IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 24, 2020, accepted December 16, 2020, date of publication December 21, 2020,
date of current version December 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3045990

New Quantum Codes Constructed by Quantum Caps in PG(3,9) and PG(4,9)

HUSHENG LI, RUIHU LI, AND QIANG FU
Department of Basic Sciences, Air Force Engineering University, Xi'an 710051, China

Corresponding author: Ruihu Li (llzsy2015@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 11901579 and Grant 11801564.

ABSTRACT In this paper, we present a computer-supported method of searching for quantum caps. By means of this method and relevant knowledge of combinatorics, many quantum caps in $PG(3, 9)$ and $PG(4, 9)$ are constructively proven to exist. Then, according to the theorem that each quantum cap corresponds to a quantum error-correcting code with $d = 4$, we obtain 278 quantum error-correcting codes. Most of these results break the GV bound, and a number of them are optimal quantum codes or have improved parameters.

INDEX TERMS Quantum cap, quantum Hamming bound, quantum error-correcting code, combinatorial construction.

I. INTRODUCTION

Compared to classic computing, quantum computing has overwhelming superiority in terms of operation and security. In 1994, Shor [1] proposed a quantum computer-based algorithm that can factor an integer in polynomial time, which is impossible for a classic computer. However, due to the quantum incoherence effect, quantum computing is more likely to produce errors. Therefore, quantum error correction is essential in quantum computing.

In 1995, Shor [2] formulated the theory of quantum error-correcting codes (QECCs) and presented an example of a quantum [[9, 1, 3]]-code that could correct one error. Since then, many methods of constructing QEECs have been being proposed. In 1998, Calderbank *et al.* [3] built the relationships between classical linear codes over the field $\mathbb{F}_4$ and 2-ary QECCs, by which abundant QEECs with excellent parameters were identified. In 2006, Ketkar *et al.* [4] proposed a nonbinary construction theorem that translated the problem of finding q-ary QECCs into the problem of determining *Hermitian* self-orthogonal linear code. For a more detailed introduction to the construction of QECCs, refer to [5]–[8].

For this paper, the cited construction is given as follows.

Lemma 1 [4]: If $\mathcal{C}$ is a q^2-ary linear code of length n, dimension k and dual distance $d^{\perp}$, which is self-orthogonal with respect to the *Hermitian* inner product, then there exists a pure quantum error-correcting code with parameters $[[n, n-2k, d^{\perp}]]_q$.

One central theme in quantum error-correction is the construction of QECCs with optimal parameters. A quantum code $[[n, k, d]]$ is optimal if there is no $[[n, k, d+1]]$ code. For the purpose of finding optimal QECCs with $d = 4$, researchers focus on quantum caps in $PG(r, q)$. In [11], [12], the notion of the quantum cap is introduced. The authors note that a quantum cap of size n in $PG(r, q)$ is equivalent to the quantum error-correcting code with parameters $[[n, n-2(r+1), 4]]_q$. Thus, many 2-ary QEECs of optimal parameters are constructed by quantum caps in $PG(r, 4)$ (see [9]–[15]).

The case of nonbinary optimal quantum codes is much more complicated. In this paper, we use mainly the quantum caps in $PG(3, 9)$ and $PG(4, 9)$ to construct 3-ary quantum codes. Among the results, most break the Gilbert-Varshamov (GV) bound, which implies having good parameters, and some are optimal according to the quantum Hamming bound. Moreover, compared to the 3-ary quantum codes of $d = 3$ in [16], [17], our results are more systematic and involve larger code lengths, some of which even have high code rates. Therefore, in some situations of one error correction in a quantum system, the quantum codes we propose are currently the best coding schemes.

Proposition 1 (Quantum Gilbert-Varshamov Bound [18]): Suppose that $n > k \geq 2$, $d \geq 2$ and $n \equiv k (\mathrm{mod}\ 2)$. Then, there exists a pure quantum code $[[n, k, d]]_q$ provided that

$$\frac{q^{n-k+2}-1}{q^2-1} > \sum_{i=1}^{d-1} (q^2-1)^{i-1} \binom{n}{i} \qquad (1)$$

The associate editor coordinating the review of this manuscript and approving it for publication was Faissal El Bouanani.

Proposition 2 (Quantum Hamming Bound [18], [19]): For any pure quantum code $[[n, k, d]]_q$, $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, then

$$q^{n-k} \geq \sum_{i=0}^{t} (q^2 - 1)^i \binom{n}{i} \tag{2}$$

The rest of this paper is organized as follows: basic concepts related to the linear code and projective cap are recalled in Sect.II. In Sect.III, a computer-supported method of searching for quantum caps is provided. In Sect.IV, 75 quantum caps in $PG(3, 9)$ are found, and related QECCs are constructed. In Sect.V, combinatorial construction and block processing are used to identify 203 quantum caps in $PG(4, 9)$, and related QECCs are obtained. Finally, we analyze the optimality of the constructed quantum codes and present conclusions.

