Mathematics

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

AIMS Mathematics, 11(6): 16952–16982.
DOI: 10.3934/math.2026694
Received: 26 March 2026
Revised: 27 May 2026
Accepted: 04 June 2026
Published: 12 June 2026

Research article

Hermitian self-orthogonal infinitesimal evaluation codes over $\mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$ and applications to quantum codes

Sami H. Saif*

Department of Mathematics, College of Science, King Saud University, P.O. Box 2455,
Riyadh 11451, Saudi Arabia

* **Correspondence:** Email: ssiaf1@ksu.edu.sa.

Abstract: In this paper, we introduced a new class of infinitesimal evaluation codes over the dual-number extension $R = \mathbb{F}_{q^2}+u\mathbb{F}_{q^2}, u^2 = 0$, obtained by evaluating polynomials at perturbed points a_i+ub_i. This evaluation produces a coupled value–derivative structure through the identity $f(a_i+ub_i) = f_0(a_i)+u(b_if_0'(a_i) + f_1(a_i))$, which enriches classical evaluation codes with first-order infinitesimal corrections. We established the Hermitian duality theory for these codes and showed that Hermitian orthogonality over R decomposes into a residue-layer condition over $\mathbb{F}_{q^2}$ together with a correction equation involving the infinitesimal parameters. This yields explicit criteria for Hermitian self-orthogonality. Using these criteria, we constructed several families of Hermitian self-orthogonal infinitesimal evaluation codes, including multiplier perturbation, locator perturbation, and subgroup–coset constructions. Via the Gray map and the Hermitian construction, these codes produce new families of q-ary quantum stabilizer codes.

Keywords: evaluation codes; Gray map; quantum codes; linear codes
Mathematics Subject Classification: 11T71, 94B15, 94B05

1. Introduction

Let $q = p^m$ be a power of an odd prime p, and let $\mathbb{F}_{q^2}$ denote the finite field with q^2 elements. A linear code $C \subseteq \mathbb{F}_{q^2}^n$ of dimension k and minimum Hamming distance d is denoted by an $[n, k, d]_{q^2}$ code. Its parameters satisfy the Singleton bound $d \leq n-k+1$, and codes attaining this bound are called *maximum distance separable* (MDS) codes. Among the most important examples are generalized Reed–Solomon (GRS) codes, which play a central role in both classical and quantum coding theory.

Quantum error-correcting codes protect quantum information against noise and decoherence. A q-ary quantum code with parameters $[[n, k, d]]_q$ encodes k logical qudits into n physical qudits and has a minimum distance d. These parameters satisfy the quantum Singleton bound $k \leq n-2d+2$, and codes attaining this bound are called *quantum MDS* codes [14, 20]. Because of their optimality, quantum MDS codes are among the most desirable objects in quantum coding theory [10, 16, 17]. Tables of the best currently known parameters for classical and quantum codes can be found in [11].

A standard approach to constructing quantum stabilizer codes is the Hermitian construction. Let $D \subseteq \mathbb{F}_{q^2}^N$ be an $\mathbb{F}_{q^2}$-linear code and let $D^{\perp_H}$ denote its Hermitian dual with respect to the inner product $\langle x, y\rangle_H = \sum_{i=1}^N x_i y_i^q$. If $D \subseteq D^{\perp_H}$, then there exists a q-ary quantum stabilizer code with parameters $[[N,\ N - 2\dim_{\mathbb{F}_{q^2}}(D),\ d]]_q$, where $d = d(D^{\perp_H} \setminus D)$ [1, 19]. Consequently, the construction of quantum codes is closely related to the construction of Hermitian self-orthogonal linear codes over $\mathbb{F}_{q^2}$.

Besides the construction of quantum MDS codes, another active direction in quantum coding theory is the construction of quantum codes with best-known, optimal, or record-breaking parameters, even when the resulting codes are not MDS. This direction is important because it improves the available parameter ranges for quantum error correction beyond the MDS regime. Recent examples include constructions from nearly self-orthogonal quasi-twisted codes [8] and from the τ-OD MP construction [6].

Over the last two decades, numerous families of quantum MDS codes have been obtained from Hermitian self-orthogonal generalized Reed–Solomon codes and related evaluation codes; see, for example, [4, 5, 12]. In these constructions, the field $\mathbb{F}_{q^2}$ provides a natural setting for Hermitian duality, and much of the existing work focuses on identifying arithmetic relations among n, k, and q that guarantee Hermitian self-orthogonality [7, 13]. Recent work has also studied precise conditions under which generalized Reed–Solomon codes are Hermitian self-orthogonal [3, 9, 15].

Despite these advances, Hermitian self-orthogonality over finite fields imposes strong algebraic constraints on evaluation codes. In particular, the orthogonality conditions are expressed entirely in terms of moment equations over $\mathbb{F}_{q^2}$, which restrict the available parameter choices. This rigidity motivates the search for alternative algebraic frameworks in which additional degrees of freedom are available while the classical field-based constructions remain visible.

The purpose of this paper is to develop such a framework. We work over the dual-number extension

$$R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}, \qquad u^2 = 0, \tag{1.1}$$

which is a finite commutative local ring with residue field $R/\langle u\rangle \cong \mathbb{F}_{q^2}$. Every element of R can be written uniquely as $a + ub$ with $a, b \in \mathbb{F}_{q^2}$, so R may be viewed as a first-order infinitesimal extension of $\mathbb{F}_{q^2}$. This ring extension introduces additional infinitesimal degrees of freedom in the evaluation process while preserving the classical $\mathbb{F}_{q^2}$ residue structure. As a result, the ring framework provides a natural mechanism for generating large families of Hermitian self-orthogonal codes whose residue codes remain classical generalized Reed–Solomon codes.

The fundamental notion studied in this paper is *infinitesimal evaluation codes*. Let

$$\alpha_i = a_i + ub_i \in R, \qquad v_i = s_i + ut_i \in R^\times, \qquad 1 \le i \le n,$$

where $a_i, b_i, s_i, t_i \in \mathbb{F}_{q^2}$. For an integer $1 \le k \le n$, we define

$$\mathcal{E}_k(\alpha, v) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) :\ f \in R[X],\ \deg f < k\} \subseteq R^n.$$

Writing $f(X) = f_0(X) + uf_1(X)$ with $f_0, f_1 \in \mathbb{F}_{q^2}[X]$, evaluation at a perturbed point satisfies

$$f(a_i + ub_i) = f_0(a_i) + u\big(b_i f_0'(a_i) + f_1(a_i)\big). \tag{1.2}$$

Thus each coordinate of a codeword records both the classical value $f_0(a_i)$ and a first-order correction term involving the derivative $f_0'(a_i)$. This produces a natural two-layer evaluation structure in which classical evaluation data interact with infinitesimal perturbations.

The first objective of this paper is to develop the algebraic theory of these infinitesimal evaluation codes. In particular, we prove the fundamental infinitesimal evaluation identity in Lemma 3.2, derive an explicit coordinate expansion in Proposition 3.3, obtain a Vandermonde-type generator matrix in Proposition 3.4, and prove injectivity of the evaluation map under the natural distinctness hypothesis on the residue locators in Proposition 3.5. We also determine the associated residue and torsion codes in Theorem 3.9 and Theorem 3.10, respectively, and establish a lower bound on the minimum Hamming distance in Proposition 3.6.

The second objective is to study Hermitian self-orthogonality over R. Extending the Frobenius involution of $\mathbb{F}_{q^2}$ coefficientwise to R, we show that Hermitian orthogonality over R decomposes into two coupled conditions: a classical Hermitian orthogonality relation for the residue code over $\mathbb{F}_{q^2}$ together with a correction equation involving the infinitesimal parameters; see Lemma 4.1 and Theorem 4.2. This decomposition leads to a Gram-matrix criterion in Proposition 4.4 and to explicit moment-type criteria for Hermitian self-orthogonality in Theorem 4.5.

The third objective is to construct explicit families of Hermitian self-orthogonal infinitesimal evaluation codes. Using the self-orthogonality criterion of Theorem 4.5, we develop several construction mechanisms, including multiplier perturbations, locator perturbations, and subgroup–coset constructions. These families provide large collections of admissible parameter choices extending classical Hermitian self-orthogonal generalized Reed–Solomon codes, including constructions related to the subgroup–coset method studied in [21].

Finally, we apply the Gray map

$$\Phi : R^n \to \mathbb{F}_{q^2}^{2n}, \qquad \Phi(a + ub) = (a, b), \tag{1.3}$$

to transfer suitable ring-linear codes over R to codes over $\mathbb{F}_{q^2}$. When the Gray image is Hermitian self-orthogonal, the Hermitian construction yields q-ary quantum stabilizer codes. In this way, the quantum codes obtained in this work arise naturally from the algebraic structure of infinitesimal evaluation codes.

The paper is organized as follows. Section 2 reviews background on the ring R, Hermitian duality, generalized Reed–Solomon codes, residue and torsion codes, and the Gray map. Section 3 develops the algebraic theory of infinitesimal evaluation codes over R. Section 4 derives the Hermitian self-orthogonality criterion and presents several explicit construction families together with their quantum consequences.

2. Preliminaries

In this section, we collect the notation and basic results used throughout the paper. Unless otherwise stated, $q = p^m$ denotes a power of an odd prime p, and $\mathbb{F}_{q^2}$ denotes the finite field with q^2 elements.

2.1. Hermitian duality over $\mathbb{F}_{q^2}$

Let

$$\overline{a} = a^q, \qquad a \in \mathbb{F}_{q^2}, \tag{2.1}$$

denote the Frobenius involution of $\mathbb{F}_{q^2}$. Its fixed field is $\mathbb{F}_q$. Associated with this involution are the trace and norm maps

$$\mathrm{Tr}(a) = a + \overline{a}, \qquad \mathrm{N}(a) = a\overline{a} = a^{q+1}, \qquad a \in \mathbb{F}_{q^2}. \tag{2.2}$$

For vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_{q^2}^n$, the *Hermitian inner product* is defined by

$$\langle x, y\rangle_H = \sum_{i=1}^{n} x_i\overline{y_i} = \sum_{i=1}^{n} x_i y_i^q. \tag{2.3}$$

If $C \subseteq \mathbb{F}_{q^2}^n$ is an $\mathbb{F}_{q^2}$-linear code, its Hermitian dual is

$$C^{\perp_H} = \{\, x \in \mathbb{F}_{q^2}^n : \langle x, c\rangle_H = 0 \text{ for all } c \in C \,\}. \tag{2.4}$$

The code C is called *Hermitian self-orthogonal* if $C \subseteq C^{\perp_H}$.

2.2. *Generalized Reed–Solomon codes*

Let $a_1, \ldots, a_n$ be pairwise distinct elements of $\mathbb{F}_{q^2}$, and let $v_1, \ldots, v_n \in \mathbb{F}_{q^2}^\times$. For an integer $1 \le k \le n$, the *generalized Reed–Solomon code* associated with the evaluation vector $a = (a_1, \ldots, a_n)$ and multiplier vector $v = (v_1, \ldots, v_n)$ is defined by

$$\mathrm{GRS}_k(a, v) = \Big\{(v_1 f(a_1), \ldots, v_n f(a_n)) : \ f \in \mathbb{F}_{q^2}[X],\ \deg f < k\Big\}. \tag{2.5}$$

It is well known that $\mathrm{GRS}_k(a, v)$ is an $[n, k, n-k+1]_{q^2}$ maximum-distance-separable (MDS) code.

2.3. *The structure of R*

Throughout the paper, we work over the dual-number extension

$$R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2} \cong \mathbb{F}_{q^2}[u]/\langle u^2\rangle, \qquad u^2 = 0. \tag{2.6}$$

Every element of R can be written uniquely in the form

$$a + ub, \qquad a, b \in \mathbb{F}_{q^2}. \tag{2.7}$$

The ring R is a finite commutative local ring with maximal ideal $\mathfrak{m} = u\mathbb{F}_{q^2}$ and residue field $R/\mathfrak{m} \cong \mathbb{F}_{q^2}$. An element $a + ub \in R$ is a unit if and only if $a \neq 0$ (see [18]).

The Frobenius involution of $\mathbb{F}_{q^2}$ extends coefficientwise to R by

$$\overline{a + ub} = a^q + ub^q, \qquad a, b \in \mathbb{F}_{q^2}. \tag{2.8}$$

2.4. *Hermitian duality over R*

For vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in R^n, the Hermitian inner product over R is defined by

$$\langle x, y\rangle_H = \sum_{i=1}^{n} x_i\overline{y_i}. \tag{2.9}$$

If $C \subseteq R^n$ is an R-linear code, its Hermitian dual is

$$C^{\perp_H} = \{\, x \in R^n : \langle x, c\rangle_H = 0 \text{ for all } c \in C \,\}. \tag{2.10}$$

2.5. Residue and torsion codes

Let $C \subseteq R^n$ be an R-linear code. The *residue code* of C is defined by

$$\mathrm{Res}(C) = \{\bar{c} : c \in C\} \subseteq \mathbb{F}_{q^2}^n, \tag{2.11}$$

where $\bar{c}$ denotes reduction modulo u. The *torsion code* of C is defined by

$$\mathrm{Tor}(C) = \{\, x \in \mathbb{F}_{q^2}^n : ux \in C \,\}. \tag{2.12}$$

Both $\mathrm{Res}(C)$ and $\mathrm{Tor}(C)$ are $\mathbb{F}_{q^2}$-linear codes and provide a bridge between the ring-linear structure of C and classical codes over $\mathbb{F}_{q^2}$.

