Journal of Algebra and Related Topics
Vol. , No. -, 2027, pp. -. Research Article

Rank-metric ideal codes in twisted group algebras with involution

Philipus Nangolo[†*]

[†]*Department of Mathematics and Economics, International University of Management, Nkurenkuru Campus, Windhoek, Namibia*
Email: p.nangolo@ium.edu.na

Abstract. Let $K = \mathbb{F}_{q^m}$, let G be a finite group of order n, and let $A = K^\alpha[G]$ be a twisted group algebra. We introduce a rank metric on A through the coefficient support over $\mathbb{F}_q$ and show that, for base-field cocycles, it is recovered from the entries of either regular representation. For a σ-unitary cocycle we construct a canonical semilinear involution and a nondegenerate coefficient pairing. The orthogonal of an idempotent ideal Ae is proved to be $A(1-e^*)$, yielding criteria for self-orthogonal, self-dual and complementary-dual ideals. The coordinate isometry transfers the rank-metric MacWilliams moment identities to these ideals. Finally, twisted cyclic algebras yield two conditional MRD constructions with parameters $[n, 1, n]$ and $[n, n-1, 2]$.

Keywords: Twisted group algebra, Rank-metric code, Involution, Ideal code, MRD code.
AMS Subject Classification 2010: 16S35, 20C05, 94B05, 11T71.

1 Introduction

Let $K = \mathbb{F}_{q^m}$ be a finite extension of $F = \mathbb{F}_q$ and let G be a finite group of order n. A normalized 2-cocycle $\alpha : G \times G \longrightarrow K^\times$ determines the twisted group algebra

$$A = K^\alpha[G] = \bigoplus_{g \in G} K u_g, \qquad u_g u_h = \alpha(g,h) u_{gh}.$$

The ordinary group algebra is recovered when $\alpha = 1$. Twisted group algebras arise naturally from projective representations and crossed-product constructions; see Karpilovsky [11]. From the coding-theoretic point of view, their left ideals provide structured linear codes. In particular, twisted group codes include constacyclic phenomena that need not be visible in ordinary group algebras. The recent unified treatment of twisted skew group codes in [2] establishes Frobenius

*Corresponding author
Received: 16 August 2026/ Revised: 11 October 2026/ Accepted: 11 October 2026
DOI: 10.22124/JART.2026.34649.1997

© 2027 University of Guilan

and semisimplicity properties, gives duality statements for the Hamming metric, and shows that a broad range of familiar codes can be represented as ideals. Twisted group codes and their complementary-dual variants have also been studied in [1, 6], while ordinary group codes are known to contain asymptotically good families [3].

Rank-metric coding theory has developed along a different line. Delsarte introduced matrix codes using the rank distance [7], while Gabidulin studied extension-field-linear codes in K^n [8]. The two models are connected by expanding each coordinate in an F-basis of K. Rank-metric duality and MacWilliams identities were clarified in [9, 15]; self-dual MRD codes were studied in [13, 14]. These results explain why rank distance is useful in random network coding, storage and multishot models [16]. General coding and duality background is available in [10]. Nevertheless, the multiplicative ideal structure of a twisted group algebra is not automatically compatible with the usual rank metric. Three points must be resolved before ideal methods can be used reliably.

First, the expression

$$\left(\sum_{g\in G} a_g u_g\right)^* = \sum_{g\in G} \sigma(a_g) u_{g^{-1}}$$

is generally not an anti-automorphism: cocycle correction factors are unavoidable. Second, the coefficient rank of an algebra element need not be read directly from an arbitrary regular-representation matrix unless the cocycle has an appropriate base-field form. Third, orthogonality must be formulated so that the dual of a left ideal is again a left ideal. Simply transplanting the ordinary group-algebra formula can give the wrong side or the wrong cocycle.

The purpose of this paper is to provide a coherent framework addressing these three issues. Its contributions are as follows.

1. For an F-valued cocycle we define the coefficient rank $\mathrm{wt}_R(x)$ and show that it equals the F-dimension of the span of all entries of either regular matrix of x. This gives a precise compatibility between the rank metric and multiplication in A.

2. If $\sigma \in \mathrm{Aut}(K)$ has order at most two and $\sigma(\alpha(g,h)) = \alpha(g,h)^{-1}$, we construct the corrected involution
$$u_g^* = u_g^{-1} = \alpha(g, g^{-1})^{-1} u_{g^{-1}}.$$
The coefficient functional then produces the standard σ-Hermitian pairing on coordinates.

3. We prove that the orthogonal of Ae, for an idempotent e, is $A(1-e^*)$. Exact algebraic criteria for self-orthogonality, self-duality and the LCD property follow. A star-orbit criterion is obtained in the commutative semisimple case.

4. We transfer the q-binomial MacWilliams moment identities to ideal codes and prove that the dual of an MRD ideal is MRD.

5. For $G = C_n$ we identify A with $K[x]/(x^n - \gamma)$ and construct two MRD ideals whenever $x^n - \gamma$ has a root $\zeta \in K$ of degree n over F. The two ideals have complementary dimensions 1 and $n-1$.

The final construction is conditional in exactly the same sense as many binomial constructions over finite fields: the field and the twisting scalar must admit an element ζ with $[F(\zeta) : F] = n$ and $\zeta^n \in F^\times$. The condition is transparent and efficiently testable; for example, it holds for quadratic extensions in odd characteristic when the twisting scalar is a nonsquare. We do not claim that all MRD codes are ideal codes, nor that the resulting ideals provide a cryptosystem by themselves. The cryptographic discussion is limited to structural consequences and possible distinguishers.

The paper is organized as follows. Section 2 fixes notation and recalls twisted algebras and rank support. Sections 3 and 4 develop the involution, pairing and regular-representation metric. Section 5 determines dual ideals. Section 6 gives the MacWilliams identities. Section 7 treats the cyclic construction, Section 8 studies star orbits and self-duality, and Sections 9 and 10 discuss computation and cryptographic consequences. Examples and open problems are given before the conclusion.

2 Twisted algebras and rank support

Throughout, $F = \mathbb{F}_q$, $K = \mathbb{F}_{q^m}$, and G is a finite group of order n with identity 1. We fix an ordering $G = \{g_1 = 1, g_2, \ldots, g_n\}$. A map $\alpha : G \times G \to K^\times$ is a normalized 2-cocycle if

$$\alpha(g,h)\alpha(gh,t) = \alpha(h,t)\alpha(g,ht), \qquad \alpha(1,g) = \alpha(g,1) = 1 \tag{1}$$

for all $g, h, t \in G$. Equation (1) is precisely the associativity condition for the multiplication $u_g u_h = \alpha(g,h)u_{gh}$. Every u_g is a unit. Substitution of (g, g^{-1}, g) into (1) gives

$$\alpha(g,g^{-1}) = \alpha(g^{-1},g), \qquad u_g^{-1} = \alpha(g,g^{-1})^{-1}u_{g^{-1}}. \tag{2}$$

Two cocycles α and α' are cohomologous if there is a normalized map $b : G \to K^\times$ such that

$$\alpha'(g,h) = b(g)b(h)b(gh)^{-1}\alpha(g,h).$$

The change of basis $u_g \mapsto b(g)^{-1}u'_g$ yields an isomorphism of the corresponding twisted algebras. Rank support, however, is sensitive to whether the change factors belong to F; this is one reason to isolate base-field cocycles.

Definition 1. *A normalized cocycle is called* base-field valued *if* $\alpha(G \times G) \subseteq F^\times$. *It is called* σ-unitary, *for* $\sigma \in \mathrm{Aut}(K)$, *if*

$$\sigma(\alpha(g,h)) = \alpha(g,h)^{-1} \quad \textit{for all } g,h \in G. \tag{3}$$

The two requirements serve different purposes. Base-field values ensure rank-support compatibility. The unitary identity ensures the existence of a canonical semilinear involution. If $\sigma = \mathrm{id}_K$, unitary means that every cocycle value has square one. If m is even and $\sigma(a) = a^{q^{m/2}}$, condition (3) says that the cocycle values lie in the norm-one subgroup for K/K^σ.

Let $\Phi : A \to K^n$ be the coefficient map

$$\Phi\left(\sum_{i=1}^{n} a_i u_{g_i}\right) = (a_1, \ldots, a_n). \tag{4}$$

Choose an F-basis $\mathcal{B} = (\beta_1, \dots, \beta_m)$ of K. Expanding the entries of $v \in K^n$ in $\mathcal{B}$ gives a matrix $M_{\mathcal{B}}(v) \in F^{m\times n}$. Its rank does not depend on $\mathcal{B}$.