II. PRELIMINARIES

A. FUNDAMENTALS OF LINEAR CODES

Let $\mathbb{F}_q$ be a finite field with q elements, and let $\mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$. A k-dimensional subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ is called a q-ary linear $[n, k]$ code and is denoted as $\mathcal{C} = [n, k]_q$. If the minimal Hamming distance of $\mathcal{C}$ is d, then $\mathcal{C}$ is denoted as $\mathcal{C} = [n, k, d]_q$.

For $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n) \in \mathbb{F}_q^n$, the *Euclidean* inner product is defined as

$$(x, y) = x \cdot y = \sum_{i=1}^{n} x_i y_i. \tag{3}$$

If $x, y \in \mathbb{F}_{q^2}^n$, their *Hermitian* inner product is defined as

$$(x, y)_h = x \cdot y^q = \sum_{i=1}^{n} x_i y_i^q. \tag{4}$$

If $\mathcal{C} = [n, k]_q$, its *Euclidean* dual code $\mathcal{C}^{\perp}$ is

$$\mathcal{C}^{\perp} = \{x \in \mathbb{F}_q^n \mid (x, y) = 0 \text{ for all } y \in \mathcal{C}\}. \tag{5}$$

For $\mathcal{C} = [n, k]_{q^2}$, its *Hermitian* dual code $\mathcal{C}^{\perp h}$ is

$$\mathcal{C}^{\perp h} = \{x \in \mathbb{F}_{q^2}^n \mid (x, y)_h = x \cdot y^q = 0 \text{ for all } y \in \mathcal{C}\}. \tag{6}$$

A code $\mathcal{C}$ is *Hermitian* self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^{\perp h}$. Let $G = (g_{i,j})$ be a generator matrix of $\mathcal{C}$ and $G^{\dagger} = (g_{i,j}^q)^T$ be the conjugate transpose of G; then, $\mathcal{C}$ is Hermitian self-orthogonal if and only if $G \cdot G^{\dagger} = 0$.

Definition 1: Let $\mathcal{C} = [n, k]_q$ and $G = (\alpha_1, \cdots, \alpha_n)$ be a generator matrix of $\mathcal{C}$. If $J = \{j_1, \cdots, j_s\} \subseteq \{1, \cdots, n\} = [n]$, $\omega(J) = \{\omega_{j_1}, \cdots, \omega_{j_s}\}$ is a subset of nonzero elements in $\mathbb{F}_q$, $G(\omega(J)) = (\beta_1, \cdots, \beta_n)$ with $\beta_{j_l} = \omega_{j_l}\alpha_{j_l}$ for $j_l \in J$ and $\beta_i = \alpha_i$ for $i \in [n] \setminus J$; then, the code $\mathcal{C}'$ with generator matrix $G(\omega(J))$ is an equivalent code of $\mathcal{C}$. J and $\omega(J)$ are called the varied set and varied value, respectively.

B. FUNDAMENTALS OF THE PROJECTIVE CAP

Let $PG(r, q)$ be the r-dimensional projective space over $\mathbb{F}_q$. An n-cap in $PG(r, q)$ is a set of n points, no three of which are collinear. Two caps in $PG(r, q)$ with no common points are called disjoint caps. For two K_1 and K_2 caps in $PG(r, q)$, if K_1 is a subset of K_2, K_1 is called a subcap of K_2, and this relation is denoted as $K_1 \subset K_2$. An n-cap is called complete if it is not contained in an $(n + 1)$-cap. The n-cap in $PG(r, q)$ with the largest size is called the maximal cap.

If we write the n points of an n-cap K in $PG(r - 1, q)$ as columns of a matrix, we obtain an $r \times n$ matrix $G_{r,n}$ such that any three columns of $G_{r,n}$ are linearly independent, and $G_{r,n}$ is called a representative matrix of K. For two different representative matrices $G_{r,n}$ and $G'_{r,n}$ of K, there are some $J \subseteq [n]$ and $\omega(J)$ such that $G'_{r,n} = G_{r,n}(\omega(J))$.

If $\mathcal{C}_{r,n}$ is generated by $G_{r,n}$, then $\mathcal{C}_{r,n}$ is called a cap code. Clearly, $\mathcal{C}_{r,n}$ is an $[n, r]$ code with dual distance 4. When $\mathcal{C}_{r,n}$ is a Hermitian self-orthogonal code, $G_{r,n}$ is called a *quantum cap*. Therefore, according to Lemma 1, we have the following.

Lemma 2 [7], [14]: The following are equivalent:

- A quantum n-cap in $PG(r - 1, q^2)$.
- An $[n, k]_{q^2}$ linear code of dual distance 4, which is self-orthogonal with respect to the Hermitian form.
- A pure quantum $[[n, n - 2r, 4]]_q$ code.

From two special quantum caps in $PG(r - 1, 9)$, we can obtain the following.

Lemma 3 [11]: Let $G_{r,n}$ and $G_{r,m}$ be quantum caps in $PG(r - 1, 9)$ and $m < n$.