2.6. Polynomial decomposition

Since R is a free $\mathbb{F}_{q^2}$-module with basis $\{1, u\}$, every polynomial $f(X) \in R[X]$ can be written uniquely in the form

$$f(X) = f_0(X) + u f_1(X), \qquad f_0, f_1 \in \mathbb{F}_{q^2}[X]. \tag{2.13}$$

2.7. Gray map

To relate codes over R with codes over $\mathbb{F}_{q^2}$, we use the $\mathbb{F}_{q^2}$-linear Gray map

$$\Phi : R \longrightarrow \mathbb{F}_{q^2}^2, \qquad \Phi(a + ub) = (a, b). \tag{2.14}$$

Extending Φ componentwise yields a map

$$\Phi : R^n \longrightarrow \mathbb{F}_{q^2}^{2n}.$$

After expanding each coordinate of $\mathbb{F}_{q^2}$ with respect to a fixed $\mathbb{F}_q$-basis, the componentwise Gray map induces an $\mathbb{F}_q$-linear map from R^n into $\mathbb{F}_q^{4n}$.

3. Infinitesimal evaluation codes over R

In this section, we introduce infinitesimal evaluation codes over $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}, u^2 = 0$ and establish the algebraic facts needed in the following sections. These codes are obtained by evaluating polynomials at infinitesimally perturbed points

$$\alpha_i = a_i + ub_i, \qquad a_i, b_i \in \mathbb{F}_{q^2}, \tag{3.1}$$

and may be viewed as ring-theoretic enlargements of classical generalized Reed–Solomon codes over $\mathbb{F}_{q^2}$.

Throughout, we denote

$$\alpha_i = a_i + ub_i \in R, \qquad v_i = s_i + ut_i \in R^\times, \qquad 1 \le i \le n,$$

where $s_i \neq 0$ for all i.

Definition 3.1. *Let* $1 \le k \le n$. *The* infinitesimal evaluation code *associated with*

$$\alpha = (\alpha_1, \ldots, \alpha_n) \in R^n, \qquad v = (v_1, \ldots, v_n) \in (R^\times)^n$$

is the R-linear code

$$\mathcal{E}_k(\alpha, v) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) : f \in R[X],\ \deg f < k\} \subseteq R^n.$$

Throughout this section, every polynomial $f(X) \in R[X]$ is written uniquely in the form

$$f(X) = f_0(X) + u f_1(X), \qquad f_0, f_1 \in \mathbb{F}_{q^2}[X].$$

The basic algebraic mechanism behind the construction is the following evaluation identity.

Lemma 3.2. *Let* $a, b \in \mathbb{F}_{q^2}$ *and* $f(X) = f_0(X) + u f_1(X) \in R[X]$. *Then,*

$$f(a + ub) = f_0(a) + u(b f_0'(a) + f_1(a)). \tag{3.2}$$

Proof. Write

$$f_0(X) = \sum_{i=0}^{m} c_i X^i, \qquad f_1(X) = \sum_{i=0}^{t} d_i X^i, \qquad c_i, d_i \in \mathbb{F}_{q^2}.$$

Thus,

$$f(X) = f_0(X) + u f_1(X) = \sum_{i=0}^{m} c_i X^i + u \sum_{i=0}^{t} d_i X^i.$$

We first compute the powers of $a + ub$. Since $u^2 = 0$, the binomial theorem gives $(a + ub)^i = \sum_{j=0}^{i} \binom{i}{j} a^{i-j} (ub)^j$. All terms with $j \ge 2$ vanish because $(ub)^2 = u^2 b^2 = 0$. Hence

$$(a + ub)^i = a^i + i a^{i-1} ub \qquad (i \ge 1). \tag{3.3}$$

Substituting (3.3) into the expression for $f_0(a + ub)$ gives

$$f_0(a + ub) = \sum_{i=0}^{m} c_i (a + ub)^i = c_0 + \sum_{i=1}^{m} c_i (a^i + i a^{i-1} ub).$$

Separating the residue and nilpotent parts yields

$$f_0(a + ub) = \sum_{i=0}^{m} c_i a^i + u\, b \sum_{i=1}^{m} i c_i a^{i-1}.$$

The first sum equals $f_0(a)$, while the second equals $b f_0'(a)$. Therefore,

$$f_0(a + ub) = f_0(a) + u\, b\, f_0'(a). \tag{3.4}$$

Next we evaluate the second component. Multiplying (3.3) by u gives $u(a + ub)^i = u(a^i + i a^{i-1} ub) = u a^i$, since $u^2 = 0$. Hence,

$$u f_1(a + ub) = u \sum_{i=0}^{t} d_i (a + ub)^i = u \sum_{i=0}^{t} d_i a^i = u f_1(a).$$

Combining this identity with (3.4) gives

$$f(a+ub) = f_0(a+ub) + uf_1(a+ub) = f_0(a) + ubf_0'(a) + uf_1(a).$$

Thus,

$$f(a+ub) = f_0(a) + u(bf_0'(a) + f_1(a)),$$

which proves the lemma. □

Combining Lemma 3.2 with the multipliers $v_i = s_i + ut_i$ yields an explicit coordinate formula for the codewords of $\mathcal{E}_k(\alpha, v)$.

Proposition 3.3. *Let $f(X) = f_0(X) + uf_1(X)$ with $\deg f < k$. Then the ith coordinate of the codeword*

$$(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \in \mathcal{E}_k(\alpha, v)$$

is

$$v_i f(\alpha_i) = s_i f_0(a_i) + u\Big(s_i(b_i f_0'(a_i) + f_1(a_i)) + t_i f_0(a_i)\Big). \tag{3.5}$$

Proof. Fix $i \in \{1, \ldots, n\}$. By hypothesis,

$$\alpha_i = a_i + ub_i, \qquad v_i = s_i + ut_i, \qquad f(X) = f_0(X) + uf_1(X).$$

By Lemma 3.2, evaluating f at $\alpha_i = a_i + ub_i$ gives

$$f(\alpha_i) = f_0(a_i) + u(b_i f_0'(a_i) + f_1(a_i)). \tag{3.6}$$

We now multiply (3.6) by $v_i = s_i + ut_i$. Since $u^2 = 0$, we obtain

$$v_i f(\alpha_i) = (s_i + ut_i)\Big(f_0(a_i) + u(b_i f_0'(a_i) + f_1(a_i))\Big).$$

Expanding this product yields

$$v_i f(\alpha_i) = s_i f_0(a_i) + u\, s_i(b_i f_0'(a_i) + f_1(a_i)) + u\, t_i f_0(a_i) + u^2 t_i(b_i f_0'(a_i) + f_1(a_i)).$$

The last term vanishes because $u^2 = 0$. Therefore,

$$v_i f(\alpha_i) = s_i f_0(a_i) + u\Big(s_i(b_i f_0'(a_i) + f_1(a_i)) + t_i f_0(a_i)\Big).$$

This is exactly (3.5). □

Formula (3.5) shows that each coordinate consists of a classical evaluation term together with an infinitesimal correction term involving the derivative of f_0 and the perturbation parameters b_i and t_i.

The code $\mathcal{E}_k(\alpha, v)$ admits the expected Vandermonde-type generator matrix.

Proposition 3.4. *A generator matrix of $C = \mathcal{E}_k(\alpha, v)$ is*

$$G = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_n\alpha_n^{k-1} \end{pmatrix}. \tag{3.7}$$

Proof. By definition,

$$C = \mathcal{E}_k(\alpha, v) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) : f \in R[X],\ \deg f < k\} \subseteq R^n.$$

Let $f(X) = c_0 + c_1X + \cdots + c_{k-1}X^{k-1}, c_0, \ldots, c_{k-1} \in R$. Then, $f(\alpha_i) = \sum_{j=0}^{k-1} c_j\alpha_i^j, 1 \le i \le n$. Hence the corresponding codeword is

$$(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) = \sum_{j=0}^{k-1} c_j(v_1\alpha_1^j, \ldots, v_n\alpha_n^j).$$

Thus every codeword of C is an R-linear combination of the k rows

$$(v_1\alpha_1^j, \ldots, v_n\alpha_n^j), \qquad 0 \le j \le k-1.$$

Conversely, let $c_0, \ldots, c_{k-1} \in R$ and consider the polynomial $f(X) = c_0 + c_1X + \cdots + c_{k-1}X^{k-1}$. Then $\deg f < k$, and the same computation shows that the linear combination $\sum_{j=0}^{k-1} c_j(v_1\alpha_1^j, \ldots, v_n\alpha_n^j)$ equals $(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \in C$. Therefore, the R-row space generated by the rows in (3.7) is exactly C, and hence that matrix is a generator matrix of C. □

As in the classical setting, the distinctness of the residue locators implies injectivity of the evaluation map.

Proposition 3.5. *Assume that $a_1, \ldots, a_n$ are pairwise distinct elements of $\mathbb{F}_{q^2}$. Then the evaluation map*

$$\mathrm{ev} : \{f \in R[X] : \deg f < k\} \longrightarrow R^n, \qquad f \longmapsto (f(\alpha_1), \ldots, f(\alpha_n))$$

is injective. Consequently, $\mathcal{E}_k(\alpha, v)$ is a free R-module of rank k, and

$$|\mathcal{E}_k(\alpha, v)| = |R|^k = q^{4k}.$$

Proof. Let

$$\mathrm{ev} : \{f \in R[X] : \deg f < k\} \longrightarrow R^n, \qquad f \longmapsto (f(\alpha_1), \ldots, f(\alpha_n))$$

be the evaluation map. To prove injectivity, suppose that $\mathrm{ev}(f) = (0, \ldots, 0)$. Thus $f(\alpha_i) = 0, 1 \le i \le n$. Write $f(X) = f_0(X) + uf_1(X)$ with $f_0, f_1 \in \mathbb{F}_{q^2}[X]$. Since $\alpha_i = a_i + ub_i$, Lemma 3.2 gives

$$f(\alpha_i) = f_0(a_i) + u\big(b_i f_0'(a_i) + f_1(a_i)\big).$$

Substituting this into $f(\alpha_i) = 0, 1 \le i \le n$, yields $f_0(a_i) + u\big(b_i f_0'(a_i) + f_1(a_i)\big) = 0$ $(1 \le i \le n)$.

Because $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$ and $1, u$ are linearly independent over $\mathbb{F}_{q^2}$, the residue and nilpotent parts must vanish separately. Hence

$$f_0(a_i) = 0 \quad \text{and} \quad b_i f_0'(a_i) + f_1(a_i) = 0, \qquad 1 \le i \le n. \tag{3.8}$$

Since $a_1, \ldots, a_n$ are pairwise distinct and $\deg f_0 < k$, the polynomial $f_0 \in \mathbb{F}_{q^2}[X]$ has at least n distinct zeros by (3.8). As $k \le n$, this forces $f_0 = 0$.

Substituting $f_0 = 0$ into (3.8) gives $f_1(a_i) = 0, 1 \le i \le n$. Again f_1 has degree $< k \le n$, so the distinctness of the a_i implies $f_1 = 0$. Therefore $f = 0$, proving that the evaluation map is injective. Since the polynomials of degree $< k$ over R form a free R-module with basis $1, X, \ldots, X^{k-1}$, this module has rank k. The injective map ev therefore identifies it with $C = \mathcal{E}_k(\alpha, v)$, showing that C is a free R-module of rank k.

Finally, $|C| = |R|^k$. Because $|R| = |\mathbb{F}_{q^2}|^2 = q^4$, we obtain $|\mathcal{E}_k(\alpha, v)| = q^{4k}$. □

The same hypothesis yields the natural lower bound on the Hamming distance.

Proposition 3.6. *Let $C = \mathcal{E}_k(\alpha, v)$, and assume that $a_1, \dots, a_n$ are pairwise distinct. Then every nonzero codeword of C has a Hamming weight at least $n - k + 1$. In particular,*

$$d_H(C) \geq n - k + 1. \tag{3.9}$$

Proof. Let $c \in C = \mathcal{E}_k(\alpha, v)$ be a nonzero codeword. By definition, there exists a polynomial

$$f(X) = f_0(X) + uf_1(X) \in R[X], \qquad \deg f < k,$$

such that

$$c = (v_1 f(\alpha_1), \dots, v_n f(\alpha_n)).$$

For each i, Proposition 3.3 gives

$$v_i f(\alpha_i) = s_i f_0(a_i) + u\Big(s_i(b_i f_0'(a_i) + f_1(a_i)) + t_i f_0(a_i)\Big). \tag{3.10}$$

Since $v_i = s_i + ut_i \in R^\times$, we have $s_i \neq 0$.

