Palestine Journal of Mathematics

Vol.15(3), (2026) , 245–253 © Palestine Polytechnic University-PPU 2026

Hull Structure in Skew-Cyclic Codes Over F_q

Nasreddine Benbelkacem

Communicated by Mohammad Ashraf

MSC 2010 Classifications: Primary 94B15, 94B60, 94B05; Secondary 94B27, 11T71.

Keywords and phrases: Hull of a linear code, Linear complementary dual codes, Skew-cyclic codes, Optimal linear codes.

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

Corresponding Author: Nasreddine Benbelkacem

Abstract. The hull of a linear code, defined as the intersection of a code with its dual, is a central concept in coding theory due to its structural significance and its applications in cryptography, secure communications, and quantum error correction. In this work, we investigate the algebraic characterization and construction of hulls of skew-cyclic codes over finite fields. We derive a closed formula for the hull dimension in the skew setting and establish explicit algebraic conditions under which a skew-cyclic code becomes linear complementary dual (LCD). Several illustrative examples, supported by computational verification, demonstrate the correctness of the theoretical results. Moreover, the proposed constructions yield skew-cyclic codes whose hulls lead to optimal linear codes, as verified using the Grassl database of linear codes [7].

1 Introduction

The *hull* of a linear code, defined as the intersection of a code with its dual, has emerged as an important tool for analyzing algebraic and geometric properties of linear codes. Hull dimensions are closely linked to the construction of *linear complementary dual* (LCD) codes, first introduced by Massey [9], which satisfy the condition $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$. LCD codes play a key role in cryptography, particularly in protecting implementations against side-channel attacks, and they also appear in the design of entanglement-assisted quantum error-correcting codes [12, 5]. While hull structures of classical cyclic and constacyclic codes have been extensively studied, their extension to *skew-cyclic codes* remains limited due to the non-commutative nature of the underlying polynomial ring. Skew-cyclic codes, introduced by Boucher, Geiselmann, and Ulmer [1], are defined as left ideals of the quotient algebra $\mathbb{F}_q[x;\theta]/\langle x^n - 1\rangle$, where θ is an automorphism of $\mathbb{F}_q$. Traditionally, the code length n was required to be divisible by the order of θ to ensure that $\langle x^n - 1\rangle$ is a two-sided ideal. However, Siap et al. [10] showed that this restriction can be removed by viewing skew-cyclic codes as $\mathbb{F}_q[x;\theta]$-modules rather than ideals, a perspective we adopt in this work. Recent works on skew-cyclic codes over rings and their applications to DNA codes have been investigated in [11, 6].

To study code equivalence, we consider a general framework in which two linear codes are said to be equivalent if one can be obtained from the other through a finite sequence of:

(i) permutations applied independently to the first α and last β coordinate positions;

(ii) multiplications of individual coordinates by nonzero field elements; and

(iii) applications of field automorphisms to coordinates.

This notion of equivalence plays a crucial role in identifying non-isomorphic constructions.

In this work, we compute the hull dimension of skew-cyclic codes using two complementary approaches. The first approach is algebraic, based on the greatest common right divisor (gcrd) of

the generator polynomial $g(x)$ and the skew reciprocal $h^\dagger(x)$ of the cofactor $h(x)$. The second approach relies on matrix representations, exploiting the structure of generator and parity-check matrices to derive the hull dimension directly from the systematic form of the generator matrix. Both approaches lead to the same closed formula. In the commutative setting, [8] computes the hull dimension from the generator matrix, and here we extend this methodology to the non-commutative skew-cyclic setting. The structure of generator and parity-check matrices for skew-cyclic codes is well established in [2], and we build on these foundations to provide a practical and efficient tool for hull analysis in the skew setting.

The main contributions of this paper may be summarized as follows:

- We establish a closed polynomial expression for the dimension of the hull of a skew-cyclic code in terms of the gcrd of its generator polynomials.
- We derive an equivalent matrix-based formulation of the hull dimension that facilitates direct computational verification.
- We provide constructive criteria ensuring that a skew-cyclic code is LCD, accompanied by explicit examples and verification using MAGMA.

To the best of our knowledge, the unified treatment combining algebraic (gcrd-based) and matrix approaches for determining the hull dimension in the skew-cyclic setting has not been explicitly developed in the literature. Moreover, the proposed framework leads to new constructions of skew-cyclic codes whose hulls attain optimal parameters.