Definition 2. *For $x = \sum_g a_g u_g \in A$, define*

$$\operatorname{supp}_F(x) = \langle a_g : g \in G\rangle_F, \qquad \operatorname{wt}_R(x) = \dim_F \operatorname{supp}_F(x). \tag{5}$$

The rank distance on A is $d_R(x, y) = \operatorname{wt}_R(x - y)$.

Thus $\operatorname{wt}_R(x) = \operatorname{rank}_F M_{\mathcal{B}}(\Phi(x))$. In particular, $0 \le \operatorname{wt}_R(x) \le \min\{m, n\}$. The usual rank inequalities imply

$$\operatorname{wt}_R(x + y) \le \operatorname{wt}_R(x) + \operatorname{wt}_R(y), \qquad \operatorname{wt}_R(ax) = \operatorname{wt}_R(x) \quad (a \in K^\times).$$

Hence d_R is a metric and every left ideal is a K-linear rank-metric code under Φ.

Definition 3. *A nonzero left ideal $C \le A$ has parameters $[n, k, d]_{q^m/q}$ if $k = \dim_K C$ and*

$$d = d_R(C) = \min\{\operatorname{wt}_R(c) : 0 \ne c \in C\}.$$

When $n \le m$, the Singleton bound is $d \le n-k+1$. The ideal is maximum rank distance *(MRD) if equality holds.*

The notation records both the extension and base fields. It also prevents confusion with the Hamming parameters of the same coefficient code.

3 Unitary cocycles and the canonical involution

Let $\sigma \in \operatorname{Aut}(K)$ satisfy $\sigma^2 = \mathrm{id}_K$. Extend σ coefficientwise to the underlying additive group of A. The naive rule $u_g \mapsto u_{g^{-1}}$ need not reverse multiplication. The correction in (2) is canonical.

Theorem 1. *Assume that α is σ-unitary. The map*

$$* : A \longrightarrow A, \qquad \left(\sum_{g\in G} a_g u_g\right)^* = \sum_{g\in G} \sigma(a_g)\alpha(g, g^{-1})^{-1} u_{g^{-1}} \tag{6}$$

is a σ-semilinear involutive anti-automorphism. Equivalently, $u_g^* = u_g^{-1}$.

Proof. For homogeneous units, $u_g^* = u_g^{-1}$ by (2). Since α is unitary,

$$(u_g u_h)^* = \sigma(\alpha(g, h))(u_{gh})^{-1} = \alpha(g, h)^{-1}(u_{gh})^{-1} = (u_g u_h)^{-1} = u_h^{-1} u_g^{-1}.$$

Semilinearity and distributivity give $(xy)^* = y^* x^*$ for arbitrary $x, y \in A$. Moreover,

$$(au_g)^{**} = \sigma^2(a)(u_g^{-1})^* = au_g,$$

because an anti-automorphism takes the inverse of a unit to the inverse of its image. Thus $*^2 = \mathrm{id}_A$. □

The unitary condition is close to necessary for this particular canonical rule.

Proposition 1. *Suppose a σ-semilinear anti-automorphism of A satisfies $u_g^* = u_g^{-1}$ for every g. Then α is σ-unitary.*

Proof. Applying $*$ to $u_g u_h = \alpha(g,h)u_{gh}$ gives

$$u_h^{-1}u_g^{-1} = \sigma(\alpha(g,h))u_{gh}^{-1}.$$

The left side equals $(u_g u_h)^{-1} = \alpha(g,h)^{-1}u_{gh}^{-1}$. Cancellation gives (3). □

Let $\tau : A \to K$ denote the coefficient of u_1:

$$\tau\left(\sum_g a_g u_g\right) = a_1.$$

The cocycle identity (2) implies a trace-like symmetry.

Lemma 1. *For all $x, y \in A$, one has $\tau(xy) = \tau(yx)$.*

Proof. Writing $x = \sum_g a_g u_g$ and $y = \sum_h b_h u_h$, only terms with $h = g^{-1}$ contribute to $\tau(xy)$. Therefore

$$\tau(xy) = \sum_{g\in G} a_g b_{g^{-1}}\alpha(g,g^{-1}).$$

After replacing g by g^{-1} and using $\alpha(g,g^{-1}) = \alpha(g^{-1},g)$, this is $\tau(yx)$. □

Definition 4. *Under the hypotheses of Theorem 1, define*

$$\langle x,y\rangle_* = \tau(xy^*). \tag{7}$$

Theorem 2. *The form (7) is a nondegenerate σ-Hermitian form. In coefficient coordinates,*

$$\left\langle \sum_g a_g u_g, \sum_g b_g u_g \right\rangle_* = \sum_{g\in G} a_g \sigma(b_g). \tag{8}$$

Furthermore,

$$\langle ax, y\rangle_* = \langle x, a^* y\rangle_* \quad (a,x,y \in A). \tag{9}$$

Proof. Since $u_g^* = u_g^{-1}$, the coefficient of u_1 in $u_g u_h^*$ is 1 if $g = h$ and 0 otherwise. This proves (8), from which nondegeneracy and the Hermitian identity follow. Finally,

$$\langle ax,y\rangle_* = \tau(axy^*) = \tau(xy^*a) = \tau\big(x(a^*y)^*\big) = \langle x, a^*y\rangle_*,$$

where Lemma 1 is used in the second equality. □

When $\sigma = \mathrm{id}_K$, the form is the Euclidean coefficient form. When K/K^σ is quadratic, it is Hermitian. Thus the correction factors in (6) disappear from the final coordinate pairing but remain essential in the algebraic proof.

4 Regular representations and the coefficient rank

Let $\rho_L, \rho_R : A \to \mathrm{End}_K(A) \cong M_n(K)$ denote left and right multiplication,

$$\rho_L(x)(z) = xz, \qquad \rho_R(x)(z) = zx,$$

expressed in the ordered basis $(u_{g_1}, \ldots, u_{g_n})$. Thus ρ_L is a representation and ρ_R is an anti-representation. For a matrix M over K, put

$$\mathrm{crk}_F(M) = \dim_F \langle M_{ij} : 1 \le i, j \le n \rangle_F.$$

This is not the ordinary matrix rank over K; it is the dimension of the F-span of all matrix entries. The distinction is important. The ordinary rank of $\rho_L(x)$ measures the dimension of the principal right annihilator quotient, whereas crk_F measures the rank support of the coefficient vector.

Theorem 3. *If α is base-field valued, then*

$$\mathrm{wt}_R(x) = \mathrm{crk}_F(\rho_L(x)) = \mathrm{crk}_F(\rho_R(x)) \qquad (x \in A). \tag{10}$$

Consequently, $d_R(x, y)$ is determined by the regular representation.

Proof. Write $x = \sum_g a_g u_g$. For a fixed $h \in G$,

$$xu_h = \sum_{g \in G} a_g \alpha(g, h) u_{gh}.$$

Every entry in the h-column of $\rho_L(x)$ is therefore either zero or $a_g \alpha(g, h)$ for a unique g. Since $\alpha(g, h) \in F^\times$, every matrix entry belongs to $\langle a_g : g \in G \rangle_F$. Thus $\mathrm{crk}_F(\rho_L(x)) \le \mathrm{wt}_R(x)$. The column corresponding to $h = 1$ is the coefficient vector of x, because $\alpha(g, 1) = 1$. Hence its entries contain every a_g, giving the reverse inequality. Similarly,

$$u_h x = \sum_{g \in G} a_g \alpha(h, g) u_{hg}.$$

The same argument applies to $\rho_R(x)$, and its column indexed by $h = 1$ again contains all coefficients of x. □

Remark 1. *The base-field hypothesis cannot simply be omitted. If cocycle values lie in $K \setminus F$, multiplication by different values may enlarge the F-span of the entries of a regular matrix even when the coefficient support of x is one-dimensional. The first column still gives* $\mathrm{wt}_R(x) \le \mathrm{crk}_F(\rho_L(x))$*, but equality may fail.*

The rank metric is stable under a restricted, but natural, cohomology action.

Proposition 2. *Let α' be cohomologous to α through a normalized cochain $b : G \to F^\times$. The algebra isomorphism*

$$T_b : K^\alpha[G] \longrightarrow K^{\alpha'}[G], \qquad u_g \longmapsto b(g)^{-1} u'_g$$

is an F-rank isometry. It maps left ideal codes to equivalent left ideal codes with the same rank distribution.

