 19)$ and $(94, 21)$, we construct quantum $[[n, 0, d]]$ codes which improve the previously known lower bounds on the largest minimum weights among quantum codes with these parameters. These codes are constructed from self-dual additive $\mathbb{F}_4$-codes based on pairs of circulant matrices.

Keywords: quantum code, self-dual additive $\mathbb{F}_4$-code, minimum weight, circulant matrix

1 Introduction

Let $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$ be the finite field of order 4, where $\bar{\omega} = \omega^2 = \omega + 1$. An additive $\mathbb{F}_4$-code $C$ of length $n$ is an additive subgroup of $\mathbb{F}_4^n$. An additive $(n, 2^k)$ $\mathbb{F}_4$-code is an additive $\mathbb{F}_4$-code of length $n$ with $2^k$ codewords. The weight $wt(x)$ of a vector $x \in \mathbb{F}_4^n$ is the number of non-zero components of $x$. The minimum non-zero weight of all codewords in $C$ is called the minimum weight of $C$. The dual code $C^*$ of the additive $\mathbb{F}_4$-code $C$ of length $n$ is defined as $\{x \in \mathbb{F}_4^n \mid x \ast y = 0 \text{ for all } y \in C\}$ under the trace inner product $x \ast y = \sum_{i=1}^{n} (x_i y_i^2 + x_i^2 y_i)$ for $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_4^n$. An additive $\mathbb{F}_4$-code $C$ is called self-orthogonal (resp. self-dual) if $C \subset C^*$ (resp. $C = C^*$).

*Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan. email: mharada@m.tohoku.ac.jp.
A useful method for constructing quantum codes from self-orthogonal additive $\mathbb{F}_4$-codes was given by Calderbank, Rains, Shor and Sloane [2] (see [2] for undefined terms concerning quantum codes). A self-orthogonal additive $(n, 2^{n-k}) \mathbb{F}_4$-code $C$ such that there is no vector of weight less than $d$ in $C^* \setminus C$, gives a quantum $[[n, k, d]]$ code, where $k \neq 0$. A self-dual additive $\mathbb{F}_4$-code of length $n$ and minimum weight $d$ gives a quantum $[[n, 0, d]]$ code. Let $d_{\text{max}}(n, k)$ denote the largest minimum weight $d$ among quantum $[[n, k, d]]$ codes. It is a fundamental problem to determine $d_{\text{max}}(n, k)$. A table on $d_{\text{max}}(n, k)$ is given in [2, Table III] for $n \leq 30$. An extended table is obtained electronically from [4].

The main aim of this note is to show the following:

**Theorem 1.** There is a quantum $[[n, 0, d]]$ code for $(n, d) = (66, 17)$, $(78, 19)$ and $(94, 21)$.

The above quantum $[[n, 0, d]]$ codes are constructed from self-dual additive $\mathbb{F}_4$-codes of length $n$ and minimum weight $d$ for the above $(n, d)$. These quantum codes improve the previously known lower bounds on $d_{\text{max}}(n, 0)$ for the above $n$.

All computer calculations in this note were done with the help of MAGMA [1].

## 2 Self-dual additive $\mathbb{F}_4$-codes and graphs

### 2.1 Self-dual additive $\mathbb{F}_4$-codes and graphs

A graph $\Gamma$ consists of a finite set $V$ of vertices together with a set of edges, where an edge is a subset of $V$ of cardinality 2. All graphs in this note are simple, that is, graphs are undirected without loops and multiple edges. The adjacency matrix of a graph $\Gamma$ with $V = \{x_1, x_2, \ldots, x_v\}$ is a $v \times v$ matrix $A = (a_{ij})$, where $a_{ij} = 1$ if $\{x_i, x_j\}$ is an edge and $a_{ij} = 0$ otherwise.