The remainder of the paper is structured as follows. Section 2 reviews the necessary algebraic preliminaries, including skew polynomial rings, skew-cyclic codes, and duality. Section 3 investigates the hull structure of skew-cyclic codes and derives the main formula for the hull dimension. Section 4 provides explicit constructions of skew-cyclic LCD codes together with several illustrative examples. Section 5 offers concluding remarks and potential directions for further research.

2 Preliminaries

Let I_n denote the $n \times n$ identity matrix, and let $\mathbf{0}$ denote either the zero vector or the all-zero matrix, with the dimension clear from the context. Vectors are written in boldface; for example, $\mathbf{x}_n = (x_1, \ldots, x_n)$ and $\mathbf{y}_m = (y_1, \ldots, y_m)$, so that $(\mathbf{x}_n, \mathbf{y}_m) = (x_1, \ldots, x_n, y_1, \ldots, y_m)$.

Let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements, where p is prime and $m \geq 1$. Let θ be a Frobenius automorphism of $\mathbb{F}_q$ defined by $\theta(\alpha) = \alpha^{p^i}$ for some fixed integer i with $1 \leq i < m$. The order of θ is m, and the fixed field of $\langle\theta\rangle$ is $\mathbb{F}_p$.

A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$. If $\mathcal{C}$ has dimension k, then it contains q^k codewords.

Definition 2.1. The *skew polynomial ring* $\mathbb{F}_q[x;\theta]$ is the set of polynomials

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad a_i \in \mathbb{F}_q,$$

with addition defined coefficientwise and multiplication determined by distributivity and the rule

$$(ax^i) \cdot (bx^j) = a\,\theta^i(b)\,x^{i+j}.$$

Remark 2.2. Unlike classical polynomial multiplication, multiplication in $\mathbb{F}_q[x;\theta]$ is generally noncommutative due to the presence of the automorphism θ. In particular, the coefficient b is transformed by θ^i when multiplied by x^i. For example, in general $xb \neq bx$, since

$$xb = \theta(b)x.$$

The ring becomes commutative only in the special case $\theta = \mathrm{id}$. This noncommutativity is the key feature that distinguishes skew-cyclic codes from classical cyclic codes.

For any $f, g \in \mathbb{F}_q[x;\theta]$ with $f \neq 0$, there exist unique $q, r \in \mathbb{F}_q[x;\theta]$ such that

$$g(x) = q(x)\, f(x) + r(x), \qquad \deg(r) < \deg(f). \tag{2.1}$$

Thus, f is a *right divisor* of g when $r = 0$. Since left and right division are distinct notions in $\mathbb{F}_q[x;\theta]$, divisibility and ideal structure must always be specified as left, right, or two-sided. The ring admits greatest common right divisors (gcrd) and least common left multiples (lclm).

A subset $\mathcal{C} \subseteq \mathbb{F}_q^n$ is called an $\mathbb{F}_q$*-skew cyclic code* of length n if:

(i) $\mathcal{C}$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$;

(ii) for any $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$, the *skew cyclic shift*

$$T_\theta(\mathbf{c}) := (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2}))$$

also belongs to $\mathcal{C}$.

It is often convenient to associate $\mathbf{a} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ with the polynomial $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ in the quotient space

$$R_n := \mathbb{F}_q[x;\theta]/\langle x^n - 1\rangle. \tag{2.2}$$

Under this correspondence, any skew-cyclic code $\mathcal{C}$ is a left ideal of R_n, generated by a right divisor g of $x^n - 1$; we write $\mathcal{C} = \langle g\rangle$.

Theorem 2.3. *[10] A code $\mathcal{C} \subseteq R_n$ is skew cyclic if and only if it is a left $\mathbb{F}_q[x;\theta]$-submodule of the left $\mathbb{F}_q[x;\theta]$-module R_n.*

A nondegenerate *inner product* on $\mathbb{F}_q^n$ is given by

$$\langle \mathbf{x}, \mathbf{y}\rangle = \sum_{i=0}^{n-1} x_i y_i \in \mathbb{F}_q. \tag{2.3}$$

The *dual code* of $\mathcal{C}$ is

$$\mathcal{C}^\perp = \{\, \mathbf{y} \in \mathbb{F}_q^n : \langle \mathbf{x}, \mathbf{y}\rangle = 0 \text{ for all } \mathbf{x} \in \mathcal{C} \,\}.$$

A code is *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$.