- If $G_{r,m}$ is a submatrix of $G_{r,n}$, then there is a quantum $n - m$ cap.
- If $G_{r,n}$ and $G_{r,m}$ are disjoint quantum caps, then there is a quantum $n + m$ cap.

In this paper, we concentrate on quantum caps in $PG(3, 9)$ and $PG(4, 9)$.

III. NEW METHOD OF SEARCHING FOR QUANTUM CAPS

Let $\mathbb{F}_3 = \{0, 1, 2\}$ be the finite field of order 3, and let $f(x) = x^2 + 2x + 2$ be a primitive polynomial in $\mathbb{F}_3[x]$. We can define that $\mathbb{F}_9 = \mathbb{F}_3/(f(x)) = \{0, 1, w, w^2, w^3, 2, w^5, w^6, w^7\}$, where w is a root of $x^2 + 2x + 2$. For ease of presentation, we use the figures 3, 4, 5, 6, 7, and 8 to represent the elements $w, w^2, w^7, w^5, w^3, and\ w^6$, respectively.

Next, we define the set $A = \{1, w^2, 2, w^6\} \subseteq \mathbb{F}_9$ and set $B = \{w, w^3, w^5, w^7\} \subseteq \mathbb{F}_9$. Clearly, the elements in set A satisfy $(1)^4 = (w^2)^4 = (2)^4 = (w^6)^4 = 1$ and the elements in set B satisfy $(w)^4 = (w^3)^4 = (w^5)^4 = (w^7)^4 = 2$. Thus, the following definition can be given.

Definition 2 [14]: Let $N : \mathbb{F}_9 \longrightarrow \mathbb{F}_3$ be the norm $(N(x) = x^4, x \in \mathbb{F}_9)$ map. Suppose $\mathcal{C}$ is an $[n, k]_9$ code, the norm code of $\mathcal{C}$ is the ternary code $N(\mathcal{C}) \subseteq \mathbb{F}_3^n$ spanning $\mathbb{F}_3$ by the norms $N(\mathbf{c}) = (N(c_1), N(c_2), \cdots, N(c_n))$, where $\mathbf{c} = (c_1, c_2, \cdots, c_n) \in \mathcal{C}$. Denote the Euclidean dual code of $N(\mathcal{C})$ by $N(\mathcal{C})^{\perp}$.

Reference [14] gives two results related to the quantum cap.

Lemma 4 [14]: If $\mathcal{C}=\ [n,k]_9$, then $\mathcal{C}$ is Hermitian self-orthogonal if and only if $(x,x)_h=0$ for all $x\in\mathcal{C}$.

The authors did not give a complete proof of the following lemma; thus, we provide a supplementary explanation.

Lemma 5 [14]: Let $\mathcal{C}$ be an $[n,k]_9$ with dual distance d. If there exists at least one codeword of $N(\mathcal{C})^{\perp}$ having weight m, then we can obtain a Hermitian self-orthogonal code with parameters $[m,\leq k]_9$ and dual distance d.

Proof: Let G be a generator matrix of $\mathcal{C}$, and let $\mathbf{v}=(v_1,v_2,\cdots,v_n)\in N(\mathcal{C})^{\perp}$ be a word of weight m. When $i\in\{i_1,\cdots,i_m\}\subseteq[n]$, $v_i\neq 0$.

Case 1: Assume the nonzero coordinates of $\mathbf{v}$ consist of only 1; then, the obtained Hermitian self-orthogonal code can be generated based on some columns of G. For more details, refer to the proof of Theorem 2 in [14].

Case 2: Assume the nonzero coordinates of $\mathbf{v}$ consist of 1 and 2 and set $J=\{j|\ v_j=2\}\subseteq\{i_1,i_2,\cdots i_m\}$. Next, choose J as the varied set and let $\omega(J)=\{w\}$, where w is a primitive element of $\mathbb{F}_9$. For the sets $A,B\subseteq\mathbb{F}_9$, it is easy to check that $w\cdot A=B$ and $w\cdot B=A$. Therefore, for equivalent code $\mathcal{C}'$ generated by $G(\omega(J))$, there must exist a codeword $\mathbf{v}'\in N(\mathcal{C}')^{\perp}$ with nonzero ordinates of all 1. By case 1, we can get a Hermitian self-orthogonal code with parameters $[m,\leq k]_9$ and dual distance d generated by some columns of $G(\omega(J))$.

Combining the above Lemma and proof with caps, we can easily obtain the following corollary.

Corollary 1: Suppose $G_{r,n}$ is an n-cap in $PG(r-1,9)$ and $\mathbf{v}$ is a codeword of $N(\mathcal{C}_{r,n})^{\perp}$ having weight m.

(1) If the nonzero coordinates of $\mathbf{v}$ consist of only 1, then there exists a quantum m-cap from $G_{r,n}$ in $PG(r',9)$, $r'\leq r-1$.

(2) If the nonzero coordinates of $\mathbf{v}$ consist of 1 and 2, then there exists a quantum m-cap from $G_{r,n}(\omega(J))$ in $PG(r',9)$, $r'\leq r-1$, where $J=\{j|v_j=2\}$ and $\forall j\in J,\omega_j=w$.