We distinguish two cases. First assume that $f_0 \neq 0$. If the ith coordinate of c is zero, then (3.10) gives

$$s_i f_0(a_i) + u\Big(s_i(b_i f_0'(a_i) + f_1(a_i)) + t_i f_0(a_i)\Big) = 0.$$

Taking residue modulo u, we obtain $s_i f_0(a_i) = 0$. Since $s_i \neq 0$, it follows that $f_0(a_i) = 0$. Thus every zero coordinate of c gives a root of the nonzero polynomial f_0 among the pairwise distinct points $a_1, \dots, a_n$. Since $\deg f_0 < k$, the polynomial f_0 has at most $k - 1$ roots. Hence c has at most $k - 1$ zero coordinates.

Now assume that $f_0 = 0$ and $f_1 \neq 0$. In this case, Lemma 3.2 gives $f(\alpha_i) = uf_1(a_i)$, and therefore

$$v_i f(\alpha_i) = (s_i + ut_i)uf_1(a_i) = us_i f_1(a_i).$$

Thus the ith coordinate of c is zero if and only if $s_i f_1(a_i) = 0$. Since $s_i \neq 0$, this is equivalent to $f_1(a_i) = 0$. Hence every zero coordinate of c gives a root of the nonzero polynomial f_1. Since $\deg f_1 < k$, the polynomial f_1 has at most $k - 1$ roots among the pairwise distinct points $a_1, \dots, a_n$. Hence c has at most $k - 1$ zero coordinates.

In both cases, every nonzero codeword $c \in C$ has at most $k - 1$ zero coordinates. Therefore,

$$\mathrm{wt}(c) \geq n - (k - 1) = n - k + 1.$$

Thus $d_H(C) \geq n - k + 1$. □

Remark 3.7. *The bound in Proposition 3.6 is the natural analogue of the classical generalized Reed–Solomon bound. Indeed, the residue code of $\mathcal{E}_k(\alpha, v)$ is a generalized Reed–Solomon code over $\mathbb{F}_{q^2}$, and the infinitesimal perturbation does not alter the set of coordinate positions on which a nonzero polynomial evaluation can vanish.*

For the Hermitian theory developed in the next section, it is convenient to record the decomposition of the generating rows with respect to the splitting

$$R^n = \mathbb{F}_{q^2}^n + u\mathbb{F}_{q^2}^n. \tag{3.11}$$

Proposition 3.8. *Let* $G_j = (v_1\alpha_1^j, \dots, v_n\alpha_n^j), 0 \le j \le k-1$. *Then,*

$$G_j = g_j + uh_j, \tag{3.12}$$

where $g_j = (s_1a_1^j, \dots, s_na_n^j)$ *and* $h_j = (t_1a_1^j + js_1b_1a_1^{j-1}, \dots, t_na_n^j + js_nb_na_n^{j-1})$, *with the convention that the derivative term is zero when* $j = 0$.

Proof. Fix j with $0 \le j \le k-1$. By definition,

$$G_j = (v_1\alpha_1^j, \dots, v_n\alpha_n^j),$$

where $\alpha_i = a_i + ub_i, v_i = s_i + ut_i, 1 \le i \le n$. We first compute α_i^j. Since $u^2 = 0$, the binomial theorem gives $(a_i + ub_i)^j = a_i^j + u\,j\,b_ia_i^{j-1}$ $(j \ge 1)$, while for $j = 0$, we have $\alpha_i^0 = 1$. Thus, for $j \ge 1$,

$$v_i\alpha_i^j = (s_i + ut_i)(a_i^j + u\,j\,b_ia_i^{j-1}).$$

Expanding and using $u^2 = 0$, we obtain $v_i\alpha_i^j = s_ia_i^j + u(t_ia_i^j + js_ib_ia_i^{j-1})$. Therefore, for $j \ge 1$,

$$G_j = (s_1a_1^j, \dots, s_na_n^j) + u(t_1a_1^j + js_1b_1a_1^{j-1}, \dots, t_na_n^j + js_nb_na_n^{j-1}).$$

When $j = 0$, we have $\alpha_i^0 = 1$, so $v_i\alpha_i^0 = v_i = s_i + ut_i$. Hence $G_0 = (s_1, \dots, s_n) + u(t_1, \dots, t_n)$. This is exactly the same formula as above if one adopts the convention that the derivative term $js_ib_ia_i^{j-1}$ is zero when $j = 0$. Thus, for every $0 \le j \le k-1$, $G_j = g_j + uh_j$, where

$$g_j = (s_1a_1^j, \dots, s_na_n^j), \quad h_j = (t_1a_1^j + js_1b_1a_1^{j-1}, \dots, t_na_n^j + js_nb_na_n^{j-1}),$$

with the stated convention for $j = 0$. This proves the proposition. □

Proposition 3.8 is precisely the form needed later when Hermitian inner products are computed row by row.

We next identify the residue code. It is exactly the classical generalized Reed–Solomon code determined by the residue locators a_i and residue multipliers s_i.

Theorem 3.9. *Let* $C = \mathcal{E}_k(\alpha, v)$. *Then,*

$$\mathrm{Res}(C) = \left\{(s_1f_0(a_1), \dots, s_nf_0(a_n)) : f_0 \in \mathbb{F}_{q^2}[X],\ \deg f_0 < k\right\}. \tag{3.13}$$

In particular,

$$\mathrm{Res}(C) = \mathrm{GRS}_k(a, s), \tag{3.14}$$

and hence $\mathrm{Res}(C)$ *is an* $[n, k, n-k+1]_{q^2}$ *MDS code.*

Proof. By definition,

$$C = \mathcal{E}_k(\alpha, v) = \{(v_1f(\alpha_1), \dots, v_nf(\alpha_n)) : f \in R[X],\ \deg f < k\}.$$

Let $c \in C$. Then there exists a polynomial

$$f(X) = f_0(X) + uf_1(X) \in R[X], \qquad f_0, f_1 \in \mathbb{F}_{q^2}[X], \qquad \deg f < k,$$

such that $c = (v_1 f(\alpha_1), \ldots, v_n f(\alpha_n))$. For each i, Proposition 3.3 gives

$$v_i f(\alpha_i) = s_i f_0(a_i) + u\Big(s_i(b_i f_0'(a_i) + f_1(a_i)) + t_i f_0(a_i)\Big).$$

Reducing modulo u, we obtain $\overline{v_i f(\alpha_i)} = s_i f_0(a_i)$. Hence,

$$\mathrm{Res}(c) = (s_1 f_0(a_1), \ldots, s_n f_0(a_n)).$$

Since $c \in C$ was arbitrary, this shows that

$$\mathrm{Res}(C) \subseteq \Big\{(s_1 f_0(a_1), \ldots, s_n f_0(a_n)) : f_0 \in \mathbb{F}_{q^2}[X],\ \deg f_0 < k\Big\}.$$

To prove the reverse inclusion, let $(s_1 f_0(a_1), \ldots, s_n f_0(a_n))$ be any vector on the right-hand side, where $f_0 \in \mathbb{F}_{q^2}[X]$ and $\deg f_0 < k$. Consider the polynomial $f(X) = f_0(X) \in R[X]$, viewed as a polynomial over R with a zero u-part. Then $\deg f < k$, so $c = (v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \in C$. By the same coordinate formula,

$$v_i f(\alpha_i) = s_i f_0(a_i) + u\Big(s_i b_i f_0'(a_i) + t_i f_0(a_i)\Big),$$

and therefore $\mathrm{Res}(c) = (s_1 f_0(a_1), \ldots, s_n f_0(a_n))$. This proves the reverse inclusion, and hence

$$\mathrm{Res}(C) = \Big\{(s_1 f_0(a_1), \ldots, s_n f_0(a_n)) : f_0 \in \mathbb{F}_{q^2}[X],\ \deg f_0 < k\Big\}.$$

By the definition of generalized Reed–Solomon codes, the right-hand side is exactly $\mathrm{GRS}_k(a, s)$. Thus

$$\mathrm{Res}(C) = \mathrm{GRS}_k(a, s).$$

Finally, since generalized Reed–Solomon codes are MDS, it follows that $\mathrm{Res}(C)$ is an $[n, k, n-k+1]_{q^2}$ MDS code. □

We now identify the torsion code of an infinitesimal evaluation code. Unlike the auxiliary set of nilpotent correction terms appearing in the coordinate expansion, the torsion code is determined entirely by the residue evaluation data.

Theorem 3.10. *Let $C = \mathcal{E}_k(\alpha, v) \subseteq R^n$. Then,*

$$\mathrm{Tor}(C) = \mathrm{GRS}_k(a, s). \tag{3.15}$$

In particular,

$$\mathrm{Tor}(C) = \mathrm{Res}(C). \tag{3.16}$$

Proof. Recall that $\mathrm{Tor}(C) = \{\, x \in \mathbb{F}_{q^2}^n : ux \in C \,\}$. We prove that this set coincides with $\mathrm{GRS}_k(a, s)$.

First, let $x = (x_1, \ldots, x_n) \in \mathrm{Tor}(C)$. Then $ux \in C$, so there exists a polynomial

$$f(X) = f_0(X) + u f_1(X) \in R[X], \qquad f_0, f_1 \in \mathbb{F}_{q^2}[X], \qquad \deg f < k,$$

such that $ux = (v_1 f(\alpha_1), \ldots, v_n f(\alpha_n))$. By Proposition 3.3, for each i, we have

$$v_i f(\alpha_i) = s_i f_0(a_i) + u\Big(s_i(b_i f_0'(a_i) + f_1(a_i)) + t_i f_0(a_i)\Big).$$

On the other hand, the i-th coordinate of ux is ux_i, whose residue part is zero. Therefore, $s_i f_0(a_i) = 0$ $(1 \le i \le n)$. Since $s_i \neq 0$, it follows that $f_0(a_i) = 0$ $(1 \le i \le n)$. Because the points $a_1, \dots, a_n$ are pairwise distinct and $\deg f_0 < k \le n$, the polynomial f_0 has at least n distinct roots. Hence $f_0 = 0$.

Substituting $f_0 = 0$ into the coordinate formula gives $v_i f(\alpha_i) = u\, s_i f_1(a_i), 1 \le i \le n$. Thus, $ux_i = u\, s_i f_1(a_i), 1 \le i \le n$. Since $x_i, s_i f_1(a_i) \in \mathbb{F}_{q^2}$, equality of these u-multiples implies $x_i = s_i f_1(a_i), 1 \le i \le n$. Therefore,

$$x = (s_1 f_1(a_1), \dots, s_n f_1(a_n)) \in \mathrm{GRS}_k(a, s),$$

because $\deg f_1 < k$. This proves that $\mathrm{Tor}(C) \subseteq \mathrm{GRS}_k(a, s)$.

Conversely, let $x = (s_1 g(a_1), \dots, s_n g(a_n)) \in \mathrm{GRS}_k(a, s)$, where $g \in \mathbb{F}_{q^2}[X]$ and $\deg g < k$. Consider the polynomial $f(X) = ug(X) \in R[X]$. Then $\deg f = \deg g < k$, so the vector $(v_1 f(\alpha_1), \dots, v_n f(\alpha_n))$ belongs to C. Since the residue part of f is zero, Lemma 3.2 gives $f(\alpha_i) = ug(a_i), 1 \le i \le n$. Hence $v_i f(\alpha_i) = (s_i + ut_i)\, ug(a_i) = u\, s_i g(a_i)$, because $u^2 = 0$. Therefore,

$$(v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) = u(s_1 g(a_1), \dots, s_n g(a_n)) = ux.$$

Thus $ux \in C$, and therefore $x \in \mathrm{Tor}(C)$. This proves that $\mathrm{GRS}_k(a, s) \subseteq \mathrm{Tor}(C)$.

Combining the two inclusions, we obtain $\mathrm{Tor}(C) = \mathrm{GRS}_k(a, s)$. Finally, Theorem 3.9 gives $\mathrm{Res}(C) = \mathrm{GRS}_k(a, s)$, and hence $\mathrm{Tor}(C) = \mathrm{Res}(C)$. □

Remark 3.11. *For a general R-linear code $C \subseteq R^n$, the residue and torsion codes need not coincide. For infinitesimal evaluation codes, however, the situation is more rigid: one always has*

$$\mathrm{Tor}(\mathcal{E}_k(\alpha, v)) = \mathrm{Res}(\mathcal{E}_k(\alpha, v)) = \mathrm{GRS}_k(a, s).$$

The reason is that if $ux \in \mathcal{E}_k(\alpha, v)$, then the residue part of the corresponding codeword must vanish. By Proposition 3.3, this forces the residue polynomial f_0 to be zero, so the perturbation terms involving b_i and t_i disappear. What remains is precisely the classical evaluation vector

$$(s_1 f_1(a_1), \dots, s_n f_1(a_n)),$$

which belongs to $\mathrm{GRS}_k(a, s)$.

