frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 24 February 2023
DOI 10.3389/fphy.2023.1148398

OPEN ACCESS

EDITED BY
Nanrun Zhou,
Shanghai University of Engineering Sciences, China

REVIEWED BY
Mingxing Luo,
Southwest Jiaotong University, China
Ma Hongyang,
Qingdao University of Technology, China

*CORRESPONDENCE
Shanqi Pang,
shanqipang@126.com
Jiao Du,
jiaodudj@126.com
Tianyin Wang,
wangtianyin79@163.com

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 20 January 2023
ACCEPTED 15 February 2023
PUBLISHED 24 February 2023

CITATION
Pang S, Yang F, Yan R, Du J and Wang T (2023), Construction of quaternary quantum error-correcting codes *via* orthogonal arrays.
Front. Phys. 11:1148398.
doi: 10.3389/fphy.2023.1148398

Construction of quaternary quantum error-correcting codes *via* orthogonal arrays

Shanqi Pang[1]*, Fuyuan Yang[1], Rong Yan[1], Jiao Du[1,2]* and Tianyin Wang[3,4]*

[1]College of Mathematics and Information Science, Henan Normal University, Xinxiang, China, [2]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China, [3]School of Mathematical Science, Luoyang Normal University, Luoyang, China, [4]Guangxi key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin, China

This paper presents a method based on orthogonal arrays of constructing pure quaternary quantum error-correcting codes. As an application of the method, some infinite classes of quantum error-correcting codes with distances 2, 3, and 4 can be obtained. Moreover, the infinite class of quantum codes with distance 2 is optimal. The advantage of our method also lies in the fact that the quantum codes we obtain have less items for a basis quantum state than existing ones.

KEYWORDS

quantum error-correcting codes, orthogonal arrays, k-uniform states, orthogonal partition, difference scheme

1 Introduction

Quantum systems are more fragile than classical systems. When quantum information travels across a noisy channel, errors are unavoidable [1–3]. The primary tool to deal with different types of quantum noises is quantum error-correcting codes (QECCs) [1, 2, 4, 5]. They play an important role in quantum information tasks, such as in entanglement purification, quantum key distribution, fault-tolerant quantum computation, and so on [6–8]. Since its discovery, code construction has come a long way [9–16]. Plenty of binary QECCs have been obtained, some of which from classical error-correcting codes (CECCs) [16–19]. Relatively speaking, there are still less studies on quaternary QECCs. We are motivated by the fact that CECCs are one-to-one connected to orthogonal arrays (OAs) [20]. It would be interesting to see if OAs can reciprocate and help QECCs, especially, quaternary ones. Therefore, the main aim of this work is to construct quaternary QECCs from OAs.

If L is an $r \times N$ array with elements from $S = \{0, 1, \ldots, s-1\}$ and every $r \times k$ subarray of L contains each k-tuple based on S as a row with same frequency, then the array is said to be an orthogonal array of strength k (for some k in the range $0 \le k \le N$). We will use OA (r, N, s, k) to denote such an array [21]. The theory of OAs has been developed significantly since the seminal work of Rao [22]. In particular, in recent years many new methods for constructing strength k OAs have been proposed, and a lot of new classes of OAs have been presented [23–29]. An OA (r, N, s, k) is said to be an irredundant orthogonal array (IrOA), if every row in any $r \times (N-k)$ subarray is unique [20]. If all of a pure quantum state's reductions to k qudits are maximally mixed, it is said to be k-uniform. And this state consists of N

subsystems with d levels. A connection between a k-uniform state and an irredundant orthogonal array (IrOA) was established by Goyeneche et al. [20]. For simplicity, the normalization factors are omitted from this paper.

Lemma 1. [20] *If* $L = \begin{pmatrix} s_1^1 & s_2^1 & \cdots & s_N^1 \\ s_1^2 & s_2^2 & \cdots & s_N^2 \\ \vdots & \vdots & \cdots & \vdots \\ s_1^r & s_2^r & \cdots & s_N^r \end{pmatrix}$ *is an* IrOA(r, N, s, k), *then the superposition of r product states,*

$$|\Phi\rangle = |s_1^1 s_2^1 \ldots s_N^1\rangle + |s_1^2 s_2^2 \ldots s_N^2\rangle + \cdots + |s_1^r s_2^r \ldots s_N^r\rangle$$

is a k-uniform state.

By using this connection in Lemma 1, a lot of k-uniform states have been constructed from OAs [20, 30–37]. This kind of k-uniform states is closely related to QECCs [12, 20]. Usually, quantum information theory benefits from OAs [38–43]. These new developments in OAs and uniform states provide a higher possibility to construct infinite classes of QECCs from OAs [35, 36].

In this work, we present a method based on OAs of constructing pure quaternary QECCs. As an application of the method, some infinite classes of QECCs with distances 2, 3, and 4 can be obtained. We know that quantum bound reflects the optimality of QECCs and is a key parameter to judge whether a construction method is effective or not. Moreover, the resulting infinite class of quantum codes with distance 2 is optimal. The advantage of our method also lies in the fact that the constructed QECCs have less items in each basis state than existing ones.

This paper is organized as follows. After introducing symbols, definitions, and required lemmas in Section 2, Section 3 presents the main results. The conclusion is drawn in Section 4.

2 Preliminaries

We introduce several symbols, definitions and lemmas used in this paper.