Proof. The cocycle relation for α' proves multiplicativity. In coefficient coordinates T_b multiplies the gth coordinate by $b(g)^{-1} \in F^\times$. Such coordinate scalings preserve the F-span of all coordinates and hence the rank weight. □

4.1 Simultaneous metric and involution equivalence

Cohomologous cocycles define isomorphic algebras, but an arbitrary cochain need not preserve both the rank metric and the canonical involution. This point matters when code equivalence is used to simplify a cocycle table. Let

$$\alpha'(g,h) = b(g)b(h)b(gh)^{-1}\alpha(g,h), \qquad b(1) = 1.$$

The isomorphism in Proposition 2 is a rank isometry when $b(g) \in F^\times$. For general K-valued b, coordinate scaling can change rank because multiplication by different extension-field elements can alter the common F-span.

Unitary compatibility has a separate norm condition. Put

$$t_b(g) = \sigma(b(g))b(g). \tag{11}$$

Proposition 3. *Assume that α is σ-unitary. Then α' is σ-unitary if and only if $t_b : G \to K^\times$ is a group character. Furthermore, the algebra isomorphism $T_b(u_g) = b(g)^{-1}u'_g$ intertwines the two canonical involutions if*

$$\sigma(b(g))b(g) = 1 \qquad (g \in G). \tag{12}$$

When $b(G) \subseteq F^\times$, it is simultaneously a rank isometry and a star-isomorphism whenever $b(g)^2 = 1$ for every g.

Proof. Write $\delta b(g,h) = b(g)b(h)b(gh)^{-1}$. Since α is unitary, α' is unitary precisely when

$$\sigma(\delta b(g,h))\delta b(g,h) = 1.$$

The left side equals $t_b(g)t_b(h)t_b(gh)^{-1}$, which is one exactly when t_b is a character. For the involutions, compare $T_b(u_g^*)$ with $T_b(u_g)^*$. Using $\alpha'(g,g^{-1}) = b(g)b(g^{-1})\alpha(g,g^{-1})$ shows that the two expressions agree under (12). The final assertion follows because every automorphism of K fixes F pointwise. □

Thus there are three nested equivalence notions: algebra isomorphism through an arbitrary cochain, rank equivalence through a base-field cochain, and involutive rank equivalence through a base-field norm-one cochain. Results about duals must use the third notion, while results concerning rank distribution alone need only the second. Treating all cohomologous cocycles as metrically identical would erase this distinction.

4.2 Rank-support spaces and generalized weights

The integer in (5) is the dimension of a more informative subspace. For $v \in K^n$, let

$$\mathrm{RS}(v) = \mathrm{rowsp}_F M_{\mathcal{B}}(v) \leq F^n.$$

Changing $\mathcal{B}$ left-multiplies the expansion matrix by an element of $\mathrm{GL}_m(F)$, so this row space is intrinsic. Put $\mathrm{RS}(x) = \mathrm{RS}(\Phi(x))$. Then $\dim_F \mathrm{RS}(x) = \mathrm{wt}_R(x)$. Notice that $\mathrm{RS}(x)$ and $\mathrm{supp}_F(x)$ have the same dimension but different ambient spaces.

For $U \leq F^n$, define

$$U_K = U \otimes_F K = \{v \in K^n : \mathrm{RS}(v) \subseteq U\}.$$

If $C \leq A$ has K-dimension k, define

$$d_r(C) = \min\{\dim_F U : \dim_K(\Phi(C) \cap U_K) \geq r\}, \qquad 1 \leq r \leq k. \tag{13}$$

The first generalized rank weight is $d_R(C)$.

Proposition 4. *For every K-linear $C \leq A$ of dimension k,*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n \tag{14}$$

and

$$d_r(C) \leq n - k + r \qquad (1 \leq r \leq k). \tag{15}$$

Proof. If U realizes $d_{r+1}(C)$, choose an $(r+1)$-dimensional subcode $D \leq \Phi(C) \cap U_K$ and an F-hyperplane $H < U$. Since H_K has codimension one in U_K, the dimension formula gives $\dim_K(D \cap H_K) \geq r$. Hence $d_r(C) \leq \dim_F H = d_{r+1}(C) - 1$, proving strictness.

For the upper bound, apply an F-linear coordinate change and project C onto $k-r$ selected coordinates. The kernel has K-dimension at least r and rank support in the complementary coordinate space of dimension $n - k + r$. This proves (15). □

Let P_g be the monomial coefficient matrix of left multiplication by u_g. If α is base-field valued, then $P_g \in \mathrm{GL}_n(F)$ and

$$\mathrm{RS}(u_g x) = \mathrm{RS}(x) P_g^{\mathsf{T}}, \qquad \mathrm{wt}_R(u_g x) = \mathrm{wt}_R(x). \tag{16}$$

Thus minimum-support spaces of a left ideal occur in orbits under a projective regular action, a restriction absent from a generic rank code.

Proposition 5. *Let C be a left ideal and let α be base-field valued. For every r, the family of spaces $U \leq F^n$ that attain (13) is invariant under $U \mapsto U P_g^{\mathsf{T}}$ for $g \in G$.*

Proof. Left multiplication by the unit u_g maps C bijectively to itself. Equation (16) maps any r-dimensional subcode supported in U to one of the same dimension supported in $U P_g^{\mathsf{T}}$. □

For $x, y \in A$ and base-field-valued α,

$$\mathrm{supp}_F(xy) \subseteq \mathrm{supp}_F(x)\,\mathrm{supp}_F(y), \tag{17}$$

where UV denotes the F-span of products uv with $u \in U$ and $v \in V$. Therefore

$$\mathrm{wt}_R(xy) \leq \min\{m, \mathrm{wt}_R(x)\,\mathrm{wt}_R(y)\}. \tag{18}$$

This elementary inequality is useful for estimating how multiplication by low-support elements changes errors, although it is not usually sharp.

5 Dual ideals and idempotent generators

We first clarify when idempotent generators cover all ideals. A twisted version of Maschke's theorem applies away from the modular case.

Proposition 6. *If* $\operatorname{char} K \nmid |G|$*, then* $K^{\alpha}[G]$ *is semisimple and every left ideal is generated by an idempotent. In arbitrary characteristic, every idempotent ideal* Ae *is projective, but a general left ideal need not be idempotent-generated.*

Proof. Let V be an A-module, $W \leq V$ an A-submodule, and $\pi : V \to W$ a K-linear projection. The standard projective-representation averaging operator

$$\overline{\pi} = \frac{1}{|G|} \sum_{g \in G} u_g^{-1} \pi u_g$$

is A-linear: cocycle scalars cancel under reindexing. It restricts to the identity on W, so every submodule splits and A is semisimple. A projection of the regular module onto a left ideal is right multiplication by an idempotent, giving $C = Ae$. Conversely, $A = Ae \oplus A(1-e)$ for every idempotent e, so Ae is projective. In modular algebras nonsplit ideals may occur. □

For a K-subspace $C \leq A$, define

$$C^{\perp} = \{y \in A : \langle c, y \rangle_* = 0 \text{ for every } c \in C\}.$$

By Theorem 2, $\dim_K C + \dim_K C^{\perp} = n$ and $(C^{\perp})^{\perp} = C$.

Proposition 7. *If* C *is a left ideal of* A*, then* $C^{\perp}$ *is a left ideal of* A*.*

Proof. Let $y \in C^{\perp}$, $a \in A$ and $c \in C$. By (9),

$$\langle c, ay \rangle_* = \langle a^* c, y \rangle_* = 0,$$

because $a^* c \in C$. Hence $ay \in C^{\perp}$. □

For $X \subseteq A$, write

$$\operatorname{Ann}_r(X) = \{z \in A : xz = 0 \text{ for every } x \in X\}.$$

Theorem 4. *For every left ideal* $C \leq A$*,*

$$C^{\perp} = \big(\operatorname{Ann}_r(C)\big)^*. \tag{19}$$

Proof. If $z \in \operatorname{Ann}_r(C)$ and $y = z^*$, then $\langle c, y \rangle_* = \tau(cz) = 0$ for all $c \in C$. Conversely, if $y \in C^{\perp}$, then for $a \in A$ and $c \in C$,

$$0 = \langle ac, y \rangle_* = \tau(acy^*).$$

Nondegeneracy of $(a, z) \mapsto \tau(az)$ implies $cy^* = 0$. Hence $y^* \in \operatorname{Ann}_r(C)$, proving the reverse inclusion. □

The central structural formula is particularly simple for idempotent ideals.

