Entanglement-assisted Quantum Codes of Distance Four Constructed from Caps in $PG(5,4)$ and $PG(6,4)$

Qiang Fu, Ruihu Li, Gen Xu, Luobin Guo

College of Science, Air Force Engineering University, Xi' an, 710051, China
llzsy110@163.com

Abstract - The entanglement-assisted (EA) formalism is a generalization of the standard stabilizer formalism, and it can transform classical linear quaternary codes into entanglement-assisted quantum error correcting codes (EAQECCs) by using of shared entangled qubits between the sender and the receiver. In this work, we give elementary recursive constructions of special quaternary codes of length n and dual distance four that constructed from known caps in projective space PG(5,4) and PG(6,4) for all length $6 \le n \le 283$. Consequently, good maximal entanglement EAQECCs of minimum distance four for such length n are constructed from the obtained quaternary codes.

Index Terms - EAQECCs, maximal entanglement, quaternary code, cap.

1. Introduction

Quantum error correcting codes (QECCs) are powerful tools for fighting against noise in quantum computation and quantum communication [1-2]. The most widely studied class of quantum codes are stabilizer (or additive) quantum codes, binary or non-binary. Under the stabilizer formalism [3-4], binary stabilizer codes can be constructed from classical codes over finite binary field F_2 or quaternary field F_4 with certain self-orthogonal (or dual containing) properties. The self-orthogonal properties form a barrier to import all classical codes into QECCs [5]. In 2006, Brun, Devetak and Hsieh devised the entanglement-assisted (EA) stabilizer formalism to break through this restriction [5], the EA-stabilizer formalism includes the standard stabilizer formalism as a special case. They showed that if shared entanglement between the encoder and decoder is available, classical linear quaternary (and binary) codes that are not self-orthogonal can be transformed into EAQECCs [5-6].

An $[[n,k,d_{ea};c]]$ EAQECC encodes k information qubits into n channel qubits with the help of c pairs of maximally-entangled Bell states. The code can correct up to $\lfloor (d_{ea}-1)/2 \rfloor$ errors acting on the n channel qubits, where d_{ea} is the minimum distance of the code. If $c=0$, then an $[[n,k,d_{ea};c]]$ EAQECC is a standard quantum code and is usually denoted as $[[n,k,d]]$. In [6-8], Lai *et. al.* discussed the construction of optimal EAQECCs. An $[[n,k,d_{ea};c]]$ EAQECC is optimal in the sense that d_{ea} is the highest achievable minimum distance for given parameters n, k and c. In [7], they showed that the maximal entanglement EAQECCs can achieve the EA-hash bound asymptotically, and constructed many optimal maximal entanglement EAQECCs with length no more than 15.

Cap is an important object of projective geometry, each cap in $PG(r,q)$ will determine two $q-$ary linear codes [8-9]. In [9], caps in $PG(r,4)$ were used to construct good QECCs of distance four. In [10], we use caps in $PG(r,4)$ for $r \le 4$ to construct optimal EAQECCs of length no more than 37. In this work, we will discuss the construction of caps with special character in $PG(5,4)$ and $PG(6,4)$, each of these caps can result in an maximal entanglement EAQECC of distance four.

We structure our work as follows. Section 2 reviews some basic concepts on linear codes, quaternary cap and maximal entanglement EAQECCs. Section 3 and 4 give explicit constructions of caps with special character in $PG(5,4)$ and $PG(6,4)$, and construct maximal entanglement EAQECCs deduced from caps that we have obtained. Section 5 discusses the constructed EAQECCs and draws a final remark.

2. Preliminaries

In this section we introduce some basic knowledge on linear codes, caps and maximal entanglement EAQECCs. Let $F_4=\{0,1,\omega,\bar{\omega}\}$ be the finite field with four elements, where $\omega^2=\bar{\omega}$, $\bar{\omega}^2=\omega$, and $\omega^3=1$. The conjugate is defined as $\bar{x}=x^2$ for all elements $x \in F_4$. Let F_4^n be the n- dimensional vector space over F_4. A k- dimensional subspace C of F_4^n is called a k- dimensional linear code of length n, and is denoted by $C=[n,k]_4$. If the minimum distance is d, then it is denoted by $C=[n,k,d]_4$.