Let $\mathbb{F}_4^n$ denote the n dimensional space over a Galois field $\mathbb{F}_4 = \mathbb{F}_2(\omega) = \{0, 1, \omega, \bar{\omega} = \omega^2\}$, $\omega^2 = \omega + 1$. For the convenience of codeword expression, we use $\mathbb{F}_4 = \{0, 1, 2, 3\}$. A^T is the transposition of matrix A. $(s) = (0, 1, \ldots, s-1)^T_{1\times s}$, and 0_r and 1_r represent the $r \times 1$ vector of 0s and 1s, respectively. We define the Kronecker product $A \otimes B$ and the Kronecker sum $A \oplus B$ as $A \otimes B = (a_{ij} \cdot B)_{mu\times nv}$ and $A \oplus B = (a_{ij} + B)_{mu\times nv}$, respectively, if $A = (a_{ij})_{m\times n}$ and $B = (b_{rs})_{u\times v}$ with entries from a finite field with binary operations (+ and ·). Here, $a_{ij} + B$ denotes the $u \times v$ matrix with elements $a_{ij} + b_{rs}$ ($1 \le r \le u$, $1 \le s \le v$). And if necessary, matrix A can always be viewed as a set of its row vectors. The strength of an orthogonal array L is denoted by t(L). We also use a k-strength OA to denote an OA of strength k for $k \ge 0$. Let $(\mathbb{C}^4)^{\otimes N} = \underbrace{\mathbb{C}^4 \otimes \mathbb{C}^4 \otimes \cdots \otimes \mathbb{C}^4}_{N}$.

Definition 1. [44] *Suppose* $S^l = \{(u_1, \ldots, u_l) | u_i \in S, i = 1, 2, \ldots, l\}$. *The number of positions in which two vectors* $v = (v_1, \ldots, v_l)$, $u = (u_1, \ldots, u_l) \in S^l$ *differ from one another is defined as the Hamming distance HD*(u, v) *between them. Let HD*(L) *represents all possible values of the Hamming distance between two distinct rows of an OA L. The minimal distance of a matrix A means the minimal Hamming distance between its distinct rows and denoted by MD*(A).

Let $k \ge 1$ and $\mathcal{A}^k$ represent the additive group of order s^k which consists all k-tuples of elements from $\mathcal{A}$. The typical vector addition is used as the binary operation. If $\mathcal{A}_0^k = \{(x_1, x_2, \ldots, x_k)\colon x_1 = \cdots = x_k \in \mathcal{A}\}$, $\mathcal{A}_0^k$ is a subgroup of $\mathcal{A}^k$ of order s, and $\mathcal{A}_i^k$, $i = 1, \ldots, s^{k-1}-1$ will be used to denoted its cosets.

Definition 2. [44] *Let D be an* $r \times c$ *matrix with elements from* $\mathcal{A}$. *For every* $r \times k$ *submatrix of D, its rows are seen as entries of* $\mathcal{A}^k$. *If in the submatrix each set* $\mathcal{A}_i^k$, $i = 0, 1, \ldots, s^{k-1}-1$, *is represented equally frequently, then the D is said to be a difference scheme of strength k. We use* $D_k(r, c, s)$ *to denote such a matrix. When* $k = 2$, *we denote* $D_k(r, c, s)$ *by* $D(r, c, s)$.

Definition 3. [29] *Let L be an OA*(r, N, s, k). *Suppose the rows of L can be partitioned into u submatrices* $\{L_1, L_2, \ldots, L_u\}$ *such that each* L_i *is an OA* $(\frac{r}{u}, N, s, k_1)$ *with* $k_1 \ge 0$. *Then the set* $\{L_1, L_2, \ldots, L_u\}$ *is called an orthogonal partition of strength* k_1 *of L. In particular,* $\{L_1, L_2, \ldots, L_u\}$ *is called a strength* k_1 *orthogonal partition of a space* $\mathbb{F}_p^n$ *if* $L = \mathbb{F}_p^n$.

Definition 4. *Let* $D = D_k(r, c, s)$. *A set of difference schemes* $\{D_1, D_2, \ldots, D_u\}$ *is called a* k_1*-strength orthogonal partition of D, if* $D_i \bigcap D_j = \emptyset$ *for* $i \ne j$ *and* $\bigcup_{i=1}^u D_i = D$.

Lemma 2. [44] *If* $s \not\equiv 2 \pmod 4$, *and* $s \le k$, *then the difference scheme* $D_k(s^{k-1}, k+1, s)$ *exists.*

Lemma 3. [34] *If* $L = OA(s^k, N, s, k)$, *then* $MD(L) = N - k + 1$.

Lemma 4. [45] *(1) Let* $D = D_k(r, c, s)$. *Then* $D \oplus (s) = OA(rs, c, s, k)$.

(2) Let $D = D_k(m, n, s)$ *and* $L = OA(r, N, s, k)$ *for* $k = 2, 3$. *Then* $D \oplus L = OA(mr, nN, s, k)$.

Lemma 5. [36] *(Expansive replacement method) Assume that* L_A *is a k-strength OA with s levels in factor 1 and that* L_B *is a k-strength OA with s rows. After building a one-to-one mapping between the levels of factor 1 in* L_A *and the rows of* L_B, *we may construct an OA of strength k by substituting each level of factor 1 in* L_A *with the matching row from* L_B.

Lemma 6. [44] *For a prime power* $s \ge 2$, *an* OA$(s^k, s+1, s, k)$ *exists if* $s \ge k - 1 \ge 0$.