Thus the residue and torsion codes are both classical generalized Reed–Solomon codes, even though the full ring-linear code $\mathcal{E}_k(\alpha, v)$ still carries additional infinitesimal data in its u-component.

The next example illustrates that the torsion and residue codes of an infinitesimal evaluation code coincide and are both classical generalized Reed–Solomon codes.

Example 3.12. *We illustrate Theorem 3.10 with a small example. Let $q = 3$, so $\mathbb{F}_{q^2} = \mathbb{F}_9$, and consider the ring $R = \mathbb{F}_9 + u\mathbb{F}_9, u^2 = 0$. Let $a = (0, 1, \alpha) \in \mathbb{F}_9^3$, where α is a primitive element of $\mathbb{F}_9$, and take multipliers $s = (1, 1, 1)$. Choose perturbation parameters $b = (1, 0, 1)$ and $t = (0, 1, 0)$, and set $\alpha_i = a_i + ub_i$ and $v_i = s_i + ut_i$. Consider the infinitesimal evaluation code*

$$C = \mathcal{E}_2(\alpha, v) \subseteq R^3.$$

By Theorem 3.9, the residue code is the generalized Reed–Solomon code

$$\mathrm{Res}(C) = \mathrm{GRS}_2(a, s) = \{(f(0), f(1), f(\alpha)) : \ f \in \mathbb{F}_9[X],\ \deg f < 2\}.$$

To determine the torsion code, suppose $x \in \mathrm{Tor}(C)$. Then $ux \in C$, so there exists $f(X) = f_0(X) + uf_1(X)$ with $\deg f < 2$ such that $ux = (v_1 f(\alpha_1), v_2 f(\alpha_2), v_3 f(\alpha_3))$. Using the coordinate expansion from Proposition 3.3, the residue part of this vector is $(f_0(0), f_0(1), f_0(\alpha))$. Since ux has a zero residue part, we must have $f_0(0) = f_0(1) = f_0(\alpha) = 0$. Because $\deg f_0 < 2$ and the evaluation points are distinct, this forces $f_0 = 0$. Hence

$$x = (f_1(0), f_1(1), f_1(\alpha)) \in \mathrm{GRS}_2(a, s).$$

Conversely, if $x = (g(0), g(1), g(\alpha)) \in \mathrm{GRS}_2(a, s)$ with $\deg g < 2$, then taking $f(X) = ug(X)$ gives $ux \in C$. Therefore,

$$\mathrm{Tor}(C) = \mathrm{GRS}_2(a, s) = \mathrm{Res}(C).$$

4. Hermitian self-orthogonality and quantum constructions

In this section, we study Hermitian self-orthogonality of the infinitesimal evaluation codes $C = \mathcal{E}_k(\alpha, v)$. We show that Hermitian orthogonality over R decomposes into a residue-layer condition over $\mathbb{F}_{q^2}$ together with a correction equation involving the infinitesimal parameters. These criteria are then used to construct families of Hermitian self-orthogonal codes and corresponding quantum stabilizer codes.

Lemma 4.1. *Let $x, y \in R^n$, where $x_i = a_i + ub_i,\ y_i = c_i + ud_i,\ a_i, b_i, c_i, d_i \in \mathbb{F}_{q^2}$. Then*

$$\langle x, y\rangle_H = \sum_{i=1}^{n} a_i c_i^q + u \sum_{i=1}^{n} (a_i d_i^q + b_i c_i^q). \tag{4.1}$$

Proof. By the definition of the Hermitian inner product over R, $\langle x, y\rangle_H = \sum_{i=1}^n x_i \overline{y_i}$. Since $y_i = c_i + ud_i$, the Frobenius involution on R gives $\overline{y_i} = c_i^q + ud_i^q$. Hence

$$x_i\overline{y_i} = (a_i + ub_i)(c_i^q + ud_i^q) = a_i c_i^q + u\big(a_i d_i^q + b_i c_i^q\big),$$

because $u^2 = 0$. Summing over i yields the required identity. □

Hermitian orthogonality over R therefore splits into two simultaneous equations.

Theorem 4.2. *Let $x, y \in R^n$ with $x_i = a_i + ub_i,\ y_i = c_i + ud_i$. Then $\langle x, y\rangle_H = 0$ if and only if*

$$\sum_{i=1}^{n} a_i c_i^q = 0 \tag{4.2}$$

and

$$\sum_{i=1}^{n} (a_i d_i^q + b_i c_i^q) = 0. \tag{4.3}$$

Proof. By Lemma 4.1,

$$\langle x, y\rangle_H = \sum_{i=1}^{n} a_i c_i^q + u \sum_{i=1}^{n} (a_i d_i^q + b_i c_i^q).$$

Since $R = \mathbb{F}_{q^2} \oplus u\mathbb{F}_{q^2}$ as an $\mathbb{F}_{q^2}$-vector space, this element is zero if and only if both components vanish. □

We now specialize to the infinitesimal evaluation code

$$C = \mathcal{E}_k(\alpha, v) \subseteq R^n, \qquad \alpha_i = a_i + ub_i, \quad v_i = s_i + ut_i.$$

By Theorem 3.9,

$$\mathrm{Res}(C) = \mathrm{GRS}_k(a, s) \subseteq \mathbb{F}_{q^2}^n.$$

Thus Hermitian self-orthogonality of C necessarily imposes Hermitian self-orthogonality on its residue code.

Proposition 4.3. *If $C \subseteq C^{\perp_H}$, then*

$$\mathrm{Res}(C) \subseteq \mathrm{Res}(C)^{\perp_H}.$$

Proof. Assume $C \subseteq C^{\perp_H}$, and let $\bar{x}, \bar{y} \in \mathrm{Res}(C)$. Then there exist $x, y \in C$ such that $\bar{x} = \mathrm{Res}(x)$ and $\bar{y} = \mathrm{Res}(y)$. Write $x_i = a_i + ub_i$ and $y_i = c_i + ud_i$. Then

$$\bar{x} = (a_1, \ldots, a_n), \qquad \bar{y} = (c_1, \ldots, c_n).$$

Since $x, y \in C \subseteq C^{\perp_H}$, we have $\langle x, y\rangle_H = 0$. By Theorem 4.2, $\sum_{i=1}^n a_i c_i^q = 0$. But this is exactly $\langle \bar{x}, \bar{y}\rangle_H$. Hence every pair of codewords of $\mathrm{Res}(C)$ is Hermitian orthogonal, so $\mathrm{Res}(C) \subseteq \mathrm{Res}(C)^{\perp_H}$. □

To make the orthogonality conditions explicit, we use the generating rows

$$G_j = (v_1\alpha_1^j, \ldots, v_n\alpha_n^j), \qquad 0 \le j \le k-1.$$

By Proposition 3.8,

$$G_j = g_j + uh_j,$$

where $g_j = (s_1 a_1^j, \ldots, s_n a_n^j)$ and

$$h_j = (t_1 a_1^j + js_1 b_1 a_1^{j-1}, \ldots, t_n a_n^j + js_n b_n a_n^{j-1}),$$

with the convention that the derivative term is zero when $j = 0$.

Proposition 4.4. *Let*

$$G = \begin{pmatrix} G_0 \\ G_1 \\ \vdots \\ G_{k-1} \end{pmatrix} \in R^{k\times n}$$

be a generator matrix of $C = \mathcal{E}_k(\alpha, v)$. Then

$$C \subseteq C^{\perp_H} \iff G\overline{G}^T = 0.$$

Equivalently,

$$\langle G_i, G_j\rangle_H = 0 \quad \textit{for all } 0 \le i, j \le k-1.$$

Proof. Since G is a generator matrix of C, the code C is the R-row space of G. Thus $C \subseteq C^{\perp_H}$ holds exactly when every pair of rows of G is Hermitian orthogonal.

By definition of the Hermitian inner product,

$$(G\overline{G}^T)_{ij} = \sum_{\ell=1}^{n} G_{i\ell}\,\overline{G_{j\ell}} = \langle G_i, G_j \rangle_H.$$

Hence $G\overline{G}^T = 0$ precisely when $\langle G_i, G_j \rangle_H = 0$ for all i, j. □

Expanding the Gram equations yields the basic self-orthogonality criterion of the paper.

Theorem 4.5. *Let $C = \mathcal{E}_k(\alpha, v), \alpha_i = a_i + ub_i, v_i = s_i + ut_i$. Then, $C \subseteq C^{\perp_H}$ if and only if, for all integers $0 \leq i, j \leq k-1$,*

$$\sum_{\ell=1}^{n} s_\ell^{q+1} a_\ell^{i+qj} = 0 \tag{4.4}$$

and

$$\sum_{\ell=1}^{n}\Big((s_\ell^q t_\ell + s_\ell t_\ell^q) a_\ell^{i+qj} + s_\ell^{q+1}(i\, b_\ell a_\ell^{i-1+qj} + j\, b_\ell^q a_\ell^{i+q(j-1)})\Big) = 0. \tag{4.5}$$

Here the terms involving $i\, a_\ell^{i-1}$ or $j\, a_\ell^{q(j-1)}$ are interpreted as zero when $i = 0$ or $j = 0$, respectively.

Proof. By Proposition 4.4, the condition $C \subseteq C^{\perp_H}$ is equivalent to

$$\langle G_i, G_j \rangle_H = 0 \qquad \text{for all } 0 \leq i, j \leq k-1,$$

where

$$G_i = (v_1\alpha_1^i, \ldots, v_n\alpha_n^i), \qquad G_j = (v_1\alpha_1^j, \ldots, v_n\alpha_n^j).$$

By Proposition 3.8, we may write

$$G_i = g_i + uh_i, \qquad G_j = g_j + uh_j,$$

where

$$g_i = (s_1 a_1^i, \ldots, s_n a_n^i), \qquad g_j = (s_1 a_1^j, \ldots, s_n a_n^j),$$

and

$$h_i = (t_1 a_1^i + i s_1 b_1 a_1^{i-1}, \ldots, t_n a_n^i + i s_n b_n a_n^{i-1}),$$
$$h_j = (t_1 a_1^j + j s_1 b_1 a_1^{j-1}, \ldots, t_n a_n^j + j s_n b_n a_n^{j-1}),$$

with the convention that the derivative terms are zero when $i = 0$ or $j = 0$.

Applying Theorem 4.2 to the vectors $G_i = g_i + uh_i$ and $G_j = g_j + uh_j$, we see that $\langle G_i, G_j \rangle_H = 0$ if and only if

$$\sum_{\ell=1}^{n} (g_i)_\ell (g_j)_\ell^q = 0 \tag{4.6}$$

and

$$\sum_{\ell=1}^{n}\Big((g_i)_\ell (h_j)_\ell^q + (h_i)_\ell (g_j)_\ell^q\Big) = 0. \tag{4.7}$$

We now compute these two sums explicitly.

For (4.6), since $(g_i)_\ell = s_\ell a_\ell^i$ and $(g_j)_\ell = s_\ell a_\ell^j$, we have

$$(g_i)_\ell (g_j)_\ell^q = (s_\ell a_\ell^i)(s_\ell a_\ell^j)^q = s_\ell^{q+1} a_\ell^{i+qj}.$$

Thus (4.6) becomes

$$\sum_{\ell=1}^{n} s_\ell^{q+1} a_\ell^{i+qj} = 0,$$

which is exactly (4.4).

Next, for (4.7), we compute

$$(h_j)_\ell^q = (t_\ell a_\ell^j + j s_\ell b_\ell a_\ell^{j-1})^q = t_\ell^q a_\ell^{qj} + j\, s_\ell^q b_\ell^q a_\ell^{q(j-1)},$$

and therefore

$$(g_i)_\ell (h_j)_\ell^q = s_\ell a_\ell^i \Big(t_\ell^q a_\ell^{qj} + j\, s_\ell^q b_\ell^q a_\ell^{q(j-1)} \Big).$$

Hence

$$(g_i)_\ell (h_j)_\ell^q = s_\ell t_\ell^q a_\ell^{i+qj} + j\, s_\ell^{q+1} b_\ell^q a_\ell^{i+q(j-1)}.$$

Similarly,

$$(h_i)_\ell = t_\ell a_\ell^i + i s_\ell b_\ell a_\ell^{i-1}, \qquad (g_j)_\ell^q = s_\ell^q a_\ell^{qj},$$

so

$$(h_i)_\ell (g_j)_\ell^q = (t_\ell a_\ell^i + i s_\ell b_\ell a_\ell^{i-1}) s_\ell^q a_\ell^{qj}.$$

Thus

$$(h_i)_\ell (g_j)_\ell^q = s_\ell^q t_\ell a_\ell^{i+qj} + i\, s_\ell^{q+1} b_\ell a_\ell^{i-1+qj}.$$

Adding the two expressions, we obtain

$$(g_i)_\ell (h_j)_\ell^q + (h_i)_\ell (g_j)_\ell^q = (s_\ell^q t_\ell + s_\ell t_\ell^q) a_\ell^{i+qj} + s_\ell^{q+1} (i\, b_\ell a_\ell^{i-1+qj} + j\, b_\ell^q a_\ell^{i+q(j-1)}).$$

Therefore (4.7) becomes

$$\sum_{\ell=1}^{n} \Big((s_\ell^q t_\ell + s_\ell t_\ell^q) a_\ell^{i+qj} + s_\ell^{q+1} (i\, b_\ell a_\ell^{i-1+qj} + j\, b_\ell^q a_\ell^{i+q(j-1)}) \Big) = 0,$$

which is exactly (4.5).