Theorem 5. *Let $e^2 = e \in A$. Then*

$$(Ae)^{\perp} = A(1 - e^*). \tag{20}$$

Moreover,

$$\dim_K Ae + \dim_K A(1 - e^*) = n. \tag{21}$$

Proof. Theorem 4 gives $(Ae)^{\perp} = (\mathrm{Ann}_r(Ae))^*$. Now $z \in \mathrm{Ann}_r(Ae)$ if and only if $ez = 0$, equivalently $z = (1 - e)z$. Therefore $\mathrm{Ann}_r(Ae) = (1 - e)A$, whose star is $A(1 - e^*)$.

For the dimension statement, right multiplication by e is an idempotent K-linear operator R_e with image Ae. The adjoint of R_e with respect to (7) is R_{e^*}, because

$$\langle xe, y\rangle_* = \tau(xey^*) = \tau\big(x(ye^*)^*\big) = \langle x, ye^*\rangle_*.$$

Hence R_e and R_{e^*} have the same rank. Since $R_{1-e^*} = I - R_{e^*}$ is the complementary idempotent,

$$\dim_K A(1 - e^*) = n - \operatorname{rank} R_{e^*} = n - \dim_K Ae.$$

The inclusion is therefore an equality. □

Corollary 1. *For an idempotent $e \in A$ the following hold.*

1. *Ae is self-orthogonal if and only if $ee^* = 0$.*
2. *Ae is self-dual if and only if $Ae = A(1 - e^*)$; in particular, $e^* = 1 - e$ is sufficient.*
3. *Ae is LCD if and only if $Ae \cap A(1 - e^*) = 0$.*
4. *If $e = e^*$, then Ae is LCD and $A = Ae \perp A(1 - e)$.*

Proof. For (1), if $ee^* = 0$, then $\langle ae, be\rangle_* = \tau(aee^*b^*) = 0$. Conversely, if Ae is self-orthogonal, then for all $a, b \in A$, $\tau(aee^*b) = 0$. Set $b = 1$ and use nondegeneracy of $(a, z) \mapsto \tau(az)$ to obtain $ee^* = 0$. Parts (2) and (3) follow from Theorem 5. If $e = e^*$, then $e(1 - e) = 0$ and the two images of the complementary right-multiplication idempotents form a direct sum, proving (4). □

The equality $e^* = 1 - e$ forces $2e = 1$ after applying $*$ only when $e = e^*$; in general e and e^* are distinct. It also implies $ee^* = 0$ and $\dim_K Ae = n/2$, so n must be even. In characteristic two, self-dual group codes may occur in modular algebras; for ordinary group algebras the existence question is described in [17]. Our formula separates the involutive algebra condition from the particular metric distribution.

For ordinary group algebras, complementary-dual ideals and self-adjoint idempotents are treated in [5]; the formula above identifies the cocycle correction required in the twisted setting. Orthogonality for modules over finite Frobenius rings is developed more generally in [18].

6 MacWilliams moments for rank-metric ideals

Assume throughout this section that $n \le m$. Let $C \le A$ be a K-linear code of dimension k and define

$$A_i(C) = |\{c \in C : \mathrm{wt}_R(c) = i\}|, \qquad 0 \le i \le n.$$

The rank-weight enumerator is $W_C(z) = \sum_{i=0}^{n} A_i(C) z^i$. Write $B_i = A_i(C^\perp)$. The Gaussian binomial coefficient is

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \prod_{j=0}^{b-1} \frac{q^{a-j}-1}{q^{b-j}-1},$$

with value zero when $b < 0$ or $b > a$.

Because (8) is the standard σ-Hermitian coefficient pairing, $C^\perp$ is, up to the rank isometry obtained by applying σ coordinatewise, the usual Euclidean dual of $\Phi(C)$. The MacWilliams moment identities for Gabidulin codes therefore transfer without alteration; compare [9, 15].

Theorem 6. *Let $C \le A$ be a K-linear code of dimension k. For every $0 \le j \le n$,*

$$\sum_{i=0}^{n-j} \begin{bmatrix} n-i \\ j \end{bmatrix}_q A_i = q^{m(k-j)} \sum_{i=0}^{j} \begin{bmatrix} n-i \\ n-j \end{bmatrix}_q B_i. \tag{22}$$

Consequently, the rank distribution of C uniquely determines that of $C^\perp$.

Proof. The coefficient map (4) is a K-linear rank isometry. By (8), $\Phi(C^\perp)$ is the σ-Hermitian dual of $\Phi(C)$. Applying σ^{-1} coordinatewise preserves rank and reduces the count to the Euclidean pairing, so we work in K^n.

For $U \le F^n$, set

$$\mathcal{M}_U = \{v \in K^n : \mathrm{RS}(v) \subseteq U\} = U_K.$$

If $s = \dim_F U$, then $|\mathcal{M}_U| = q^{ms}$ and $\mathcal{M}_U^\perp = \mathcal{M}_{U^\perp}$. Elementary orthogonal-space identities give

$$|C \cap \mathcal{M}_U| = \frac{|C|}{q^{m(n-s)}} |C^\perp \cap \mathcal{M}_{U^\perp}|. \tag{23}$$

Indeed, $(C \cap \mathcal{M}_U)^\perp = C^\perp + \mathcal{M}_{U^\perp}$; comparing cardinalities of the intersection and sum proves (23).

Fix j and sum (23) over all $(n-j)$-dimensional spaces $U \le F^n$. A word of rank i occurs on the left once for every such U containing its i-dimensional rank support. The number of choices is

$$\begin{bmatrix} n-i \\ n-j-i \end{bmatrix}_q = \begin{bmatrix} n-i \\ j \end{bmatrix}_q.$$

On the right, $U \mapsto U^\perp$ runs over all j-dimensional subspaces. A dual word of rank i is contained in $\begin{bmatrix} n-i \\ j-i \end{bmatrix}_q = \begin{bmatrix} n-i \\ n-j \end{bmatrix}_q$ of them. Since $|C|/q^{mj} = q^{m(k-j)}$, the two counts give (22).

Finally, the coefficient of B_j in the jth identity is $\begin{bmatrix} n-j \\ n-j \end{bmatrix}_q = 1$, while no B_i with $i > j$ occurs. The resulting system is triangular and uniquely determines the dual distribution. □

For $j = 0$, (22) reads $\sum_i A_i = q^{mk} = |C|$. For $j = n$, it gives $1 = q^{m(k-n)}|C^\perp|$. Intermediate values contain the genuine metric information.

6.1 Recursive transform and consistency tests

The triangular proof gives a practical MacWilliams transform. Put $B_0 = 1$. For $1 \le j \le n$, recursively define

$$B_j = q^{-m(k-j)} \sum_{i=0}^{n-j} \begin{bmatrix} n-i \\ j \end{bmatrix}_q A_i - \sum_{t=0}^{j-1} \begin{bmatrix} n-t \\ n-j \end{bmatrix}_q B_t. \tag{24}$$

Although a negative power of q appears formally when $j < k$, the first sum has the required divisibility because it counts shortened subcodes through (23). Formula (24) is useful computationally: a proposed rank distribution can be rejected if it produces a negative or nonintegral B_j.

The identity at $j = 1$ is

$$\sum_{i=0}^{n-1} \begin{bmatrix} n-i \\ 1 \end{bmatrix}_q A_i = q^{m(k-1)} \left(\begin{bmatrix} n \\ 1 \end{bmatrix}_q + B_1 \right). \tag{25}$$

Thus a dual distance of at least two is equivalent to the vanishing of the correction B_1 in (25). At $j = 2$, the additional term is $\begin{bmatrix} n-1 \\ n-2 \end{bmatrix}_q B_1 + B_2$, so dual distance at least three forces both corrections to vanish. In general, $d_R(C^\perp) > j$ if and only if the first j recursive corrections vanish.

For an ideal $C = Ae$, all these checks can be performed without constructing an orthogonal nullspace: the comparison distribution is obtained by enumerating $A(1-e^*)$. Agreement between direct enumeration and (24) simultaneously tests the involution, cocycle factors, rank expansion and idempotent arithmetic.