LCD (Linear Complementary Dual) codes, introduced by Massey, satisfy $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$. More generally, the *hull* of $\mathcal{C}$ is

$$\mathrm{Hull}(\mathcal{C}) := \mathcal{C} \cap \mathcal{C}^\perp.$$

The hull has been widely used in coding theory, and hulls of cyclic and constacyclic codes have been extensively investigated.

Theorem 2.4. *[3] If $\mathcal{C}$ is a skew cyclic code of length n over $\mathbb{F}_q$, then its dual $\mathcal{C}^\perp$ is also a skew cyclic code of length n.*

Definition 2.5. For a skew cyclic code $\mathcal{C}$, its *hull* is

$$\mathrm{Hull}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^\perp.$$

Theorem 2.6. *If $\mathcal{C}$ is a skew cyclic code of length n over $\mathbb{F}_q$, then $\mathcal{C} \cap \mathcal{C}^\perp$ is also a skew cyclic code of length n.*

Proof. Since $\mathcal{C}$ is invariant under T_θ, and by Theorem 2.4, $\mathcal{C}^\perp$ is also invariant under T_θ, the intersection $\mathcal{C} \cap \mathcal{C}^\perp$ is closed under T_θ. Hence it is skew cyclic. The ideal-theoretic interpretation in R_n yields the same conclusion: $\mathcal{C}$ and $\mathcal{C}^\perp$ are principal left submodules of R_n, and so is their intersection. □

For $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n$, the *Hamming weight* is

$$\mathrm{wt}(\mathbf{x}) = |\{\, i : x_i \neq 0 \,\}|.$$

The Hamming distance between $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ is

$$d_H(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y}).$$

The *minimum distance* of a code $\mathcal{C}$ is

$$d_{\min}(\mathcal{C}) = \min\{\, \mathrm{wt}(\mathbf{x}) : \mathbf{x} \in \mathcal{C},\ \mathbf{x} \neq \mathbf{0} \,\}.$$

3 The Hull of Skew-Cyclic Codes

We present a characterization of the *dimension of the hull* in terms of the *right greatest common divisor (right-gcd)* of $g(x)$ and $h^\dagger(x)$, where $h^\dagger(x)$ denotes the *skew reciprocal polynomial* of $h(x)$ satisfying $x^n - 1 = h(x)g(x)$. The hull dimension can be expressed in two equivalent ways:

(i) via the *generator polynomials* $g(x)$ and $h^\dagger(x)$, and

(ii) via the corresponding *generator matrices* G and H of $\mathcal{C}$ and $\mathcal{C}^\perp$.

Theorem 3.1. *Let $\mathcal{C} = \langle g(x)\rangle$ be a skew-cyclic code of length n over $\mathbb{F}_q$, with $x^n - 1 = h(x)g(x)$ and let $h^\dagger(x)$ denote the skew reciprocal of $h(x)$. Then*

$$\mathcal{C} \cap \mathcal{C}^\perp = \langle \mathrm{lclm}(g(x), h^\dagger(x))\rangle.$$

Proof. Let $\ell(x) = \mathrm{lclm}(g(x), h^\dagger(x))$ denote the least common left multiple of $g(x)$ and $h^\dagger(x)$. By definition, there exist polynomials $a(x), b(x) \in \mathcal{R}_n$ such that

$$\ell(x) = a(x)g(x) = b(x)h^\dagger(x).$$

If $c(x) \in \langle \ell(x)\rangle$, then $c(x) = q(x)\ell(x)$ for some $q(x) \in \mathcal{R}_n$. It follows that

$$c(x) = q(x)a(x)g(x) = q(x)b(x)h^\dagger(x),$$

so $c(x)$ is a multiple of both $g(x)$ and $h^\dagger(x)$, and therefore $c(x) \in \mathcal{C} \cap \mathcal{C}^\perp$.

Conversely, if $c(x) \in \mathcal{C} \cap \mathcal{C}^\perp$, then $c(x)$ is a multiple of both $g(x)$ and $h^\dagger(x)$, hence a multiple of their least common left multiple $\ell(x)$.