Example 1: From [20], there exists a 20-cap in $PG(5,9)$, which is denoted by G^*, where

$$G^*=\begin{pmatrix}11111111111111111111\\33333333333333333333\\07887044440788704444\\12474218481247421848\\07887044447887044440\\12474218482474218481\end{pmatrix}$$

Assume $\mathcal{C}^*$ is its related linear code. By calculation it is easy to get that $\mathbf{v}_1=(11111111110101010101)$, $\mathbf{v}_2=(22222222221111111111)\in N(\mathcal{C}^*)^{\perp}$. Thus, a quantum 10-cap in $PG(4,9)$ can be obtained by deleting the 11th, 13th, 15th, 17th and 19th columns of G^*. When the varied set $J=\{1,2,3,4,5,6,7,8,9,10\}$, one can also derive that $G^*(\omega(J))$ is a quantum 20-cap in $PG(5,9)$.

It is noteworthy that the dimensions of all obtained quantum caps in $PG(3,9)$ and $PG(4,9)$ are unchanged.

IV. QUANTUM CAPS IN PG(3,9)

According to [21], the largest size of known caps in $PG(3,9)$ is a complete 82-cap that contains three types of points denoted by $(x_1,x_2,x_3,x_4)^T\in\mathbb{F}_9^4$, as follows:

type 1: $x_1=1,x_2^2+2x_3x_4=w^3$;

type 2: $x_1=0,x_3=-\frac{x_2^2}{2},x_4=1$;

type 3: $x_1=x_2=x_4=0,x_3=2$.

It is easy to verify that there are 82 points in total and that 82-cap has a representative matrix $G_{4,82}$, where $G_{4,82}=(G_{4,28},G_{4,27},G'_{4,27})$,

$$G_{4,28}=\begin{pmatrix}1111111111111111111111111111\\0000000011111111333333334444\\1347268513472685134726851347\\5862743131586274627431584315\end{pmatrix},$$

$$G_{4,27}=\begin{pmatrix}111111111111111111111111111\\444477777777222222226666666\\268513472685134726851347268\\862715862743315862746274315\end{pmatrix},$$

$$G'_{4,27}=\begin{pmatrix}111111111111111110000000000\\688888888555555550134726850\\513472685134726850142814282\\843158627158627431111111110\end{pmatrix}.$$

It is easy to check that $G_{4,82}\cdot G^{\dagger}_{4,82}=0$. Hence, $G_{4,82}$ generates a Hermitian self-orthogonal code $\mathcal{C}_{4,82}$, and it is a quantum cap.

First, we choose $G_{4,82}$ as the starting point. From $G_{4,82}$, we can directly find a quantum 8-cap that is defined as:

$$G_{4,8}=\begin{pmatrix}11111100\\14766618\\33646812\\13771511\end{pmatrix}.$$

According to Lemma 3, there is also a quantum 74-cap.

Then, after computation, the norm code $N(\mathcal{C}_{4,82})$ and its Euclidean dual code $N(\mathcal{C}_{4,82})^{\perp}$ can be obtained. We find that when $75\leq t\leq 81$, there exists a codeword of weight t whose nonzero coordinates consist of 1 and 2 contained in $N(\mathcal{C}_{4,82})^{\perp}$. Thus, by Corollary 1, there exists quantum caps of sizes 75, 76, 77, 78, 79, 80, and 81 from $G_{4,82}(\omega(J))$ with different varied sets. These seven quantum caps and corresponding varied sets are listed in table 1.

TABLE 1. Quantum caps and corresponding varied sets.

sizes of quantum cap	*varied sets*
75	{1}
76	{1,2}
77	{1,2,5}
78	{2,9,14,15}
79	{42,54,62,67,70,76,80}
80	{59,72,73,79,80,82}
81	{42,47,54,55,56,57,61,73,78}

Next, to reduce the amount of computation, we choose the latter 54-cap as the starting point. Let $G_{4,54} = (G_{4,27}, G'_{4,27})$ and denote its corresponding code by $\mathcal{C}_{4,54}$. From the code $N(\mathcal{C}_{4,54})^{\perp}$, we find that it contains the codeword of weight t, where $t \in \{9, 10, \cdots, 34\} \cup \{41, 42, \cdots, 47\}$, whose nonzero coordinates consist of only 1. Therefore, there exists a quantum cap of size t from $G_{4,82}$, where $9 \leq t \leq 73$.

On the basis of the above results, the following theorem is true.

Theorem 1: Assume $s \in \{8, 9, \cdots, 82\}$; then, there exists a quantum s-cap in $PG(3, 9)$ and a related pure $[[s, s-8, 4]]_3$ quantum error-correcting code.

V. QUANTUM CAPS IN PG(4,9)

In this section, to obtain quantum caps in $PG(4, 9)$, two solutions are proposed. The first is to use quantum caps in $PG(3, 9)$ to combinatorially construct quantum caps in $PG(4, 9)$. Second, we find the corresponding matrix of the 212-cap, which is the largest size of known cap in $PG(4, 9)$. We then divide this matrix into 5 blocks and search for quantum caps.

