AIMS Mathematics, 11(11): 38141–38169.
DOI: 10.3934/math.20261473
Received: 05 August 2026
Revised: 22 October 2026
Accepted: 02 November 2026
Published: 16 November 2026

https://www.aimspress.com/journal/Math

Research article

Quantum codes over split semisimple rings: coordinate-correct Gray maps and exact distances

Qingyu Zhang[1,*] **and Yong Zhang**[2]

[1] School of Physics and Electronic Engineering, Jiangsu University, Zhenjiang 212013, China

[2] School of Mathematics and Statistics, Yancheng Teachers University, Yancheng 224002, China

* **Correspondence:** Email: zhangqingyu2026@126.com.

Abstract: Quantum error-correcting (QEC) and entanglement-assisted quantum error-correcting (EAQEC) constructions from ring-linear codes require both duality preservation and rigorous distance analysis. For odd q, we distinguish coefficient coordinates from Chinese remainder theorem (CRT) coordinates in $R_{q,v} = \mathbb{F}_q[v]/\langle v^3 - v\rangle$ and give the explicit change of basis. No invertible coefficient–coordinate matrix satisfying $MM^T = aI_3$ with $a \in \mathbb{F}_q^*$ preserves Euclidean duals for every $R_{q,v}$-linear code. Over a split semisimple ring $\mathcal{R} = \bigoplus_{i=1}^{s} e_i\mathbb{F}_q$, a component Gray map with mixing matrix $B \in GL_s(\mathbb{F}_q)$ preserves duals for every $\mathcal{R}$-linear code if and only if BB^T is nonsingular diagonal. Matrices satisfying this criterion and the nonsingular-by-columns (NSC) condition exist for every $s \geq 2$ and every odd $q > 2s - 1$. The NSC condition requires $s \leq q$; for orders three and four, existence is equivalent to $q > 3$. The matrix-product description gives exact classical distances for nested constituents. Counterexamples identify defects in specific component decompositions, duality claims, and a five-case distance formula. In particular, the reported $[[21, 13, 6]]_7$ parameters violate the quantum Singleton bound, whereas the corrected repeated-root construction yields $[[21, 13, 3]]_7$. Nested cyclic Reed–Solomon constituents yield the exact QEC families $[[3(q-1), 3q-15, 4]]_q$ for odd prime powers $q \geq 9$ and $[[3(q-1), 3q+3-11t, 3t]]_q$ for even $t \geq 2$ and odd prime powers $q > 6t - 1$, together with the exact EAQEC family $[[3(q-1), 3q-14, 6; 5]]_q$ for odd prime powers $q \geq 7$. Dual-distance bounds and explicit words outside the hull establish the quantum distances in these families; the general construction theorems retain lower bounds when the additional distance checks are unavailable.

Keywords: cyclic codes; semilocal rings; Gray maps; matrix-product codes; quantum error-correction; entanglement-assisted quantum codes
Mathematics Subject Classification: 94B05, 94B60, 94B70

1. Introduction

Quantum codes protect quantum memory [1]. The Calderbank–Shor–Steane (CSS) and stabilizer formalisms connect quantum codes to classical orthogonality [2, 3]. Nonbinary formulations extend the stabilizer framework to finite fields [4, 5]. Entanglement assistance relaxes the self-orthogonality requirement [6, 7]. Hulls and code intersections provide formulas for the required entanglement (see [8–10]). Cyclic codes are useful in both settings because generator polynomials and defining sets make dimensions and duals explicit [11–13]. Matrix-product codes provide a way to combine cyclic constituents and control distance [14, 15]. Ring-based quantum-code constructions provide the immediate algebraic context for the present coordinate question [16–18]. Related constructions use cyclic codes over non-chain rings [19, 20]. Recent work has developed nonsingular-by-columns (NSC) quasi-orthogonal matrices and their quantum-code applications [21–23]. Related matrix-product constructions use constacyclic codes and Euclidean hulls to obtain entanglement-assisted quantum codes [24, 25].

This paper examines the split semisimple ring

$$R_{q,v} = \mathbb{F}_q[v]/\langle v^3 - v\rangle$$

and the quantum error-correcting (QEC) and entanglement-assisted quantum error-correcting (EAQEC) constructions of [26, 27]. For odd q, $R_{q,v} \cong \mathbb{F}_q^3$ by the Chinese remainder theorem (CRT), so coefficient coordinates and component coordinates must be distinguished. We show that the inherited coefficient projections are not the CRT constituents, that the condition $MM^T = aI$ is not a universal duality criterion, and that the five-case distance formula in [27] fails on explicit small codes. The aim is not to invalidate every entry in that literature but to give a coordinate-correct verification procedure.

The contribution of the present study is an explicit CRT-coordinate characterization and its consequences for coefficient–coordinate constructions. Theorem 4.1 specializes the symmetric-basis framework for duality-preserving Gray maps [28] to the split setting and gives a direct necessity proof. Its transported form identifies the coefficient–coordinate obstruction. For compatible NSC matrices, lower-unitriangular orthogonalization and NSC preservation are known [21, Theorem 3.6]. Theorem 4.6 adds a finite-grid argument over nonzero squares to guarantee suitable column scalings for the Euclidean construction over $\mathbb{F}_q$ when $q > 2s - 1$. Theorems 4.10 and 4.11 establish the exact existence boundaries in orders three and four.

Throughout, the paper distinguishes a false general statement, a construction whose published derivation is invalid, and an independently impossible parameter set. The phrase "does not exist" is reserved for the last situation, such as the Singleton-bound contradiction for $[[21, 13, 6]]_7$; other affected parameter rows are described as requiring independent verification.

The paper gives a necessary-and-sufficient duality criterion for split semisimple rings, a matrix construction for order s when $q > 2s - 1$, the necessary bound $s \le q$, and the sharp boundary $q > 3$ in orders three and four. These results yield the corrected $[[21, 13, 3]]_7$ construction, exact QEC families with unbounded distance, and a cross-field QEC/EAQEC catalog. For the explicit EAQEC constructions, minimum-weight words outside the hull establish the quantum distances.

The main contributions are as follows:

(i) We separate CRT and coefficient coordinates by an explicit transport matrix and prove the universal

duality criterion, including the impossibility, in odd characteristic, of universal Euclidean-duality preservation by invertible coefficient-coordinate matrices satisfying $MM^T = aI_3$ with $a \in \mathbb{F}_q^*$.

(ii) We give explicit counterexamples and correct the repeated-root output $[[21, 13, 6]]_7$ to $[[21, 13, 3]]_7$.

(iii) We establish the all-orders field-size bounds and the exact order-three and order-four boundary $q > 3$.

(iv) From nested cyclic constituents, we derive exact QEC constructions and EAQEC constructions with exact distances when outside-hull witnesses are identified; these include the unbounded-distance family and the cross-field catalog.

Section 2 fixes notation for cyclic, matrix-product, and quantum codes. Section 3 derives the correct ring coordinates and presents counterexamples. Section 4 characterizes all duality-preserving component Gray maps, proves uniform all-orders existence, and resolves the third- and fourth-order boundaries sharply. Section 5 combines those results with exact matrix-product distances to rebuild the QEC and EAQEC constructions. Section 6 records the computational protocol, a cross-field parameter catalog, and detailed examples. Section 7 gives the concluding synthesis, scope, and open directions.

2. Preliminaries

2.1. Cyclic codes, reciprocals, hulls, and sums

Let q be a prime power, and let $\mathbb{F}_q$ be the field with q elements. Vectors use the Euclidean inner product

$$\langle x, y\rangle = \sum_j x_j y_j.$$

For a linear code $C \subseteq \mathbb{F}_q^n$, its dual, hull, and Euclidean sum are, respectively,

$$C^\perp = \{y : \langle x, y\rangle = 0 \text{ for all } x \in C\}, \qquad \mathrm{Hull}(C) = C \cap C^\perp, \qquad \mathrm{Sum}(C) = C + C^\perp.$$

The minimum Hamming distance is denoted by $d(C)$ with $d(\{0\}) = \infty$ when a minimum appears inside a formula. A cyclic code is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ and has a unique monic generator $f(x) \mid x^n - 1$. If $x^n - 1 = f(x)h(x)$, then $\dim C = n - \deg f$. For a polynomial $a(x) = a_0 + \cdots + a_r x^r$ with $a_0 \neq 0$, its monic reciprocal is denoted by $a^*(x)$. The Euclidean dual of $\langle f\rangle$ is $\langle h^*\rangle$ [11, 12].

Because all relevant polynomials divide $x^n - 1$, ideal intersection and addition in the cyclic quotient give

$$\mathrm{Hull}(\langle f\rangle) = \langle \mathrm{lcm}(f, h^*)\rangle, \tag{2.1}$$

$$\mathrm{Sum}(\langle f\rangle) = \langle \gcd(f, h^*)\rangle. \tag{2.2}$$

Consequently,

$$\dim \mathrm{Hull}(\langle f\rangle) = n - \deg \mathrm{lcm}(f, h^*), \qquad \dim \mathrm{Sum}(\langle f\rangle) = n - \deg \gcd(f, h^*).$$

These identities do not estimate a distance; their role is to isolate the polynomial part of the construction from the separate Gray-image problem.

The framework is written for cyclic constituents because their generator polynomials, reciprocal polynomials, hulls, and sums are explicit. Ideal or monomial codes in modular group algebras could be considered in a future extension if the corresponding dual, hull, nestedness, and distance data were available. The present results do not claim that every ideal-code family can be substituted without additional hypotheses.

2.2. Matrix-product codes

Let $C_1, \ldots, C_s \subseteq \mathbb{F}_q^n$ be linear codes, and let $A = (a_{ij}) \in \mathbb{F}_q^{s\times\ell}$ have full row rank. The matrix-product code is

$$[C_1, \ldots, C_s]A = \left\{ \left(\sum_{i=1}^{s} a_{i1}c_i, \ldots, \sum_{i=1}^{s} a_{i\ell}c_i \right) : c_i \in C_i \right\}.$$

For $1 \le i \le s$, let $D_i(A)$ be the minimum distance of the length-ℓ code spanned by the first i rows of A. The standard matrix-product bound is

$$d([C_1, \ldots, C_s]A) \ge \min_{1\le i\le s}\{d(C_i)D_i(A)\}. \tag{2.3}$$

If $C_1 \supseteq C_2 \supseteq \cdots \supseteq C_s$, equality holds in (2.3) [14, 15]. To see attainability, fix i, take a minimum word $c \in C_i$, and write a minimum word λ in the span of the first i rows as

$$\lambda = \sum_{j=1}^{i} \mu_j A_j.$$

Nestedness gives $\mu_j c \in C_j$ for $j \le i$, so the corresponding matrix-product word is $(\lambda_1 c, \ldots, \lambda_\ell c)$ and has weight $d(C_i)D_i(A)$. Minimizing over i gives the matching upper bound. The NSC hypothesis introduced later is used solely to identify $D_i(A) = s + 1 - i$. This also shows why equality need not survive when the constituents are not nested.