Lemma 7. [12] *If the reductions of all states in a subspace Q of* $(\mathbb{C}^s)^{\otimes N}$ *to any given k parties are equal, then Q is an* $((N,K,k+1))_s$ *QECC, and vice versa. Furthermore, if any state in Q is k-uniform, then Q is pure, and vice versa.*

We can also define a QECC $((N,K,k+1))_s$ according to Lemma 7, where N denotes the code length, K is the dimension of the encoding state, $k+1$ denotes the distance, and s denotes the levels number. For $s = 2$, it is simply $((N, K, k+1))$.

Lemma 8. [46] *(quantum Singleton bound) If* $K > 1$ *in an* $((N,K,k+1))_s$ *then* $K \le s^{N-2k}$. *Similarly, a pure* $((N,1,k+1))_s$ *satisfies* $2k \le N$.

Definition 5. *A QECC such that the equality in Lemma 8 holds is called optimal.*

3 Construction of $((N,K,k+1))_4$ QECC

This section provides a construction method of quaternary quantum error-correcting codes (QECCs) from orthogonal arrays

(OAs). In Theorem 1, we use Lemma 4 (2) to construct QECCs with distance 2. Theorems 2 and 3 produce QECCs with distances 3 and 4 from the OAs with orthogonal partitions. In Theorem 4, we study the existence of QECCs with any distance by using a special construction of OAs.

Theorem 1. *For every $N \geq 2$, there is a QECC $((N,K,2))_4$ for each integer $1 \leq K \leq 4^{N-2}$ where the $((N,4^{N-2},2))_4$ code is optimal.*

Proof. When $N \geq 5$, a difference scheme $D = D_{N-1}(4^{N-2}, N, 4)$ exists by Lemma 2. Let $L = D \oplus (4) = OA\ (4^{N-1}, N, 4, N-1)$. By Lemma 3, $MD(L) = N - (N-1) + 1 = 2$. Set $D = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_{4^{N-2}} \end{pmatrix}$. Let $L_i = d_i \oplus (4) = OA\ (4, N, 4, 1)$ for $i = 1, 2, \ldots, 4^{N-2}$. Then $t\ (L_i) = 1$, $MD\ (L_i) = N$.

From Lemma 1, $L_1, L_2, \ldots, L_{4^{N-2}}$ can generate 4^{N-2} 1-uniform states $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_{4^{N-2}}\rangle$. They can be used as a set of orthogonal basis to generate a subspace Q of $(\mathbb{C}^4)^{\otimes N}$. Thus Q is an optimal $((N,4^{N-2},2))_4$ code by Lemma 7 and Definition 5.

In addition, for any integer $1 \leq K \leq 4^{N-2}-1$, if Q_K is the subspace spanned by $|\varphi_1\rangle, \ldots, |\varphi_K\rangle$, then it is a $((N,K,2))_4$ code.

When $1 < N < 5$, we can construct the following QECCs $((N,4^{N-2},2))_4$.

When $N = 2$, an optimal $((2,1,2))_4$ code can be generated with a basis $|\varphi\rangle = |01\rangle + |12\rangle + |23\rangle + |30\rangle$.

When $N = 3$, take $D(4,3,4) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 3 \\ 0 & 3 & 1 \end{pmatrix} = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix}$. Let $A_i = d_i \oplus (4)$ and $A = \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{pmatrix}$. Obviously, A and A_i are OAs for $i = 1, 2, 3, 4$. From Lemma 3, $MD(A) = 2$, and by Lemma 7, an optimal $((3,4,2))_4$ QECC can be obtained from $A_1, \ldots, A_4$.

When $N = 4$, take $D(4,2,4) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix}$. Then $B_{4(i-1)+j} = d_i \oplus ((4)\ (j-1) \oplus (4))$ is an $OA\ (4, 4, 4, 1)$ for $i, j = 1, 2, 3, 4$ and $B = \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_{16} \end{pmatrix} = D(4,2,4) \oplus \mathbb{F}_4^2$ is an $OA\ (64, 4, 4, 2)$. By simple calculation, we have $MD(B) = 2$. By Lemma 7, an optimal $((4,16,2))_4$ QECC can be obtained from $B_1, \ldots, B_{16}$.

Remark. The quantum codes obtained by Theorem 1 have less items in a basis state than existing ones. For example, every basis states of the $((3,4,2))_4$ code has four items. It has far less number of items for a basis state than the $((3,4,2))_4$ in [13]. Compared with the codes $[[N,N-2,2]]_4$ in [47] for $N = 9 + 6m$ with $0 \leq m \leq 165$, we have the codes for all $N \geq 2$.

Theorem 2. *Suppose L is an $OA(r, N, 4, 2)$ with $MD(L) \geq 3$. A QECC $((N,K,3))_4$ exists, if there are vectors $b_1, b_2, \ldots, b_K$ in $\mathbb{Z}_4^N$ that fulfill $HD(b_u, b_v) \geq 3$ and $|HD(b_u, b_v) - HD(L)| \geq 3$ for $u \neq v$.*

Proof: Let $X = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_K \end{pmatrix}$, where $X_u = 1_r \otimes b_u + L$ for $1 \leq u \leq K$. Both X and X_u are 2-strength OAs. Let $x_1 = b_u + l_1, x_2 = b_v + l_2 \in X$ for $l_1, l_2 \in L$. Then we can compute the Hamming distance (HD) between x_1 and x_2 and the minimum distance (MD) of X.