Proposition 8. *Suppose C has dimension k and $A_i = 0$ for $1 \le i \le n-k$. Then its complete rank distribution is uniquely determined by q, m, n and k.*

Proof. Under the coefficient isometry, C is an extension-field-linear MRD code. The Delsarte–Gabidulin rank-enumerator theorem determines its distribution from q, m, n, k; equivalently, one solves the triangular MacWilliams system after applying the dual-MRD theorem. See [15, Section 3]. □

Corollary 2. *If C is an $[n, k, n-k+1]_{q^m/q}$ MRD ideal, then $C^\perp$ is an $[n, n-k, k+1]_{q^m/q}$ MRD ideal.*

Proof. The coefficient isometry identifies C with a K-linear MRD code and $C^\perp$, up to a semilinear rank isometry, with its ordinary rank-metric dual. The dual-MRD theorem [15, Theorem 37] gives minimum distance $k+1$. The ideal property follows from Proposition 7. □

For an idempotent ideal $C = Ae$, Theorem 5 converts this metric statement into an algebraic one: if Ae is MRD, so is $A(1-e^*)$. This gives a direct way to generate a dual pair without solving new parity-check equations.

7 Twisted cyclic algebras and MRD ideal families

Let $G = C_n = \langle g \rangle$. A standard cocycle representative is obtained by choosing $\gamma \in K^\times$ and setting

$$u_{g^i} u_{g^j} = \begin{cases} u_{g^{i+j}}, & i+j < n, \\ \gamma u_{g^{i+j-n}}, & i+j \geq n. \end{cases}$$

Writing $u = u_g$, one has $u^n = \gamma$ and

$$K^\alpha[C_n] \cong K[x]/(x^n - \gamma), \qquad u \longleftrightarrow x. \tag{26}$$

When $\gamma \in F^\times$, the cocycle is base-field valued. The ideals are the γ-constacyclic codes under coefficient coordinates, a connection also encompassed by [2].

We now impose the key arithmetic hypothesis.

Assumption 1. *There is an element $\zeta \in K$ such that*

$$[F(\zeta) : F] = n, \qquad \zeta^n = \gamma \in F^\times, \qquad n \leq m. \tag{27}$$

The evaluation map

$$\mathrm{ev}_\zeta : K[x]/(x^n - \gamma) \longrightarrow K, \qquad f(x) \longmapsto f(\zeta)$$

is a surjective K-algebra homomorphism. Its kernel is the ideal generated by $x - \zeta$ and has dimension $n - 1$ over K.

Theorem 7. *Under Assumption 1,*

$$C_\zeta = (x - \zeta) \subseteq K[x]/(x^n - \gamma) \tag{28}$$

is an $[n, n-1, 2]_{q^m/q}$ MRD ideal.

Proof. The dimension is $n - 1$. It suffices to exclude nonzero rank-one codewords. Suppose $0 \neq f(x) = \sum_{i=0}^{n-1} a_i x^i \in C_\zeta$ has rank one. Then there are $\lambda \in K^\times$ and $c_i \in F$, not all zero, such that $a_i = \lambda c_i$. Since $f(\zeta) = 0$,

$$c_0 + c_1\zeta + \cdots + c_{n-1}\zeta^{n-1} = 0.$$

This contradicts $[F(\zeta) : F] = n$. Thus $d_R(C_\zeta) \geq 2$. The Singleton bound gives $d_R(C_\zeta) \leq n - (n-1) + 1 = 2$. □

There is a complementary one-dimensional ideal. Define

$$h_\zeta(x) = \frac{x^n - \zeta^n}{x - \zeta} = x^{n-1} + \zeta x^{n-2} + \cdots + \zeta^{n-2}x + \zeta^{n-1}. \tag{29}$$

In the quotient, $(x - \zeta)h_\zeta = 0$ and $xh_\zeta = \zeta h_\zeta$. Hence Kh_ζ is an ideal.

Theorem 8. *Under Assumption 1,*

$$D_\zeta = Kh_\zeta(x) \tag{30}$$

is an $[n, 1, n]_{q^m/q}$ *MRD ideal. If* $\operatorname{char} F \nmid n$*, then*

$$e_\zeta = \frac{h_\zeta(x)}{n\zeta^{n-1}} \tag{31}$$

is an idempotent and $D_\zeta = Ae_\zeta$*.*

Proof. The coefficient set of h_ζ is $\{1, \zeta, \ldots, \zeta^{n-1}\}$, which is F-linearly independent. Therefore every nonzero scalar multiple has rank weight n. This proves the parameters and the MRD property.

For the idempotent statement, evaluation of (29) at ζ gives $h_\zeta(\zeta) = n\zeta^{n-1}$. The relations $xh_\zeta = \zeta h_\zeta$ and linearity imply $f(x)h_\zeta = f(\zeta)h_\zeta$ for all f. Consequently,

$$e_\zeta^2 = \frac{h_\zeta(\zeta)h_\zeta(x)}{n^2\zeta^{2n-2}} = e_\zeta.$$

□

If an admissible involution is also present, Corollary 2 shows that the orthogonal of either family is an MRD ideal of complementary dimension. The orthogonal need not equal the other displayed ideal unless the involution and the evaluation root are matched. The following gives the exact relationship in the Euclidean case when it is defined.

Proposition 9. *Assume* $\sigma = \mathrm{id}_K$*,* $\gamma^2 = 1$*, and* $\operatorname{char} F \nmid n$*. In the involution of Theorem 1,* $x^* = x^{-1} = \gamma^{-1}x^{n-1}$*. Moreover,*

$$e_\zeta^* = e_{\zeta^{-1}}, \qquad (Ae_\zeta)^\perp = A(1 - e_{\zeta^{-1}}),$$

where $e_{\zeta^{-1}}$ *is defined by* (31) *with* ζ *replaced by* ζ^{-1}*.*

Proof. The formula for x^* follows from $x^n = \gamma$. Formula (31) can be rewritten as

$$e_\zeta = \frac{1}{n}\sum_{i=0}^{n-1} \zeta^{-i}x^i.$$

For $1 \le i < n$, the relations $x^n = \zeta^n = \gamma$ give $x^{-i} = \gamma^{-1}x^{n-i}$ and $\zeta^{-i} = \gamma^{-1}\zeta^{n-i}$. Since $\gamma^2 = 1$, applying $*$ and reindexing yields

$$e_\zeta^* = \frac{1}{n}\sum_{j=0}^{n-1} \zeta^j x^j = e_{\zeta^{-1}}.$$

Notice that $(\zeta^{-1})^n = \gamma^{-1} = \gamma$, so the latter idempotent is defined in the same quotient. The orthogonal formula now follows from Theorem 5. □

7.1 Existence of admissible roots

Assumption 1 is equivalent to the existence of an irreducible binomial factor of degree n over F whose root lies in K and whose nth power is in F. Standard irreducibility criteria for binomials can be used; see Lidl and Niederreiter [12]. Two simple cases illustrate that the construction is nonempty.

Example 1. Let q be odd, choose a nonsquare $\gamma \in F_q^\times$, take $K \supseteq F_{q^2}$ and let $\zeta^2 = \gamma$. Then $[F_q(\zeta) : F_q] = 2$. The two ideals in $K[x]/(x^2 - \gamma)$ have parameters $[2, 1, 2]_{q^m/q}$; here both are one-dimensional MRD ideals. An idempotent generator is

$$e_\zeta = \frac{x + \zeta}{2\zeta}.$$

Example 2. Suppose $x^n - \gamma$ is irreducible over F_q and $n \mid m$. If ζ is any root in $F_{q^n} \subseteq K$, then Assumption 1 holds. Theorems 7 and 8 provide a dual-dimension pair of MRD ideal parameters even though A is defined over the larger coefficient field K.

The phrase "conditional family" is important: irreducibility of $x^n - \gamma$ is an arithmetic restriction, not an automatic consequence of $n \mid m$. It can be checked through the prime divisors of n and the multiplicative order of γ.

Let $s = \mathrm{ord}_{F_q^\times}(\gamma)$. The standard binomial criterion gives an explicit test.

Proposition 10. *The polynomial $x^n - \gamma \in F_q[x]$ is irreducible if and only if*

1. *every prime divisor of n divides s;*
2. *$\gcd(n, (q-1)/s) = 1$; and*
3. *if $4 \mid n$, then $q \equiv 1 \pmod 4$.*

Whenever these conditions hold and $n \mid m$, both MRD ideals of Theorems 7 and 8 exist in $K[x]/(x^n - \gamma)$.