Theorem 2: Let $G_{r,m}$ and $G_{r,n}$ be quantum subcaps of the same large cap in $PG(r-1, q)$ with sizes m and n, respectively. Denote the cap code of $G_{r,m}$ by $\mathcal{C}_{r,m}$. If $\mathcal{C}_{r,m}$ contains a word of weight m, then there exists a quantum $(m+n)$-cap in $PG(r, q)$.

proof: Assume $G_{r+1,m+n} = \begin{pmatrix} \mathbf{c}' & 0 \\ G_{r,m} & G_{r,n} \end{pmatrix}$, where $\mathbf{c}'$ is a codeword of $\mathcal{C}_{r,m}$ having weight m. Clearly, any three columns of $G_{r+1,m+n}$ are linearly independent, so $G_{r,m+n}$ is still a cap. Then, since $G_{r,m}$ and $G_{r,n}$ are quantum caps, we have $\mathbf{c}' \cdot G^{\dagger}_{r,m} = 0$, $G_{r,m} \cdot G^{\dagger}_{r,m} = G_{r,n} \cdot G^{\dagger}_{r,n} = 0$, $\mathbf{c}' \cdot (\mathbf{c}')^{\dagger} = 0$. Thus, $G_{r+1,m+n} \cdot (G_{r+1,m+n})^{\dagger} = 0$. $G_{r+1,m+n}$ is a quantum cap of size $m+n$ in $PG(r, q)$.

A. COMBINATORIAL CONSTRUCTION OF QUANTUM CAPS

By means of Theorem 2, quantum subcaps of the 82-cap in $PG(3, 9)$ can be used to combinatorially construct quantum caps in $PG(4, 9)$.

Case 1. In Sect.IV, we have given the representative matrix $G_{4,8}$ of quantum 8-cap in $PG(3, 9)$. Denote the corresponding linear code by $\mathcal{C}_{4,8}$. According to its representative matrix, there exists a word of weight 8 contained in $\mathcal{C}_{4,8}$ that is defined as $\mathbf{c}' = (14766618)$. Hence, we can obtain the matrix $G_{5,8+n} = \begin{pmatrix} \mathbf{c}' & 0 \\ G_{4,8} & G_{4,n} \end{pmatrix}$, where $G_{4,n}$ is the quantum n-cap constructed in Sect.IV. According to Theorem 2, there exists a quantum $(8+n)$-cap in $PG(4, 9)$, $8 \leq n \leq 82$.

Case 2. Let $G_{4,81}$, $G_{4,n}$ be the quantum 81-cap and quantum n-cap in $PG(3, 9)$, respectively, where $10 \leq n \leq 82$. Denote the corresponding linear code of $G_{4,81}$ by $\mathcal{C}_{4,81}$. After a computer search, we find there exists a word $\mathbf{c}'$ of weight 81 contained in $\mathcal{C}_{4,81}$, where $\mathbf{c}' =$ (664755743443766715377351546453133238151841548728 486118578818875716138835871781551). Similarly, we can obtain the matrix $G_{5,81+n} = \begin{pmatrix} \mathbf{c}' & 0 \\ G_{4,81} & G_{4,n} \end{pmatrix}$. Thus, there exists a quantum $(81+n)$-cap in $PG(4, 9)$.

A summary of the results in case 1 and case 2 indicates that there exists a quantum cap in $PG(4, 9)$ of size t, where $t \in \{16, 17, \cdots, 163\}$.

TABLE 2. The existing quantum caps from 5 blocks.

block's label	*sizes of quantum caps that exist*
$G^1_{5,43}$	12, 15, 18, 21, 24, 27, 30
$G^2_{5,43}$	15, 18, 21, 24, 27, 30, 33, 36
$G^3_{5,43}$	12, 18, 21, 24, 30
$G^4_{5,43}$	12, 15, 18, 21, 24, 27, 30, 33
$G_{5,40}$	11, 12, $\cdots$, 30

B. BLOCK PROCESSING OF THE 212-CAP IN PG(4,9)

Currently, the known maximum cap in $PG(4, 9)$ is the 212-cap constructed by Edel and Bierbrauer ([16], [21]). This cap is also complete, and we give its representative matrix as follows: $G_{5,212} = (G^1_{5,43}, G^2_{5,43}, G^3_{5,43}, G^4_{5,43}, G_{5,40})$, shown at the bottom of the next page.

Through the first conclusion of Corollary 1, we search for all possible quantum caps that these five blocks contain. The search results are listed as follows.

The former four blocks of $G_{5,212}$ include quantum subcaps of sizes 30, 36, 30, and 33, respectively. If we denote the union of the former four blocks as $G_{5,172}$, we can conclude that a quantum 129-cap is contained in $G_{5,172}$. By deleting the columns of the quantum 129 subcap from $G_{5,172}$, a new 43-cap can be obtained and defined as $\overline{G}_{5,43}$, shown at the bottom of the next page.