(1) HD (x_1, x_2) = MD$(L) \geq 3$, if $u = v$, $l_1 \neq l_2$.
(2) HD (x_1, x_2) = HD $(b_u, b_v) \geq 3$, if $u \neq v$, $l_1 = l_2$.
(3) If $u \neq v$ and $l_1 \neq l_2$, we have HD $(x_1, x_2) \geq$HD $(b_u + l_2, x_2)$ − HD $(b_u + l_2, x_1)$ or HD $(x_1, x_2) \geq$HD $(b_u + l_2, x_1)$ − HD $(b_u + l_2, x_2)$, hence HD $(x_1, x_2) \geq |$HD (b_u, b_v) − HD$(L)| \geq 3$.

Therefore, MD$(X) \geq 3$. We can obtain K states from $\{X_1, X_2, \ldots, X_K\}$ and Lemma 1. Let Q be a subspace of $(\mathbb{C}^4)^{\otimes N}$ with the K states to be an orthogonal basis. Thus Q is a QECC $((N,K,3))_4$ by Lemma 7.

Theorem 3. *There exists a QECC $((3p,4^{p-n+1},3))_4$ with $\frac{4^{n-1}+2}{3} \leq p \leq \frac{4^n-1}{3}$ for $n \geq 3$ and with $3 \leq p \leq 5$ for $n = 2$.*

Proof. Let $\{D_1, D_2, D_3, D_4\}$ be orthogonal partition of the difference scheme $D\ (16, 3, 4) = (0_{16}, (4) \oplus 0_4, 0_4 \oplus (4))$ and $\{L_1, L_2, \ldots, L_{4^{p-n}}\}$ be an orthogonal partition of strength two of $\mathbb{F}_4^p$. Let Y_i denote the ith row of $\mathbb{F}_4^{p-n}$ with $\frac{4^{n-1}+2}{3} \leq p \leq \frac{4^n-1}{3}$ for $n \geq 3$. Take

$$M = \begin{pmatrix} D_1 \oplus L_1 \\ \vdots \\ D_1 \oplus L_{4^{p-n}} \\ D_2 \oplus L_1 \\ \vdots \\ D_4 \oplus L_{4^{p-n}} \end{pmatrix} = \begin{pmatrix} M_1 \\ \vdots \\ M_{4^{p-n}} \\ M_{4^{p-n}+1} \\ \vdots \\ M_{4^{p-n+1}} \end{pmatrix},$$

where $L_i = (a_1, \ldots, a_n, ((a_{n+1}, \ldots, a_p) + 1_{4^n} \otimes Y_i))$ for $i = 1, 2, \ldots, 4^{p-n}$ and $(a_1, a_2, \ldots, a_p)$ is an $OA\ (4^n, p, 4, 2)$.

Because D_j is a 2-strength difference scheme and L_i is a 2-strength OA, it follows from Lemma 4 that $M_k = D_j \oplus L_i$ is a 2-strength OA for $k = 1, 2, \ldots, 4^{p-n+1}$. Let $m_1 = d_1 \oplus l_1$, $m_2 = d_2 \oplus l_2 \in M_k$ for $d_1, d_2 \in D_j$, $l_1, l_2 \in L_i$. Then we have

$$HD(m_1, m_2) = \begin{cases} 3 \cdot HD(l_1, l_2),\ if\ d_1 = d_2, \\ p \cdot HD(d_1, d_2),\ if\ l_1 = l_2, \\ (3 - HD(d_1, d_2)) \cdot HD(l_1, l_2) + (p - HD(l_1, l_2)) \cdot \\ HD(d_1, d_2),\ if\ d_1 \neq d_2, l_1 \neq l_2. \end{cases}$$

Therefore, $MD\ (M_k) \geq 3$ and M_k is an IrOA for any k. Furthermore, M is an OA and has strength two because it is equal to $D(16,3,4) \oplus \mathbb{F}_4^p$ after row permutations. Similarly, we can obtain $MD(M) \geq 3$. From Lemma 1, $M_1, M_2, \ldots, M_{4^{p-n+1}}$ can generate 4^{p-n+1} states. They can be used as a basis to form a subspace Q of $(\mathbb{C}^4)^{\otimes 3p}$. From Lemma 7, Q is a QECC $((3p,4^{p-n+1},3))_4$.

Similarly, when $3 \leq p \leq 5$ and $n = 2$, we can construct a $((3p,4^{p-1},3))_4$ QECC.

Example 1. *Let the following + be the operation in $\mathbb{F}_4$. Let* $D_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 3 \\ 0 & 3 & 1 \end{pmatrix}$, $D_2 = \begin{pmatrix} 0 & 0 & 3 \\ 0 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 3 & 2 \end{pmatrix}$, $D_3 = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 3 & 3 \end{pmatrix}$,

TABLE 1 Some new QECCs with larger distance by Theorem 7.