For $x, y \in F_4$, their Hermitian inner product is

$$(x,y)_h = x_1\bar{y}_1 + x_2\bar{y}_2 + ... + x_n\bar{y}_n = \sum_{i=1}^{n} x_i y_i^2 .$$

The dual of $C=[n,k]_4$ is $C^{\perp h}=\{x \mid (x,y)_h=0 \ , \forall\, y \in C\}$, and $C^{\perp h}=[n,n-k]_4$.

An $n-$cap K in $PG(k-1,4)$ is a set of n points, no three of which are collinear. If we write the n points as columns of a matrix, we obtain a matrix $\boldsymbol{K}$ of size $k \times n$ such that every set of three columns is linearly independent, and we usually call $\boldsymbol{K}$ an cap, hence the code with check matrix $\boldsymbol{K}$ is an $[n,n-k,\ge 4]_4$. We call the code with generator matrix $\boldsymbol{K}$ cap code, this cap code is an $[n,k]_4$ code. If G is a sub-matrix of a cap matrix $\boldsymbol{K}$, which is formed by some columns of $\boldsymbol{K}$, then G is also a cap.

Definition 1 Let $G_m=(\alpha_1,\alpha_2,...,\alpha_m)$ be an $m-$ cap in

$PG(k-1,4)$, and denote $N_m = \{1,2,...,m\}$. If $J=\{j_1,j_2,...,j_s\}\subset N_m$ then $G_J = (\alpha_{j_1},\alpha_{j_2},...,\alpha_{j_s})$ is also an $s-$cap, and is called a sub-cap of G_m with index set J.

An $[[n,k,d;c]]$ is called an maximal entanglement EAQECC if $k+c=n$. According to [11], for linear code $C=[n,m,d]_4$, $C^{\perp h}$ EA stabilizes an $[[n,\ 2m+c-n,\ d;\ c]]$, where $c=rank(HH^{\dagger})$, H is a check matrix of C and $H^{\dagger}$ is the conjugate transpose of H. From this, one can deduce the following:

Lemma 1 If K is a $n-$cap in $PG(k-1,4)$ such that $k=rank(KK^{\dagger})$, the code of K EA stabilizes an $[[n,n-k,\ d\geq 4;k]]$ maximal-entanglement EAQECC.

In the following two sections, we will try to construct sub-caps satisfying Lemma 1 from known caps, then derive $[[n,n-k,d\geq 4;k]]$ maximal entanglement EAQECCs. To simplify statements, in each cap or matrix, we use 2 and 3 to represent ω and $\bar{\omega}$, respectively. And, let $1_m=(1,1,\cdots,1)$ and $0_m=(0,0,\cdots,0)$ be the all one vector and the all zero vector of length m, respectively. $C=[n,m,d]_4$ is denoted as $C=[n,\ m,d]$.

3. EAQECCs constructed from caps in $PG(5,4)$

To construct an $[[n,n-6,4;6]]$ maximal entanglement EAQECCs, due to Lemma 1, we should firstly construct an $C=[n,n-6,\ 4]$ classical code.

A. *Construction of 126-cap*

Firstly we use one 30-cap in $PG(4,4)$ [12] as follows.

Let

$$H_{5\times 30}=\begin{pmatrix}
111111111111111111111111111111\\
231213002312310023123100322113\\
000000232323231212121213131313\\
112233001122330011223300112233\\
000000111111112222222233333333
\end{pmatrix},$$

$$B=\begin{pmatrix}H_{5\times 30}\\ 0_{30}\end{pmatrix}.$$

We use random algorithm for constructing a 126-cap from the matrix B. We choose any two column vectors of B, delete the vector in $PG(5,4)$, which is collinear with these two column vectors in B. Then add a column left to B, in this way, we can obtain one matrix $H_{6\times 126}=[B|H_2|H_3|H_4]$ that generates a 126-cap, where