We have shown that, for each pair $0 \le i, j \le k-1$,

$$\langle G_i, G_j \rangle_H = 0$$

is equivalent to the simultaneous validity of (4.4) and (4.5). By Proposition 4.4, this is equivalent to $C \subseteq C^{\perp_H}$. The convention for the terms involving $i a_\ell^{i-1}$ and $j a_\ell^{q(j-1)}$ when $i = 0$ or $j = 0$ is exactly the one already built into Proposition 3.8. This completes the proof. □

The first family of equations is exactly the Hermitian self-orthogonality condition for the residue generalized Reed–Solomon code.

Corollary 4.6. *The residue code* $\mathrm{Res}(C) = \mathrm{GRS}_k(a, s)$ *is Hermitian self-orthogonal if and only if*

$$\sum_{\ell=1}^{n} s_\ell^{q+1} a_\ell^{i+qj} = 0 \qquad \text{for all } 0 \le i, j \le k-1.$$

Proof. By Theorem 3.9, $\mathrm{Res}(C) = \mathrm{GRS}_k(a, s)$. Hence $\mathrm{Res}(C)$ is Hermitian self-orthogonal if and only if

$$\mathrm{GRS}_k(a, s) \subseteq \mathrm{GRS}_k(a, s)^{\perp_H}.$$

Now apply Theorem 4.5 to the special case $b_\ell = t_\ell = 0$ for all ℓ. In that case, the nilpotent correction equation (4.5) disappears, and the self-orthogonality condition reduces exactly to

$$\sum_{\ell=1}^{n} s_\ell^{q+1} a_\ell^{i+qj} = 0 \qquad \text{for all } 0 \le i, j \le k-1.$$

This is precisely the required criterion. □

Thus Hermitian self-orthogonality over R consists of the classical residue-layer moment equations together with the correction equations (4.5). In particular, every Hermitian self-orthogonal generalized Reed–Solomon code over $\mathbb{F}_{q^2}$ admits the trivial infinitesimal lift obtained by taking $b_i = t_i = 0$ for all i.

Theorem 4.7. *Let* $C_0 = \mathrm{GRS}_k(a, s) \subseteq \mathbb{F}_{q^2}^n$ *be Hermitian self-orthogonal. Then there exist choices of parameters* $b_1, \ldots, b_n, t_1, \ldots, t_n \in \mathbb{F}_{q^2}$ *such that the infinitesimal evaluation code* $C = \mathcal{E}_k(\alpha, v)$ *satisfies*

$$C \subseteq C^{\perp_H} \qquad \text{and} \qquad \mathrm{Res}(C) = C_0.$$

Proof. Since $C_0 = \mathrm{GRS}_k(a, s)$ is Hermitian self-orthogonal by hypothesis, Corollary 4.6 gives

$$\sum_{\ell=1}^{n} s_\ell^{q+1} a_\ell^{i+qj} = 0 \qquad \text{for all } 0 \le i, j \le k-1.$$

We now choose $b_1 = \cdots = b_n = 0, t_1 = \cdots = t_n = 0$. With this choice, $\alpha_\ell = a_\ell, v_\ell = s_\ell, 1 \le \ell \le n$. Hence the associated infinitesimal evaluation code is

$$C = \mathcal{E}_k(\alpha, v) = \{(s_1 f(a_1), \ldots, s_n f(a_n)) : f \in R[X],\ \deg f < k\}.$$

By Theorem 4.5, the Hermitian self-orthogonality of C is equivalent to the validity of (4.4) and (4.5) for all $0 \le i, j \le k-1$. The field-layer condition (4.4) holds by the displayed moment equations above. The nilpotent condition (4.5) is automatically satisfied, because all parameters b_ℓ and t_ℓ are zero. Therefore

$$C \subseteq C^{\perp_H}.$$

It remains to identify the residue code. By Theorem 3.9,

$$\mathrm{Res}(C) = \mathrm{GRS}_k(a, s) = C_0.$$

Thus there exist choices of parameters $b_1, \ldots, b_n, t_1, \ldots, t_n \in \mathbb{F}_{q^2}$ such that

$$C \subseteq C^{\perp_H} \qquad \text{and} \qquad \mathrm{Res}(C) = C_0.$$

This proves the theorem. □

We now pass from ring-linear codes over R to field-linear codes over $\mathbb{F}_{q^2}$ by means of the Gray map Φ. The Gray map Φ is $\mathbb{F}_{q^2}$-linear and injective. If $C \subseteq R^n$ is free of rank k over R, then $\Phi(C)$ is an $\mathbb{F}_{q^2}$-linear code of length $2n$ and dimension $2k$.

For a general Hermitian self-orthogonal code $C \subseteq R^n$, the Gray image need not be Hermitian self-orthogonal over $\mathbb{F}_{q^2}$. We therefore focus on families for which $\Phi(C)$ can be described explicitly.

Remark 4.8. *The Gray map $\Phi(a + ub) = (a, b)$ does not preserve Hermitian self-orthogonality in general. For example, let $C = \langle u \rangle = u\mathbb{F}_{q^2} \subseteq R$. For $ux, uy \in C$, one has $\langle ux, uy \rangle_H = ux\, uy^q = 0$, since $u^2 = 0$. Hence $C \subseteq C^{\perp_H}$ over R. However, $\Phi(C) = \{(0, x) : x \in \mathbb{F}_{q^2}\} \subseteq \mathbb{F}_{q^2}^2$, and $\langle (0, 1), (0, 1) \rangle_H = 1 \neq 0$. Thus $\Phi(C) \nsubseteq \Phi(C)^{\perp_H}$. Therefore, in the quantum-code constructions below, the condition $\Phi(C) \subseteq \Phi(C)^{\perp_H}$ is verified directly for the specific families under consideration.*

We also recall the standard Hermitian construction for quantum stabilizer codes.

Theorem 4.9 (c.f. [2])**.** *Let $D \subseteq \mathbb{F}_{q^2}^N$ be an $\mathbb{F}_{q^2}$-linear code such that*

$$D \subseteq D^{\perp_H}.$$

Then there exists a q-ary quantum stabilizer code with parameters

$$[[N,\ N - 2\dim_{\mathbb{F}_{q^2}}(D),\ d]]_q, \qquad d = d(D^{\perp_H} \setminus D). \tag{4.8}$$

Accordingly, whenever $C \subseteq R^n$ is a free Hermitian self-orthogonal code of rank k such that $\Phi(C) \subseteq \Phi(C)^{\perp_H}$, one obtains a q-ary quantum stabilizer code with parameters

$$[[2n,\ 2n - 4k,\ d]]_q, \qquad d = d(\Phi(C)^{\perp_H} \setminus \Phi(C)). \tag{4.9}$$

We next present several explicit construction families.

Theorem 4.10. *Let*

$$C_0 = \mathrm{GRS}_k(a, s) \subseteq \mathbb{F}_{q^2}^n$$

be a Hermitian self-orthogonal generalized Reed–Solomon code. Fix $\beta, \gamma \in \mathbb{F}_{q^2}$, and define

$$\alpha_\ell = (1 + u\beta)a_\ell, \qquad v_\ell = (1 + u\gamma)s_\ell, \qquad 1 \le \ell \le n.$$

Let

$$C = \mathcal{E}_k(\alpha, v) \subseteq R^n.$$

Then

$$C \subseteq C^{\perp_H}, \qquad \mathrm{Res}(C) = C_0, \qquad C = C_0 + uC_0, \qquad \Phi(C) = C_0 \times C_0.$$

In particular,

$$\Phi(C) \subseteq \Phi(C)^{\perp_H}.$$

Consequently, there exists a q-ary quantum stabilizer code with parameters

$$[[2n,\ 2n - 4k,\ d]]_q,$$

where

$$d = d((C_0^{\perp_H} \times C_0^{\perp_H}) \setminus (C_0 \times C_0)).$$

If C_0 is MDS and $k < n/2$, then $d = k + 1$.

Proof. Set

$$b_\ell = \beta a_\ell, \qquad t_\ell = \gamma s_\ell, \qquad 1 \le \ell \le n.$$

Then

$$\alpha_\ell = a_\ell + ub_\ell = (1 + u\beta)a_\ell, \qquad v_\ell = s_\ell + ut_\ell = (1 + u\gamma)s_\ell.$$

We first prove that $C \subseteq C^{\perp_H}$ over R. Since $C_0 = \mathrm{GRS}_k(a, s)$ is Hermitian self-orthogonal, Corollary 4.6 gives

$$\sum_{\ell=1}^{n} s_\ell^{q+1} a_\ell^{i+qj} = 0 \qquad \text{for all } 0 \le i, j \le k - 1. \tag{4.10}$$

By Theorem 4.5, it remains to verify the nilpotent condition (4.5). Substituting $b_\ell = \beta a_\ell$ and $t_\ell = \gamma s_\ell$, we obtain

$$s_\ell^q t_\ell + s_\ell t_\ell^q = (\gamma + \gamma^q)s_\ell^{q+1}$$

and

$$i\, b_\ell a_\ell^{i-1+qj} + j\, b_\ell^q a_\ell^{i+q(j-1)} = (i\beta + j\beta^q)a_\ell^{i+qj}.$$

Hence the left-hand side of (4.5) becomes

$$(\gamma + \gamma^q + i\beta + j\beta^q) \sum_{\ell=1}^{n} s_\ell^{q+1} a_\ell^{i+qj},$$

which vanishes by (4.10). Therefore $C \subseteq C^{\perp_H}$.

Next, by Theorem 3.9, the residue code of C is $\mathrm{Res}(C) = \mathrm{GRS}_k(a, s) = C_0$. We now prove that $C = C_0 + uC_0$. Let $f(X) = f_0(X) + uf_1(X) \in R[X]$ with $\deg f < k$. By Proposition 3.3, for each $1 \le \ell \le n$,

$$v_\ell f(\alpha_\ell) = s_\ell f_0(a_\ell) + u\Big(s_\ell(\beta a_\ell f_0'(a_\ell) + f_1(a_\ell)) + \gamma s_\ell f_0(a_\ell)\Big).$$

Thus every codeword of C has the form

$$(s_1 f_0(a_1), \ldots, s_n f_0(a_n)) + u(s_1 g(a_1), \ldots, s_n g(a_n)),$$

where

$$g(X) = f_1(X) + \beta X f_0'(X) + \gamma f_0(X).$$

Since $\deg f_0 < k$, we have $\deg(X f_0') < k$, and hence $\deg g < k$. Therefore both components belong to C_0, so $C \subseteq C_0 + uC_0$.

Conversely, let $x, y \in C_0$. Then there exist polynomials $f_0(X), g(X) \in \mathbb{F}_{q^2}[X]$, both of degree $< k$, such that

$$x = (s_1 f_0(a_1), \ldots, s_n f_0(a_n)), \qquad y = (s_1 g(a_1), \ldots, s_n g(a_n)).$$

Define

$$f_1(X) = g(X) - \beta X f_0'(X) - \gamma f_0(X).$$

Since $\deg f_0 < k$ and $\deg g < k$, we have $\deg f_1 < k$. For $f(X) = f_0(X) + uf_1(X)$, the preceding coordinate formula gives

$$(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) = x + uy.$$

Thus $x + uy \in C$, and hence $C_0 + uC_0 \subseteq C$. Therefore $C = C_0 + uC_0$.

Applying the Gray map $\Phi(a+ub)=(a,b)$ componentwise gives $\Phi(C)=C_0\times C_0$.

We now verify the Hermitian self-orthogonality of the Gray image directly. Let $(x_1,x_2),(y_1,y_2)\in\Phi(C)=C_0\times C_0$. Then $x_1,x_2,y_1,y_2\in C_0$. Since the Hermitian inner product on $\mathbb{F}_{q^2}^{2n}$ is the direct-sum Hermitian inner product, we have $\langle(x_1,x_2),(y_1,y_2)\rangle_H=\langle x_1,y_1\rangle_H+\langle x_2,y_2\rangle_H$. Because $C_0\subseteq C_0^{\perp_H}$, both terms on the right-hand side are zero. Therefore $\langle(x_1,x_2),(y_1,y_2)\rangle_H=0$ for all $(x_1,x_2),(y_1,y_2)\in\Phi(C)$, and hence $\Phi(C)\subseteq\Phi(C)^{\perp_H}$.