d	m	QECC	n_d
5	2	$((n_d, 1, 5))_4$	$16 \le n_d \le 34$
6	2	$((n_d, 1, 6))_4$	$20 \le n_d \le 34$
7	2	$((n_d, 1, 7))_4$	$24 \le n_d \le 34$
8	2	$((n_d, 1, 8))_4$	$28 \le n_d \le 34$
9	2	$((n_d, 1, 9))_4$	$32 \le n_d \le 34$
10	3	$((n_d, 1, 10))_4$	$54 \le n_d \le 195$
32	3	$((n_d, 1, 32))_4$	$186 \le n_d \le 195$
33	3	$((n_d, 1, 33))_4$	$192 \le n_d \le 195$
34	4	$((n_d, 1, 34))_4$	$264 \le n_d \le 1028$
100	4	$((n_d, 1, 100))_4$	$792 \le n_d \le 1028$
109	4	$((n_d, 1, 109))_4$	$864 \le n_d \le 1028$
127	4	$((n_d, 1, 127))_4$	$1008 \le n_d \le 1028$
128	4	$((n_d, 1, 128))_4$	$1016 \le n_d \le 1028$
129	4	$((n_d, 1, 129))_4$	$1024 \le n_d \le 1028$
130	5	$((n_d, 1, 130))_4$	$1290 \le n_d \le 5120$

$D_4 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 2 & 2 \\ 0 & 3 & 0 \end{pmatrix}$. *In Theorem 3, we take $3 \le p \le 5$ and $n = 2$. Let $(a_1, a_2, \ldots, a_p)$ be an OA $(16, p, 4, 2)$ and L_i=$(a_1, a_2, (a_3, \ldots, a_p) + 1_{16} \otimes Y_i)$, where Y_i denotes the ith row of $\mathbb{F}_4^{p-2}$ for $i = 1, 2, \ldots, 4^{p-2}$. Then $\{L_1, L_2, \ldots, L_{4^{p-2}}\}$ is an orthogonal partition of strength 2 of $\mathbb{F}_4^p$. We can obtain QECCs $((9, 4^2, 3))_4$, $((12, 4^3, 3))_4$ and $((15, 4^4, 3))_4$. With $6 \le p \le 21$ for $n = 3$, Theorem 3 produces QECCs $((18, 4^4, 3))_4, ((21, 4^5, 3))_4, \ldots, ((63, 4^{19}, 3))_4$.*

Theorem 4. *If an OA$(4^n, p, 4, 3)$ exists for $p > n \ge 3$, then there is a $((4p, 4^{p-n+1}, 4))_4$ QECC.*

Proof. This can be proved in the same way as Theorem 3.

Example 2. *Let $D_1 = (0_{16}, (4) \oplus 0_4, 0_4 \oplus (4), (4) \oplus (4))$, $D_2 = (0_{16}, (4) \oplus 0_4, 0_4 \oplus (4), 1 + (4) \oplus (4))$, $D_3 = (0_{16}, (4) \oplus 0_4, 0_4 \oplus (4), 2 + (4) \oplus (4))$, $D_4 = (0_{16}, (4) \oplus 0_4, 0_4 \oplus (4), 3 + (4) \oplus (4))$. Then the difference scheme $D_3(64, 4, 4) = (0_{64}, (4) \oplus 0_{16}, 0_4 \oplus (4) \oplus 0_4, 0_{16} \oplus (4))$ has a 3-strength orthogonal partition $\{D_1, D_2, D_3, D_4\}$. Take $p = 5, 6$ and $n = 3$ in Theorem 4. Let $(a_1, a_2, \ldots, a_p)$ be an OA$(64, p, 4, 3)$ and L_i=$(a_1, a_2, a_3, (a_4, \ldots, a_p) + 1_{64} \otimes Y_i)$, where Y_i denotes the ith row of $\mathbb{F}_4^{p-3}$ for $i = 1, 2, \ldots, 4^{p-3}$. Then $\{L_1, L_2, \ldots, L_{4^{p-3}}\}$ is an orthogonal partition strength 3 of $\mathbb{F}_4^p$. By Theorem 4, two new QECCs $((20, 4^3, 4))_4$ and $((24, 4^4, 4))_4$ can be obtained.*

Theorem 5. *Let L^N denote an OA$(r, N, 4, k)$. Let $Y = [0_s \oplus L^{N_1}, (s) \oplus L^{N_2}]$ for $s \le 4$ and $N_1 + N_2 \le N$. If $MD(Y) \ge k + 1$, then there exists an $((N_1 + N_2, s, k + 1))_4$ QECC.*

Proof. Let $Y_i = [L^{N_1}, i - 1 + L^{N_2}]$ for $i = 1, 2, \ldots, s$. Since Y_i is isomorphic to Y_1, Y_i is an OA and $t(Y_i) = k$. And we have $Y = \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_s \end{pmatrix}$. If $MD(Y) \ge k + 1$, then Y_i is an $IrOA$ $(r, N_1 + N_2, 4, k)$. By Lemma 7, an $((N_1 + N_2, s, k + 1))_s$ QECC exists.

Example 3. *As illustrations for small size codes, we obtain $((6,2,3))_4$, $((7,4,3))_4$ and $((5,4,3))_4$.*

Take an OA $(32, 7, 4, 2) = (a_1, a_2, \ldots, a_7)$ in [48]. For the case $s = 2$, take $Y = (0_2 \oplus (a_5, a_6), (2) \oplus (a_2, a_3, a_4, a_7))$. Then $MD(Y) = 3$. Application of Theorem 5 yields a new $((6,2,3))_4$ code.

Let $s = 4$ and $Y = (0_4 \oplus (a_4, a_5, a_6), (4) \oplus (a_1, a_2, a_3, a_7))$. Then $MD(Y) = 3$. By Theorem 5, we can construct a $((7,4,3))_4$ code in [47].