When $A \in GL_s(\mathbb{F}_q)$ is square,

$$([C_1, \ldots, C_s]A)^\perp = [C_1^\perp, \ldots, C_s^\perp](A^{-1})^T. \tag{2.4}$$

Indeed, the block inner product of $(c_1, \ldots, c_s)A$ and $(y_1, \ldots, y_s)(A^{-1})^T$ reduces to $\sum_i \langle c_i, y_i\rangle$. Matrix-product hulls and Euclidean sums have been used directly in recent quantum-code constructions [29, 30]; Eq (2.4) identifies the exact matrix condition needed in the present ring setting.

2.3. Quantum construction formulas

If a field-linear $[N, k, d]_q$ code D satisfies $D^\perp \subseteq D$, the CSS construction gives a quantum code

$$[[N, 2k - N, d_Q]]_q, \qquad d_Q = \min\{\mathrm{wt}_H(z) : z \in D \setminus D^\perp\} \ge d. \tag{2.5}$$

For an arbitrary $[N, k, d]_q$ code D, put $\ell = \dim(D \cap D^\perp)$, and when $D \ne \mathrm{Hull}(D)$, define

$$d_{\mathrm{out}}(D) = \min\{\mathrm{wt}_H(z) : z \in D \setminus \mathrm{Hull}(D)\}. \tag{2.6}$$

The equal-code Euclidean entanglement-assisted construction gives

$$[[N, k - \ell, d_{\mathrm{out}}(D); N - k - \ell]]_q, \tag{2.7}$$

where the last parameter is the number of maximally entangled pairs. Indeed, applying the Euclidean construction to the pair $D^{\perp}, D^{\perp}$ gives the symplectic dual $D \times D$ and intersection $\mathrm{Hull}(D) \times \mathrm{Hull}(D)$. Its minimum symplectic weight outside that intersection is exactly $d_{\mathrm{out}}(D)$. One component must lie outside the hull, and a word $(z, 0)$ attains the bound. Moreover, $c = \mathrm{rank}(HH^T) = N - k - \ell$ for a parity-check matrix H, and $d_{\mathrm{out}}(D) \geq d(D)$ [6–8]. We use the corrected arbitrary-field formulation (see [31]). Hull-controlled maximum distance separable (MDS) and EAQEC constructions illustrate how strongly ℓ can influence the final trade-off [32–34].

Every unassisted q-ary quantum code satisfies the quantum Singleton bound [5, 35]

$$2d_Q \leq N - K + 2. \tag{2.8}$$

Thus, a candidate parameter set must pass a numerical feasibility check even when it arises from a plausible algebraic derivation.

3. CRT decomposition and verification of existing claims

3.1. The two coordinate systems

Assume throughout this section that q is odd. Because

$$v^3 - v = v(v-1)(v+1)$$

has three pairwise coprime factors over $\mathbb{F}_q$, the ring $R_{q,v}$ is not only semilocal but split semisimple. The CRT therefore gives the explicit isomorphism

$$R_{q,v} \cong \mathbb{F}_q[v]/\langle v \rangle \oplus \mathbb{F}_q[v]/\langle v-1 \rangle \oplus \mathbb{F}_q[v]/\langle v+1 \rangle \cong \mathbb{F}_q^3. \tag{3.1}$$

For a code $C \subseteq R_{q,v}^n$, its Euclidean ring dual is

$$C^{\perp} = \{y \in R_{q,v}^n : \sum_{j=1}^{n} x_j y_j = 0 \text{ in } R_{q,v} \text{ for every } x \in C\}.$$

This ring-valued inner product is the dual used below; under the CRT isomorphism, it decomposes componentwise. The CRT isomorphism is the evaluation map $r(v) \mapsto (r(0), r(1), r(-1))$. Define

$$e_0 = 1 - v^2, \qquad e_+ = \frac{v^2 + v}{2}, \qquad e_- = \frac{v^2 - v}{2}. \tag{3.2}$$

Then, $e_i^2 = e_i$, $e_i e_j = 0$ for $i \neq j$, and $e_0 + e_+ + e_- = 1$. These idempotents are the primitive coordinate selectors associated with the three CRT factors.

Proposition 3.1. *Every $r = a + bv + cv^2 \in R_{q,v}$ has the unique expansion*

$$r = e_0 a + e_+(a + b + c) + e_-(a - b + c). \tag{3.3}$$

If $u = (a, b, c)$ is the coefficient vector, and $x = (r(0), r(1), r(-1))$ is the CRT vector, then

$$x = uT, \qquad T = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix}, \qquad T^{-1} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}. \tag{3.4}$$

Proof. The idempotent e_0 evaluates to $(1, 0, 0)$ at $(0, 1, -1)$, whereas e_+ and e_- evaluate to $(0, 1, 0)$ and $(0, 0, 1)$, respectively. Hence, the CRT coordinates of r are $(a, a + b + c, a - b + c)$, which proves Eq (3.3) and the formula for T. Solving for a, b, and c gives $a = x_0$, $b = (x_+ - x_-)/2$, and $c = -x_0 + (x_+ + x_-)/2$, yielding T^{-1}. □

The raw coefficient projections are defined in [26, Section 2], immediately before an un-numbered idempotent decomposition. That identification is used in Theorem 3.3 there and cited in [27, Lemma 2.5]. Of the three projections, the first is correct because $r(0) = a$; the other two treat the coefficients (b, c) as if they were the CRT values $(r(1), r(-1)) = (a + b + c, a - b + c)$. For the length-one $R_{q,v}$-linear code $C = e_0\mathbb{F}_q$, the three raw coefficient projections are $\mathbb{F}_q$, $\{0\}$, and $\mathbb{F}_q$ because $e_0 t = t - tv^2$. The asserted reconstruction from those projections would be $e_0\mathbb{F}_q \oplus e_-\mathbb{F}_q$, which has dimension two over $\mathbb{F}_q$, whereas C has dimension one. Thus, the failure is confined to the second and third identifications, a partial coincidence that can conceal the error in small examples. The correct constituents of an $R_{q,v}$-linear code C are

$$C_i = \{x \in \mathbb{F}_q^n : e_i x \in C\}, \qquad i \in \{0, +, -\}.$$

They satisfy $C = e_0C_0 \oplus e_+C_+ \oplus e_-C_-$ because multiplication of a codeword by e_i isolates its ith CRT component and remains inside the $R_{q,v}$-linear code. Conversely, the sum of three isolated components belongs to C. Uniqueness follows from orthogonality of the idempotents, which also gives

$$C^\perp = e_0C_0^\perp \oplus e_+C_+^\perp \oplus e_-C_-^\perp.$$

3.2. A duality counterexample

Let a coefficient-coordinate Gray map be $\phi_M(a + bv + cv^2) = (a, b, c)M$, where $M \in GL_3(\mathbb{F}_q)$, and denote its coordinatewise extension to $R_{q,v}^n$ by Φ_M. By Proposition 3.1, its action on the CRT vector is

$$\phi_M(r) = xB, \qquad B = T^{-1}M. \tag{3.5}$$

Thus, $MM^T = aI$ describes orthogonality in the coefficient basis, and ring duality is diagonal in the CRT basis. Congruence by T^{-1} generally destroys diagonality.

Proposition 3.2. *The condition $MM^T = aI_3$ does not imply $\Phi_M(C^\perp) = \Phi_M(C)^\perp$ for every $R_{q,v}$-linear code C.*

Proof. Take $q = 3$, and set $M = A$, where A is the coefficient matrix displayed in [27, Lemma 2.8],

$$M = \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \qquad AA^T = 4I_3 \text{ in [27]}, \quad MM^T = I_3 \text{ over } \mathbb{F}_3.$$

The orthogonal idempotents $e_0 = 1 - v^2$ and $e_+ = (v^2 + v)/2$ have coefficient vectors $(1, 0, -1)$ and $(0, 2, 2)$ over $\mathbb{F}_3$. Their images are

$$\phi_M(e_0) = (0, 2, 1), \qquad \phi_M(e_+) = (1, 0, 1),$$

whose field inner product equals 1. However, $e_0e_+ = 0$ in the ring. For $C = e_0\mathbb{F}_3$, one has $e_+ \in C^\perp$, but $\phi_M(e_+) \notin \phi_M(C)^\perp$. This disproves the universal claim. □

The displayed M is the coefficient matrix appearing in [27, Lemma 2.8]. Here, it serves only as a counterexample; no claim is made that the same matrix was used in every downstream numerical distance calculation in that paper. Corollary 4.3 is broader: It applies to every coefficient matrix satisfying $MM^T = aI_3$ in odd characteristic, which covers the scalar-orthogonality class used in the earlier constructions.

The displayed M is $2I_3$ followed by a swap of its first two output coordinates. Such a permutation preserves both Hamming weight and the Euclidean inner product. It is therefore convenient in distance computations to use the isometric normal form $2I_3$. In CRT coordinates, that normal form has

$$B_0 = 2T^{-1} = \begin{pmatrix} 2 & 0 & -2 \\ 0 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix}. \tag{3.6}$$

The off-diagonal entries of $B_0B_0^T$ include -2, so the reason for Proposition 3.2 is visible directly in component coordinates.

3.3. A distance counterexample and a feasibility contradiction

Proposition 3.3. *For the Gray map of [27], the minimum-distance formula stated there is false even for $q = 3$ and $n = 4$.*

Proof. Work over $\mathbb{F}_3$, and set

$$C_0 = C_+ = \langle x^2 + 1 \rangle, \qquad C_- = \langle x^2 - 1 \rangle$$

as cyclic codes of length four. Both constituent distances are two. The formula for the case $f_0 = f_+ \neq f_-$ predicts

$$\min\{3d(C_0), 2d(C_-), d(\langle \mathrm{lcm}(f_0, f_-) \rangle)\} = 4,$$

because the least common multiple is $x^4 - 1$ and hence generates the zero code, whose distance is read as ∞. Under the alternative convention $d(\{0\}) = 0$, the formula predicts zero, which is equally false because the image contains the following word of weight two. Thus, the counterexample is independent of the zero-code convention. Choose

$$c_0 = (0, 0, 0, 0), \quad c_+ = (0, 1, 0, 1), \quad c_- = (0, 2, 0, 1).$$

These words lie in the stated constituents. Under the component matrix B_0 in (3.6), the three length-four output blocks are

$$(0, 0, 0, 0), \qquad (0, 2, 0, 0), \qquad (0, 0, 0, 2),$$

up to the harmless output permutation. The resulting Gray word has weight two. Conversely, take any nonzero constituent tuple and choose a nonzero constituent word. That word has at least two nonzero coordinate positions. At each such position, the constituent tuple is nonzero, and multiplication by the invertible matrix B_0 gives a nonzero image tuple. Every nonzero image word therefore has a Hamming weight of at least two. Together with the displayed word, this proves that the minimum distance is exactly two, without enumeration. □

The next proposition corrects the repeated-root instance behind the reported quantum parameters. It also separates a statement valid for every invertible mixing matrix from the additional NSC and duality hypotheses needed for an exact CSS code.