$$H_2=\begin{pmatrix}
111111111111111111111111111111\\
231213112321132232213133232213123\\
112233232323231212121213131333\\
112233001122330011223300112233 11\\
000000111111112222222233333333 00\\
111111111111111111111111111111 22
\end{pmatrix}$$

$$H_3=\begin{pmatrix}
111111111111111111111111111111\\
121333321213112321132223121323 12\\
112223232323121212121313131322 33\\
223300112233001122330011223311 22\\
000011111111222222223333333300 00\\
222222222222222222222222222333 33
\end{pmatrix}$$

$$H_4=\begin{pmatrix}
111111111111111111111111111000000\\
132232213133321213113212311111 11\\
112323232312121212131313231213\\
330011223300112233001122330000000\\
001111111122222222333333330000 00\\
333333333333333333333333333112233
\end{pmatrix}$$

This cap has the same weight polynomial as that of the 126-cap given in [8].

B. *Permutation on 126-cap*

Although this matrix generates one 126-cap, but as our demand is to seek for a matrix $H_{6\times 126}$ that generates a 126-cap, at the same time that by selecting the first n column vectors, the sub-matrix $H_{6\times n}$ of $H_{6\times 126}$ also satisfies: $rank(H_{6\times n}H_{6\times n}^{\dagger})\geq 5$ ($6\leq n\leq 63$). So we use permutation on the above matrix $H_{6\times 126}$, and we get a desired cap as $G_{126}=[H_1'|H_2'|H_3'|H_4']$, where

$$H_1'=\begin{pmatrix}
111111111111111111111111011011101\\
312232310211110131312222121132313\\
120111131111132221330123222231331\\
301212020232300310122220230310 03\\
320232312302331122310010010101 02\\
120132130030230202110233112212 10
\end{pmatrix}$$

$$H_2'=\begin{pmatrix}
111111111111111111111111110111111\\
333210310233222103323331311311 22\\
211333113213211210232331120222 21\\
111230330111110201310312102130 21\\
223313231001122130101110200021 22\\
230230100311101200322102110301 32
\end{pmatrix}$$

$$H_3'=\begin{pmatrix}
111111111101111111111111111111111\\
211222322111011131332121312122 21\\
211123233013233122313331211213 22\\
130000121303030233301222321212 13\\
123311101001231220323013133231 22\\
023233333020011332230303021222 31
\end{pmatrix}$$

$$H_4'=\begin{pmatrix}
111110111111111111111111111111\\
211221133123332312313223233311\\
233221333313223112323330312222\\
023120233320312332121113033022\\
233210330033213322013130300202\\
103113101111223330202230232311
\end{pmatrix}$$

C. Construction of sub-cap of the 126-cap G_{126}

If $6 \le n \le 63$ and $n \ne 12, 16, 33, 35, 41, 44, 50, 55, 61$, let $I_n = \{1, ..., n\}$ .If $n = 12, 16, 35, 41, 44, 45$, let $I_n = \{1, ..., n-1, n+2\}$. For $n = 50, 61$, define $I_n = \{1, 2, ..., n-1, n+3\}$. And, define $I_{33} = \{1, 2, ..., 32, 37\}$. For $64 \le n \le 120$, define $J_n = \{1, 2, ..., 126\} \setminus I_{n'}$, where $n' = 126 - n$ and with $6 \le n' \le 63$. For $6 \le n \le 63$, denote G_{I_n} be the cap with index set I_n , and for $64 \le n \le 120$, denote G_{J_n} be the sub-cap of G_{126} with index set J_n .

It is easy to check that: for $6 \le n \le 63$, the sub-cap G_{I_n} of G_{126} generates a code $[n, 6]$ satisfying Lemma 1. Since G_{126} generates an $[n, 6]$ self-orthogonal code, one can deduce the sub-cap G_{J_n} of G_{126} with index set J_n also satisfies Lemma 1 for $64 \le n \le 120$. Thus we have

Theorem 1 If $6 \le n \le 120$, there exists $[[n, n-6, 4; 6]]$ maximal entanglement EAQECC.