For $\overline{G}_{5,43}$, it is easy to check that it contains quantum caps of sizes 15, 18, 21, 24, and 27. In combination with the disjoint quantum 129-cap, we can construct quantum subcaps of $G_{5,172}$ with sizes of 144, 147, 150, 153, and 156. Moreover, since the last block $G_{5,40}$ contains quantum caps of size t, $11 \leq t \leq 30$, which are disjoint with all the quantum caps from $G_{5,172}$, one can derive by pairwise combination that there exists quantum caps in $PG(4, 9)$ of size t, where $t \in \{11, 12, \cdots, 15\} \cup \{164, 165, \cdots, 186\}$.

Next, the above discussion indicates that $G_{5,172}$ contains a quantum 156 subcap. Therefore, by deleting the columns of the quantum 156-cap from $G_{5,172}$, we can obtain a 16-cap. Denote this 16-cap by $G_{5,16}$. Then, by combining $G_{5,16}$ with the last block of $G_{5,212}$, an 56-cap can be constructed and defined as $G_{5,56} = (G_{5,16}, G_{5,40})$. Denote the generated code of $G_{5,56}$ by $\mathcal{C}_{5,56}$. We can then obtain the norm code $N(\mathcal{C}_{5,56})$ and its Euclidean dual code $N(\mathcal{C}_{5,56})^{\perp}$.

After computation, we find that when $t \in \{31, 32, \cdots, 44\}$ $\cup\{48\}$, there exists a codeword of weight t whose nonzero coordinates consist of only 1 contained in $N(\mathcal{C}_{5,56})^{\perp}$. By Corollary 1, there exists quantum caps of sizes t from $G_{5,56}$.

TABLE 3. Quantum caps and related varied sets.

size of quantum cap	*varied sets*
10	{10,16,27,49,50}
45	{1,3}
46	{5}
47	{6}
49	{15,50}
50	{49}
51	{3,37,43}
52	{45,46}
53	{2,13,14,15,16,18,19,21,23,30,39,40,44,53}
54	{8,13,16,17,24,27,28,35,39,43,44,49,54}
55	{1,7,11,14,15,17,21,22,23,24,39,43,49,51}
56	{21,22,23,24,29,30,31,32,45,46}

In addition, when $t \in \{10\} \cup \{45, 46, \cdots, 56\} \backslash \{48\}$, $N(\mathcal{C}_{5,56})^{\perp}$ includes the codeword of weight t whose nonzero coordinates consists of 1 and 2. Thus, we can also obtain quantum caps with sizes of the same values from $G_{5,56}(\omega(J))$, where the varied sets J are all different. The sizes of the quantum caps and their related varied sets are listed below.

Thus far, we have obtained the quantum $t-$cap from $G_{5,56}$ or its variation, where $t \in \{10\} \cup \{31, 32, \cdots, 56\}$. Then, by combining these results with the disjoint quantum 156 subcap of $G_{5,172}$, we can obtain quantum cap of size t, $187 \leq t \leq 212$, and a solitary quantum 10-cap in $PG(4, 9)$.

Thus, by combining all the results in Sect.V, the following theorem can be obtained.

Theorem 3: Assume $s \in \{10, 12, \cdots, 212\}$; then, there exists a quantum s-cap in $PG(4, 9)$ and a related pure $[[s, s - 10, 4]]_3$ quantum error-correcting code.

VI. PARAMETER ANALYSIS OF QUANTUM CODE

In this section, the constructed quantum codes are analyzed in detail. It is easy to check that when $10 \leq s_1 \leq 82$ and $20 \leq s_2 \leq 212$, both quantum codes $[[s_1, s_1 - 8, 4]]_3$ and $[[s_2, s_2 - 10, 4]]_3$ break the GV bound. Thus, most of the constructed quantum codes are of great parameters. Then, according to the quantum Hamming bound, we can also give the following theorem.

Theorem 4: Assume $15 \leq s_1 \leq 82$ and $44 \leq s_2 \leq 212$; then, all $[[s_1, s_1 - 8, 4]]_3$ and $[[s_2, s_2 - 10, 4]]_3$ quantum error-correcting codes are optimal.

$$G^1_{5,43} = \begin{pmatrix} 0063005710203060006300571020306057753663844 \\ 0514601830582780051460183058278026385247712 \\ 0265085372162638107340672351641334877216085 \\ 0514034241367348051403424136734826388571820 \\ 1111111111111111111111111111111111111111111 \end{pmatrix},$$

$$G^2_{5,43} = \begin{pmatrix} 8577557753663844857757548846371526438754884 \\ 6614326385247712661430476302440158610047630 \\ 3051445682351406770821325725407460625627115 \\ 7560226388571820756027254854640152043725485 \\ 1111111111111111111111111111111111111111111 \end{pmatrix},$$

$$G^3_{5,43} = \begin{pmatrix} 6371526438547846832157843654784683215784363 \\ 2440158610512371852368542751237185236854277 \\ 8783051703074608611325478383053204627158641 \\ 4640152043086103172368875108610317236887516 \\ 1111111111111111111111111111111111111111111 \end{pmatrix},$$