Proposition 3.4. *In [27, Example 1], let $S = \mathrm{Sum}(C)$ be formed from the correct CRT constituents. For every $B \in GL_3(\mathbb{F}_7)$,*

$$d(\Phi_B(S)) \leq 3.$$

If B is NSC, and BB^T is nonsingular diagonal, then $d(\Phi_B(S)) = 3$, $d(\Phi_B(S)^\perp) \geq 6$, and the corrected CSS code has parameters

$$[[21, 13, 3]]_7.$$

Proof. Write $x^7 - 1 = (x + 6)^7$ over $\mathbb{F}_7$. The example takes $f_0 = f_+ = x + 6$ and $f_- = (x + 6)^5$. Proposition 5.2, which appears later but is independent of this coordinate analysis, gives the three constituents of S as

$$\langle x + 6\rangle, \qquad \langle x + 6\rangle, \qquad \langle (x + 6)^2\rangle.$$

They are nested MDS codes with parameters $[7, 6, 2]_7$, $[7, 6, 2]_7$, and $[7, 5, 3]_7$. The nested matrix-product equality in Theorem 5.1 therefore gives

$$d(\Phi_B(S)) = \min\{2D_1(B), 2D_2(B), 3D_3(B)\}.$$

For every invertible B, its three rows span $\mathbb{F}_7^3$, so $D_3(B) = 1$, and the distance is at most three. If B is NSC, then $(D_1, D_2, D_3) = (3, 2, 1)$, and the distance is exactly three.

The dual constituents have parameters $[7, 1, 7]_7$, $[7, 1, 7]_7$, and $[7, 2, 6]_7$. When BB^T is nonsingular diagonal, Theorem 4.1 identifies $\Phi_B(S)^\perp$ with the component image of $S^\perp$ up to nonzero row scalings. The general matrix-product bound is therefore

$$d(\Phi_B(S)^\perp) \geq \min\{3 \cdot 7, 2 \cdot 7, 1 \cdot 6\} = 6.$$

Finally, $\dim \Phi_B(S) = 6 + 6 + 5 = 17$, and $S^\perp \subseteq S$. The CSS dimension is $2(17) - 21 = 13$, and no minimum word of weight three lies in the dual because the latter has distance at least six. Hence, the CSS distance is exactly three. □

The parameter set $[[21, 13, 6]]_7$ appears in [27, Example 1], immediately after the displayed equality $d_H(\Phi(C)) = 6$. The quantum Singleton bound supplies an independent feasibility check. Substitution into (2.8) gives

$$2d = 12 > 21 - 13 + 2 = 10.$$

No quantum code with the reported parameters exists. This contradiction is independent of Propositions 3.2–3.4. It also shows why every proposed quantum parameter set should be checked against universal bounds after the algebraic construction.

Table 1 records the source, pinpoint location, and status of the claims used by the published construction. In [26], the raw projections and their claimed decomposition appeared in Section 2; Lemma 2.2 therein stated Gray-duality transport, Lemma 2.3 concerned image-code parameters, Theorem 2.4 addressed self-orthogonality under a scalar Gram condition, and Theorem 3.4 stated constituent duality. And [27, Lemma 2.6] cited the earlier Lemma 2.3 for duality, although that lemma

concerns parameters rather than duality. The first two defects concern statements inherited from [26]; the five-case equality and the listed outputs appeared in [27]. The final row is intentionally classified as unresolved rather than false. Failure of a general proof invalidates the inference, but a particular parameter set may still exist for an independently verified field code. The displayed equality following [27, Example 1] is un-numbered.

Table 1. Sources and status of the claims supporting the construction in [27].

Claim or output	Origin	Status	Evidence	Consequence
Raw coefficient projections are CRT constituents	[26, Sec. 2; Thm. 3.3]; cited in [27, Lemma 2.5]	Disproved	Length-one code $e_0\mathbb{F}_q$	Component decompositions must be recomputed
$MM^T = aI$ universally preserves duality	[26, Lem. 2.2; Thms. 2.4, 3.4]; reused in [27, Lem. 2.6]	Disproved	Proposition 3.2 and Corollary 4.3	Dual containment and hull transfer do not follow
Five-case Gray-distance equality	[27, Lemma 2.8]	Disproved	Proposition 3.3; 34 failures among 186 tested triples	Reported distances require independent verification
$[[21, 13, 6]]_7$ QEC output	[27, Example 1]	Disproved and corrected	Proposition 3.4; quantum Singleton bound	Corrected construction gives $[[21, 13, 3]]_7$
Table 3, including $q = 7, n = 6, a = 2, k = 4$: $[[18, 3, 5; 9]]_7$	[27, Table 3]	Requires independent verification	Derived through the affected duality and distance steps	No nonexistence claim is made without direct field-code analysis

4. Duality-preserving Gray maps

4.1. A necessary and sufficient condition

Let

$$\mathcal{R} = \bigoplus_{i=1}^{s} e_i\mathbb{F}_q \tag{4.1}$$

be a finite, commutative split semisimple ring, where the e_i are pairwise orthogonal idempotents summing to one. Equivalently, $\mathcal{R} \cong \mathbb{F}_q^s$. Semisimplicity means that the Jacobson radical is zero, and splitness means that every simple factor is the base field $\mathbb{F}_q$ itself rather than a proper extension. Every $\mathcal{R}$-linear code has a unique decomposition

$$C = \bigoplus_{i} e_i C_i,$$

where $C_i = \{x \in \mathbb{F}_q^n : e_i x \in C\}$. For an element

$$r = \sum_i e_i x_i,$$

write $x = (x_1, \ldots, x_s)$, and define

$$\phi_B(r) = xB \in \mathbb{F}_q^s, \tag{4.2}$$

where $B \in GL_s(\mathbb{F}_q)$. Extend ϕ_B coordinatewise to $\mathcal{R}^n$. After a fixed permutation arranging the output in s blocks of length n, its image on a code is

$$\Phi_B(C) = [C_1, \ldots, C_s]B. \tag{4.3}$$

Interleaving the blocks coordinate by coordinate only applies a fixed permutation and does not affect duality or distance. More explicitly, if Π is the corresponding permutation matrix on $\mathbb{F}_q^{sn}$, then an interleaved image is $\Phi_B(C)\Pi$ and $(u\Pi) \cdot (v\Pi) = u \cdot v$ for all u, v. At the component level, replacing B by BP for a permutation matrix P gives $(BP)(BP)^T = BB^T$. Here and throughout, "Gray map" denotes an $\mathbb{F}_q$-linear coordinate map $\mathcal{R}^n \to \mathbb{F}_q^{sn}$; it is not assumed to preserve Hamming weight or to be an isometry unless this is stated explicitly. Every distance statement refers to the Hamming distance of the image code.

Theorem 4.1. *For $B \in GL_s(\mathbb{F}_q)$, the equality*

$$\Phi_B(C^\perp) = \Phi_B(C)^\perp \tag{4.4}$$

holds for every length and every $\mathcal{R}$-linear code C if and only if

$$BB^T = \operatorname{diag}(d_1, \ldots, d_s), \qquad d_i \in \mathbb{F}_q^*. \tag{4.5}$$

Theorem 4.1 gives an explicit CRT-coordinate characterization in the split setting. It is a specialization of the symmetric-basis framework in [28, Definition 3.13 and Theorem 3.17], whose duality results also apply to all ring-linear codes under the stated basis hypotheses. In the image coordinates, multiplication by an element with CRT coordinates $(a_1, \ldots, a_s)$ has a matrix $B^{-1} \operatorname{diag}(a_1, \ldots, a_s)B$. These matrices are all symmetric exactly when BB^T commutes with every diagonal matrix, equivalently when BB^T is diagonal. The length-one argument below proves necessity directly. We use this explicit characterization to obtain the coefficient–coordinate criterion and Corollary 4.3 rather than claim a new general principle of duality-preserving Gray maps.

Proof. Suppose first that $BB^T = D$ is nonsingular diagonal. Equation (2.4) and $(B^{-1})^T = D^{-1}B$ give

$$\Phi_B(C)^\perp = [C_1^\perp, \ldots, C_s^\perp]D^{-1}B.$$

Multiplication of the ith constituent by $d_i^{-1} \neq 0$ leaves that linear code unchanged. The right-hand side is therefore

$$[C_1^\perp, \ldots, C_s^\perp]B = \Phi_B(C^\perp).$$

Conversely, assume (4.4) for every code. For a fixed i, take length one with $C_i = \{0\}$ and $C_j = \mathbb{F}_q$ for $j \neq i$. Then, $C_i^\perp = \mathbb{F}_q$, and $C_j^\perp = \{0\}$, so (4.4) says that the span of row i of B equals the span of row i of $(B^{-1})^T$. Both rows are nonzero. Hence, $(B^{-1})^T = \Lambda B$ for a nonsingular diagonal matrix Λ. Multiplication on the right by B^T yields $\Lambda BB^T = I$; consequently, $BB^T = \Lambda^{-1}$. This is a nonsingular diagonal matrix. □

Corollary 4.2. *For $R_{q,v}$ and a coefficient–coordinate matrix $M \in GL_3(\mathbb{F}_q)$, the associated Gray map preserves Euclidean duals for every code if and only if*

$$T^{-1}MM^TT^{-T} \quad \text{is nonsingular diagonal}, \tag{4.6}$$

where T is given in (3.4).

Proof. Equation (3.5) gives $BB^T = T^{-1}MM^TT^{-T}$. The result follows from Theorem 4.1. □

Corollary 4.3. *Let q be odd. No coefficient-coordinate matrix $M \in GL_3(\mathbb{F}_q)$ satisfying $MM^T = aI_3$ with $a \in \mathbb{F}_q^*$ preserves Euclidean duality for every $R_{q,v}$-linear code.*

Proof. If $MM^T = aI_3$, then

$$T^{-1}MM^TT^{-T} = aT^{-1}T^{-T} = a\begin{pmatrix} 2 & -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}.$$

Because q is odd and $a \neq 0$, the entries $-a/2$ are nonzero. The matrix is therefore not diagonal, so Corollary 4.2 excludes universal duality preservation. □

The scalar-orthogonality condition is thus not merely insufficient for the particular matrix in Proposition 3.2; it is incompatible with universal ring-duality preservation throughout the odd-characteristic setting of $R_{q,v}$. The obstruction is basis-dependent congruence, not a failure of orthogonal matrices themselves. Component coordinates remove the ambiguity and turn the correct design problem into the row orthogonality of B.

4.2. Uniform existence and sharp low-order boundaries

An $s \times s$ matrix is NSC if every $i \times i$ minor formed from its first i rows is nonzero for $1 \leq i \leq s$. Equivalently, those rows generate an $[s, i, s + 1 - i]$ MDS code; hence, $D_i(B) = s + 1 - i$. A matrix with nonsingular diagonal BB^T is often called quasi-orthogonal. General triangular orthogonalization and many concrete or algorithmically generated NSC quasi-orthogonal matrices are known [21–23]. Recent work has also studied broader orthogonality decompositions over quadratic extensions [36]. We first record an elementary obstruction inherent in the NSC property and then turn the Vandermonde-scaling strategy into a symbolic base-field guarantee in every order. The finite-grid lemma used in the latter proof is the nonvanishing principle underlying the combinatorial Nullstellensatz [37]; a proof is included for self-containedness.

Lower-unitriangular orthogonalization and its preservation of the NSC property are established in [21, Theorem 3.6]. The additional step in Theorem 4.6 is a finite-grid argument over the nonzero squares of $\mathbb{F}_q$. It guarantees column scalings for which all leading Gram determinants are nonzero. The theorem thus supplies the sufficient field-size range $q > 2s - 1$ for the Euclidean construction over the base field; no novelty is claimed for triangular orthogonalization itself. Theorems 4.10 and 4.11 establish exact existence boundaries in orders three and four.