Thus, we have

$$\mathcal{C} \cap \mathcal{C}^\perp = \langle \ell(x)\rangle = \langle \mathrm{lclm}(g(x), h^\dagger(x))\rangle.$$

□

3.1 Computing the Hull Dimension from the Generator Polynomials $g(x)$ and $h^\dagger(x)$

The hull dimension of a skew-cyclic code can be computed directly from its generator polynomials. In [4], skew LCD codes are characterized via the greatest common right divisor $\mathrm{gcrd}(g(x), h^\dagger(x))$. Building on this approach, the following theorem gives an explicit formula for the hull dimension of a general skew-cyclic code.

Theorem 3.2. *Let $\mathcal{C} = \langle g(x)\rangle \subseteq \mathcal{R}_n = \mathbb{F}_q[x;\theta]/\langle x^n - 1\rangle$ with $x^n - 1 = h(x)g(x)$ and $h^\dagger(x)$ the skew reciprocal of $h(x)$. Then*

$$\dim_{\mathbb{F}_q}(\mathrm{Hull}(\mathcal{C})) = \deg\big(\mathrm{gcrd}(g(x), h^\dagger(x))\big).$$

In particular, $\mathcal{C}$ is LCD if and only if $\mathrm{gcrd}(g(x), h^\dagger(x)) = 1$.

Proof. From the previous theorem, we know that

$$\mathrm{Hull}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^\perp = \langle \mathrm{lclm}(g(x), h^\dagger(x))\rangle.$$

Since $\mathcal{C} = \langle g(x)\rangle$ and $\mathcal{C}^\perp = \langle h^\dagger(x)\rangle$, we have

$$x^n - 1 = g(x)h(x) = h^\dagger(x)g^\dagger(x).$$

By the noncommutative analogue of the sum and intersection relation,

$$\langle g(x)\rangle + \langle h^\dagger(x)\rangle = \langle \mathrm{gcrd}(g(x), h^\dagger(x))\rangle,$$

and

$$\langle g(x)\rangle \cap \langle h^\dagger(x)\rangle = \langle \mathrm{lclm}(g(x), h^\dagger(x))\rangle,$$

it follows that

$$\deg(x^n - 1) = \deg(\text{lclm}(g(x), h^\dagger(x))) + \deg(\text{gcrd}(g(x), h^\dagger(x))).$$

Since $\deg(x^n - 1) = n$, we obtain

$$\dim_{\mathbb{F}_q}(\text{Hull}(\mathcal{C})) = n - \deg(\text{lclm}(g(x), h^\dagger(x))) = \deg(\text{gcrd}(g(x), h^\dagger(x))).$$

Finally, $\mathcal{C}$ is LCD if and only if its hull is trivial, i.e.,

$$\text{Hull}(\mathcal{C}) = \{0\} \quad \Longleftrightarrow \quad \text{gcrd}(g(x), h^\dagger(x)) = 1.$$

This completes the proof. □

Remark 3.3. The above result can be interpreted as follows. The generator polynomial $g(x)$ determines the structure of the code $\mathcal{C}$, while the skew reciprocal $h^\dagger(x)$ characterizes its dual. The intersection $\mathcal{C} \cap \mathcal{C}^\perp$ therefore corresponds to polynomials that are simultaneously multiples of both $g(x)$ and $h^\dagger(x)$. The degree of their greatest common right divisor measures precisely how much these two structures overlap, which explains why it determines the dimension of the hull.

Remark 3.4. This extends the classical hull dimension formula for cyclic codes to skew-cyclic codes. For $\theta = \text{id}$, it reduces to

$$\dim_{\mathbb{F}_q}(\text{Hull}(\mathcal{C})) = \deg(\text{gcd}(g(x), h^\dagger(x))).$$

Example 3.5. Let $n = 6$ and $\mathbb{F}_9 = \mathbb{F}_2(w)$ with $w^2 = w + 1$, and let $\theta(\alpha) = \alpha^3$. Consider the skew polynomial $g(x) = w^2 + w^5x + w^7x^2 + x^3$, which divides $x^6 - 1$ in $\mathbb{F}_9[x; \theta]$. Then $x^6 - 1 = h(x)g(x)$, where

$$h(x) = w^2 + w^5x + wx^2 + x^3.$$

Let $\mathcal{C} = \langle g(x) \rangle$ be a $[6, 3, 4]_9$ *self-dual optimal skew-cyclic code*. The skew reciprocal of $h(x)$ is $h^\dagger(x) = 1 + w^3x + w^5x^2 + w^6x^3$. Computing the greatest common right divisor, we obtain $\text{gcrd}(g(x), h^\dagger(x)) = g(x)$, so that $\dim_{\mathbb{F}_9}(\text{Hull}(\mathcal{C})) = 3$. Hence, the hull of $\mathcal{C}$ is generated by $\text{Hull}(\mathcal{C}) = \langle g(x) \rangle$.