Proof. The equivalence of the three arithmetic conditions with irreducibility is the finite-field binomial criterion in [12, Theorem 3.75]. An irreducible polynomial of degree n splits over F_{q^n}, which is a subfield of K when $n \mid m$. Any root ζ then has degree n and satisfies $\zeta^n = \gamma$. □

7.2 Explicit generator and check matrices

The two constructions have sparse matrices. In the basis $(1, x, \ldots, x^{n-1})$, the evaluation-kernel ideal has generator matrix

$$G_\zeta = \begin{bmatrix} -\zeta & 1 & 0 & \cdots & 0 \\ 0 & -\zeta & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & -\zeta & 1 \end{bmatrix} \in K^{(n-1)\times n}. \tag{32}$$

Indeed, its rows are the coefficient vectors of $x^j(x-\zeta)$ for $0 \le j \le n-2$. A check row is

$$H_\zeta = \begin{bmatrix} 1 & \zeta & \zeta^2 & \cdots & \zeta^{n-1} \end{bmatrix}, \qquad G_\zeta H_\zeta^{\mathsf{T}} = 0. \tag{33}$$

Thus membership in C_ζ requires one evaluation equation rather than a full matrix nullspace computation.

The line ideal D_ζ has generator row

$$L_\zeta = \begin{bmatrix} \zeta^{n-1} & \zeta^{n-2} & \cdots & \zeta & 1 \end{bmatrix}. \tag{34}$$

The coefficient set is an F-basis of $F(\zeta)$, so every nonzero word has rank n. Its complete rank distribution is therefore

$$A_0(D_\zeta) = 1, \qquad A_n(D_\zeta) = q^m - 1, \qquad A_i(D_\zeta) = 0 \quad (0 < i < n). \tag{35}$$

The MacWilliams moments in Section 6 then determine the distribution of the Hermitian dual of D_ζ without enumeration.

Encoding in C_ζ can be written systematically. Given $(b_0, \ldots, b_{n-2}) \in K^{n-1}$, multiplication by (32) produces

$$(-\zeta b_0,\ b_0 - \zeta b_1, \ldots, b_{n-3} - \zeta b_{n-2},\ b_{n-2}). \tag{36}$$

The formula needs $n-1$ multiplications by ζ and $n-2$ additions. Encoding in D_ζ needs scalar multiplication of (34). The algebraic structure therefore yields linear-time encoders for both extremal families.

For clarity, the main parameters are summarized below.

Table 1: Twisted cyclic MRD ideal families under Assumption 1.

Ideal	Generator	k	d_R	MRD equality
C_ζ	$x-\zeta$	$n-1$	2	$2 = n-(n-1)+1$
D_ζ	$h_\zeta(x)$	1	n	$n = n-1+1$

These matrices also show why the degree condition is indispensable. If $[F(\zeta) : F] = r < n$, then the row (34) has rank at most r, while a nonzero polynomial in $F[x]$ of degree below n vanishing at ζ produces a rank-one word in C_ζ. Both MRD conclusions then fail simultaneously.

8 Self-dual and LCD ideals through star orbits

This section assumes that A is commutative and semisimple over K. Thus

$$1 = e_1 + \cdots + e_s, \qquad e_i e_j = 0 \ (i \ne j), \tag{37}$$

where the e_i are primitive central idempotents. The involution permutes the set $\{e_1, \ldots, e_s\}$; write $\pi(i)$ for the index satisfying $e_i^* = e_{\pi(i)}$. Since $*^2 = 1$, every orbit of π has length one or two.

Every ideal has the form

$$C_I = Ae_I, \qquad e_I = \sum_{i \in I} e_i$$

for a unique subset $I \subseteq \{1, \dots, s\}$. The dual formula becomes

$$C_I^{\perp} = A(1 - e_I^*) = A \sum_{j \notin \pi(I)} e_j = C_{\{1,\dots,s\} \setminus \pi(I)}. \tag{38}$$

Theorem 9. *Under (37), the following statements hold.*

1. *C_I is self-dual if and only if $I = \{1, \dots, s\} \setminus \pi(I)$.*
2. *A self-dual ideal exists if and only if π has no fixed points. In that case there are exactly $2^{s/2}$ self-dual ideals.*
3. *C_I is LCD if and only if $I = \pi(I)$, that is, I is a union of star orbits.*

Proof. Part (1) follows immediately from uniqueness of the primitive-idempotent support and (38). On a two-cycle $\{i, \pi(i)\}$, the equation in (1) requires choosing exactly one index. On a fixed point it requires simultaneously choosing and not choosing the same index, which is impossible. This proves (2) and the enumeration. Finally, $C_I \cap C_I^{\perp}$ has primitive support $I \cap (\{1, \dots, s\} \setminus \pi(I))$. It is zero precisely when $I \subseteq \pi(I)$; applying π and using finiteness yields $I = \pi(I)$. □

Remark 2. *Theorem 9 classifies ideal self-duality, not self-duality up to rank-metric equivalence. A code can be equivalent to its dual without being equal to it, a distinction also relevant for generalized twisted Gabidulin codes [14].*

In the noncommutative semisimple case, Wedderburn components are matrix algebras and primitive left ideals inside a star-stable component may possess isotropic submodules. The fixed-point obstruction in Theorem 9 is therefore no longer sufficient by itself. One must analyse the induced Hermitian form on each simple component. The following componentwise statement remains useful.

Proposition 11. *Let $A = \bigoplus_{t=1}^{r} A_t$ be a decomposition into simple two-sided ideals such that $*$ permutes the components. Write t^* for the index determined by $A_t^* = A_{t^*}$, and let $C = \bigoplus_t C_t$ be a left ideal with $C_t = C \cap A_t$. Then*

$$(C^{\perp})_t = \{y \in A_t : \tau(xy^*) = 0 \text{ for every } x \in C_{t^*}\}. \tag{39}$$

Consequently, C is self-dual if and only if equality of C_t with the right-hand side of (39) holds for every t. On a two-component star orbit this condition determines either component from the other; on a star-fixed component it is precisely self-duality for the restricted nondegenerate form.

Proof. Write $x = \sum_s x_s$ and $y = \sum_t y_t$ according to the two-sided component decomposition. Since $y_t^* \in A_{t^*}$ and distinct two-sided components annihilate one another,

$$\langle x, y \rangle_* = \sum_t \tau(x_{t^*} y_t^*).$$

The summands can be tested independently, which proves (39). The global form is nondegenerate; hence its restriction to a paired sum $A_t \oplus A_{t^*}$ is nondegenerate, and on a fixed component the restricted form is nondegenerate. The asserted self-duality criterion follows orbit by orbit. □

This reduction turns the global existence problem into Hermitian linear algebra over the division rings occurring in the Wedderburn decomposition. Over finite fields those division rings are fields, but the involution may act nontrivially on their centres.

9 A noncommutative matrix-type example

The preceding cyclic examples are commutative. We now display the involution and idempotent conditions in a genuinely noncommutative twisted algebra. Let $\operatorname{char} K \neq 2$ and let $G = C_2 \times C_2 = \{1, a, b, ab\}$. Choose a cocycle with values in $\{1, -1\} \subseteq F^\times$ so that, writing $u = u_a$ and $v = u_b$,

$$u^2 = v^2 = 1, \qquad vu = -uv. \tag{40}$$

The resulting twisted group algebra has basis $(1, u, v, uv)$ and is noncommutative. The assignment

$$u \longmapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad v \longmapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{41}$$

extends to an isomorphism $A \cong M_2(K)$. Thus the algebra is semisimple and every left ideal is idempotent-generated.

The cocycle is base-field valued and unitary for $\sigma = \mathrm{id}_K$. Since $u^{-1} = u$, $v^{-1} = v$ and $(uv)^{-1} = vu = -uv$, the canonical involution is

$$(a_0 + a_1 u + a_2 v + a_3 uv)^* = a_0 + a_1 u + a_2 v - a_3 uv. \tag{42}$$

Although (42) looks like a sign change, it is the unique anti-automorphism dictated by inversion of the homogeneous units. In the matrix realization it is ordinary transpose.