Let $L^5 = (a_1, a_2, \ldots, a_5)$ be an OA $(16, 5, 4, 2)$ and $Y = (0_4 \oplus (a_2, a_3), (4) \oplus (a_1, a_4, a_5))$. Then $MD(Y) = 3$ and we obtain an optimal $((5,4,3))_4$ code from Theorem 5. Every basis states of the $((5,4,3))_4$ code has 64 items. Compared to $((5,4,3))_4$ in [14], it includes less items for its base states.

Theorem 6. *Let $L = OA(r, N, 4, k)$ with MD$(L) \ge k + 1$. We can construct a QECC $((N,K,k + 1))_4$ if there are vectors $b_1, b_2, \ldots, b_K$ in $\mathbb{Z}_4^N$ such that* MD$\begin{pmatrix} 1_r \otimes b_1 + L \\ 1_r \otimes b_2 + L \\ \vdots \\ 1_r \otimes b_K + L \end{pmatrix} \ge k + 1$.

Proof: Let $M = \begin{pmatrix} M_1 \\ M_2 \\ \vdots \\ M_K \end{pmatrix} = \begin{pmatrix} 1_r \otimes b_1 + L \\ 1_r \otimes b_2 + L \\ \vdots \\ 1_r \otimes b_K + L \end{pmatrix}$. Evidently, MD$(M) \ge k + 1$ and M_i is an OA $(r, N, 4, k)$. By Lemma 7, there is a QECC $((N,K,k + 1))_4$.

Example 4. *For $N = 7$ and $r = 32$, take $L = OA(32, 7, 4, 2)$ in [48]. We can get $b_1, b_2, \ldots, b_{10} \in \mathbb{Z}_4^7$ which meet the requirements in Theorem 6 where $b_1 = (0000000)$, $b_2 = (0001103)$, $b_3 = (0011332)$, $b_4 = (0012030)$, $b_5 = (0013200)$, $b_6 = (0020021)$, $b_7 = (0022113)$, $b_8 = (0023323)$, $b_9 = (0030210)$, $b_{10} = (0031313)$. Then we can construct a new $((7,10,3))_4$ QECC, which is better than the code $((7,4,3))_4$ in [47].*

Theorem 7. *If m is an integer satisfying $4^{m-1} + 3 < 2d \le 4^m + 3$, then there exists a QECC $((n_d, 1, d))_4$ for $2m(d - 1) \le n_d \le (4^m + 1)m$.*

Proof: Let $q = 4^m$. From Lemma 6, there exists $L_B = OA\ (q^{d-1}, q + 1, q, d - 1)$. By Lemma 3, $MD\ (L_B) = q - d + 3$. When the q levels, $0, 1, \ldots, q - 1$, are replaced respectively by distinct rows of $\mathbb{Z}_4^m$, we can construct $L_C = $ OA $(q^{d-1}\ (q + 1)m, 4, d - 1)$. Removing the last $0, 1, 2, \ldots, (q - 2d + 3)m$ columns from L_C, an $L = OA\ (q^{d-1}, n_d, 4, d - 1)$ for $2m\ (d - 1) \le n_d \le (4^m + 1)m$ can be obtained and $MD(L) \ge d$. By Lemma 7, the desired QECC $((n_d, 1, d))_4$ exists.

Remark. When $m = 1$, two optimal QECCs $((2,1,2))_4$ and $((4,1,3))_4$ can be obtained.

Example 5. *By giving different values to d in Theorem 7, some new QECCs with larger distances can be obtained, which are listed in Table 1.*

Theorem 8. *Construction of new codes $((16,1,6))_4$, $((24,1,8))_4$, $((23,81,5))_4$, $((15,4,5))_4$, $((14,16,4))_4$, $((23,4,7))_4$, $((20,256,4))_4$ and $((6,1,4))_4$ from Lemma 7.*

Proof: An IrOA (4^8, 16, 4, 5) with MD = 6 obtained by using product of two OA (2^8, 16, 2, 5)s in [49] and an IrOA (4^{12}, 24, 4, 7) with MD = 8 obtained by using product of two OA (2^{12}, 24, 2, 7)s in [49] can generate two new QECCs $((16,1,6))_4$ and $((24,1,8))_4$ respectively. By using product of two OA (4608,23,2,4)s obtained from the ((23,9,5)) QECC in Example 7 in [15], we can get an OA (4608^2, 23, 4, 4) with an orthogonal partition $\{C_1, C_2, \ldots, C_{81}\}$ of strength 4 which can generate a new QECC $((23,81,5))_4$.

An IrOA (4^8, 15, 4, 5) with an orthogonal partition $\{A_1, A_2, A_3, A_4\}$ of strength 4, an IrOA (4^8, 14, 4, 5) with an orthogonal partition $\{B_1, B_2, \ldots, B_{16}\}$ of strength 3, an IrOA (4^{12}, 23, 4, 7) with an orthogonal partition $\{E_1, E_2, E_3, E_4\}$ of strength 6 and an IrOA (4^{12}, 20, 4, 7) with an orthogonal partition $\{F_1, F_2, \ldots, F_{256}\}$ of strength 3 produce four new QECCs $((15,4,5))_4$, $((14,16,4))_4$, $((23,4,7))_4$ and $((20,256,4))_4$ respectively. In particular, an IrOA (64,6,4,3) in [48] yields an optimal QECC $((6,1,4))_4$ in [50].