3.2 Computing the Dimension of the Hull from Generator and Parity-Check Matrices

Matrix representations offer an efficient way to compute the hull dimension. In the commutative case, this uses generator matrices [8], while for skew-cyclic codes, the generator and parity-check structure is described in [2]. Here, we extend these ideas to give a direct formula for the hull dimension from the systematic generator matrix.

Let $\mathcal{C}$ be a skew-cyclic code of length n over $\mathbb{F}_q$, generated by the skew polynomial

$$g(x) = g_0 + g_1x + \cdots + g_rx^r \in R_n,$$

where $x^n - 1 = h(x)g(x)$ for some $h(x) \in R_n$. The generator matrix of the $[n, k]$-skew cyclic code $\mathcal{C}$, with $k = n - \deg(g)$, is given by

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \cdots & \theta(g_{r-1}) & \theta(g_r) & \cdots & 0 \\ 0 & 0 & \theta^2(g_0) & \theta^2(g_1) & \cdots & \theta^2(g_{r-1}) & \theta^2(g_r) & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \theta^{k-1}(g_0) & \theta^{k-1}(g_1) & \cdots & \theta^{k-1}(g_{r-1}) & \theta^{k-1}(g_r) \end{pmatrix}. \quad (3.1)$$

Let

$$h(x) = h_0 + h_1x + \cdots + h_{n-r}x^{n-r}$$

be the skew cofactor. Its skew reciprocal polynomial is

$$h^{\dagger}(x) = h_{n-r} + \theta(h_{n-r-1})x + \cdots + \theta^{n-r-1}(h_1)x^{n-r-1} + \theta^{n-r}(h_0)x^{n-r}.$$

A parity-check matrix of $\mathcal{C}$ is then

$$H = \begin{pmatrix} h_{n-r} & \cdots & \theta^{n-r-1}(h_1) & \theta^{n-r}(h_0) & 0 & \cdots & 0 \\ 0 & \theta(h_{n-r}) & \cdots & \cdots & \theta^{n-r+1}(h_0) & \cdots & 0 \\ 0 & \ddots & \ddots & \cdots & \cdots & \cdots & \vdots \\ \vdots & & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & \cdots & 0 & \theta^{n-r-1}(h_{n-r}) & \cdots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{pmatrix}. \tag{3.2}$$

Applying Gaussian row operations to (3.1), and using the fact that all entries lie in the field $\mathbb{F}_q$, we obtain a systematic generator matrix of the form

$$G = \Big(I_k \mid \Theta(P)\Big), \tag{3.3}$$

where $\Theta(P)$ is a $k \times (n-k)$ matrix whose entries consist of sums and products of elements $\theta^i(g_j)$.

The dual code $\mathcal{C}^{\perp}$, with respect to the inner product in (2.3), has generator matrix

$$H = \Big(-\Theta(P)^T \mid I_{n-k}\Big). \tag{3.4}$$

Clearly, $HG^T = \mathbf{0}$, and H serves as a valid parity-check matrix of $\mathcal{C}$. Similarly, G is a parity-check matrix for $\mathcal{C}^{\perp}$. Therefore,

$$\mathcal{C} = \{\mathbf{c} \in \mathbb{F}_q^n : H\mathbf{c}^T = \mathbf{0}\}, \qquad \mathcal{C}^{\perp} = \{\mathbf{c} \in \mathbb{F}_q^n : G\mathbf{c}^T = \mathbf{0}\}.$$

The hull of $\mathcal{C}$ satisfies

$$\mathrm{Hull}(\mathcal{C}) = \left\{ \mathbf{c} \in \mathbb{F}_q^n : \begin{pmatrix} G \\ H \end{pmatrix} \mathbf{c}^T = \mathbf{0} \right\}. \tag{3.5}$$

Hence,

$$\dim(\mathrm{Hull}(\mathcal{C})) = n - \mathrm{rank}\begin{pmatrix} G \\ H \end{pmatrix} = n - \mathrm{rank}\begin{pmatrix} I_k & \Theta(P) \\ -\Theta(P)^T & I_{n-k} \end{pmatrix}.$$