Proposition 12. *Let $e = a_0 + a_1 u + a_2 v + a_3 uv \in A$ be neither zero nor one. Then $e^2 = e$ if and only if*

$$a_0 = \frac{1}{2}, \qquad a_1^2 + a_2^2 - a_3^2 = \frac{1}{4}. \tag{43}$$

Every such Ae has K-dimension two. Moreover:

1. *$e = e^*$ if and only if $a_3 = 0$, in which case Ae is LCD;*
2. *$e^* = 1 - e$ if and only if $a_1 = a_2 = 0$ and $a_3^2 = -1/4$, in which case Ae is self-dual.*

Proof. Under (41),

$$e \longmapsto \begin{bmatrix} a_0 + a_1 & a_2 + a_3 \\ a_2 - a_3 & a_0 - a_1 \end{bmatrix}.$$

A nontrivial idempotent in $M_2(K)$ has trace one and determinant zero. These conditions are precisely (43); its matrix rank is one, so the left ideal has dimension two. The first assertion follows from (42) and Corollary 1. Comparing the four coefficients in $e^* = 1 - e$ gives $a_0 = 1/2$, $a_1 = a_2 = 0$, while the idempotent equation gives $a_3^2 = -1/4$. The self-duality conclusion again follows from Corollary 1. □

This example makes three distinctions visible. First, a nontrivial cocycle can convert the algebra of an abelian group into a noncommutative simple algebra. Second, star-fixed idempotents yield LCD ideals, whereas idempotents paired with their complements yield self-dual ideals. Third, neither property implies good rank distance. Indeed, for a self-dual idempotent in Proposition 12,

$$\mathrm{wt}_R(e) = \dim_F \langle 1, a_3 \rangle_F \leq 2.$$

The resulting $[4, 2, d]_{q^m/q}$ ideal therefore satisfies $d \leq 2$, below the MRD target 3. If -1 is a nonsquare in F but becomes a square in K, then a_3 has degree two over F and the displayed idempotent has rank exactly two. If -1 is already a square in F, its rank is one.

More generally, (43) defines a quadric of candidate two-dimensional ideal codes. Proposition 15 below shows that a rank-three candidate must use coefficients generating an extension of degree at least three. Hence searches may discard all rational points of this quadric defined over subfields of degree one or two. This is a substantial reduction compared with enumerating every generator matrix in $K^{2\times 4}$.

10 Generator matrices and computation

The framework leads to direct finite algorithms. Fix the ordered group basis. For $x = \sum_g a_g u_g$, the left and right regular matrices have entries

$$\rho_L(x)_{r,h} = a_{g_r h^{-1}} \alpha(g_r h^{-1}, h), \tag{44}$$
$$\rho_R(x)_{r,h} = a_{h^{-1} g_r} \alpha(h, h^{-1} g_r), \tag{45}$$

where rows are indexed by g_r and columns by h. Each formula follows by extracting the coefficient of u_{g_r} from, respectively, $x u_h$ and $u_h x$.

If $C = Ae$, the columns of $\rho_R(e)$ are the coefficient vectors of $u_h e$. Equivalently, the rows of $\rho_R(e)^{\mathsf{T}}$ span C. This use of the right regular matrix is essential when A is noncommutative: the columns of $\rho_L(e)$ span the right ideal eA, not the left ideal Ae. Theorem 5 gives a generator matrix for the dual from $1 - e^*$ without computing a nullspace.

Algorithm 1 Idempotent ideal and dual construction

Input: $F \subseteq K$, multiplication table of G, cocycle α, involution σ, and candidate $e \in K^{\alpha}[G]$.

Verify the cocycle identity (1) and normalization.

Verify $\sigma^2 = 1$ and the unitary condition (3).

Compute e^2 and reject unless $e^2 = e$.

Form e^* using (6).

Build $\rho_R(e)$ and $\rho_R(1 - e^*)$ using (45).

Row reduce $\rho_R(e)^{\mathsf{T}}$ to obtain G_C.

Row reduce $\rho_R(1 - e^*)^{\mathsf{T}}$ to obtain $G_{C^{\perp}}$.

Expand entries in an F-basis of K to compute rank weights.

Return: G_C, $G_{C^{\perp}}$ and their rank distributions.

The complexity of exhaustive rank-distribution computation is exponential in k, since $|C| = q^{mk}$. Structural tests are cheaper. Cocycle verification uses $O(n^3)$ field operations, regular matrices use $O(n^2)$ operations, and Gaussian elimination uses $O(n^3)$ operations. Self-orthogonality of an idempotent ideal is tested by one algebra multiplication ee^* instead of by checking all generator inner products.

For the cyclic MRD ideals, no exhaustive search is needed. The degree of ζ over F can be computed from the least r such that $\zeta^{q^r} = \zeta$. Theorem 7 then certifies distance two, while Theorem 8 certifies distance n. This illustrates a general principle: distance proofs should exploit the algebraic description rather than enumerate codewords.

10.1 A reproducible small example

Take $F = \mathbb{F}_3$, $K = \mathbb{F}_9 = F(\zeta)$ with $\zeta^2 = -1$, and $A = K[x]/(x^2 + 1)$. Since -1 is nonsquare in F_3, $\{1, \zeta\}$ is an F-basis. The ideals

$$C = (x - \zeta), \qquad D = K(x + \zeta)$$

both have K-dimension one. The generator coefficient vectors are $(-\zeta, 1)$ and $(\zeta, 1)$, respectively, and both have F-rank two. Thus both are $[2, 1, 2]_{9/3}$ MRD codes. Because $2 \neq 0$ in F_3,

$$e = \frac{x + \zeta}{2\zeta}$$

is an idempotent generator for D. Direct multiplication gives $xe = \zeta e$ and $e^2 = e$. This example separates rank and Hamming metrics: each nonzero word has Hamming weight two and rank weight two, but in larger degrees a full-support word need not have full rank.

10.2 Cocycle and basis invariance checks

Any implementation should test three invariances.

1. A change of the F-basis of K acts on every expansion matrix by an element of $\mathrm{GL}_m(F)$ and preserves rank.

2. Reordering G permutes coefficient columns and simultaneously conjugates regular matrices by a permutation matrix.

3. Replacing α by an F-cohomologous cocycle applies the rank isometry in Proposition 2.

Failure of any one of these tests indicates that the implementation is using ordinary K-matrix rank or has misplaced a cocycle factor.

11 Cryptographic interpretation and limitations

Rank-metric codes appear in network coding and in several cryptographic designs, but an algebraic family should not be declared secure merely because its decoding problem is nontrivial. Ideal structure creates both efficient algorithms and possible distinguishers. The present framework identifies the following information that is visible from a public generator matrix of an ideal code.

First, left multiplication by every u_g stabilizes C. In coefficient coordinates these transformations are monomial matrices whose nonzero entries are cocycle values. Thus the automorphism group of the public code contains a projective regular image of G. This symmetry can distinguish ideal codes from random rank-metric codes unless it is deliberately hidden.

Second, the left idealiser

$$\mathcal{I}_\ell(C) = \{a \in A : aC \subseteq C\}$$

equals A for a left ideal represented inside its native algebra, while the right idealiser

$$\mathcal{I}_r(C) = \{a \in A : Ca \subseteq C\}$$

may expose the stabilizer of the generating idempotent. Idealisers and centralisers are established invariants in rank- and sum-rank equivalence problems. A large idealiser is useful for fast encoding but may be a strong structural fingerprint.

Third, if $C = Ae$ is public together with the native multiplication, then $C^\perp = A(1 - e^*)$ is obtained immediately. Dual computation is not a hard problem. Similarly, the star-orbit decomposition in the semisimple commutative case reveals all LCD and self-dual ideal choices once the primitive idempotents are known.

These observations lead to a cautious design principle.

Proposition 13. *Let $C \leq A$ be a nonzero proper left ideal and let P_g be the coefficient matrix of left multiplication by u_g. Then*

$$P_g \Phi(C) = \Phi(C) \quad (g \in G),$$

and the matrices satisfy the projective multiplication law

$$P_g P_h = \alpha(g,h) P_{gh}.$$

If α is base-field valued, every P_g is a rank isometry.

Proof. Since u_g is a unit and C is a left ideal, $u_g C \subseteq C$ and $u_g^{-1} C \subseteq C$, so equality holds. The projective law is the regular representation of $u_g u_h = \alpha(g,h) u_{gh}$. When $\alpha(g,h) \in F^\times$, P_g is a coordinate permutation followed by base-field coordinate scalings, which preserves coefficient rank. □

Consequently, any McEliece-type use must analyse whether an ambient rank isometry sufficiently conceals this projective regular subgroup. Theorem 13 does not constitute an attack, but it specifies a necessary distinguisher test. Security also requires concrete decoding algorithms, parameter selection, resistance to key recovery and reductions or well-studied assumptions. None of these follows from the MRD property alone.