4. Construction of EAQECCs from caps in $PG(6,4)$

In this section, we will construct maximal entanglement EAQECCs with parameters $[[n, n-7, 4; 7]]$. According to Lemma 1, we should firstly construct caps $H = H_{7\times n}$, such that $rank(HH^{\dagger}) = 7$ and an $[n, n-7, 4]$ classical codes with parity check matrix $H_{7\times n}$ can be obtained. Following we will give out the main process in obtaining $H_{7\times n}$.

A. Construction of a 252-cap

Let $G = H_{6\times 126}$ be the cap given in Section 3. Applying elementary row operation on $\begin{pmatrix} G \\ 1_{126} \end{pmatrix}$, we can change it into $\begin{pmatrix} G' \\ 1_{126} \end{pmatrix}$, where $\begin{pmatrix} G' \\ 1_{126} \end{pmatrix} = \begin{pmatrix} 1_{120} & 0_5 & 0 \\ X & Y & 0_5 \\ 1_{120} & 1_5 & 1 \end{pmatrix}$. Construct:

$$H_{7\times 252} = \begin{pmatrix} G & G' \\ 0_{126} & 1_{126} \end{pmatrix}$$

Then it is easy to check $H_{7\times 252}$ is a cap and $H_{7\times 252} H_{7\times 252}^{\dagger} = 0$.

B. Construction of a 288-cap

Let 17-cap in $PG(3,4)$ be as follows:

$$H_{17} = \begin{pmatrix} 11111111111111110 \\ 02223113121123331 \\ 00332130120322110 \\ 00012212022011131 \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 1 & 0 \\ \alpha_1 & \cdots & \alpha_{16} & \beta \end{pmatrix},$$

We can construct one 288-cap using method of recursive construction [10] from this 17-cap. The 288-cap $H_{7\times 288}$ consists of three kinds of column vectors:

(1) $(1, \alpha_i, \alpha_j)^T$, (2) $(0, \beta^T, \alpha_j)^T$, (3) $(0, \alpha_j, \beta^T)^T$, $i = 1, ..., 16$.

The numbers of these three kinds of vectors are 256, 16, 16 respectively. This cap code and its dual are with weight polynomials $Wt_{288}(z) = 1 + 1089z^{202} + 270z^{203} + ... + 90z^{267} + 6z^{271}$ and $Wt_{288}^{\perp}(z) = 1 + 1808625y^4 + \ldots$, respectively.

C. Sub-caps of the 252-cap and related codes

If $7 \le n \le 121$, let $H_{6\times(n-1)}$ be an $(n-1)$ -cap satisfying Lemma 1, then the matrix

$$H_n' = \begin{pmatrix} H_{6\times(n-1)} & 0_6^T \\ 0_{n-1} & 1 \end{pmatrix}$$

forms an $n-$ cap, which is a sub-cap of the 252-cap, this $n-$ cap satisfies Lemma 1 and gives an $[n, n-7, 4]$. As for $122 \le n \le 126$, we define $I_{122} = \{7, ..., 128\}$, $I_{123} = \{7, ..., 128, 133\}$, $I_{124} = \{7, ..., 130\}$, $I_{125} = \{7, ..., 130, 132\}$, and $I_{126} = \{7, ..., 132\}$ respectively. It is easy to check that the n -cap with index set I_n also satisfies Lemma 1 and gives an $[n, n-7, 4]$ for $122 \le n \le 126$. If $127 \le n \le 245$, let $n' = 252 - n$ and with $7 \le n' \le 126$, define $J_n = \{1, 2, ..., 252\} \setminus I_{n'}$. For $H_{7\times 252}$ generates a self-orthogonal code, we have an $n-$ cap satisfies Lemma 1 and give an $[n, n-7, 4]$ code for $127 \le n \le 245$.