Let $\Gamma$ be a graph and let $A_\Gamma$ be an adjacency matrix of $\Gamma$. Let $C(\Gamma)$ denote the additive $\mathbb{F}_4$-code generated by the rows of $A_\Gamma + \omega I$, where $I$ denotes the identity matrix. Then $C(\Gamma)$ is self-dual [3]. In addition, it was shown in [3] that for any self-dual additive $\mathbb{F}_4$-code $C$, there is a graph $\Gamma$ such that $C(\Gamma)$ is equivalent to $C$ (see [2] for the definition of equivalence of codes). Hence, for constructing self-dual additive $\mathbb{F}_4$-codes, it is sufficient to consider only matrices $A + \omega I$, where $A$ are symmetric $(1, 0)$-matrices with the diagonal entries 0. Using this, a classification of self-dual additive $\mathbb{F}_4$-codes was done for lengths up to 12 [3, Section 5].
2.2 Self-dual additive $\mathbb{F}_4$-codes based on circulant matrices

An $n \times n$ matrix is circulant if it has the following form:

$$
\begin{pmatrix}
  r_0 & r_1 & \cdots & r_{n-2} & r_{n-1} \\
  r_{n-1} & r_0 & \cdots & r_{n-3} & r_{n-2} \\
  r_{n-2} & r_{n-1} & \cdots & r_{n-4} & r_{n-3} \\
  \vdots & \vdots & \cdots & \vdots & \vdots \\
  r_1 & r_2 & \cdots & r_{n-1} & r_0 \\
\end{pmatrix}
$$

In [5] and [7], self-dual additive $\mathbb{F}_4$-codes of length $n$ having generator matrices $A + \omega I$ were considered for symmetric circulant matrices $A$ with the diagonal entries 0. In this note, we concentrate on (adjacency) matrices of the following form:

$$
M(A, B) = \begin{pmatrix} A & B \\ B^T & A \end{pmatrix},
$$

where $A$ are $n \times n$ symmetric circulant $(1,0)$-matrices with the diagonal entries 0 and $B$ are $n \times n$ circulant $(1,0)$-matrices. Then we define self-dual additive $\mathbb{F}_4$-codes $C(A, B)$ of length $2n$ having generator matrices $M(A, B) + \omega I$, where $M(A, B)$ have the form \((1)\). We remark that a different method for constructing self-dual additive $\mathbb{F}_4$-codes based on pairs of circulant matrices was given in [6].

A self-dual additive $\mathbb{F}_4$-code is called Type II if it is even. It is known that a Type II additive $\mathbb{F}_4$-code must have even length. A self-dual additive $\mathbb{F}_4$-code, which is not Type II, is called Type I. Although the following proposition is somewhat trivial, we give a proof for completeness.

**Proposition 2.** Let $C(A, B)$ be a self-dual additive $\mathbb{F}_4$-code of length $2n$ generated by the rows of $M(A, B) + \omega I$. Let $r_A$ and $r_B$ denote the first rows of $A$ and $B$, respectively.

1) Suppose that $n$ is even. Then $C(A, B)$ is Type II if and only if $w + \text{wt}(r_B)$ is odd, where $w$ denotes the weight of the $(n/2 + 1)$st coordinate of $r_A$.

2) Suppose that $n$ is odd. Then $C(A, B)$ is Type II if and only if $\text{wt}(r_B)$ is odd.
Proof. Let $\Gamma$ be the graph with adjacency matrix $M(A,B)$. Since $A$ and $B$ are circulant, the degrees of the vertices of $\Gamma$ are equal to $\text{wt}(r_A) + \text{wt}(r_B)$. By Theorem 15 in [3], the codes $C(A,B)$ are Type II if and only if all the vertices of $\Gamma$ have odd degree. Since $A$ is symmetric, $\text{wt}(r_A) \equiv w \pmod{2}$ if $n$ is even, and $\text{wt}(r_A)$ is even if $n$ is odd. The results follow.