The cyclic MRD families in Section 7 are deliberately extreme-dimensional. The $[n, 1, n]$ family carries only one extension-field symbol, while the $[n, n-1, 2]$ family corrects no more than a very small rank error. Their value is structural: they prove that the intersection of the ideal and MRD properties is nonempty and provide test cases for duality. Cryptographically useful intermediate-rate MRD ideals remain an open construction problem.

12 Further examples and parameter bounds

We collect consequences that can guide the search for intermediate-rate families. For $x \in A$, let

$$\mathrm{Ann}_r(x) = \{a \in A : xa = 0\}.$$

Ordinary matrix rank of the regular representation satisfies

$$\mathrm{rank}_K \, \rho_L(x) = n - \dim_K \mathrm{Ann}_r(x). \tag{46}$$

This invariant differs from $\mathrm{wt}_R(x)$ but can restrict possible ideal generators.

Proposition 14. *Let $e^2 = e$, and let $\rho_R(e)$ denote right multiplication by e. Then*

$$\mathrm{rank}_K \, \rho_R(e) = \dim_K Ae, \qquad \mathrm{crk}_F \, \rho_L(e) = \mathrm{crk}_F \, \rho_R(e) = \mathrm{wt}_R(e)$$

when α is base-field valued. Hence an $[n, k, d]_{q^m/q}$ idempotent ideal satisfies

$$d \le \mathrm{wt}_R(e) \le \min\{m, n\}, \qquad \mathrm{rank}_K \, \rho_R(e) = k.$$

Proof. The image of $\rho_R(e)$ is Ae. The coefficient-rank identities are Theorem 3, and the distance inequality holds because $e \in Ae$. □

For noncommutative A, one should consistently use the right regular representation for the dimension of Ae and the left regular representation for the projective symmetry action. Both representations recover coefficient rank under a base-field cocycle by the same proof as Theorem 3.

Proposition 15. *Let $C = Ae$ have dimension k, and suppose e has all coefficients in a proper intermediate field $F \subseteq L \subsetneq K$. Then*

$$d_R(C) \leq \mathrm{wt}_R(e) \leq [L : F].$$

In particular, if C is MRD, then

$$[L : F] \geq n - k + 1.$$

Proof. All coefficients of e lie in the $[L : F]$-dimensional F-space L, so $\mathrm{wt}_R(e) \leq [L : F]$. Since e is a nonzero codeword, the first inequality follows. Substitute the MRD distance. □

Thus an idempotent defined over too small a subfield cannot generate a high-distance ideal. This explains why ordinary group-algebra idempotents with coefficients in F have rank weight one and cannot themselves belong to an MRD ideal of distance greater than one. Twisting alone does not solve the problem; extension-field coefficients in the idempotent are essential.

Corollary 3. *If $e \in F^\alpha[G]$ is a nonzero idempotent viewed inside $K^\alpha[G]$, then $d_R(Ae) = 1$. Hence such an ideal is MRD only when $k = n$.*

Proof. The coefficient rank of e is one, so the minimum rank distance is one. The Singleton equality then forces $k = n$. □

This obstruction sharply narrows computational searches: candidate idempotents for non-trivial MRD ideals must not descend to the base field.

13 Open problems

The results above suggest several concrete problems.

Problem 1. *Classify triples (F, K, G) and base-field-valued cocycles α for which $K^\alpha[G]$ contains an MRD left ideal of every dimension $1 \leq k \leq n$. Even the cyclic case for $2 \leq k \leq n-2$ is open in this formulation.*

Problem 2. *Determine whether an uncertainty inequality connects $\dim_K Ax$, $\mathrm{wt}_R(x)$ and the support of a twisted Fourier transform. Analogous inequalities for group-algebra ideals under the Hamming metric are studied in [4].*

Problem 3. *When a cocycle is not base-field valued, find an intrinsic rank metric on A that is simultaneously cohomology invariant and exactly compatible with the full regular matrix, without replacing coefficient rank by ordinary matrix rank.*

Problem 4. *For a noncommutative semisimple twisted group algebra with involution, classify self-dual left ideals componentwise and determine which of them are MRD or near-MRD. Proposition 11 reduces existence to the star-fixed Wedderburn components, but distance couples all components through the group basis.*

Problem 5. *Develop a decoding algorithm for intermediate-rate twisted ideal codes whose complexity uses multiplication in A. The cyclic extremal families admit trivial syndrome descriptions, but they do not address the general decoding problem.*

These problems separate algebraic existence, metric optimality and cryptographic suitability. Solving only one does not settle the other two.

14 Conclusion

We have developed a rank-metric framework for left ideals in twisted group algebras. Two compatibility hypotheses play distinct roles. A cocycle with values in the base field makes coefficient rank visible in the entries of the regular representation. A σ-unitary cocycle produces the canonical semilinear involution $u_g^* = u_g^{-1}$. Together with the identity-coefficient functional, this involution yields the standard coordinate Hermitian form without suppressing the cocycle corrections required by multiplication.

The formula

$$(Ae)^\perp = A(1 - e^*)$$

is the main bridge between ideal structure and duality. It gives immediate criteria for self-orthogonal, self-dual and LCD ideals and reduces the commutative semisimple classification to star orbits of primitive idempotents. Because the coefficient map is a rank isometry, the classical q-binomial MacWilliams moments transfer to this setting, and duals of MRD ideals remain MRD.

The cyclic construction demonstrates that metric optimality and ideal structure can coexist. If ζ has degree n over F and $\zeta^n \in F^\times$, the evaluation kernel $(x-\zeta)$ is an $[n, n-1, 2]$ MRD ideal, while the complementary line generated by $(x^n - \zeta^n)/(x - \zeta)$ is an $[n, 1, n]$ MRD ideal. These families also expose the principal limitation of the present theory: new intermediate-rate MRD ideals require subtler idempotents that do not descend to the base field.

Finally, the algebraic symmetry that facilitates encoding and dual construction can be cryptographically visible. Any application must analyse projective regular automorphisms, idealisers and star decompositions as potential distinguishers. The framework therefore provides both a construction language and a checklist of structural information that a security analysis must confront.

Acknowledgments

The author thanks the anonymous referees for comments that may improve the presentation.

References

[1] S. Assuena and A. L. M. Pereira, *LCD and self-orthogonal twisted group codes over finite commutative chain rings*, preprint, arXiv:2507.04013, 2025.

[2] A. Behajaina, M. Borello, J. de la Cruz and W. Willems, *Twisted skew G-codes*, Des. Codes Cryptogr., **92** (2024), 1803–1821.

[3] M. Borello and W. Willems, *Group codes over fields are asymptotically good*, Finite Fields Appl., **68** (2020), 101738.

[4] M. Borello, W. Willems and G. Zini, *On ideals in group algebras: an uncertainty principle and the Schur product*, Forum Math., **34** (2022), 1345–1354.

[5] J. de la Cruz and W. Willems, *On group codes with complementary duals*, Des. Codes Cryptogr., **86** (2018), 2065–2073.

[6] J. de la Cruz and W. Willems, *Twisted group codes*, IEEE Trans. Inform. Theory, **67** (2021), 5178–5184.

[7] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, J. Combin. Theory Ser. A, **25** (1978), 226–241.

[8] E. M. Gabidulin, *Theory of codes with maximum rank distance*, Probl. Inf. Transm., **21** (1985), 1–12.

[9] M. Gadouleau and Z. Yan, *MacWilliams identity for codes with the rank metric*, EURASIP J. Wireless Commun. Netw., **2008** (2008), Article 754021.

[10] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[11] G. Karpilovsky, *Projective Representations of Finite Groups*, Marcel Dekker, New York, 1985.

[12] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[13] G. Nebe and W. Willems, *On self-dual MRD codes*, Adv. Math. Commun., **10** (2016), 633–642.

[14] K. Otal, F. Ozbudak and W. Willems, *Self-duality of generalized twisted Gabidulin codes*, Adv. Math. Commun., **12** (2018), 707–721.

[15] A. Ravagnani, *Rank-metric codes and their duality theory*, Des. Codes Cryptogr., **80** (2016), 197–216.

[16] D. Silva, F. R. Kschischang and R. Koetter, *A rank-metric approach to error control in random network coding*, IEEE Trans. Inform. Theory, **54** (2008), 3951–3967.

[17] W. Willems, *Codes in group algebras*, in: W. C. Huffman, J.-L. Kim and P. Solé (eds.), Concise Encyclopedia of Coding Theory, CRC Press, Boca Raton, 2021, 363–384.

[18] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math., **121** (1999), 555–575.