We next compute the Hermitian dual of the Gray image, since this is needed for the distance appearing in the Hermitian construction. We now prove $\Phi(C)^{\perp_H}=(C_0\times C_0)^{\perp_H}=C_0^{\perp_H}\times C_0^{\perp_H}$. To prove this, let $(z_1,z_2)\in(C_0\times C_0)^{\perp_H}$. Then $\langle(z_1,z_2),(x,y)\rangle_H=0$ for all $x,y\in C_0$. Equivalently, $\langle z_1,x\rangle_H+\langle z_2,y\rangle_H=0$ for all $x,y\in C_0$. Taking $y=0$ gives $\langle z_1,x\rangle_H=0$ for all $x\in C_0$, so $z_1\in C_0^{\perp_H}$. Taking $x=0$ gives $\langle z_2,y\rangle_H=0$ for all $y\in C_0$, so $z_2\in C_0^{\perp_H}$. Hence $(C_0\times C_0)^{\perp_H}\subseteq C_0^{\perp_H}\times C_0^{\perp_H}$. Conversely, if $z_1,z_2\in C_0^{\perp_H}$, then for all $x,y\in C_0$, $\langle(z_1,z_2),(x,y)\rangle_H=\langle z_1,x\rangle_H+\langle z_2,y\rangle_H=0$. Thus $C_0^{\perp_H}\times C_0^{\perp_H}\subseteq(C_0\times C_0)^{\perp_H}$. Therefore, $(C_0\times C_0)^{\perp_H}=C_0^{\perp_H}\times C_0^{\perp_H}$. Since $\Phi(C)=C_0\times C_0$, we obtain $\Phi(C)^{\perp_H}=C_0^{\perp_H}\times C_0^{\perp_H}$.

Since C is free of rank k over R, the code $\Phi(C)$ is an $\mathbb{F}_{q^2}$-linear code of length $2n$ and dimension $2k$. Therefore, by the Hermitian construction, there exists a q-ary quantum stabilizer code with parameters

$$[[2n,\ 2n-2\dim_{\mathbb{F}_{q^2}}\Phi(C),\ d]]_q=[[2n,\ 2n-4k,\ d]]_q,$$

where $d=d(\Phi(C)^{\perp_H}\setminus\Phi(C))$. Using the dual computation above, this becomes

$$d=d((C_0^{\perp_H}\times C_0^{\perp_H})\setminus(C_0\times C_0)).$$

Finally, assume that C_0 is MDS. Then C_0 has parameters

$$[n,k,n-k+1]_{q^2},$$

and its Hermitian dual $C_0^{\perp_H}$ has parameters

$$[n,n-k,k+1]_{q^2}.$$

If $k<n/2$, then $k+1<n-k+1=d(C_0)$. Thus every minimum-weight codeword of $C_0^{\perp_H}$ has a weight of $k+1$ and cannot lie in C_0, because every nonzero codeword of C_0 has a weight of at least $n-k+1$. Hence $d(C_0^{\perp_H}\setminus C_0)=k+1$. Now the set

$$(C_0^{\perp_H}\times C_0^{\perp_H})\setminus(C_0\times C_0)$$

contains vectors of the form $(z,0)$, where $z\in C_0^{\perp_H}\setminus C_0$. Hence its minimum Hamming weight is at most $k+1$.Conversely, let $(z_1,z_2)\in(C_0^{\perp_H}\times C_0^{\perp_H})\setminus(C_0\times C_0)$. Then at least one of z_1,z_2, say z_i, lies in $C_0^{\perp_H}\setminus C_0$. Since $z_i\notin C_0$ and $0\in C_0$, we have $z_i\neq 0$. As a nonzero codeword of the MDS code $C_0^{\perp_H}$, whose minimum distance is $k+1$, we obtain $\mathrm{wt}(z_i)\geq k+1$. Therefore $\mathrm{wt}(z_1,z_2)=\mathrm{wt}(z_1)+\mathrm{wt}(z_2)\geq\mathrm{wt}(z_i)\geq k+1$. Consequently,

$$d((C_0^{\perp_H}\times C_0^{\perp_H})\setminus(C_0\times C_0))=k+1.$$

This completes the proof. □

Example 4.11. *Let $q = 3$, $n = 6$, and $k = 2$. Let $\alpha \in \mathbb{F}_9$ satisfy $\alpha^2 = 2$, and set $\omega = 1 + \alpha$, which has multiplicative order* 8 *in $\mathbb{F}_9^\times$. Define*

$$a = (\omega,\ 2\alpha,\ 1 + 2\alpha,\ 2 + 2\alpha,\ \alpha,\ 2 + \alpha), \qquad s = (1,\ \omega,\ \omega,\ \omega,\ 1,\ 1).$$

Then

$$C_0 = \mathrm{GRS}_2(a, s) \subseteq \mathbb{F}_9^6$$

is a Hermitian self-orthogonal MDS code.

Choose any $\beta, \gamma \in \mathbb{F}_9$, and define

$$\alpha_\ell = (1 + u\beta)a_\ell, \qquad v_\ell = (1 + u\gamma)s_\ell, \qquad 1 \le \ell \le 6.$$

Let $C = \mathcal{E}_2(\alpha, v) \subseteq R^6$. By Theorem 4.10,

$$C \subseteq C^{\perp_H}, \qquad \mathrm{Res}(C) = C_0, \qquad C = C_0 + uC_0.$$

Applying the Gray map gives

$$\Phi(C) = C_0 \times C_0 \subseteq \mathbb{F}_9^{12},$$

which is Hermitian self-orthogonal of length 12 *and dimension* 4*. Hence the Hermitian construction yields a quantum stabilizer code with parameters* $[[12, 4, 3]]_3$.

We next present another lifting mechanism obtained by perturbing the multipliers by trace-zero elements, which automatically annihilates the nilpotent Hermitian moment equations.

Theorem 4.12. *Let $C_0 = \mathrm{GRS}_k(a, s) \subseteq \mathbb{F}_{q^2}^n$ be a Hermitian self-orthogonal generalized Reed–Solomon code. Choose elements $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_{q^2}$ satisfying*

$$\lambda_\ell + \lambda_\ell^q = 0 \qquad (1 \le \ell \le n).$$

Define

$$\alpha_\ell = a_\ell, \qquad v_\ell = s_\ell(1 + u\lambda_\ell), \qquad 1 \le \ell \le n,$$

and let $C = \mathcal{E}_k(\alpha, v) \subseteq R^n$. Then

$$C \subseteq C^{\perp_H} \qquad \textit{and} \qquad \mathrm{Res}(C) = C_0.$$

Proof. Since

$$v_\ell = s_\ell(1 + u\lambda_\ell) = s_\ell + u(s_\ell\lambda_\ell),$$

we have

$$t_\ell = s_\ell\lambda_\ell, \qquad b_\ell = 0, \qquad 1 \le \ell \le n.$$

We first prove that $C \subseteq C^{\perp_H}$. Since $C_0 = \mathrm{GRS}_k(a, s)$ is Hermitian self-orthogonal, Corollary 4.6 gives

$$\sum_{\ell=1}^{n} s_\ell^{q+1} a_\ell^{i+qj} = 0 \qquad \text{for all } 0 \le i, j \le k - 1. \tag{4.11}$$

By Theorem 4.5, it remains to verify the nilpotent condition (4.5). Since $b_\ell = 0$, the derivative terms disappear and the left-hand side becomes

$$\sum_{\ell=1}^{n} (s_\ell^q t_\ell + s_\ell t_\ell^q) a_\ell^{i+qj}.$$

Using $t_\ell = s_\ell \lambda_\ell$, we obtain

$$s_\ell^q t_\ell + s_\ell t_\ell^q = s_\ell^{q+1} \lambda_\ell + s_\ell^{q+1} \lambda_\ell^q = s_\ell^{q+1} (\lambda_\ell + \lambda_\ell^q).$$

By hypothesis $\lambda_\ell + \lambda_\ell^q = 0$, so each summand vanishes and the nilpotent condition holds for all $0 \le i, j \le k-1$. Hence

$$C \subseteq C^{\perp_H}.$$

Finally, since $\alpha_\ell = a_\ell$ and the residue part of v_ℓ is s_ℓ, Theorem 3.9 gives

$$\mathrm{Res}(C) = \mathrm{GRS}_k(a, s) = C_0.$$

□

Corollary 4.13. *Let*

$$T = \{\lambda \in \mathbb{F}_{q^2} : \lambda + \lambda^q = 0\}.$$

Then T is a one-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^2}$, and hence $|T| = q$. Consequently every Hermitian self-orthogonal generalized Reed–Solomon code

$$C_0 = \mathrm{GRS}_k(a, s) \subseteq \mathbb{F}_{q^2}^n$$

admits exactly q^n trace-zero multiplier lifts of the form described in Theorem 4.12.

Proof. Consider the map

$$L : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}, \qquad L(\lambda) = \lambda + \lambda^q.$$

This map is $\mathbb{F}_q$-linear because $(x + y)^q = x^q + y^q$ and $c^q = c$ for all $c \in \mathbb{F}_q$. By definition,

$$T = \ker(L).$$

The map L is the trace map $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$, which is a nonzero $\mathbb{F}_q$-linear functional. Therefore $\ker(L)$ is a nonzero proper $\mathbb{F}_q$-subspace of the two-dimensional $\mathbb{F}_q$-vector space $\mathbb{F}_{q^2}$. Hence

$$\dim_{\mathbb{F}_q} T = 1, \qquad |T| = q.$$

For each choice of $(\lambda_1, \ldots, \lambda_n) \in T^n$, Theorem 4.12 produces a trace-zero multiplier lift. Conversely every lift of that form arises from such an n-tuple. Thus the number of lifts equals

$$|T^n| = q^n.$$

□

Corollary 4.14. *Under the hypotheses of Theorem 4.12, assume*

$$\lambda_1 = \cdots = \lambda_n = \lambda, \qquad \lambda + \lambda^q = 0.$$

Then

$$C = C_0 + uC_0, \qquad \Phi(C) = C_0 \times C_0.$$

Hence $\Phi(C) \subseteq \Phi(C)^{\perp_H}$*, and therefore one obtains a q-ary quantum stabilizer code with parameters*

$$[[2n,\ 2n-4k,\ d]]_q,$$

where

$$d = d((C_0^{\perp_H} \times C_0^{\perp_H}) \setminus (C_0 \times C_0)).$$

If C_0 *is MDS and* $k < n/2$*, then* $d = k+1$*.*

Proof. By Theorem 4.12, the code C satisfies $C \subseteq C^{\perp_H}$ and $\mathrm{Res}(C) = C_0$. Since $\alpha_\ell = a_\ell$ and $v_\ell = s_\ell(1+u\lambda)$, we have

$$b_\ell = 0, \qquad t_\ell = s_\ell \lambda.$$

Let $f(X) = f_0(X) + uf_1(X) \in R[X]$ with $\deg f < k$. By Proposition 3.3,

$$v_\ell f(\alpha_\ell) = s_\ell f_0(a_\ell) + u\, s_\ell(f_1(a_\ell) + \lambda f_0(a_\ell)).$$

Thus every codeword has the form

$$(s_1 f_0(a_1), \ldots, s_n f_0(a_n)) + u(s_1 g(a_1), \ldots, s_n g(a_n)),$$

where

$$g(X) = f_1(X) + \lambda f_0(X).$$

Hence $C \subseteq C_0 + uC_0$. The reverse inclusion follows by defining

$$f_1(X) = g(X) - \lambda f_0(X),$$

which yields $C = C_0 + uC_0$.