To compute this rank, we perform a block row operation by adding $\Theta(P)$ times the second block row to the first. This yields

$$\mathrm{rank}\begin{pmatrix} G \\ H \end{pmatrix} = \mathrm{rank}\begin{pmatrix} I_k + \Theta(P)\Theta(P)^T & \Theta(P) \\ 0 & I_{n-k} \end{pmatrix}.$$

Since the lower-right block is the identity matrix, its contribution to the rank is $n-k$. Therefore,

$$\dim(\mathrm{Hull}(\mathcal{C})) = k - \mathrm{rank}\big(I_k + \Theta(P)\Theta(P)^T\big).$$

We therefore obtain the following characterization.

Theorem 3.6. *Let $\mathcal{C}$ be an $[n,k]$-skew cyclic code over $\mathbb{F}_q$ with generator matrix $G = \Big(I_k \mid \Theta(P)\Big)$. Then the dimension of the hull of $\mathcal{C}$ is*

$$\dim(\mathrm{Hull}(\mathcal{C})) = k - \mathrm{rank}\big(I_k + \Theta(P)\Theta(P)^T\big).$$

This result also provides an immediate characterization of special classes of skew-cyclic codes. If the matrix $\big(I_k + \Theta(P)\Theta(P)^T\big)$ is nonsingular, then $\dim(\mathrm{Hull}(\mathcal{C})) = 0$, and $\mathcal{C}$ is a skew LCD code. Conversely, if $\mathrm{rank}\big(I_k + \Theta(P)\Theta(P)^T\big) = 0$, then $\dim(\mathrm{Hull}(\mathcal{C})) = k$, and $\mathcal{C}$ is self-orthogonal. Hence, the rank of $\big(I_k + \Theta(P)\Theta(P)^T\big)$ provides a direct and practical criterion for identifying LCD and self-orthogonal skew-cyclic codes.

Example 3.7. Let $n = 6$ and $\mathbb{F}_4 = \mathbb{F}_2(w)$ with $w^2 = w + 1$, and let $\theta(\alpha) = \alpha^2$. Consider the skew polynomial

$$g(x) = w + w^2x + w^2x^2 + x^3,$$

which divides $x^6 - 1$ in $\mathbb{F}_4[x; \theta]$. A generator matrix of the resulting code is

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & w^2 & w & w \\ 0 & 1 & 0 & w & w^2 & w \\ 0 & 0 & 1 & w & w & w^2 \end{pmatrix}.$$

This gives an optimal $[6, 3, 4]_4$ skew-cyclic code, and its dual is generated by

$$H_1 = \begin{pmatrix} w^2 & w & w & 1 & 0 & 0 \\ w & w^2 & w & 0 & 1 & 0 \\ w & w & w^2 & 0 & 0 & 1 \end{pmatrix}.$$

The hull dimension is

$$\dim(\mathrm{Hull}(\mathcal{C})) = 3 - \mathrm{rank}\left(I_3 + \begin{pmatrix} w & w^2 & w^2 \\ w^2 & w & w^2 \\ w^2 & w^2 & w \end{pmatrix} \right) = 3 - 1 = 2.$$

Thus the hull yields an optimal $[6, 2, 4]_4$ linear code. Additional optimal LCD skew-cyclic codes over $\mathbb{F}_4$ appear in Table 1.

Table 1. Examples of optimal LCD skew-cyclic codes over $\mathbb{F}_4$

No.	Parameters	$g(x) \in \mathbb{F}_4[x; \theta]$
1	$[6, 3, 4]_4$	$1 + w^2x + wx^2 + x^3$
2	$[8, 4, 4]_4$	$w^2 + x + x^2 + x^4$
3	$[10, 4, 6]_4$	$w^2 + x + w^2x^2 + x^4 + x^5 + x^6$

4 Examples and Applications

Based on the algebraic characterization and results of Section 3, we present explicit computational examples illustrating skew-cyclic codes whose hulls attain optimal parameters. Before listing these examples, we outline a computational procedure for generating skew-cyclic codes and computing their hulls over $\mathbb{F}_q$.