4 Conclusion

Binary QECCs have been widely studied, but the research on quaternary QECCs is still rare. In the study, from OAs we construct a large number of pure quaternary QECCs, some of which are optimal. The advantage of the method presented is that the quantum codes we obtain have fewer items for a basis quantum state compared with the existing ones. In future, we intend to construct more optimal QECCs with the distance ≥ 3 and investigate the q-ary QECCs for other prime powers and non-primes q from OAs.

Data availability statement

The raw data supporting the conclusion of this article will be made available by the authors, without undue reservation.

Author contributions

Supervision, SP; conceptualization, SP and FY; investigation, SP, FY, RY, JD, and TW; methodology, FY and RY; validation, FY, RY, JD, and TW; writing—original draft, FY; writing—review and editing, SP and FY All authors have read and agreed to the published version of the manuscript.

Funding

This work is supported by National Natural Science Foundation of China (Grant Nos. 11971004, 622722 08, 62172196); Open Foundation of State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications (Grant No. SKLNST-2022-1-01); Science and Tech-nology Research Project of Henan Province (202102210163); The Open Foundation of Guangxi Key Laboratory of Trusted Software (Grant No. KX202040).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

1. Peter W. Scheme for reducing decoherence in quantum computer memory. *Phys Rev A* (1995) 52:R2493–6. –R2496. doi:10.1103/physreva.52.r2493

2. Knill E, Laflamme R. Theory of quantum error-correcting codes. *Phys Rev A* (1997) 55:900–11. 900–911. doi:10.1103/physreva.55.900

3. Knill E, Laflamme R, Viola L. Theory of quantum error correction for general noise. *Phys Rev Lett* (2000) 84:2525–8. doi:10.1103/physrevlett.84.2525

4. Charles H, Bennett D, DiVincenzo P, John AS, Wootters WK. Mixed-state entanglement and quantum error correction. *Phys Rev A* (1996) 54:3824–51. doi:10.1103/physreva.54.3824

5. Steane AM. Error correcting codes in quantum theory. *Phys Rev Lett* (1996) 77:793–7. doi:10.1103/physrevlett.77.793

6. Glancy S, Knill E, Vasconcelos HM. Entanglement purification of any stabilizer state. *Phys Rev A* (2006) 74:032319. doi:10.1103/physreva.74.032319

7. Artur K. *Ekert.* Quantum Cryptography and bell's Theorem. Boston, MA: Springer US (1992).

8. Gottesman D. Theory of fault-tolerant quantum computation. *Phys Rev A* (1998) 57:127–37. doi:10.1103/physreva.57.127

9. Keqin F. Quantum codes $[[6,2,3]]_p$ and $[[7,3,3]]_p$ exist. *IEEE Trans Inf Theor* (2002) 48(8):2384–91. doi:10.1109/TIT.2002.800469

10. Keqin F, Ma Z. A finite gilbert-varshamov bound for pure stabilizer quantum codes. *IEEE Trans Inf Theor* (2004) 50(12):3323–5. doi:10.1109/tit.2004.838088

11. Keqin F, Xing C. A new construction of quantum error-correcting codes. *Trans Am Math Soc* (2008) 360(4):2007–19. doi:10.1090/s0002-9947-07-04242-0

12. Shi F, Mao-Sheng L, Lin C, Zhang X. *k*-uniform quantum information masking. *Phys Rev A* (2021) 104:032601. doi:10.1103/PhysRevA.104.032601

13. Wang Z, Yu S, Fan H, Oh CH. Quantum error-correcting codes over mixed alphabets. *Phys Rev A* (2013) 88:022328. doi:10.1103/physreva.88.022328

14. Hu D, Tang W, Zhao M, Chen Q, Yu S, Oh CH. Graphical nonbinary quantum error-correcting codes. *Phys Rev A* (2008) 78:012306. doi:10.1103/physreva.78.012306

15. Pang S, Xu H, Chen M. Construction of binary quantum error-correcting codes from orthogonal array. *Entropy* (2022) 24(7):1000. doi:10.3390/e24071000

16. Grassl M. *Bounds on the minimum distance of additive quantum codes* (2014). Availabe at: http://www.codetables.de

17. Grassl M, Beth T. Relations between classical and quantum errorcorrecting codes. In: Proceedings Workshop "Physik und Informatik"; Heidelberg, Mrz (1999).

18. Grassl M, Beth T. *A note on non-additive quantum codes* (1997). *arXiv preprint quant-ph/9703016*.

19. Beth T, Grassl M. The quantum hamming and hexacodes. *Fortschritte der Physik* (1998) 46(4-5):459–91. doi:10.1002/(sici)1521-3978(199806)46:4/5<459::aid-prop459>3.0.co;2-h

20. Dardo G, Karol Ż. Genuinely multipartite entangled states and orthogonal arrays. *Phys Rev A* (2014) 90:022316. doi:10.1103/physreva.90.022316

21. Pang S, Zhang Y, Liu S. Further results on the orthogonal arrays obtained by generalized hadamard product. *Stat Probab Lett* (2004) 68(1):17–25. doi:10.1016/j.spl.2004.03.001

22. Rao CR. *Hypercubes of strength 'd' leading to confounded designs in factorial experiments*. Karnataka: Indian Academy of Science (1946).