Applying the Gray map $\Phi(a+ub) = (a,b)$ gives

$$\Phi(C) = C_0 \times C_0 \subseteq C_0^{\perp_H} \times C_0^{\perp_H} = \Phi(C)^{\perp_H}.$$

By the Hermitian construction, one obtains a quantum code

$$[[2n,\ 2n-4k,\ d]]_q.$$

If C_0 is MDS with parameters $[n,k,n-k+1]_{q^2}$, then $C_0^{\perp_H}$ has parameters $[n,n-k,k+1]_{q^2}$. Since $k < n/2$, the minimum weight $k+1$ of $C_0^{\perp_H}$ is realized outside C_0. Hence,

$$d = k+1.$$

□

Remark 4.15. *The trace-zero multiplier construction complements the uniform scaling family introduced earlier. In the uniform scaling case, one sets*

$$\alpha_\ell = (1 + u\beta)a_\ell, \qquad v_\ell = (1 + u\gamma)s_\ell,$$

which introduces a global infinitesimal deformation of both evaluation points and multipliers. In contrast, the trace-zero family keeps the evaluation points fixed and perturbs only the multipliers via $v_\ell = s_\ell(1 + u\lambda_\ell)$*, where the trace-zero condition* $\lambda_\ell + \lambda_\ell^q = 0$ *forces the nilpotent Hermitian moment equations to vanish termwise. Thus the two constructions represent complementary mechanisms for producing Hermitian self-orthogonal lifts of* C_0*: the uniform scaling family uses global infinitesimal symmetries, while the trace-zero family allows* n *independent local perturbations.*

Example 4.16. *Let* $q = 5$*,* $n = 13$*, and* $k = 2$*. Let* $C_0 = \mathrm{GRS}_2(a, s) \subseteq \mathbb{F}_{25}^{13}$ *be a Hermitian self-orthogonal generalized Reed–Solomon code (for example, obtained via the subgroup–coset construction described earlier). Choose* $\lambda \in \mathbb{F}_{25}$ *such that* $\lambda + \lambda^5 = 0$*, and define* $\alpha_\ell = a_\ell,\ v_\ell = s_\ell(1 + u\lambda),\ 1 \le \ell \le 13$.

The resulting infinitesimal evaluation code

$$C = \mathcal{E}_2(\alpha, v) \subseteq R^{13}$$

satisfies

$$C \subseteq C^{\perp_H}, \qquad \mathrm{Res}(C) = C_0, \qquad C = C_0 + uC_0.$$

Hence

$$\Phi(C) = C_0 \times C_0 \subseteq \mathbb{F}_{25}^{26},$$

which is Hermitian self-orthogonal of dimension 4*. The Hermitian construction therefore yields a* 5*-ary quantum stabilizer code with parameters* $[[26, 18, 3]]_5$.

We now specialize our infinitesimal constructions to the subgroup–coset families of Hermitian self-orthogonal generalized Reed–Solomon codes over $\mathbb{F}_{q^2}$.

H. Assume that

$$h \mid (q + 1), \qquad h \ge 3,$$

and let

$$n = r\frac{q^2 - 1}{h} + 1, \qquad 1 < r < \min\{q, h\}, \qquad 2 \nmid (r + h).$$

Set

$$m = \frac{q^2 - 1}{h}, \qquad \theta = w^h,$$

where w is a fixed primitive element of $\mathbb{F}_{q^2}$. Define

$$a = (0,\ w,\ w\theta, \dots, w\theta^{m-1},\ w^2,\ w^2\theta, \dots, w^2\theta^{m-1},\ \dots,\ w^r,\ w^r\theta, \dots, w^r\theta^{m-1}) \in \mathbb{F}_{q^2}^n.$$

Finally, let

$$1 \le k \le \left(\frac{r + h - 1}{2}\right)\frac{q + 1}{h} - 1.$$

Under hypothesis (H), the residue-layer subgroup–coset construction provides a Hermitian self-orthogonal generalized Reed–Solomon seed over $\mathbb{F}_{q^2}$.

Theorem 4.17. *(cf. [21]) Assume hypothesis (H). Then there exist* $s_0, \ldots, s_r \in \mathbb{F}_{q^2}^{\times}$ *such that the generalized Reed–Solomon code*

$$C_0 = \mathrm{GRS}_k(a, s) \subseteq \mathbb{F}_{q^2}^n,$$

with multiplier vector

$$s = (s_0,\ \underbrace{s_1, \ldots, s_1}_{m\ times},\ \ldots,\ \underbrace{s_r, \ldots, s_r}_{m\ times}),$$

is Hermitian self-orthogonal.

We now lift this residue-layer family to infinitesimal evaluation codes over $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$.

Theorem 4.18. *Assume hypothesis (H), and let* $C_0 = \mathrm{GRS}_k(a, s) \subseteq \mathbb{F}_{q^2}^n$ *be as in Theorem 4.17. Fix* $\beta \in \mathbb{F}_{q^2}$*, and choose* $\lambda_0, \ldots, \lambda_r \in \mathbb{F}_{q^2}$ *satisfying*

$$\lambda_\ell + \lambda_\ell^q = 0 \qquad (0 \le \ell \le r).$$

Define the locators by

$$\alpha_0 = 0, \qquad \alpha_{\ell,\nu} = (1 + u\beta)w^\ell\theta^\nu, \qquad 1 \le \ell \le r, \quad 0 \le \nu \le m-1,$$

and define the multiplier vector blockwise by

$$v = (s_0(1+u\lambda_0),\ \underbrace{s_1(1+u\lambda_1), \ldots, s_1(1+u\lambda_1)}_{m\ times},\ \ldots,\ \underbrace{s_r(1+u\lambda_r), \ldots, s_r(1+u\lambda_r)}_{m\ times}).$$

Let

$$C = \mathcal{E}_k(\alpha, v) \subseteq R^n.$$

Then

$$C \subseteq C^{\perp_H} \qquad \text{and} \qquad \mathrm{Res}(C) = C_0 = \mathrm{GRS}_k(a, s).$$

Proof. By Theorem 4.17, the residue code $C_0 = \mathrm{GRS}_k(a, s)$ is Hermitian self-orthogonal. The above choice of multipliers is blockwise trace-zero, and the locator perturbation is uniform on the nonzero residue coordinates. Since $C_0 = \mathrm{GRS}_k(a, s)$ is Hermitian self-orthogonal, the Hermitian moment identities

$$\sum_{\xi=1}^{n} s_\xi^{q+1} a_\xi^{i+qj} = 0 \qquad (0 \le i, j \le k-1)$$

hold.

For the lifted code, we have

$$\alpha_\xi = (1+u\beta)a_\xi, \qquad v_\xi = s_\xi(1+u\lambda_\xi),$$

where λ_ξ is constant on each block and satisfies $\lambda_\xi + \lambda_\xi^q = 0$. Substituting these expressions into the Hermitian self-orthogonality criterion for infinitesimal evaluation codes (Theorem 4.5) shows that all nilpotent terms vanish and the remaining terms factor through the residue moment sums above. Hence

$$C \subseteq C^{\perp_H}.$$

Finally, Theorem 3.9 gives

$$\mathrm{Res}(C) = \mathrm{GRS}_k(a, s) = C_0.$$

□

Corollary 4.19. *Assume hypothesis (H). Then the family in Theorem 4.18 contains exactly q^{r+3} codes, corresponding to the free choice of $\beta \in \mathbb{F}_{q^2}$ and $\lambda_0, \dots, \lambda_r \in T$, where*

$$T = \{\lambda \in \mathbb{F}_{q^2} : \lambda + \lambda^q = 0\}.$$

In particular, if $\beta = 0$, one recovers exactly q^{r+1} blockwise trace-zero multiplier lifts.

Proof. By Corollary 4.13, the trace-zero space T has cardinality q. The parameter β may be chosen arbitrarily in $\mathbb{F}_{q^2}$, giving q^2 possibilities, while each of the $r + 1$ parameters $\lambda_0, \dots, \lambda_r$ may be chosen independently from T, giving q^{r+1} possibilities. Hence the total number of codes is

$$q^2 \cdot q^{r+1} = q^{r+3}.$$

The special case $\beta = 0$ leaves only the $r + 1$ blockwise trace-zero parameters. □

The Gray-compatible specialization is obtained by taking a single trace-zero parameter on all blocks.

Corollary 4.20. *Assume hypothesis (H), and let $C = \mathcal{E}_k(\alpha, v) \subseteq R^n$ be the code from Theorem 4.18. Assume in addition that*

$$\lambda_0 = \lambda_1 = \cdots = \lambda_r = \lambda \qquad \text{with} \qquad \lambda + \lambda^q = 0.$$

Then

$$C = C_0 + uC_0, \qquad \Phi(C) = C_0 \times C_0.$$

In particular,

$$\Phi(C) \subseteq \Phi(C)^{\perp_H}.$$

Hence there exists a q-ary quantum stabilizer code with parameters

$$[[2n,\ 2n - 4k,\ d]]_q,$$

where

$$d = d((C_0^{\perp_H} \times C_0^{\perp_H}) \setminus (C_0 \times C_0)).$$

If C_0 is MDS and $k < n/2$, then $d = k + 1$, so the resulting quantum code has parameters

$$[[2n,\ 2n - 4k,\ k + 1]]_q.$$

Proof. Under the assumption $\lambda_0 = \cdots = \lambda_r = \lambda$, the locators and multipliers can be written uniformly as

$$\alpha_\xi = (1 + u\beta)a_\xi, \qquad v_\xi = (1 + u\lambda)s_\xi \qquad \text{for every coordinate } \xi.$$

Thus C is exactly the uniform scaling lift of the Hermitian self-orthogonal code $C_0 = \mathrm{GRS}_k(a, s)$. Therefore Theorem 4.10 applies directly and yields

$$C = C_0 + uC_0, \qquad \Phi(C) = C_0 \times C_0, \qquad \Phi(C) \subseteq \Phi(C)^{\perp_H},$$

together with the stated quantum parameters. □

Example 4.21. *Assume hypothesis (H) with* $q = 7, h = 8, r = 3, k = 2$. *Then,* $m = \frac{q^2-1}{h} = \frac{49-1}{8} = 6, n = 1 + rm = 19$. *Let* w *be a primitive element of* $\mathbb{F}_{49}$, *and set* $\theta = w^8$. *Then* θ *has multiplicative order* 6, *and the locator vector is*

$$a = (0,\ w^t\theta^\ell \mid t = 1,2,3,\ \ell = 0,\dots,5) \in \mathbb{F}_{49}^{19}.$$

Choose $s_0 = s_1 = s_2 = 1$, *and choose* $s_3 \in \mathbb{F}_{49}^\times$ *satisfying* $s_3^8 = 6$. *Then, by Theorem 4.17, the residue code* $C_0 = \mathrm{GRS}_2(a, s) \subseteq \mathbb{F}_{49}^{19}$ *is Hermitian self-orthogonal. Since* C_0 *is generalized Reed–Solomon, it has parameters* $[19, 2, 18]_{49}$.

Now choose $\beta = 0$ *and choose* $\lambda \in \mathbb{F}_{49}$ *satisfying* $\lambda + \lambda^7 = 0$. *Then Corollary 4.20 yields an infinitesimal evaluation code* $C = \mathcal{E}_2(\alpha, v) \subseteq R^{19}$ *such that* $C = C_0 + uC_0$ *and* $\Phi(C) = C_0 \times C_0$. *Hence the Hermitian construction gives a* 7*-ary quantum stabilizer code with parameters* $[[38, 30, 3]]_7$.

Example 4.22. *Assume hypothesis (H) with* $q = 11, h = 4, r = 3, k = 3$. *Then* $m = \frac{q^2-1}{h} = \frac{121-1}{4} = 30, n = 1 + rm = 91$. *Moreover,*

$$k = 3 \leq \left(\frac{r + h - 1}{2}\right)\frac{q+1}{h} - 1 = \left(\frac{3 + 4 - 1}{2}\right)\frac{12}{4} - 1 = 8.$$

Let ω *be a primitive element of* $\mathbb{F}_{121}$, *and set* $\theta = \omega^4$. *Then* θ *has a multiplicative order of* 30, *and the locator vector is*

$$a = (0,\ \omega, \omega\theta, \dots, \omega\theta^{29},\ \omega^2, \omega^2\theta, \dots, \omega^2\theta^{29},\ \omega^3, \omega^3\theta, \dots, \omega^3\theta^{29}) \in \mathbb{F}_{121}^{91}.$$

Choose block multipliers $s_0, s_1, s_2, s_3 \in \mathbb{F}_{121}^\times$ *such that*

$$C_0 = \mathrm{GRS}_3(a, s) \subseteq \mathbb{F}_{121}^{91}$$

is Hermitian self-orthogonal, where

$$s = (s_0,\ \underbrace{s_1, \dots, s_1}_{30 \text{ times}},\ \underbrace{s_2, \dots, s_2}_{30 \text{ times}},\ \underbrace{s_3, \dots, s_3}_{30 \text{ times}}).$$

For example, one may take $s_0 = s_1 = s_2 = 1$ *and choose* $s_3 \in \mathbb{F}_{121}^\times$ *satisfying* $s_3^{12} = 2$. *Then* C_0 *is a* $[91, 3, 89]_{121}$ *MDS code.*

Now fix $\beta = 1$, *choose* $\lambda \in \mathbb{F}_{121}$ *such that* $\lambda + \lambda^{11} = 0$, *and set* $\lambda_0 = \lambda_1 = \lambda_2 = \lambda_3 = \lambda$. *Then Corollary 4.20 gives an infinitesimal evaluation code*

$$C = \mathcal{E}_3(\alpha, v) \subseteq R^{91}$$

such that

$$C = C_0 + uC_0 \qquad \text{and} \qquad \Phi(C) = C_0 \times C_0 \subseteq \mathbb{F}_{121}^{182}.$$

Hence the Hermitian construction yields a quantum stabilizer code with parameters

$$[[182, 170, 4]]_{11}.$$

In this case, Corollary 4.19 gives $q^{r+3} = 11^6$ *admissible parameter choices.*

Example 4.23. *Assume hypothesis (H) with* $q = 13, h = 7, r = 4, k = 4$. *Then* $m = \frac{q^2-1}{h} = 24, n = 1 + rm = 97$.