Algorithm 1 Hull of a skew-cyclic code (input: generator $g(x)$)

Require: Integers n, finite field $\mathbb{F}_q$, automorphism θ, and a monic right-divisor generator $g(x)$ of $x^n - 1$

Ensure: Hull code $\mathrm{Hull}(C)$ of $C = \langle g(x) \rangle$, and its parameters

1: $f(x) \leftarrow x^n - 1$ ▷ Modulus polynomial
2: Compute $(h(x), r(x)) \leftarrow \mathrm{RQuotrem}(f, g)$
3: Compute $h^\dagger(x) \leftarrow \mathrm{SkewReciprocal}(h)$
4: $d(x) \leftarrow \mathrm{gcrd}(g(x), h^\dagger(x))$
5: $k_{\mathrm{hull}} \leftarrow \deg(d)$
6: Construct generator matrix G of C using shifts of $g(x)$ modulo $f(x)$
7: Compute hull code $H \leftarrow C \cap C^\perp$
8: **return** $(d(x),\ k_{\mathrm{hull}},\ (n, k_{\mathrm{hull}}, d_{\mathrm{min}}))$

Tables 2 and 3 present representative examples of optimal skew-cyclic codes and their hulls, computed using MAGMA. Each generator polynomial $g(x)$ defines a distinct left submodule

$g(x)$	θ-cyclic code	Hull θ-cyclic code
$1+x+wx^2+x^3+w^2x^4+x^5+x^6$	$[12,6,6]^{**}$	$[12,6,6]$
$w^2+wx+x^2+w^2x^4+wx^5+x^6+w^2x^8+wx^9+x^{10}$	$[12,2,9]^{*}$	$[12,2,9]$
$w+x+x^3+x^4+x^5+w^2x^6+x^8$	$[12,4,7]^{*}$	$[12,4,7]$
$w+x+wx^2+x^4+x^6+x^7$	$[12,5,6]^{*}$	$[12,5,6]$
$1+w^2x+x^2+w^2x^3+wx^4+x^5+wx^6+x^7$	$[12,5,6]$	$[12,3,8]$
$w+w^2x+wx^3+x^4+w^2x^6+x^8+x^{10}+x^{11}$	$[20,9,8]^{*}$	$[20,9,8]$
$w^2+x+w^2x^2+wx^3+wx^4+wx^6+x^8+x^9$	$[20,11,4]$	$[20,9,8]$
$1+wx+w^2x^2+wx^3+wx^4+w^2x^5+x^6+x^8+wx^9+x^{10}+w^2x^{11}+wx^{12}+x^{14}+x^{15}+w^2x^{16}+w^2x^{17}+x^{18}+x^{19}+x^{20}+x^{21}$	$[28,7,13]$	$[28,2,22]$
$w^2+x+w^2x^2+x^4+x^5+wx^8+x^9+w^2x^{10}+x^{13}$	$[28,15,8]$	$[28,3,20]$
$w+wx+x^4+x^6+x^7+wx^8+wx^9+w^2x^{12}+wx^{13}+x^{14}+x^{15}+x^{16}+x^{18}+x^{19}$	$[28,9,12]$	$[28,7,16]$
$1+wx^3+wx^4+w^2x^5+x^6+w^2x^7+x^8+x^9+wx^{10}+w^2x^{11}+wx^{12}+x^{13}+w^2x^{14}+x^{15}+x^{16}+x^{17}$	$[28,11,12]^{*}$	$[28,11,12]$
$w+w^2x+x^2+wx^3+w^2x^5+wx^6+x^7+x^8+wx^9+x^{10}+wx^{11}+wx^{13}+w^2x^{15}+wx^{16}+x^{17}+x^{18}+wx^{19}+w^2x^{20}+x^{21}+x^{22}$	$[30,8,13]$	$[30,2,24]$
$1+wx+wx^3+wx^4+wx^5+w^2x^6+x^7+w^2x^8+w^2x^9+x^{10}+x^{11}+wx^{12}+x^{15}+x^{16}+wx^{17}+x^{18}+wx^{20}+x^{23}$	$[30,7,16]$	$[30,6,18]$

Table 2. Optimal hull skew-cyclic codes over $\mathbb{F}_4$.