Proposition 4.4. *If an $s \times s$ NSC matrix exists over $\mathbb{F}_q$ with $s \geq 2$, then $s \leq q$.*

Proof. Let $B = (b_{ij})$ be NSC. Its first-row entries are nonzero, so the ratios

$$\rho_j = \frac{b_{2j}}{b_{1j}}, \qquad 1 \le j \le s$$

are defined. If $\rho_j = \rho_k$ for distinct columns j, k, then the corresponding 2×2 minor of the first two rows is zero, contrary to the NSC condition. Thus, $\rho_1, \dots, \rho_s$ are distinct elements of $\mathbb{F}_q$, which forces $s \le q$. □

Lemma 4.5. *Let F be a field, let $P \in F[z_1, \dots, z_s]$ be nonzero, and let $S_j \subseteq F$ satisfy $|S_j| > \deg_{z_j} P$ for every j. Then, P is nonzero at some point of $S_1 \times \cdots \times S_s$.*

Proof. For $s = 1$, this is the root bound for a nonzero polynomial. Induct on s, writing P as a polynomial in z_s whose nonzero leading coefficient is a polynomial in the first $s - 1$ variables. The induction hypothesis makes that coefficient nonzero at some point of $S_1 \times \cdots \times S_{s-1}$; the resulting univariate polynomial has fewer roots than $|S_s|$. □

Theorem 4.6. *Let $s \ge 2$, and let q be odd with $q > 2s - 1$. There exists $B \in GL_s(\mathbb{F}_q)$ such that B is NSC and such that*

$$BB^T = \operatorname{diag}(d_1, \dots, d_s), \qquad d_i \in \mathbb{F}_q^*.$$

Consequently, one Gray matrix simultaneously preserves Euclidean duals for every code over $\bigoplus_{i=1}^{s} e_i\mathbb{F}_q$ and has row-span distances $D_i(B) = s + 1 - i$.

Proof. Choose distinct $\alpha_1, \dots, \alpha_s \in \mathbb{F}_q$, and form the Vandermonde matrix

$$A = (\alpha_j^{i-1})_{1 \le i,j \le s}.$$

It is NSC because every leading-row minor is a nonzero Vandermonde determinant. Let A_i denote its first i rows, and introduce

$$\Delta_i(z_1, \dots, z_s) = \det(A_i \operatorname{diag}(z_1, \dots, z_s) A_i^T).$$

The Cauchy–Binet formula gives

$$\Delta_i(z_1, \dots, z_s) = \sum_{\substack{J \subseteq \{1,\dots,s\} \\ |J| = i}} \det(A_{i,J})^2 \prod_{j \in J} z_j. \tag{4.7}$$

Every displayed coefficient is nonzero, so each Δ_i is a nonzero multiaffine polynomial. Because $\mathbb{F}_q[z_1, \dots, z_s]$ is an integral domain, the product of the nonzero polynomials $\Delta_1, \dots, \Delta_{s-1}$ is nonzero; hence, the avoidance polynomial below is not identically zero. For $i = s$, there is only one term in (4.7), namely

$$\Delta_s(z_1, \dots, z_s) = \det(A)^2 z_1 \cdots z_s,$$

which is automatically nonzero on $(\mathbb{F}_q^*)^s$ and need not be included in the avoidance polynomial. Therefore,

$$P(z_1, \dots, z_s) = \prod_{i=1}^{s-1} \Delta_i(z_1, \dots, z_s)$$

is nonzero, and $\deg_{z_j} P \le s-1$ for every j.

Let $S = (\mathbb{F}_q^*)^2$ be the set of nonzero squares. Because

$$|S| = (q-1)/2 > s-1 \ge \deg_{z_j} P$$

for every j, Lemma 4.5 applies to the same set in every coordinate and supplies $(z_1, \dots, z_s) \in S^s$ with $P(z_1, \dots, z_s) \neq 0$. Choose $u_j \in \mathbb{F}_q^*$ with $u_j^2 = z_j$, and put $U = \mathrm{diag}(u_1, \dots, u_s)$. The first $s-1$ leading principal minors of $G = (AU)(AU)^T$ are nonzero by construction, and the last is $\det(A)^2 \prod_j z_j \neq 0$. Let G_i denote the leading $i \times i$ principal block, and set $\Delta_0 = 1$. Then, the no-pivot elimination coefficients are $d_i = \Delta_i/\Delta_{i-1} \neq 0$. Thus, the finite-field LDL^T factorization exists without pivoting:

$$G = L_0 D L_0^T,$$

where L_0 is lower unitriangular, and D is nonsingular diagonal. Setting $L = L_0^{-1}$ and

$$B = LAU$$

gives $BB^T = D$. This triangular orthogonalization step is the one established in [21, Theorem 3.6].

It remains to check that orthogonalization has not destroyed the distance property. For each i, the first i rows of LAU equal $L_i A_i U$, where L_i is lower unitriangular. For every i-element column set J, the corresponding leading-row minor is

$$\det((L_i A_i U)_J) = \det(L_i) \det((A_i)_J) \prod_{j \in J} u_j.$$

Hence, every corresponding $i \times i$ minor is the associated minor of A_i multiplied by $\det(L_i) = 1$ and by nonzero selected diagonal entries of U. It is nonzero, so B is NSC. The duality conclusion follows from Theorem 4.1. □

The proof of Theorem 4.6 gives a finite construction procedure: Enumerate the square-weight vectors until P is nonzero, choose their square roots, and perform no-pivot LDL^T elimination. The finite-grid argument guarantees termination. This is an effective construction, not a uniform closed-form formula for the weights or a polynomial-time complexity claim. The field-size range is sufficient, not a claimed sharp boundary. For $s = 2$, the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ is NSC and has a Gram matrix $2I_2$ over every odd field, including $\mathbb{F}_3$; thus, the sufficient inequality is not necessary even in the smallest order. When $s = 3$, the theorem covers $q > 5$; the next results add $q = 5$, exclude $q = 3$, and sharpen the third-order answer to $q > 3$. For a 3×3 matrix, the NSC condition reduces to nonzero first-row entries, three nonzero 2×2 minors from the first two rows, and a nonzero determinant. After the third-order classification, the same target boundary is established in order four by combining Proposition 4.4, the uniform theorem, and two small-field witnesses.

Proposition 4.7. *Assume* $\mathrm{char}(\mathbb{F}_q) \notin \{2, 3\}$. *The matrix*

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ -2 & 1 & 1 \end{pmatrix} \tag{4.8}$$

satisfies

$$BB^T = \mathrm{diag}(3, 2, 6). \tag{4.9}$$

It is NSC. Consequently,

$$D_1(B) = 3, \qquad D_2(B) = 2, \qquad D_3(B) = 1. \tag{4.10}$$

In coefficient coordinates, the same Gray map is represented by

$$M = TB = \begin{pmatrix} -1 & 3 & 1 \\ 2 & 0 & -2 \\ -2 & 2 & 0 \end{pmatrix}. \tag{4.11}$$

Proof. The three rows of B are pairwise orthogonal and have squared norms 3, 2, and 6, proving (4.9). Every entry of the first row is nonzero. The 2×2 minors formed from the first two rows and any two columns are 1, -1, and -2, and $\det B = 6$. All are nonzero under the characteristic assumption, so B is NSC. The row-span distances in (4.10) follow. Direct multiplication by T gives Eq (4.11). □

The two properties of B serve different parts of the construction. Equation (4.9) invokes Theorem 4.1; nonsingularity by columns invokes the sharp matrix-product distance theorem. Their coexistence closes a gap that cannot be resolved by selecting a coefficient matrix solely from $MM^T = aI$.

Proposition 4.8. *No matrix $B \in GL_3(\mathbb{F}_3)$ is simultaneously NSC and duality-preserving for every code over $\mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3$.*

Proof. If B is NSC, every entry of its first row is nonzero. Each nonzero element of $\mathbb{F}_3$ has square one, so the squared norm of that row is $1 + 1 + 1 = 0$. Universal duality preservation would require BB^T to be nonsingular diagonal by Theorem 4.1, in particular with a nonzero first diagonal entry. This is impossible. □

Proposition 4.9. *Let $q = 3^m$ with $m \geq 2$. Choose*

$$t \in \mathbb{F}_q \setminus \{0, 1, -1\}, \qquad a^2 = -t^{-1}, \tag{4.12}$$

and define

$$B_t = \begin{pmatrix} 1 & 1 & a \\ 0 & 1 & at \\ a(t-1) & -at & 1 \end{pmatrix}. \tag{4.13}$$

Admissible pairs (t, a) always exist. Every such B_t is NSC and satisfies

$$B_t B_t^T = \mathrm{diag}(a^2 - 1,\ 1 - t,\ t - t^{-1}). \tag{4.14}$$

There are $q - 5$ admissible pairs when m is even and $q - 3$ when m is odd.

Proof. Let χ be the quadratic character of $\mathbb{F}_q^*$. The equation for a in (4.12) is solvable precisely when

$$\chi(-t^{-1}) = 1 \quad \text{or, equivalently,} \quad \chi(t) = \chi(-1).$$

This condition selects $(q-1)/2$ nonzero values of t. If m is even, then $q \equiv 1 \pmod 4$, and both 1 and -1 are selected; because $q \geq 9$, removing them leaves $(q-5)/2 > 0$ choices. If m is odd, then $m \geq 3$, $q \equiv 3$

(mod 4), and only -1 is selected; removing it leaves $(q-3)/2 > 0$ choices. Each selected t has exactly two square roots a, which also proves the stated pair counts.

The first two rows of B_t are orthogonal because $1 + a^2 t = 0$. The third row is their cross product, so it is orthogonal to both. Direct calculation using $a^2 = -t^{-1}$ gives their squared norms

$$a^2 - 1, \qquad 1 - t, \qquad (a^2 - 1)(1 - t) = t - t^{-1},$$

which are all nonzero because $t \notin \{0, 1, -1\}$. This proves (4.14). The three 2×2 minors from the first two rows are

$$1, \qquad at, \qquad a(t-1),$$

and $\det B_t = t - t^{-1}$. Together with the nonzero first-row entries, these identities prove the NSC property. □

Theorem 4.10. *Let q be odd. There exists a matrix $B \in GL_3(\mathbb{F}_q)$ that is simultaneously NSC and duality-preserving for every code over $\mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q$ if and only if $q > 3$.*

Proof. Proposition 4.8 proves nonexistence when $q = 3$. For $q > 3$ in characteristic other than three, Proposition 4.7 supplies the required matrix. If $q = 3^m$ with $m \geq 2$, Proposition 4.9 supplies B_t. In both positive cases, the Gram matrix is nonsingular diagonal, so universal duality follows from Theorem 4.1; the matrix is NSC by the same proposition. □

The threshold in Theorem 4.10 closes the characteristic-three extension-field gap rather than merely adding isolated examples. In coefficient coordinates, every matrix above becomes $M = TB$. It therefore satisfies the transported criterion (4.6), although MM^T need not be scalar; this is exactly why the sharp existence theorem is consistent with Corollary 4.3.