D. Sub-caps of 288-cap and codes

The 288-cap we have obtained in B. doesn't meet the demand $rank(H_i H_i^{\dagger}) \ge 6$. Applying a permutation on this 288-cap, we get a new 288-cap, whose last 42 columns are the sub-cap of the original 288-cap $H_{7\times 288}$ with index set J , where J is the following order set:

J ={141, 169, 69, 134, 283, 159, 154, 67, 142, 182, 195, 115, 107, 287, 9, 251, 261, 230, 25, 80, 98, 197, 37, 207, 27, 189, 146, 222, 206, 256, 253, 97, 201, 59, 5, 211, 148, 138, 257, 177, 179, 247}.

Denote the new 288-cap as $G_{288} = (\gamma_1, \gamma_2, ..., \gamma_{246}, ..., \gamma_{288})$. Then define index set I_n of sub-cap of G_{288} as follows:

1) If n =246, or $251 \le n \le 256$, or $258 \le n \le 260$, or $262 \le n \le 267$, or $269 \le n \le 277$, or n =280, define $I_n = \{1, ..., n\}$;

2) If n =247, 248, 250, 257, 278, 279, 281, 283, define $I_n = \{1, ..., n-1, n+1\}$;

3) If n =261, 268, 282, define $I_n = \{1, ..., n-1, n+3\}$;

4) If $n = 249, 276$, define $I_{249} = \{1, ..., 247, 249, 250\}$ and $I_{276} = \{1, ..., 275, 276\}$.

It is easy to check that: for $246 \le n \le 283$, each sub-cap G_{I_n} satisfies Lemma 1 and gives an $[n, n-7, 4]$ code.

Summarizing the sub-caps in Step 3 and 4, we have

Theorem 2 If $7 \le n \le 283$, there exists $[[n, n-7, 4; 7]]$ maximal entanglement EAQECC.

5. Conclusions

In this paper, we have constructed maximal entanglement EAQECCs from a class of dual codes determined by caps in $PG(5,4)$ and $PG(6,4)$. However the codes generated by caps in $PG(5,4)$ and $PG(6,4)$ are not always good enough. Hence in the future, we may try to seek for families of classical codes

with good parameters generated from finite geometries, and construct EAQECCs from such code families.

Acknowledgment

The research work was supported by National Natural Science Foundation of China under Grant No. 11071255.

References

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory", Phys. Rev. A, vol. 52, pp.2493-2396, 1995.

[2] M. Steane, "Error correcting codes in quantum theory", Phys. Rev. Lett, vol. 77, 793-797, 1996.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor, et al, "Quantum error correction via codes over GF(4)", IEEE Trans. Inf.Theory, 44, pp.1369-1387, 1998.

[4] D. Gottesman, "Stabilizer codes and quantum error correction", Ph.D. Thesis, California Institute of Technology, 1997. arXiv: quant-ph/9707027, (1997).

[5] T. Brun, I. Devetak, M. H. Hsieh, "Correcting quantum errors with entanglement, Science", vol. 314, pp. 436-439, 2006.

[6] Y. Lai, T. A. Brun, "Entanglement increases the error-correcting ability of quantum error-correcting codes", Phys. Rev. A, vol. 88, 012320, 2013.

[7] Y. Lai, T. A. Brun, M. M. Wilde, "Dualities and Identities for Entanglement-Assisted Quantum Codes", Quantum Information Processing, Published on line with DOI 10.1007/s11128-013-0704-8. See also: arXiv: 1010. 5506v2. (2011).

[8] G. Glynn, "A 126-cap of PG (5, 4) and its corresponding [126, 6, 88]-code", Util. Math., vol. 55, pp. 201-210, 1999.

[9] V. Tonchev, "Quantum codes from caps", Discrete Mathematics, vol. 308, pp. 6368-6372, 2008.

[10] Ruihu Li, Qiang Fu, Luobin Guo, "Construction of entanglement-assisted quantum codes with maximal entanglement from projective caps", unpublished.

[11] M. M. Wilde, T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding", Phys. Rev. A, vol. 77, 064302, 2008.

[12] Xuejun Zhao, "Research on some problems about self-orthogonal codes", P h. D. Thesis, Air Force Engineering University, 2011.