$g(x)$	θ-cyclic code	Hull θ-cyclic code
$w^2+w^7x+wx^2+x^3$	$[6,3,4]^{**}$	$[6,3,4]$
$w^2+w^7x+w^3x^2+w^3x^3+x^4$	$[6,2,5]^{*}$	$[6,2,5]$
$1+x+w^3x^2+x^3$	$[6,3,4]$	$[6,2,5]$
$w^6+w^3x+2x^2+w^6x^3+wx^4+x^5$	$[8,3,6]^{*}$	$[8,3,6]$
$w+w^7x^2+w^7x^3+x^4$	$[8,4,4]$	$[8,3,6]$
$1+w^6x+2x^2+w^6x^3+w^2x^4+2x^5+x^6+w^6x^8+w^7x^9+wx^{10}+wx^{11}+w^3x^{12}+w^5x^{13}+w^6x^{14}+w^7x^{15}+x^{16}$	$[22,6,14]^{*}$	$[22,6,14]$
$2+w^6x+x^2+w^6x^3+wx^4+w^3x^5+x^6$	$[22,16,5]$	$[22,6,14]$

Table 3. Optimal hull skew-cyclic codes over $\mathbb{F}_9$.

in $\mathbb{F}_q[x;\theta]/\langle x^n-1\rangle$, and the corresponding code parameters $(n,k,d_{\min})$ and hull parameters $(n,k_{\text{hull}},d_{\min}^{\text{hull}})$ were verified computationally. In these tables, ** indicates a self-dual skew-cyclic code, while * denotes a self-orthogonal skew-cyclic code. The optimality of several constructed skew-cyclic codes and their hulls is established through comparison with the Grassl database of best-known linear codes [7]. In addition, code equivalence tests carried out using MAGMA confirm that these codes attain the best known parameters.

5 Conclusion

In this work, we developed a coherent algebraic framework for analyzing and constructing the *hulls of skew-cyclic codes* over finite fields. Within this framework, explicit algebraic conditions

were established to determine the hull dimension in terms of the greatest common right divisor of the generator polynomial and the skew reciprocal of its complementary factor in $x^n - 1$. The main objective was to construct skew-cyclic codes whose hulls are optimal, rather than focusing solely on LCD properties. Future work will extend these results to skew-constacyclic and ring-based codes, explore Gray image relations over Galois rings, and perform systematic Magma-based searches for new families of skew-cyclic codes with optimal hulls.

References

[1] D. Boucher, W. Geiselmann, F. Ulmer, *Skew-cyclic codes*, Applicable Algebra in Engineering, Communication and Computing, **18(4)**, 379–389, (2007).

[2] D. Boucher, P. Solé, F. Ulmer, *Skew constacyclic codes over Galois rings*, Advances in Mathematics of Communications, **2(3)**, 273–292, (2008).

[3] D. Boucher, F. Ulmer, *Self-dual skew codes and factorization of skew polynomials*, Journal of Symbolic Computation, **60**, 47–61, (2014).

[4] R. Boulanouar, A. Batoul, D. Boucher, *An overview on skew constacyclic codes and their subclass of LCD codes*, Advances in Mathematics of Communications, **15(4)**, 611–632, (2021).

[5] C. Carlet, S. Mesnager, C. Tang, Y. Qi, *New characterization and parametrization of LCD codes*, IEEE Transactions on Information Theory, **65(1)**, 39–49, (2018).

[6] K. Chatouh, *Linear skew cyclic codes over the ring R*, Palestine Journal of Mathematics, **13(4)**, 1213–1226, (2024).

[7] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, (2007).

[8] C. Li, P. Zeng, *Constructions of linear codes with one-dimensional hull*, IEEE Transactions on Information Theory, **65(3)**, 1668–1676, (2018).

[9] J. L. Massey, *Linear codes with complementary duals*, Discrete Mathematics, **106**, 337–342, (1992).

[10] I. Siap, T. Abualrub, N. Aydin, P. Seneviratne, *Skew cyclic codes of arbitrary length*, International Journal of Information and Coding Theory, **2(1)**, 10–20, (2011).

[11] A. Singh, R. Kumar, O. Prakash, *On DNA codes over additive skew cyclic codes*, Palestine Journal of Mathematics, **13(4)**, 1459–1471, (2024).

[12] J. Wang, R. Li, J. Lv, G. Guo, Y. Liu, *Entanglement-assisted quantum error correction codes with length* $n = q^2 + 1$, Quantum Information Processing, **18(9)**, (2019).

Author information

Nasreddine Benbelkacem, Departement and Laboratory of Algebra and Number Theory, Faculty of Mathematics, University of Science and Technology Houari Boumediene., Algiers, Algeria.
E-mail: nasreddine.benbelkacem@usthb.edu.dz

Received: 2025-12-07
Accepted: 2026-05-19