Theorem 4.11. *Let q be odd. There exists a matrix $B \in GL_4(\mathbb{F}_q)$ that is simultaneously NSC and duality-preserving for every code over $\mathbb{F}_q^4$ if and only if $q > 3$.*

Proof. If such a matrix exists, Proposition 4.4 gives $4 \leq q$; because q is odd, this is equivalent to $q > 3$. Conversely, Theorem 4.6 with $s = 4$ covers every odd $q > 7$. The two remaining fields are covered by

$$B_5 = \begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & 1 & 2 & 1 \\ 2 & 1 & 2 & 0 \\ 3 & 1 & 4 & 1 \end{pmatrix}, \qquad B_7 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 3 & 4 & 5 \\ 1 & 6 & 6 & 1 \\ 6 & 3 & 4 & 1 \end{pmatrix}, \tag{4.15}$$

where the subscripts indicate the base fields. Direct multiplication gives

$$B_5 B_5^T = \operatorname{diag}(2, 1, 4, 2), \qquad B_7 B_7^T = \operatorname{diag}(4, 5, 4, 6).$$

For completeness, list the leading-row minors in lexicographic column order. At sizes $1, 2, 3, 4$, they are respectively

$$\begin{aligned} B_5 :&\quad (1,1,1,2),\ (1,2,1,1,4,2),\ (2,2,2,4),\ (4), \\ B_7 :&\quad (1,1,1,1),\ (1,2,3,1,2,1),\ (2,6,6,2),\ (5). \end{aligned}$$

Every listed entry is nonzero in its stated field, so both matrices are NSC. Their nonsingular diagonal Gram matrices give universal duality preservation by Theorem 4.1. □

Thus, the exact boundary $q > 3$ persists from order three to order four, although the two proofs close different gaps. Order three requires a family in characteristic three, whereas order four requires the isolated base-field witnesses in (4.15). Proposition 4.4 also shows that no order-s extension can exist when $s > q$ independently of duality.

Example 4.12. *(The smallest positive characteristic-three case) Let* $\mathbb{F}_9 = \mathbb{F}_3[z]/\langle z^2 + 1\rangle$. *Taking* $t = z$ *and* $a = 1 + 2z$ *in Proposition 4.9 gives*

$$B_z = \begin{pmatrix} 1 & 1 & 1+2z \\ 0 & 1 & 1+z \\ 2z & 2+2z & 1 \end{pmatrix}, \qquad B_z B_z^T = \operatorname{diag}(2+z,\ 1+2z,\ 2z).$$

Its determinant is $2z$, *so* B_z *is an explicit NSC duality-preserving Gray matrix over the smallest field not covered by Proposition 4.7.*

5. Exact distances and corrected quantum constructions

5.1. Gray images as matrix-product codes

Theorem 5.1. *Let* $C = \bigoplus_{i=1}^{s} e_i C_i$ *be a code over the ring in* (4.1), *and let* $B \in GL_s(\mathbb{F}_q)$. *Then,*

$$d(\Phi_B(C)) \geq \min_{1\leq i\leq s}\{d(C_i)D_i(B)\}. \tag{5.1}$$

If $C_1 \supseteq \cdots \supseteq C_s$, *equality holds. In particular, for odd* $q > 2s - 1$ *and with* B *supplied by Theorem 4.6,*

$$d(\Phi_B(C)) = \min_{1\leq i\leq s}\{(s+1-i)d(C_i)\}. \tag{5.2}$$

For $s \in \{3, 4\}$, *the weaker and sharp field condition* $q > 3$ *is sufficient for* (5.2). *In particular, for* $s = 3$,

$$d(\Phi_B(C)) = \min\{3d(C_1), 2d(C_2), d(C_3)\}. \tag{5.3}$$

Proof. By definition, $\Phi_B(C) = [C_1, \ldots, C_s]B$. Equation (5.1) is therefore (2.3). Equality under nestedness is the exact nested matrix-product result of [15]. An $s \times s$ NSC matrix has $D_i(B) = s + 1 - i$, so Theorem 4.6 gives (5.2). Theorems 4.10 and 4.11 improve the field range in orders three and four, respectively; the former gives (5.3) over every odd $q > 3$. □

Theorem 5.1 also explains Proposition 3.3. Listing several families of ring codewords proves upper bounds on the minimum distance. It cannot prove equality unless all possible cancellations between mixed constituents are controlled. Matrix-product row-span distances perform exactly that control. For nonnested constituents, (5.1) remains valid, but equality should not be asserted without an independent proof.

5.2. Correct hull and sum formulas

Proposition 5.2. *Let*

$$C = e_0 C_0 \oplus e_+ C_+ \oplus e_- C_-, \qquad C_i = \langle f_i(x)\rangle, \qquad x^n - 1 = f_i(x)h_i(x).$$

Using the CRT constituents, not raw coefficient projections, one has

$$\mathrm{Hull}(C) = \bigoplus_{i\in\{0,+,-\}} e_i\langle \mathrm{lcm}(f_i, h_i^*)\rangle, \tag{5.4}$$

$$\mathrm{Sum}(C) = \bigoplus_{i\in\{0,+,-\}} e_i\langle \gcd(f_i, h_i^*)\rangle. \tag{5.5}$$

Moreover, if B satisfies (4.5)*, then*

$$\Phi_B(\mathrm{Hull}(C)) = \mathrm{Hull}(\Phi_B(C)), \qquad \Phi_B(\mathrm{Sum}(C)) = \mathrm{Sum}(\Phi_B(C)). \tag{5.6}$$

Proof. Orthogonality of the idempotents gives

$$C^\perp = \bigoplus_i e_i C_i^\perp.$$

Intersections and sums are therefore computed componentwise. Equations (2.1) and (2.2) prove (5.4) and (5.5). If (4.5) holds, Theorem 4.1 gives

$$\Phi_B(C^\perp) = \Phi_B(C)^\perp.$$

Because Φ_B is a vector-space isomorphism, it preserves intersections and sums, proving (5.6). □

5.3. QEC codes from corrected Euclidean sums

Theorem 5.3. *Let $q > 3$ be odd, and choose any matrix B supplied by Theorem 4.10. For $i = 0, +, -$, let*

$$g_i = \gcd(f_i, h_i^*),$$

and suppose $g_0 \mid g_+ \mid g_-$. Put

$$\delta_S = \min\{3d(\langle g_0\rangle), 2d(\langle g_+\rangle), d(\langle g_-\rangle)\}. \tag{5.7}$$

Then, there exists a QEC code

$$\left[\left[3n, 3n - 2\sum_i \deg g_i, d_Q\right]\right]_q, \qquad d_Q \geq \delta_S. \tag{5.8}$$

If $d(\Phi_B(\mathrm{Sum}(C))^\perp) > \delta_S$, then $d_Q = \delta_S$.

Proof. Proposition 5.2 gives the constituents of $S = \mathrm{Sum}(C)$. The divisibility hypothesis implies $\langle g_0\rangle \supseteq \langle g_+\rangle \supseteq \langle g_-\rangle$. Hence, $D = \Phi_B(S)$ has dimension $k_D = 3n - \sum_i \deg g_i$ and exact distance δ_S by Theorem 5.1. Because

$$S^\perp = C \cap C^\perp \subseteq S,$$

Theorem 4.1 gives $D^\perp \subseteq D$. Equation (2.5) yields (5.8). Finally, if every nonzero word of $D^\perp$ has weight larger than δ_S, a minimum word of D cannot lie in $D^\perp$, so the CSS distance equals δ_S. □

5.4. EAQEC codes from corrected hulls

Theorem 5.4. *Let $q > 3$ be odd, choose any matrix B supplied by Theorem 4.10, and let $C = e_0\langle f_0\rangle \oplus e_+\langle f_+\rangle \oplus e_-\langle f_-\rangle$ be a cyclic $R_{q,v}$-code as in Proposition 5.2. Suppose that $f_0 \mid f_+ \mid f_-$. Define*

$$k = 3n - \sum_i \deg f_i, \tag{5.9}$$

$$\ell = \sum_i \left(n - \deg \operatorname{lcm}(f_i, h_i^*)\right), \tag{5.10}$$

$$\delta = \min\{3d(\langle f_0\rangle), 2d(\langle f_+\rangle), d(\langle f_-\rangle)\}. \tag{5.11}$$

Let $D = \Phi_B(C)$, assume $k > \ell$, and set

$$\delta_{\mathrm{EA}} = d_{\mathrm{out}}(D) = \min\{\mathrm{wt}_H(z) : z \in D \setminus \mathrm{Hull}(D)\}. \tag{5.12}$$

Then, $\delta_{\mathrm{EA}} \geq \delta$, and there exists an EAQEC code

$$[[3n, k - \ell, \delta_{\mathrm{EA}}; 3n - k - \ell]]_q. \tag{5.13}$$

Proof. The divisibility hypothesis is equivalent to $\langle f_0\rangle \supseteq \langle f_+\rangle \supseteq \langle f_-\rangle$. Thus, $D = \Phi_B(C)$ has dimension k and exact classical distance δ by Theorem 5.1. Because $D \setminus \mathrm{Hull}(D)$ is a subset of the nonzero words of D, Eq (5.12) gives $\delta_{\mathrm{EA}} \geq \delta$. Equations (5.4) and (5.6) show that $\dim \mathrm{Hull}(D) = \ell$. Applying the exact equal-code construction (2.7) with $N = 3n$ proves (5.13). □

Theorems 5.3 and 5.4 use the same sequence of verified steps: CRT constituents determine cyclic duals, Theorem 4.1 transfers duality, Theorem 5.1 fixes the classical distance, and only then are CSS or entanglement-assisted parameters formed. Omitting any one of these steps reopens the gap exposed in Section 3. For the explicit QEC families in Corollary 6.1, the repeated-root construction in Proposition 3.4, and Example 6.2, the classical distance is exact by Theorem 5.1, and the stated dual-distance bounds establish equality for the CSS distance. Theorem 5.3 gives the lower bound $d_Q \geq \delta_S$ unless its additional dual-distance condition is satisfied. Similarly, Theorem 5.4 gives the exact classical image distance δ and the quantum-distance lower bound $\delta_{\mathrm{EA}} \geq \delta$; equality is established for the explicit EAQEC constructions by a minimum-weight word outside the hull.

6. Computational verification and explicit examples

6.1. Reproducible verification protocol

The exhaustive searches over $q = 3, 5, 7$ used prime-field arithmetic with polynomial coefficients stored in ascending order. Monic divisors of $x^n - 1$ were generated from the complete factorization in $\mathbb{F}_q[x]$. A generator matrix for $\langle f(x)\rangle$ consisted of the coefficient vectors of $f, xf, \ldots, x^{n-\deg f-1}f$. Minimum distances in the reported small cases were obtained by enumerating every nonzero message vector, not by random search. The generator matrix of the image code was assembled from the constituent generator matrices and the stated component matrix. The cross-field catalog was checked separately through defining sets modulo $q - 1$, which applies equally to prime and extension fields; for the four rows with $q = 9$, the accompanying implementation additionally performed polynomial

division and reciprocation, as well as greatest common divisor (GCD) and least common multiple (LCM) calculations in $\mathbb{F}_9 = \mathbb{F}_3[z]/\langle z^2 + 1\rangle$. The verification scripts are available from Zenodo.