$$G^4_{5,43} = \begin{pmatrix} 6006300750021005577775533664488007500840075 \\ 4384783627134612506062583050278521378155213 \\ 5872745218463573204610853761428725485461587 \\ 3573675708220561428281464138734068101370681 \\ 1111111111111111111111111111111111111111111 \end{pmatrix},$$

$$G_{5,40} = \begin{pmatrix} 0084633612216336122148368346000000000021 \\ 7815607443206074432047830625112473730020 \\ 7438086103173204250684123765480076531230 \\ 0137475268454752684536752814008176764420 \\ 1111111111111111111111111111111011111100 \end{pmatrix}.$$

$$\overline{G}_{5,43} = \begin{pmatrix} 6006301057756875488412484673446833753648585 \\ 1688403726382641603005601182171877628508313 \\ 6063302434872304651535737858332017405618447 \\ 1064434326385741038505038385803166816384131 \\ 1111111111111111111111111111111111111111111 \end{pmatrix}.$$

TABLE 4. Comparison of the QECCs in this paper and those in [22], [23].

QECCs in this paper	QECCs in [22]	QECCs in [23]
$[[22, 14, 4]]_3$	$[[22, 12, 4]]_3$	–
$[[25, 17, 4]]_3$	$[[25, 15, 4]]_3$	–
$[[26, 18, 4]]_3$	$[[26, 16, 4]]_3$	–
$[[28, 20, 4]]_3$	$[[28, 18, 4]]_3$	–
$[[30, 22, 4]]_3$	–	$[[30, 20, 4]]_3$
$[[31, 23, 4]]_3$	$[[31, 21, 4]]_3$	–
$[[33, 25, 4]]_3$	$[[33, 23, 4]]_3$	–
$[[56, 48, 4]]_3$	–	$[[56, 44, 4]]_3$

TABLE 5. Comparison of the QECCs in this paper and those in [16].

QECCs in this paper	QECCs in [16]	QECCs in this paper	QECCs in [16]
$[[11, 3, 4]]_3$	$[[11, 1, 4]]_3$	$[[130, 120, 4]]_3$	$[[121, 112, 4]]_3$
$[[21, 13, 4]]_3$	$[[21, 11, 4]]_3$	$[[140, 130, 4]]_3$	$[[140, 118, 4]]_3$
$[[33, 25, 4]]_3$	$[[33, 23, 3]]_3$	$[[146, 136, 4]]_3$	$[[146, 122, 4]]_3$
$[[41, 33, 4]]_3$	$[[41, 31, 4]]_3$	$[[147, 137, 4]]_3$	$[[147, 133, 3]]_3$
$[[52, 44, 4]]_3$	$[[52, 40, 4]]_3$	$[[154, 144, 4]]_3$	$[[154, 138, 3]]_3$
$[[57, 49, 4]]_3$	$[[57, 43, 4]]_3$	$[[160, 150, 4]]_3$	$[[160, 146, 4]]_3$
$[[65, 57, 4]]_3$	$[[65, 47, 4]]_3$	$[[161, 151, 4]]_3$	$[[161, 147, 4]]_3$
$[[70, 62, 4]]_3$	$[[70, 52, 4]]_3$	$[[176, 166, 4]]_3$	$[[176, 163, 3]]_3$
$[[71, 63, 4]]_3$	$[[71, 57, 3]]_3$	$[[176, 166, 4]]_3$	$[[176, 153, 4]]_3$
$[[73, 65, 4]]_3$	$[[73, 61, 3]]_3$	$[[193, 183, 4]]_3$	$[[193, 177, 3]]_3$
$[[104, 94, 4]]_3$	$[[104, 91, 4]]_3$	$[[200, 190, 4]]_3$	$[[200, 178, 3]]_3$
$[[105, 95, 4]]_3$	$[[105, 91, 4]]_3$	$[[201, 191, 4]]_3$	$[[201, 179, 3]]_3$
$[[112, 102, 4]]_3$	$[[112, 96, 4]]_3$	$[[205, 195, 4]]_3$	$[[205, 189, 3]]_3$
$[[121, 111, 4]]_3$	$[[121, 106, 4]]_3$	$[[208, 198, 4]]_3$	$[[208, 192, 4]]_3$

Proof: For $15 \leq s_1 \leq 82$, it is not difficult to check $\sum_{i=0}^{2} 8^i \binom{s_1}{i} > 3^8$. One can derive that a pure $[[s_1, s_1 - 8, 5]]_3$ code does not exist by quantum Hamming bound; thus, $[[s_1, s_1 - 8, 4]]_3$ is an optimal code. Similarly, we can check for $44 \leq s_2 \leq 212$, $\sum_{i=0}^{2} 8^i \binom{s_2}{i} > 3^{10}$, which implies that $[[s_2, s_2 - 10, 4]]_3$ is an optimal code.

In addition, by comparing all constructed results with the quantum codes in [16], [22], [23], 248 quantum codes are found to be new and some have better parameters. Here, we list only the QECCs that have better parameters than those of the quantum codes in [16], [22], [23].