23. Ji L, Yin J. Constructions of new orthogonal arrays and covering arrays of strength three. *J Comb Theor Ser A* (2010) 117(3):236–47. doi:10.1016/j.jcta.2009.06.002

24. Yin J, Wang J, Ji L, Yang L. On the existence of orthogonal arrays $OA(3, 5, 4n + 2)$. *J Comb Theor Ser A* (2011) 118(1):270–6. doi:10.1016/j.jcta.2010.03.013

25. Pang S, Zhu Y, Wang Y. A class of mixed orthogonal arrays obtained from projection matrix inequalities. *J Inequalities Appl* (2015) 2015:241. –9. doi:10.1186/s13660-015-0765-6

26. Pang S, Chen L. Generalized Latin matrix and construction of orthogonal arrays. *Acta Mathematicae Applicatae Sinica, English Ser* (2017) 33(4):1083–92. doi:10.1007/s10255-017-0720-z

27. Pang S, Xiao L, Wang J. Construction of asymmetric orthogonal arrays of strength <i>t</i> from orthogonal partition of small orthogonal arrays. *IEICE Trans Fundamentals Electron Commun Comp Sci* (2018) 101(8):1267–72. doi:10.1587/transfun.e101.a.1267

28. Pang S, Xu W, Chen G, Wang Y. Construction of symmetric and asymmetric orthogonal arrays of strength t from orthogonal partition. *Indian J Pure Appl Math* (2018) 49(4):663–9. doi:10.1007/s13226-018-0293-4

29. Pang S, Wang J, Dennis K, Lin J, Liu M. Construction of mixed orthogonal arrays with high strength. *Ann Stat* (2021) 49(5):2870–84. doi:10.1214/21-aos2063

30. Dardo G, Daniel A, Latorre José I, Riera A, Życzkowski K. Absolutely maximally entangled states, combinatorial designs, and multiunitary matrices. *Phys Rev A* (2015) 92:032316. doi:10.1103/physreva.92.032316

31. Dardo G, Jakub B, Karol Ż. Multipartite entanglement in heterogeneous systems. *Phys Rev A* (2016) 94:012346. doi:10.1103/physreva.94.012346

32. Dardo G, Zahra R, Di Martino S, Karol Ż. Entanglement and quantum combinatorial designs. *Phys Rev A* (2018) 97:062326. doi:10.1103/physreva.97.062326

33. Huber F, Otfried G, Jens S. Absolutely maximally entangled states of seven qubits do not exist. *Phys Rev Lett* (2017) 118:200502. doi:10.1103/physrevlett.118.200502

34. Pang S, Zhang X, Xiao L, Zhang Q. Two and three-uniform states from irredundant orthogonal arrays. *npj Quan Inf* (2019) 5(1):52–10. doi:10.1038/s41534-019-0165-8

35. Pang S, Zhang X, Du J, Wang T. Multipartite entanglement states of higher uniformity. *J Phys A: Math Theor* (2020) 54(1):015305. doi:10.1088/1751-8121/abc9a4

36. Pang S, Zhang X, Fei S, Zheng Z. Quantum k-uniform states for heterogeneous systems from irredundant mixed orthogonal arrays. *Quan Inf Process* (2021) 20(4):156–46. doi:10.1007/s11128-021-03040-0

37. Scott AJ. Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions. *Phys Rev A* (2004) 69:052330. doi:10.1103/physreva.69.052330

38. Werner RF. All teleportation and dense coding schemes. *J Phys A: Math Gen* (2001) 34(35):7081–94. doi:10.1088/0305-4470/34/35/332

39. Rotteler M, Wocjan P. Equivalence of decoupling schemes and orthogonal arrays. *IEEE Trans Inf Theor* (2006) 52(9):4171–81. doi:10.1109/tit.2006.880059

40. Pang S, Wang X, Wang J, Du J, Miao F. Construction and count of 1-resilient rotation symmetric boolean functions. *Inf Sci* (2018) 450:336–42. doi:10.1016/j.ins.2018.03.052

41. Zhang Y, Lu Y, Pang S. Orthogonal arrays obtained by orthogonal decomposition of projection matrices. *Stat Sinica* (1999) 9(2):595–604.

42. Zhang Y, Pang S, Wang Y. Orthogonal arrays obtained by generalized hadamard product. *Discrete Math* (2001) 238(1):151–70. The Third Shanghai Conference. doi:10.1016/s0012-365x(00)00421-0

43. Pang S, Yan R, Sen L. Schematic saturated orthogonal arrays obtained by using the contractive replacement method. *Commun Statistics-Theory Methods* (2017) 46(18):8913–24. doi:10.1080/03610926.2016.1197253

44. Samad HA, Sloane N, James A, John S. *Orthogonal arrays: Theory and applications*. Berlin, Germany: Springer Science and Business Media (1999).

45. Chen G, Lei J. Constructions of mixed orthogonal arrays of strength three. *SCIENTIA SINICA Mathematica* (2017) 47:545–64. doi:10.1360/012016-23

46. Rains EM. Nonbinary quantum codes. *IEEE Trans Inf Theor* (1999) 45(6):1827–32. doi:10.1109/18.782103

47. Edel Y. *Some good quantum twisted codes* (2020). Available at: https://www.mathi.uni-heidelberg.de/yves/Matritzen/QTBCH/QTBCHIndex.html.

48. Eendebak P, Schoen E *Complete series of non-isomorphic orthogonal arrays* (2021). Available at: http://www.pietereendebak.nl/oapackage/series.html.

49. Sloane NJA *A library of orthogonal arrays* (2022). Available at: http://neilsloane.com/oadir/index.html.

50. Huber F, Markus G. Quantum codes of maximal distance and highly entangled subspaces. *Quantum* (2020) 4:284. doi:10.22331/q-2020-06-18-284