For $\mathbb{F}_9 = \mathbb{F}_3[z]/\langle z^2 + 1\rangle$, the extension-field verification routine finds exactly two admissible values of t; for $\mathbb{F}_{27} = \mathbb{F}_3[z]/\langle z^3 - z - 1\rangle$, it finds twelve. For every admissible value, it verifies the full Gram matrix, the three leading-row 2×2 minors, all first-row entries, and the determinant. These even- and odd-degree test fields independently exercise both quadratic-character cases in the proof of Proposition 4.9; the theorem itself remains symbolic and does not depend on the computation.

For the all-orders construction, the all-orders verification routine starts from a Vandermonde matrix, searches only nonzero-square column weights, performs finite-field Gram–Schmidt elimination, and then exhaustively checks every leading-row minor. Orders 4, 5, and 6 pass over $\mathbb{F}_{11}$, $\mathbb{F}_{13}$, and $\mathbb{F}_{17}$, respectively, with nonsingular diagonal Gram matrices. The same routine independently verifies all minors and Gram entries of B_5 and B_7 in (4.15). These cases test both the scalable algorithm and the two small-field witnesses; the proofs of Theorems 4.6 and 4.11, rather than the finite test list, establish the stated results.

We exhaustively checked the five-case formula for the following pairs:

$$(q, n) = (3, 3), (3, 4), (3, 5), (5, 3).$$

For each pair, all ordered triples of nonzero cyclic codes whose total constituent dimension was at most six were tested. This finite search comprised 186 triples. Exact enumeration found 34 disagreements between the published prediction and the actual Gray distance. Proposition 3.3 is the smallest transparent witness selected from those failures. The count is not used as a statistical estimate; it records exhaustive behavior on the declared test domain. The Appendix lists all 34 discrepancies.

Positive examples were required to pass four checks. Each f_i divided $x^n - 1$ exactly; reciprocal, GCD, and LCM degrees agreed with direct generator-matrix ranks; constituent distances were exhaustively enumerated; and the final parameters satisfied dimension identities and applicable quantum bounds. Full Gray-code enumeration was avoided only when its dimension was large, in which case, Theorem 5.1 supplied an exact proof from nested constituents. Small dual codes were enumerated directly when the exact CSS distance required excluding $D^{\perp}$.

6.2. A cross-field family and parameter catalog

The positive output need not be restricted to isolated searches. Let $n = q - 1$, fix a primitive element $\alpha \in \mathbb{F}_q$, and for $0 \le r < n$, define

$$f_r^{(b)}(x) = \prod_{j=0}^{r-1}(x - \alpha^{b+j}), \qquad C_r^{(b)} = \langle f_r^{(b)}(x)\rangle, \tag{6.1}$$

where exponents are read modulo n, and $f_0^{(b)} = 1$. The defining set is $Z_r(b) = \{b, b + 1, \ldots, b + r - 1\} \pmod n$. The Bose–Chaudhuri–Hocquenghem bound and the Singleton bound give

$$C_r^{(b)} = [n, n - r, r + 1]_q. \tag{6.2}$$

Thus, these are cyclic Reed–Solomon codes, and $C_{r_0}^{(b)} \supseteq C_{r_1}^{(b)} \supseteq C_{r_2}^{(b)}$ whenever $r_0 \le r_1 \le r_2$. Their hull dimensions have the closed form

$$\eta_r(b) = \dim \mathrm{Hull}(C_r^{(b)}) = r - |Z_r(b) \cap (-Z_r(b))|. \tag{6.3}$$

Indeed, the defining set of the Euclidean dual is $-Z_r(b)^c$; the generator of the hull code has defining set $Z_r(b) \cup (-Z_r(b)^c)$, and taking the complement gives (6.3). Also, $C_r^{(b)}$ is dual-containing exactly when $Z_r(b) \cap (-Z_r(b)) = \varnothing$.

Generalized Reed–Solomon and matrix-product routes to quantum codes are well-established [38]; the role of (6.1) here is to turn the coordinate-correct Euclidean theory into closed same-field consequences with exact, rather than designed, quantum distance.

Corollary 6.1. *Let q be an odd prime power, and put $n = q - 1$.*

(a) Let $0 \le r_0 \le r_1 \le r_2$ satisfy $r_2 \ge 1$ and $2r_2 < n$, and set

$$\delta = \min\{3(r_0 + 1), 2(r_1 + 1), r_2 + 1\}.$$

Then, there exists a QEC code with the exact distance

$$[[3(q-1), 3(q-1) - 2(r_0 + r_1 + r_2), \delta]]_q. \tag{6.4}$$

(b) If $q \ge 7$, then there exists an EAQEC code with the exact distance

$$[[3(q-1), 3q - 14, 6; 5]]_q. \tag{6.5}$$

(c) Let $t \ge 2$ be even. If $q > 6t - 1$, then there exists a QEC code with the exact distance

$$[[3(q-1), 3q + 3 - 11t, 3t]]_q. \tag{6.6}$$

In particular, part (a) gives

$$[[3(q-1), 3q - 15, 4]]_q \quad (q \ge 9), \tag{6.7}$$

whereas part (c) with $t = 2$ recovers $[[3(q-1), 3q - 19, 6]]_q$ for $q \ge 13$.

Proof. Choose a matrix from Theorem 4.10. For (a), take $b = 1$. The condition $2r_2 < n$ makes $Z_{r_2}(1) = \{1, \ldots, r_2\}$ disjoint from its negative modulo n, so all three constituents are dual-containing. Theorem 5.1 gives a dual-containing image D with parameters

$$[3n, 3n - (r_0 + r_1 + r_2), \delta]_q.$$

The distance condition needed below is automatic: $\delta \le r_2 + 1$, and $2r_2 < n = q - 1$ gives $r_2 + 1 < q - r_2$. For $r_i > 0$, the dual constituent is the MDS code $[n, r_i, n - r_i + 1]_q$; for $r_i = 0$, it is the zero code. Put $d_i^\perp = n - r_i + 1$ in the first case and $d_i^\perp = \infty$ in the second. Because $(B^{-1})^T = (BB^T)^{-1}B$ is obtained from B by nonzero row scalings, the general matrix-product bound yields

$$d(D^\perp) \ge \min\{3d_0^\perp, 2d_1^\perp, d_2^\perp\} = q - r_2 > \delta,$$

where the equality follows from $r_0 \le r_1 \le r_2$, and the last term is finite because $r_2 \ge 1$. Thus, the CSS distance is exactly δ, and its dimension is $2 \dim D - 3n = 3n - 2(r_0 + r_1 + r_2)$. Taking $(r_0, r_1, r_2) = (1, 2, 3)$ gives (6.7).

For (b), oddness of q makes $n = q - 1 = 2m$ even, and $q \geq 7$ gives $m \geq 3$. Set $b = m - 2$, and use $(r_0, r_1, r_2) = (1, 2, 5)$. The first two defining sets are disjoint from their negatives, whereas

$$Z_5(m-2) = \{m-2, m-1, m, m+1, m+2\}$$

is fixed by negation modulo $2m$. Equation (6.3) gives $(\eta_1, \eta_2, \eta_5) = (1, 2, 0)$ and $\ell = 3$. The classical image has dimension $k = 3n - 8$ and exact distance six. Because

$$\dim \mathrm{Hull}(C_1^{(b)}) = 1 < \dim C_1^{(b)} = n - 1,$$

the generator word $f_1^{(b)}$ does not belong to the first constituent hull and has weight two. Equation (5.6) therefore places its image outside Hull(D); the three nonzero entries in the first row of an NSC matrix give image weight six. Thus, $d_{\mathrm{out}} = 6$, and Theorem 5.4 gives

$$K = k - \ell = 3q - 14, \qquad c = 3n - k - \ell = 5.$$

For (c), specialize part (a) to

$$(r_0, r_1, r_2) = \left(t - 1, \frac{3t}{2} - 1, 3t - 1\right).$$

These are ordered non-negative integers because $t \geq 2$ is even. Moreover, $q > 6t - 1$ is exactly $2r_2 < n$, and all three weighted constituent distances equal $3t$. Finally,

$$r_0 + r_1 + r_2 = \frac{11t}{2} - 3,$$

so (6.4) becomes (6.6). □

For example, Part (c) gives $[[72, 34, 12]]_{25}$, $[[108, 48, 18]]_{37}$, and $[[144, 62, 24]]_{49}$ from

$$(t, q) = (4, 25), (6, 37), (8, 49),$$

respectively. These instances illustrate that the exact distance is not restricted to a fixed constant.

Table 2 uses $b = 1$. Every displayed largest defining set is disjoint from its negative, so all three constituents are dual-containing. The image distance is exact by Theorem 5.1. Put $d_i^{\perp} = n - r_i + 1$ when $r_i > 0$ and $d_i^{\perp} = \infty$ when $r_i = 0$. Because

$$(B^{-1})^T = (BB^T)^{-1}B$$

differs from B only by nonzero row scalings, the same row-span distances apply to the dual image. Consequently,

$$d(D^{\perp}) \geq \min\{3d_0^{\perp}, 2d_1^{\perp}, d_2^{\perp}\} > d(D)$$

for every listed row. Hence, the CSS distance, not merely its lower bound, equals the tabulated value. For a row indexed by (r_0, r_1, r_2), the quantum Singleton ceiling is

$$d_{\mathrm{QS}} = \left\lfloor \frac{N - K + 2}{2} \right\rfloor = r_0 + r_1 + r_2 + 1.$$

The last two columns report this universal ceiling and, where available, the exact online bound returned by the cited database for the corresponding alphabet [39]. The three direct query pages were accessed on 21 October 2026 and confirm the covered comparisons [40–42]; the catalog is reproducible but is not presented as a record claim.

Table 2. Exact CSS codes from nested cyclic Reed–Solomon constituents.

q	n	(r_0, r_1, r_2)	Exact QEC code	d_{QS}	Online comparison
5	4	$(0, 1, 1)$	$[[12, 8, 2]]_5$	3	below $[[12, 8, 3]]_5$ by one
7	6	$(0, 1, 2)$	$[[18, 12, 3]]_7$	4	below $[[18, 12, 4]]_7$ by one
7	6	$(1, 1, 2)$	$[[18, 10, 3]]_7$	5	below $[[18, 10, 5]]_7$ by two
9	8	$(0, 2, 3)$	$[[24, 14, 3]]_9$	6	database unavailable for $q^2 = 81$
9	8	$(1, 2, 3)$	$[[24, 12, 4]]_9$	7	database unavailable for $q^2 = 81$
11	10	$(1, 2, 4)$	$[[30, 16, 5]]_{11}$	8	database unavailable for $q^2 = 121$
11	10	$(1, 3, 4)$	$[[30, 14, 5]]_{11}$	9	database unavailable for $q^2 = 121$
11	10	$(2, 3, 4)$	$[[30, 12, 5]]_{11}$	10	database unavailable for $q^2 = 121$
13	12	$(1, 2, 5)$	$[[36, 20, 6]]_{13}$	9	database unavailable for $q^2 = 169$
13	12	$(1, 3, 5)$	$[[36, 18, 6]]_{13}$	10	database unavailable for $q^2 = 169$
13	12	$(2, 3, 5)$	$[[36, 16, 6]]_{13}$	11	database unavailable for $q^2 = 169$

For the EAQEC catalog, take $(r_0, r_1, r_2) = (1, 2, 5)$ when $q \geq 7$ and $(0, 1, 2)$ when $q = 5$. Equation (6.2) gives exact image distance six in the first case and three in the second. The minimum word represented by $f_{r_0}^{(b)}$ is outside the hull, and the first row of every matrix supplied by Theorem 4.10 has three nonzero entries. Its image therefore attains the classical minimum outside the hull, proving that the EAQEC distance is exact. With

$$k = 3n - \sum_i r_i \quad \text{and} \quad \ell = \sum_i \eta_{r_i}(b),$$

Table 3 follows from Theorem 5.4. Because EAQEC comparisons depend essentially on the entanglement coordinate c, the rows are asserted as exact, reproducible constructions but not as new records.