3 Self-dual additive $\mathbb{F}_4$-codes $C(A, B)$

For lengths $n = 14, 16, \ldots, 40$, by exhaustive search, we found all distinct self-dual additive $\mathbb{F}_4$-codes $C(A, B)$ with generator matrices $M(A, B) + \omega I$. Then we determined the largest minimum weight $d_{\text{max}}(n)$ among all self-dual additive $\mathbb{F}_4$-codes $C(A, B)$ for these lengths. This computation was done by the MAGMA function MinimumWeight. We denote by $d_{\text{max}}(n)$ the largest minimum weight among all self-dual additive $\mathbb{F}_4$-codes $C(A, B)$ of length $n$. In Table 1 we list the values $d_{\text{max}}(n)$ for $n = 14, 16, \ldots, 40$. Our present state of knowledge about $d_{\text{max}}(n, 0)$ is also listed in the table. For these lengths, the self-dual additive $\mathbb{F}_4$-codes give quantum $[[n, 0, d]]$ codes such that $d = d_{\text{max}}(n, 0)$ or $d$ attains the known lower bound on $d_{\text{max}}(n, 0)$ by the method in [2]. An example of self-dual additive $\mathbb{F}_4$-codes $C(A, B)$ with minimum weight $d_{\text{max}}(n)$ is given in Table 2, where the supports $\text{supp}(r_A)$ (resp. $\text{supp}(r_B)$) of the first rows of matrices $A$ (resp. $B$) are listed. By Proposition 2 $C_{n,I}$ are Type I ($n = 16, 18, \ldots, 28, 32, 34, 40$), and $C_{n,II}$ are Type II ($n = 14, 16, \ldots, 40$). Our computer search shows that the largest minimum weights among all Type I self-dual additive $\mathbb{F}_4$-codes of lengths $14, 30, 36$ and $38$ are $5, 9, 11$ and $11$, respectively.

As described above, self-dual additive $\mathbb{F}_4$-codes having generator matrices $A + \omega I$ were considered for circulant matrices $A$ with the diagonal entries $0$ [5] and [7]. The largest minimum weight $d'_{\text{max}}(n)$ among such codes was determined for lengths up to $50$ [5] and [7]. The values $d_{\text{max}}(n)$ and $d'_{\text{max}}(n)$ are also listed in Table 1 to compare the values $d_{\text{max}}(n)$ and $d'_{\text{max}}(n)$. We remark that $d_{\text{max}}(36) > d'_{\text{max}}(36)$.

4 New self-dual additive $\mathbb{F}_4$-codes

For lengths $n \geq 41$, by non-exhaustive search, we tried to find self-dual additive $\mathbb{F}_4$-codes $C(A, B)$ with large minimum weight.
The self-dual additive $\mathbb{F}_4$-code $C_{66} = C(A, B)$ is defined as the code with generator matrix $M(A, B) + \omega I$, where the supports $\text{supp}(r_A)$ and $\text{supp}(r_B)$ are as follows:

\begin{align*}
\{2, 3, 4, 5, 6, 8, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 27, 29, 30, 31, 32, 33\}, \\
\{3, 4, 5, 8, 10, 11, 12, 16, 20, 21, 25, 26, 28, 29, 30, 33\},
\end{align*}

respectively. We verified that $C_{66}$ has minimum weight 17. This computation was done by the MAGMA function `MinimumWeight`. We also verified that $C_{66}$ has no codeword of weight less than 17, by using the MAGMA function `VerifyMinimumWeightUpperBound`. Hence, we have the following:

**Proposition 3.** There is a self-dual additive $\mathbb{F}_4$-code of length 66 and minimum weight 17.

Let $A_i(C)$ denote the number of codewords of weight $i$ in a self-dual additive $\mathbb{F}_4$-code $C$. By the MAGMA function `NumberOfWords`, we have

\begin{align*}
A(C_{66})_0 &= 1, A(C_{66})_1 = \cdots = A(C_{66})_{16} = 0, A(C_{66})_{17} = 3168, \\
A(C_{66})_{18} &= 36003, A(C_{66})_{19} = 273174, A(C_{66})_{20} = 1924626.
\end{align*}
The self-dual additive $\mathbb{F}_4$-code $C_{78} = C(A, B)$ is defined as the code with generator matrix $M(A, B) + \omega I$, where the supports $\text{supp}(r_A)$ and $\text{supp}(r_B)$ are as follows:

\{2, 4, 6, 8, 9, 10, 11, 13, 15, 19, 22, 26, 28, 30, 31, 32, 33, 35, 37, 39\},
\{2, 4, 6, 8, 9, 15, 17, 18, 19, 21, 25, 26, 27, 28, 29, 30, 32, 33, 36, 37\},

respectively. We verified that $C_{78}$ has minimum weight 19. This computation was done by the MAGMA function $\text{MinimumWeight}$. We also verified that $C_{78}$ has no codeword of weight less than 19, by using the MAGMA function $\text{VerifyMinimumWeightUpperBound}$. Hence, we have the following:

**Proposition 4.** There is a self-dual additive $\mathbb{F}_4$-code of length 78 and minimum weight 19.
By the MAGMA function \texttt{NumberOfWords}, we have

\[ A(C_{78})_0 = 1, A(C_{78})_1 = \cdots = A(C_{78})_{18} = 0, \]
\[ A(C_{78})_{19} = 2808, A(C_{78})_{20} = 24336. \]

The self-dual additive $\mathbb{F}_4$-code $C_{94} = C(A, B)$ is defined as the code with generator matrix $M(A, B) + \omega I$, where the supports $\text{supp}(r_A)$ and $\text{supp}(r_B)$ are as follows:

\[
\{2, 6, 7, 10, 11, 12, 16, 18, 19, 20, 29, 30, 31, 33, 37, 38, 39, 42, 43, 47\}, \\
\{2, 4, 9, 12, 13, 14, 16, 17, 21, 22, 24, 25, 26, 30, 31, 34, 35, 37, 38, 39, 40, 46\},
\]

respectively. We verified that $C_{94}$ has minimum weight 21, by using the MAGMA function \texttt{MinimumWeight}. We also verified that $C_{94}$ has no codeword of weight less than 21, by using the MAGMA function \texttt{VerifyMinimumWeightUpperBound}. We verified that $C_{94}$ has minimum weight 21. Hence, we have the following:

\textbf{Proposition 5.} There is a self-dual additive $\mathbb{F}_4$-code of length 94 and minimum weight 21.

Finally, by the method in [2], Propositions 3, 4 and 5 yield Theorem 1. The quantum $[[n, 0, d]]$ codes described in Theorem 1 improve the previously known lower bounds on $d_{\text{max}}(n, 0)$ ($n = 66, 78$ and $94$). More precisely, we give our present state of knowledge about $d_{\text{max}}(n, 0)$:

\[ 17 \leq d_{\text{max}}(66, 0) \leq 24, \]
\[ 19 \leq d_{\text{max}}(78, 0) \leq 28, \]
\[ 21 \leq d_{\text{max}}(94, 0) \leq 32. \]

\textbf{Acknowledgment.} This work was supported by JSPS KAKENHI Grant Number 15H03633.

\textbf{References}

[1] W. Bosma, J. Cannon and C. Playoust. The Magma algebra system I: The user language, \textit{J. Symbolic Comput.} \textbf{24} (1997), 235–265.
[2] A.R. Calderbank, E.R. Rains, P.W. Shor and N.J.A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inform. Theory* **44** (1998), 1369–1387.

[3] L.E. Danielsen and M.G. Parker, On the classification of all self-dual additive codes over GF(4) of length up to 12, *J. Combin. Theory Ser. A* **113** (2006), 1351–1367.

[4] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Online available at [http://www.codetables.de](http://www.codetables.de) Accessed on 2017-04-14.

[5] M. Grassl and M. Harada, New self-dual additive $\mathbb{F}_4$-codes constructed from circulant graphs, *Discrete Math.* **340** (2017), 399–403.

[6] T.A. Gulliver and J.-L. Kim, Circulant based extremal additive self-dual codes over GF(4), *IEEE Trans. Inform. Theory* **50** (2004), 359–366.

[7] Z. Varbanov, Additive circulant graph codes over GF(4), *Math. Maced.* **6** (2008), 73–79.