Moreover,

$$k = 4 \le \left(\frac{r+h-1}{2}\right)\frac{q+1}{h} - 1 = \left(\frac{4+7-1}{2}\right)\frac{14}{7} - 1 = 9.$$

Let w *be a primitive element of* $\mathbb{F}_{169}$, *and set* $\theta = w^7$.

Consider the locator vector

$$a = (0,\ w, w\theta, \ldots, w\theta^{23},\ w^2, w^2\theta, \ldots, w^2\theta^{23},\ w^3, w^3\theta, \ldots, w^3\theta^{23},\ w^4, w^4\theta, \ldots, w^4\theta^{23}) \in \mathbb{F}_{169}^{97}.$$

Choose $s_0 = s_1 = s_2 = s_3 = 1$, *and choose* $s_4 \in \mathbb{F}_{169}^{\times}$ *such that* $s_4^{14} = 4$.

Then the residue code $C_0 = \mathrm{GRS}_4(a, s) \subseteq \mathbb{F}_{169}^{97}$ *is Hermitian self-orthogonal and is a* $[97, 4, 94]_{169}$ *MDS code.*

Now choose $\beta = 1$ *and* $\lambda \in \mathbb{F}_{169}$ *satisfying* $\lambda + \lambda^{13} = 0$. *Then Corollary 4.20 yields an infinitesimal evaluation code*

$$C = \mathcal{E}_4(\alpha, v) \subseteq R^{97}$$

such that

$$\Phi(C) = C_0 \times C_0 \subseteq \mathbb{F}_{169}^{194}.$$

Hence the Hermitian construction gives a quantum stabilizer code with parameters

$$[[194, 178, 5]]_{13}.$$

A Magma computation also confirms that

$$d(\Phi(C)^{\perp_H} \setminus \Phi(C)) = 5.$$

In this case, the family contains $q^{r+3} = 13^7$ *admissible parameter choices.*

Definition 4.24. *Let* $D \subseteq \mathbb{F}_{q^2}^N$ *be a Hermitian self-orthogonal code. The quantum stabilizer code with parameters* $[[N, K, d]]_q$ *obtained from* D *is called* pure *if* D *contains no nonzero vector of Hamming weight smaller than* d.

The quantum stabilizer codes listed in Table 1 are pure. Indeed, in these examples, $D = \Phi(C) = C_0 \times C_0$, where C_0 is an MDS Hermitian self-orthogonal GRS code. Hence $d_H(D) = n - k + 1$ and $d_H(D^{\perp_H}) = k + 1$. Since $k < n/2$, we have $n - k + 1 > k + 1$, so D contains no nonzero vectors of weight smaller than the quantum distance $d = k + 1$.

The parameters of the quantum codes obtained in the preceding examples are summarized in Table 1. For each choice of parameters q, n, h, k, the Hermitian construction produces a q-ary quantum stabilizer code with parameters $[[2n, 2n - 4k, d]]_q$. The corresponding code over $\mathbb{F}_{q^2}$ has parameters $[[n, n - 2k, d]]_{q^2}$, and in all cases listed in the table, these codes are MDS. Moreover, the quantum stabilizer code and the associated $\mathbb{F}_{q^2}$-linear code share the same minimum distance d, reflecting the fact that the stabilizer construction is derived directly from the Hermitian self-orthogonal structure of the underlying $\mathbb{F}_{q^2}$-code. The parameters listed in the table were also compared with the best-known bounds available in the tables of Grassl [11], confirming the optimality of the underlying $\mathbb{F}_{q^2}$-codes.

Table 1. Quantum codes obtained from the constructions of Section 4.

q	n	h	k	Stabilizer $[[2n, 2n-4k, d]]_q$	Status	Quantum $[[n, n-2k, d]]_{q^2}$	Status
3	6	–	2	$[[12, 4, 3]]_3$	best-known	$[[6, 2, 3]]_9$	MDS
5	13	–	2	$[[26, 18, 3]]_5$	–	$[[13, 9, 3]]_{25}$	MDS
7	19	8	2	$[[38, 30, 3]]_7$	–	$[[19, 15, 3]]_{49}$	MDS
7	19	8	3	$[[38, 26, 4]]_7$	–	$[[19, 13, 4]]_{49}$	MDS
7	19	8	4	$[[38, 22, 5]]_7$	–	$[[19, 11, 5]]_{49}$	MDS
11	91	4	2	$[[182, 174, 3]]_{11}$	–	$[[91, 87, 3]]_{121}$	MDS
11	91	4	3	$[[182, 170, 4]]_{11}$	–	$[[91, 85, 4]]_{121}$	MDS
11	91	4	4	$[[182, 166, 5]]_{11}$	–	$[[91, 83, 5]]_{121}$	MDS
13	97	7	2	$[[194, 186, 3]]_{13}$	–	$[[97, 93, 3]]_{169}$	MDS
13	97	7	3	$[[194, 182, 4]]_{13}$	–	$[[97, 91, 4]]_{169}$	MDS
13	97	7	4	$[[194, 178, 5]]_{13}$	–	$[[97, 89, 5]]_{169}$	MDS

We compare the codes in Table 1 with three closely related quantum-code approaches. The Hermitian self-orthogonal GRS construction in [21] produces quantum MDS codes by choosing evaluation points and multipliers over $\mathbb{F}_{q^2}$ satisfying Hermitian orthogonality conditions. Ezerman et al. [8] constructed record-oriented quantum codes from nearly self-orthogonal quasi-twisted codes via Construction X, while Cao and Zhou [6] use the τ-OD matrix-product construction to obtain flexible families of quantum codes, including many record-breaking examples. The present method is different in its algebraic source: it starts from infinitesimal evaluation over $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$, where evaluation at $a_i + ub_i$ introduces the value–derivative correction term $b_i f_0'(a_i) + f_1(a_i)$. In the examples, the Gray image has the product form $C_0 \times C_0$, where C_0 is an MDS Hermitian self-orthogonal GRS code; hence the resulting quantum codes have parameters $[[2n, 2n-4k, d]]_q$ with $d \geq k+1$. Thus the tables are intended to show that the infinitesimal-evaluation framework gives competitive quantum-code parameters through a ring-theoretic first-order lift of classical GRS data, rather than to claim that all listed codes are record-breaking.

Regarding the status labels in Table 1, the label "new" has been replaced by "best known" for the q-ary stabilizer codes $[[2n, 2n-4k, d]]_q$. Since these parameters are subsumed by the τ-OD matrix-product construction of Cao and Zhou [6], which achieves the same minimum distances, no claim is made that they constitute new parameter records. The label "best known" is used in its standard comparative sense: to the best of our knowledge, no code with the same length, dimension, and alphabet size but strictly larger minimum distance appears in Grassl's table or in the comparison sources considered here. The associated q^2-ary codes $[[n, n-2k, d]]_{q^2}$ remain quantum MDS, as they arise directly from MDS Hermitian self-orthogonal GRS codes. The table is therefore not intended as a record-breaking claim but as evidence that the infinitesimal-evaluation framework—a ring-theoretic first-order lift of classical GRS data over $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$—yields quantum-code parameters that are competitive with those produced by substantially different algebraic methods.

5. Conclusions

We introduced infinitesimal evaluation codes over the dual-number extension $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}, u^2 = 0$, and developed their Hermitian self-orthogonality theory. Evaluation at the points $a_i + ub_i$ leads to a coupled value–derivative structure, allowing classical generalized Reed–Solomon codes over $\mathbb{F}_{q^2}$ to be lifted to ring-linear codes over R. We proved that Hermitian orthogonality over R decomposes into a residue-layer condition together with a correction equation involving the infinitesimal parameters. Using this criterion, we constructed several families of Hermitian self-orthogonal infinitesimal evaluation codes. In Gray-compatible cases, these yield q-ary quantum stabilizer codes via the Hermitian construction.

These results show that infinitesimal perturbations over R provide a natural mechanism for extending classical Hermitian self-orthogonal generalized Reed–Solomon constructions and generating new families of quantum codes.

Use of Generative-AI tools declaration

The author declares that he has not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The author would like to extend his sincere appreciation to the Ongoing Research Funding program, (ORF-2026-1530), King Saud University, Riyadh, Saudi Arabia.

Conflicts of interest

The author declares no conflict of interest.

References

1. 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
2. A. Ashikhmin, E. Knill, Nonbinary quantum stabilizer codes, *IEEE Trans. Inf. Theory*, **47** (2001), 3065–3072. https://doi.org/10.1109/18.959288
3. S. Ball, R. Vilar, Determining when a truncated generalised Reed–Solomon code is Hermitian self-orthogonal, *IEEE Trans. Inf. Theory*, **68** (2022), 3922–3931. https://doi.org/10.1109/tit.2022.3150277
4. S. Ball, Some constructions of quantum MDS codes, *Des. Codes Cryptogr.*, **89** (2021), 811–821. https://doi.org/10.1007/s10623-021-00846-y
5. J. Bierbrauer, Y. Edel, Quantum twisted codes, *J. Combin. Des.*, **8** (2000), 174–188. https://doi.org/10.1002/(SICI)1520-6610
6. M. Cao, K. Zhou, Quantum codes using the τ-OD MP construction, *IEEE Trans. Inf. Theory*, **72** (2026), 268–284. https://doi.org/10.1109/TIT.2025.3633795
7. B. Chen, S. Ling, G. Zhang, Application of constacyclic codes to quantum MDS codes, *IEEE Trans. Inf. Theory*, **61** (2015), 1474–1484. https://doi.org/10.1109/TIT.2015.2388576

8. M. F. Ezerman, M. Grassl, S. Ling, F. Özbudak, B. Özkaya, Characterization of nearly self-orthogonal quasi-twisted codes and related quantum codes, *IEEE Trans. Inf. Theory*, **71** (2025), 499–517. https://doi.org/10.1109/TIT.2024.3503420

9. W. Fang, J. Wen, F. W. Fu, Quantum MDS codes with new length and large minimum distance, *Discrete Math.*, **347** (2024), 113662. https://doi.org/10.1016/j.disc.2023.113662

10. M. Grassl, T. Beth, M. Rötteler, On optimal quantum codes, *Int. J. Quantum Inf.*, **2** (2004), 55–64. https://doi.org/10.1142/s0219749904000079

11. M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, online tables, 2009. Available from: `https://www.codetables.de`.

12. L. Jin, S. Ling, J. Luo, C. Xing, Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes, *IEEE Trans. Inf. Theory*, **56** (2010), 4735–4740. https://doi.org/10.1109/TIT.2010.2054174

13. L. Jin, H. Kan, J. Wen, Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes, *Des. Codes Cryptogr.*, **84** (2017), 463–471. https://doi.org/10.1007/s10623-016-0281-9

14. G. G. La Guardia, New quantum MDS codes, *IEEE Trans. Inf. Theory*, **57** (2011), 5551–5554. https://doi.org/10.1109/TIT.2011.2159039

15. F. Li, Y. Liu, R. Jiang, Quantum MDS codes induced by the projective linear transformation, *Finite Fields Appl.*, **111** (2026), 102764. https://doi.org/10.1016/j.ffa.2025.102764

16. E. M. Rains, Quantum weight enumerators, *IEEE Trans. Inf. Theory*, **44** (1998), 1388–1394. https://doi.org/10.1109/18.681316

17. E. M. Rains, Nonbinary quantum codes, *IEEE Trans. Inf. Theory*, **45** (1999), 1827–1832. https://doi.org/10.1109/18.782103

18. S. H. Saif, Constructions and enumerations of self-dual and LCD double circulant codes over a local ring, *Mathematics*, **13** (2025), 3527. https://doi.org/10.3390/math13213527

19. S. H. Saif, S. Aldossari, Quantum and DNA codes from cyclic codes over the ring $\mathbb{Z}_{p^2}[u]/\langle u^2 - \alpha \rangle$, *AIMS Math.*, **11** (2026), 7497–7528. https://doi.org/10.3934/math.2026307

20. X. Shi, Q. Yue, X. Zhu, Construction of some new quantum MDS codes, *Finite Fields Appl.*, **46** (2017), 347–362. https://doi.org/10.1016/j.ffa.2017.04.002

21. R. Wan, X. Zheng, S. Zhu, Construction of quantum MDS codes from Hermitian self-orthogonal generalized Reed–Solomon codes, *Cryptogr. Commun.*, **17** (2025), 181–205. https://doi.org/10.1007/s12095-024-00752-9