Table 3. Exact EAQEC codes from the same cross-field family.

q	n	b	(r_0, r_1, r_2)	ℓ	Exact EAQEC code
5	4	0	$(0, 1, 2)$	1	$[[12, 8, 3; 2]]_5$
5	4	1	$(0, 1, 2)$	2	$[[12, 7, 3; 1]]_5$
7	6	0	$(1, 2, 5)$	2	$[[18, 8, 6; 6]]_7$
7	6	1	$(1, 2, 5)$	3	$[[18, 7, 6; 5]]_7$
9	8	1	$(1, 2, 5)$	5	$[[24, 11, 6; 3]]_9$
9	8	2	$(1, 2, 5)$	3	$[[24, 13, 6; 5]]_9$
11	10	1	$(1, 2, 5)$	7	$[[30, 15, 6; 1]]_{11}$
11	10	3	$(1, 2, 5)$	3	$[[30, 19, 6; 5]]_{11}$
13	12	2	$(1, 2, 5)$	7	$[[36, 21, 6; 1]]_{13}$
13	12	4	$(1, 2, 5)$	3	$[[36, 25, 6; 5]]_{13}$

6.3. An explicit QEC code over $\mathbb{F}_7$

Example 6.2. *(A length-18 QEC code over $\mathbb{F}_7$) This is the $q = 7$ row with $(r_0, r_1, r_2) = (0, 1, 2)$ in Table 2, expanded here with direct enumeration of $D^\perp$ rather than only the matrix-product lower bound. Let $q = 7$, $n = 6$, and take*

$$g_0 = 1, \qquad g_+ = x + 2, \qquad g_- = x^2 - 2x - 1. \tag{6.8}$$

These polynomials form a divisibility chain and divide $x^6 - 1$. They may be used directly as the three constituent generators of a dual-containing ring code or obtained as $g_i = \gcd(f_i, h_i^*)$ by taking $f_i = g_i$. Their field parameters and hull dimensions are shown in Table 4.

Table 4. Constituent checks for Example 6.2.

i	$g_i = f_i$	$[n, k_i, d_i]_7$	$\dim \mathrm{Hull}(\langle f_i \rangle)$	$\deg g_i$
0	1	$[6, 6, 1]_7$	0	0
+	$x + 2$	$[6, 5, 2]_7$	1	1
−	$x^2 - 2x - 1$	$[6, 4, 3]_7$	2	2

For each constituent, $f_i \mid h_i^*$, so the ring code equals its Euclidean sum. With B from (4.8)*, Theorem 5.1 gives the field-linear code*

$$D = [\langle 1 \rangle, \langle x + 2 \rangle, \langle x^2 - 2x - 1 \rangle]B$$

with parameters

$$[18, 15, \min\{3, 4, 3\}]_7 = [18, 15, 3]_7.$$

Direct enumeration of the three-dimensional dual gives $d(D^\perp) = 12$. Therefore, a weight-three word of D is not in $D^\perp$, and the CSS distance is exactly three. Theorem 5.3 yields

$$[[18, 2(15) - 18, 3]]_7 = [[18, 12, 3]]_7.$$

Example 6.2 establishes the corrected construction, but it is not optimal for its length and dimension. The cited online table of bounds for quantum codes records a $[[18, 12, 4]]_7$ code [41]; in that database URL, the query value $q = 49$ denotes the stabilizer alphabet parameter 7^2. The value of Example 6.2 is therefore methodological. Every parameter follows from a visible polynomial, an exact nested-distance theorem, and a direct dual-distance check.

6.4. An explicit EAQEC code over $\mathbb{F}_7$

Example 6.3. *(A length-18 EAQEC code over $\mathbb{F}_7$) Unlike the catalog in Section 6.2, this example comes from a separately searched nested cyclic chain rather than the consecutive-root family* (6.1)*. Again, let $q = 7$ and $n = 6$, but now choose*

$$\begin{aligned} f_0 &= x + 2, \\ f_+ &= x^2 - 2x - 1 = (x + 2)(x + 3), \\ f_- &= x^5 + 2x^4 - 3x^3 + x^2 + 2x - 3 = f_+(x^3 - 3x^2 - x + 3). \end{aligned} \tag{6.9}$$

All three divide $x^6 - 1$, so $f_0 \mid f_+ \mid f_-$. Exhaustive enumeration and reciprocal-polynomial arithmetic give Table 5.

Table 5. Constituent checks for Example 6.3.

i	f_i	$[n, k_i, d_i]_7$	$\dim \mathrm{Hull}(\langle f_i \rangle)$	h_i^* or hull data
0	$x + 2$	$[6, 5, 2]_7$	1	$\deg \mathrm{lcm}(f_0, h_0^*) = 5$
+	$x^2 - 2x - 1$	$[6, 4, 3]_7$	2	$\deg \mathrm{lcm}(f_+, h_+^*) = 4$
−	$x^5 + 2x^4 - 3x^3 + x^2 + 2x - 3$	$[6, 1, 6]_7$	1	$h_-^* = x + 3$

The Gray image

$$D = [C_0, C_+, C_-]B$$

has

$$k = 5 + 4 + 1 = 10, \qquad d(D) = \min\{3 \cdot 2, 2 \cdot 3, 1 \cdot 6\} = 6.$$

Its hull dimension is $\ell = 1 + 2 + 1 = 4$. To establish the quantum distance rather than only the classical distance, take the weight-two word represented by $f_0 = x + 2$ in C_0. It does not belong to

$$\mathrm{Hull}(C_0) = \langle \mathrm{lcm}(f_0, h_0^*) \rangle,$$

whose generator has degree five. The component tuple $(f_0, 0, 0)$ therefore lies outside the ring hull, and its Gray image consists of three copies of f_0 because the first row of B is $(1, 1, 1)$. This gives a weight-six word in $D \setminus \mathrm{Hull}(D)$. Because

$$d_{\mathrm{out}}(D) \geq d(D) = 6,$$

one has $d_{\mathrm{out}}(D) = 6$. Thus, $c = 18 - k - \ell = 4$ and $K = k - \ell = 6$. Theorem 5.4 gives the exact EAQEC code

$$[[18, 6, 6; 4]]_7. \tag{6.10}$$

The $q = 7, n = 6, a = 2, k = 4$ row of Table 3 in [27] reports the tuple $[[18, 3, 5; 9]]_7$. Three independently verified outputs now give a transparent comparison:

$$[[18, 6, 6; 4]]_7, \qquad [[18, 7, 6; 5]]_7, \qquad [[18, 8, 6; 6]]_7.$$

The first is Example 6.3, and the other two are the $q = 7$ rows of Table 3. Each has larger encoded dimension, larger distance, and lower entanglement consumption than the reported tuple. Among the three codes, increasing K is accompanied by increasing c, so they display a nontrivial rate–entanglement tradeoff rather than one code dominating the other two. This comparison is illustrative, not a claim that the reported baseline has been independently realized: Table 1 shows why that entry requires independent verification. Recent matrix-product constructions already produce the broad families of length-$3n$ EAQEC codes and flexible hull parameters [22, 24, 25]. The value of the comparison is therefore its fully traceable derivation from corrected ring coordinates, not a claim of global optimality over that broader literature.

7. Concluding remarks

The central issue is coordinate transport. Ring multiplication and duality split along primitive idempotents, whereas (a, b, c) is a coefficient vector. Theorem 4.1 shows that universal Euclidean-duality preservation is equivalent in CRT coordinates to a nonsingular diagonal Gram matrix; consequently, the scalar condition

$$MM^T = aI$$

cannot be universal for odd q. This criterion applies to every split semisimple ring, not only $R_{q,v}$.

Duality does not by itself prove distance. Nonsingularity by columns gives the matrix-product lower bound, and nested constituents make it exact; for nonnested constituents, an independent distance proof is still required. The same distinction determines the EAQEC distance, which is the minimum weight outside the hull. Theorem 4.6 supplies compatible matrices for $q > 2s - 1$, NSC gives the necessary bound $s \leq q$, and the order-three and order-four classifications sharpen the exact boundary to $q > 3$.

The analysis identifies the coordinate and distance defects inherited by [26, 27] without claiming that every parameter in those papers is false. It corrects the repeated-root example to $[[21, 13, 3]]_7$ and supplies exact QEC constructions together with EAQEC constructions whose distances are exact when an outside-hull witness is identified, including the unbounded-distance family $[[3(q-1), 3q+3-11t, 3t]]_q$ and the cross-field catalog. Because

$$R_{q,v} \cong \mathbb{F}_q^3,$$

these images are matrix-product codes over a field; the ring presentation organizes constituents but does not create extra field-linear freedom.

The remaining questions concern the interval $s \leq q \leq 2s - 1$ for $s \geq 5$, equivalence classes of admissible matrices, broader cyclic searches, and repeated-root lengths. These extensions should preserve the order established here. Prove coordinate and duality statements first, prove classical distances second, and form quantum parameters last.

Author contributions

Qingyu Zhang: conceptualization, methodology, formal analysis, software, validation, investigation, writing—original draft, and writing—review and editing; Yong Zhang: formal analysis (verification and revision of mathematical proofs and code parameters), validation (computational checks), and writing—review and editing (critical revision and organization). All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

Generative-AI tools were used for language polishing and code preparation. All mathematical results, proofs, computations, and conclusions were independently established and verified by the authors, who take full responsibility for the content.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (Grant No. 11871417) and the 2026 Jiangsu Provincial Teacher Development Research Project (Grant No. 2026jsfz-b004).

Conflict of interest

The authors declare no conflicts of interest.

Data and code availability

No external dataset was used; the scripts and README for reproducing the computational checks reported in this paper are available on Zenodo (DOI: `10.5281/zenodo.24163761`). The same record includes a CSV listing all 34 discrepancies found in the exhaustive check of 186 ordered triples described in Section 6.1.