VII. CONCLUSION

From the known maximum caps in $PG(3, 9)$ and $PG(4, 9)$, we have found 278 quantum caps of different sizes, whose representative matrices can be directly obtained. Then, by use of these quantum caps, we also constructed 278 related quantum error-correcting codes with $d = 4$ in succession. According to the GV bound and quantum Hamming bound, most of the quantum codes are optimal.

Although our codes could only correct one error in the quantum system, compared to the known 3-ary quantum codes of $d = 3$, our codes have larger sizes and parts of them have higher rates. In other words, for the case of a high rate with only one error correction required, the quantum codes we constructed are the best coding schemes at present.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 1994, pp. 124–134.

[2] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, pp. 2493–2496, Oct. 1995.

[3] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[4] A. Ketkar, A. Klappenecker, and S. Kumar, "Nonbinary stablizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.

[5] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.

[6] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999.

[7] J. Bierbrauer and Y. Edel, "Quantum twisted codes," *J. Combinat. Des.*, vol. 8, no. 3, pp. 174–188, 2000.

[8] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 2, no. 1, pp. 55–64, 2004.

[9] V. D. Tonchev, "Quantum codes from caps," *Discrete Math.*, vol. 308, no. 24, pp. 6368–6372, Dec. 2008.

[10] J. Bierbrauer, G. Faina, M. Giulietti, S. Marcugini, and F. Pambianco, "The geometry of quantum codes," *Innov. Incidence Geometry, Algebr., Topol. Combinat.*, vol. 6, no. 1, pp. 53–71, 2008.

[11] J. Bierbrauer and Y. Edel, "Large caps in projective Galois spaces," *Current Research Topics in Galois Geometry*. 2010, pp. 81–94.

[12] D. Bartoli, J. Bierbrauer, S. Marcugini, and F. Pambianco, "Geometric constructions of quantum codes," in *Error-Correcting Codes, Finite Geometries and Cryptography* (AMS, Series: Contempo-rary Mathematics 523), vol. 523, A. A. Bruen and D. L. Wehlau, Eds. Providence, RI, USA, 2010, pp. 149–154.

[13] D. Bartoli, G. Faina, S. Marcugini, and F. Marcugini, "New quantum caps in PG (4, 4)," *J. Combinat. Des.*, vol. 20, no. 10, pp. 448–466, Jan. 2012.

[14] J. Bierbrauer, D. Bartoli, G. Faina, S. Marcuginim, F. Pambianco, and Y. Edel, "The structure of quaternary quantum caps," *Des., Codes Cryptogr.*, vol. 72, no. 3, pp. 733–747, Sep. 2014.

[15] R. Li, Q. Fu, L. Guo, and X. Li, "Construction of quantum caps in projective space PG(r,4) and quantum codes of distance 4," *Quantum Inf. Process.*, vol. 15, no. 2, pp. 689–720, Feb. 2016.

[16] Y. Edel's. [Online]. Available: https://www.mathi.uni-heidelberg.de/ỹves/Matritzen/QTBCH/QTBCHIndex.html

[17] L. Jin, S. Ling, J. Luo, and C. Xing, "Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4735–4740, Sep. 2010.

[18] K. Feng and Z. Ma, "A finite Gilbert-Varshamov bound for pure stabilizer quantum codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3323–3325, Dec. 2004.

[19] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A, Gen. Phys.*, vol. 54, pp. 1862–1868, Sep. 1996.

[20] Y. Edel and J. Bierbrauer, "Recursive constructions for large caps," *Bull. Belg. Math. Soc. Simon Stevin*, vol. 6, no. 2, pp. 249–258. 1999.

[21] Y. Edel and J. Bierbrauer, "Large caps in small spaces," *Des., Codes, Cryptogr.*, vol. 23, no. 2, pp. 197–212, 2001.

[22] M. F. Ezerman, S. Ling, B. Özkaya, and P. Solé, "Good stabilizer codes from quasi-cyclic codes over F_4 and F_9," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2019, pp. 2898–2902.

[23] J. Lv, R. Li, and J. Wang, "Constructions of quasi-twisted quantum codes," *Quantum Inf. Process.*, vol. 19, p. 274, Jul. 2020.

HUSHENG LI received the bachelor's degree from Air Force Engineering University, in 2019. He is currently pursuing the master's degree with the Quantum Information Laboratory, Air Force Engineering University. His research interests include coding theory and cryptography.

RUIHU LI received the Ph.D. degree from the Northwestern Polytechnical University of Technology, in 2004. He is currently a Professor with the Department of Basic Sciences, Air Force Engineering University. His research interests include group theory, coding theory, and cryptography.

QIANG FU received the B.E. degree in applied mathematics from Northwest University, Xi'an, China, in 2012, and the M.S. degree in applied mathematics and the Ph.D. degree in information and communication engineering from Air Force Engineering University, in 2015, and 2018, respectively. He is currently a Lecturer with Air Force Engineering University. His research interests include algebraic coding, distribution storage coding, and erasure coding.