References

1. P. W. Shor, Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A*, **52** (1995), R2493. https://doi.org/10.1103/PhysRevA.52.R2493
2. A. R. Calderbank, P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A*, **54** (1996), 1098–1105. https://doi.org/10.1103/PhysRevA.54.1098
3. A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inf. Theory*, **44** (1998), 1369–1387. https://doi.org/10.1109/18.681315
4. A. Ashikhmin, E. Knill, Nonbinary quantum stabilizer codes, *IEEE Trans. Inf. Theory*, **47** (2001), 3065–3072. https://doi.org/10.1109/18.959288
5. A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inf. Theory*, **52** (2006), 4892–4914. https://doi.org/10.1109/TIT.2006.883612
6. T. Brun, I. Devetak, M. H. Hsieh, Correcting quantum errors with entanglement, *Science*, **314** (2006), 436–439. https://doi.org/10.1126/science.1131563
7. M. M. Wilde, T. A. Brun, Optimal entanglement formulas for entanglement-assisted quantum coding, *Phys. Rev. A*, **77** (2008), 064302. https://doi.org/10.1103/PhysRevA.77.064302
8. C. Galindo, F. Hernando, R. Matsumoto, D. Ruano, Entanglement-assisted quantum error-correcting codes over arbitrary finite fields, *Quantum Inf. Process.*, **18** (2019), 116. https://doi.org/10.1007/s11128-019-2234-5
9. K. Guenda, T. A. Gulliver, S. Jitman, S. Thipworawimon, Linear ℓ-intersection pairs of codes and their applications, *Des. Codes Cryptogr.*, **88** (2020), 133–152. https://doi.org/10.1007/s10623-019-00676-z
10. F. R. F. Pereira, S. Mancini, Entanglement-assisted quantum codes from cyclic codes, *Entropy*, **25** (2023), 37. https://doi.org/10.3390/e25010037

11. W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511807077
12. S. Ling, C. Xing, *Coding theory: a first course*, Cambridge University Press, 2004. https://doi.org/10.1017/CBO9780511755279
13. S. A. Aly, A. Klappenecker, P. K. Sarvepalli, On quantum and classical BCH codes, *IEEE Trans. Inf. Theory*, **53** (2007), 1183–1188. https://doi.org/10.1109/TIT.2006.890730
14. T. Blackmore, G. H. Norton, Matrix-product codes over $\mathbb{F}_q$, *Appl. Algebra Eng. Commun. Comput.*, **12** (2001), 477–500. https://doi.org/10.1007/PL00004226
15. F. Hernando, K. Lally, D. Ruano, Construction and decoding of matrix-product codes from nested codes, *Appl. Algebra Eng. Commun. Comput.*, **20** (2009), 497–507. https://doi.org/10.1007/s00200-009-0113-5
16. X. Liu, H. Liu, Quantum codes from linear codes over finite chain rings, *Quantum Inf. Process.*, **16** (2017), 240. https://doi.org/10.1007/s11128-017-1695-7
17. M. Ashraf, G. Mohammad, Quantum codes over $\mathbb{F}_p$ from cyclic codes over $\mathbb{F}_p[u,v]/\langle u^2-1, v^3-v, uv-vu\rangle$, *Cryptogr. Commun.*, **11** (2019), 325–335. https://doi.org/10.1007/s12095-018-0299-0
18. Y. Gao, J. Gao, F. W. Fu, Quantum codes from cyclic codes over the ring $\mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_r\mathbb{F}_q$, *Appl. Algebra Eng. Commun. Comput.*, **30** (2019), 161–174. https://doi.org/10.1007/s00200-018-0366-y
19. O. P. Pandey, S. Pathak, A. K. Shukla, V. Mishra, A. K. Upadhyay, A study of QECCs and EAQECCs construction from cyclic codes over the ring $\mathbb{F}_q + v_1\mathbb{F}_q + v_2\mathbb{F}_q + \cdots + v_s\mathbb{F}_q$, *Quantum Inf. Process.*, **23** (2024), 31. https://doi.org/10.1007/s11128-023-04240-6
20. X. Zhang, QEC and EAQEC codes from cyclic codes over non-chain rings, *Quantum Inf. Process.*, **21** (2022), 389. https://doi.org/10.1007/s11128-022-03734-z
21. M. Cao, Quantum error-correcting codes from matrix-product codes related to quasi-orthogonal and quasi-unitary matrices, *ArXiv*, 2022. https://doi.org/10.48550/arXiv.2012.15691
22. M. Cao, F. Wei, G. Luo, Entanglement-assisted quantum error-correcting codes using matrix-product codes, *Des. Codes Cryptogr.*, **93** (2025), 4473–4500. https://doi.org/10.1007/s10623-025-01685-x
23. Y. Li, S. Zhu, E. Martínez-Moro, On general self-orthogonal matrix-product codes associated with Toeplitz matrices, *Cryptogr. Commun.*, **17** (2025), 397–420. https://doi.org/10.1007/s12095-024-00763-6
24. X. Xu, W. Zhang, X. Liu, Matrix-product codes related to constacyclic codes and their applications to EAQEC codes, *Discrete Math.*, **347** (2024), 113878. https://doi.org/10.1016/j.disc.2024.113878
25. J. Liu, P. Hu, X. Liu, The Euclidean hulls of matrix product codes and their applications to EAQEC codes, *Quantum Inf. Process.*, **24** (2025), 275. https://doi.org/10.1007/s11128-025-04899-z
26. S. Ali, G. Mohammad, Jeelani, N. Khan, P. Sharma, On quantum and LCD codes over the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, *Quantum Inf. Process.*, **21** (2022), 306. https://doi.org/10.1007/s11128-022-03654-y
27. H. Li, X. Liu, Cyclic codes over a semi-local ring and their applications to QEC and EAQEC codes, *Quantum Inf. Process.*, **24** (2025), 49. https://doi.org/10.1007/s11128-025-04666-0
28. S. Szabo, F. Ulmer, Duality preserving Gray maps for codes over rings, *J. Algebra Appl.*, **16** (2017), 1750161. https://doi.org/10.1142/S0219498817501614

29. X. Liu, H. Liu, L. Yu, Entanglement-assisted quantum codes from matrix-product codes, *Quantum Inf. Process.*, **18** (2019), 183. https://doi.org/10.1007/s11128-019-2300-z

30. J. Liu, P. Hu, X. Liu, Application of Euclidean sums of matrix-product codes to quantum codes, *Quantum Inf. Process.*, **22** (2023), 202. https://doi.org/10.1007/s11128-023-03954-x

31. C. Galindo, F. Hernando, R. Matsumoto, D. Ruano, Correction to: Entanglement-assisted quantum error-correcting codes over arbitrary finite fields, *Quantum Inf. Process.*, **20** (2021), 216. https://doi.org/10.1007/s11128-021-03066-4

32. G. Luo, X. Cao, Two new families of entanglement-assisted quantum MDS codes from generalized Reed–Solomon codes, *Quantum Inf. Process.*, **18** (2019), 89. https://doi.org/10.1007/s11128-019-2207-8

33. G. Luo, X. Cao, X. Chen, MDS codes with hulls of arbitrary dimensions and their quantum error correction, *IEEE Trans. Inf. Theory*, **65** (2019), 2944–2952. https://doi.org/10.1109/TIT.2018.2874953

34. W. Fang, F. W. Fu, L. Li, S. Zhu, Euclidean and Hermitian hulls of MDS codes and their applications to EAQECCs, *IEEE Trans. Inf. Theory*, **66** (2020), 3527–3537. https://doi.org/10.1109/TIT.2019.2950245

35. M. Grassl, T. Beth, M. Rötteler, On optimal quantum codes, *Int. J. Quantum Inf.*, **2** (2004), 55–64. https://doi.org/10.1142/S0219749904000079

36. M. Cao, K. Zhou, Quantum codes and optimal pure quantum (r, δ)-LRCs via the MP construction, *ArXiv*, 2026. https://doi.org/10.48550/arXiv.2606.14253

37. N. Alon, Combinatorial nullstellensatz, *Combin. Probab. Comput.*, **8** (1999), 7–29. https://doi.org/10.1017/S0963548398003411

38. T. Zhang, G. Ge, Quantum codes from generalized Reed–Solomon codes and matrix-product codes, *ArXiv*, 2015. https://doi.org/10.48550/arXiv.1508.00978

39. M. Grassl, *Bounds on the minimum distance of quantum codes*, 2026. Available from: `https://www.codetables.de/QECC/index.html`.

40. M. Grassl, *Bounds on* $[[12, 8]]_5$, 2026. Available from: `https://www.codetables.de/QECC/QECC.php?k=8&n=12&q=25`. Accessed 21 October 2026.

41. M. Grassl, *Bounds on* $[[18, 12]]_7$, 2026. Available from: `https://www.codetables.de/QECC/QECC.php?k=12&n=18&q=49`. Accessed 21 October 2026.

42. M. Grassl, *Bounds on* $[[18, 10]]_7$, 2026. Available from: `https://www.codetables.de/QECC/QECC.php?k=10&n=18&q=49`. Accessed 21 October 2026.

Appendix

Complete Gray-distance discrepancy table

The following table (Table A.1) lists all 34 discrepancies found among 186 tested ordered triples. Here q is the field size, n is the constituent length, and f_1, f_2, f_3 are the constituent generator polynomials

in order. The last two columns show the distance predicted by the published formula and the distance obtained by exhaustive enumeration.

Table A.1. The 34 discrepancies among 186 tested ordered triples.

q	n	f_1	f_2	f_3	Predicted	Enumerated
3	4	x^2+1	x^2+1	x^2-1	4	2
3	4	x^2+1	x^2-1	x^2+1	4	2
3	4	x^2-1	x^2+1	x^2-1	4	2
3	4	x^2-1	x^2-1	x^2+1	4	2
3	4	x^2-1	x^2-1	x^3+x^2+x+1	6	4
3	4	x^2-1	x^2-1	x^3-x^2+x-1	6	4
3	4	x^2-1	x^3+x^2+x+1	x^2-1	6	4
3	4	x^2-1	x^3-x^2+x-1	x^2-1	6	4
3	4	x^3+x^2+x+1	$x+1$	x^2+1	4	2
3	4	x^3+x^2+x+1	$x+1$	x^2-1	4	2
3	4	x^3+x^2+x+1	$x-1$	x^2+1	4	2
3	4	x^3+x^2+x+1	$x-1$	x^2-1	4	2
3	4	x^3+x^2+x+1	x^2+1	$x+1$	4	2
3	4	x^3+x^2+x+1	x^2+1	$x-1$	4	2
3	4	x^3+x^2+x+1	x^2+1	x^2-1	4	2
3	4	x^3+x^2+x+1	x^2-1	$x+1$	4	2
3	4	x^3+x^2+x+1	x^2-1	$x-1$	4	2
3	4	x^3+x^2+x+1	x^2-1	x^2+1	4	2
3	4	x^3+x^2+x+1	x^3+x^2+x+1	x^3-x^2+x-1	8	4
3	4	x^3+x^2+x+1	x^3-x^2+x-1	x^3+x^2+x+1	8	4
3	4	x^3-x^2+x-1	$x+1$	x^2+1	4	2
3	4	x^3-x^2+x-1	$x+1$	x^2-1	4	2
3	4	x^3-x^2+x-1	$x-1$	x^2+1	4	2
3	4	x^3-x^2+x-1	$x-1$	x^2-1	4	2
3	4	x^3-x^2+x-1	x^2+1	$x+1$	4	2
3	4	x^3-x^2+x-1	x^2+1	$x-1$	4	2
3	4	x^3-x^2+x-1	x^2+1	x^2-1	4	2
3	4	x^3-x^2+x-1	x^2-1	$x+1$	4	2
3	4	x^3-x^2+x-1	x^2-1	$x-1$	4	2
3	4	x^3-x^2+x-1	x^2-1	x^2+1	4	2
3	4	x^3-x^2+x-1	x^3+x^2+x+1	x^3-x^2+x-1	8	4
3	4	x^3-x^2+x-1	x^3-x^2+x-1	x^3+x^2+x+1	8	4
5	3	$x-1$	$x-1$	x^2+x+1	6	4
5	3	$x-1$	x^2+x+1	$x-1$	6	4

AIMS Press

© 2026 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0)