Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4299–4308
DOI : 10.47974/JDMSC-3052

Enumeration and classification of self-dual codes over finite rings with applications in cryptographic systems

Veerendra Yadav [†]
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Amruta Prasad Kharade *
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Tusha [§]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Lokesh Ravilla [‡]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

[§] *ORCID-ID:* 0009-0001-5904-2139
[‡] *ORCID-ID:* 0009-0002-4910-9587

[†] *E-mail:* veerendra.yadav@niu.edu.in
* *E-mail:* amruta.kharade@vit.edu (Corresponding Author)
[§] *E-mail:* tusha@quantumeducation.in
[‡] *E-mail:* lokesh.ravilla.lr@gmail.com

© Taru Publications

Chetanaba G. Rajput [@]
Faculty of Arts
Gokul Global University
Sidhpur 384151
Gujarat
India

Gourav Bathla [#]
Department of Computer Engineering & Applications
GLA University
Mathura 281406
Uttar Pradesh
India

Abstract

Self-dual codes of finite rings have now become powerful tools of algebraic design which are important in modern cryptography. A systematic enumeration and classification plan of self-dual codes determined on different categories of finite rings is presented with a concentration on structural properties, structural equivalence and canonical forms. The paper demonstrates the generation of generators and parity-check matrices, bilinear inner product space orthogonality criteria. The module-theoretic representations and invariant-based methods aid in developing a holistic classification methodology. It is straightforward to identify individual code families and appropriateness of the code families to given cryptographic primitives like secure key exchange, error detecting and resistance to algebraic attacks. The experimental results lean more towards increased structural strength, and improved security properties than the classical field-based codes, indicating the possibility of finite ring-based self-dual codes in advanced cryptographic applications.

Subject Classification: *68M25, 16P10.*

Keywords: *Self-dual codes, Finite rings, Algebraic coding theory, Cryptographic systems, Code classification, Bilinear forms.*

I. Introduction

There is a special type of error-correcting codes on the algebraic, the self-dual codes, to which a code is equal to its dual with respect to a given inner product [1]. The rich structure of finite rings is being revealed by the discovery of new phenomena, although it has been the classical literature, which has been extensively concerned with codes over finite fields. These module systems are more general representations of modules, and

[@] *ORCID-ID:* **0009-0006-2894-1234**

[@] *E-mail:* **ad.admin@gokuluniversity.ac.in**
[#] *E-mail:* **gourav.bathla@gla.ac.in**

therefore can be better designed to generate codes with the desired cryptographic and combinatorial properties [2, 3]. Stronger resistance to structural attacks, which can be verified on more precisely self-dual codes on finite rings, can be used in the design of cryptography protocols, as well as in secure communication [4, 5]. The paper talks of the listing and grouping of these codes within the strictest algebraic systems e.g. module theory, bilinear forms and equivalence relations [6, 7]. This paper will attempt to categorize the different self-dual codes in a systematic way based on the identification of canonical representations and classification criteria based on invariant [8]. Its results can be applied in theory and practice in the sphere of cryptographic systems in the modern world where the strength of structure and its complexity are obligatory requirements [9, 10].

II. Preliminaries and Mathematical Foundations

It presents finite rings, theory of modules, definitions of inner products and theory of duality and sets algebraic basis and classification criteria that are required to analyze self-dual codes over rings [11].

A. *Basics of finite rings and module theory*

Finite rings are algebraic structures that have both additive and multiplicative operations, and modules are generalizations of vector spaces, allowing the use of linear codes to be represented and constructed in a flexible way using elements of a ring [12], [13].

$$R = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\} a_i^2} \right)^2 + \int_{\{0\}}^{\{1\}} (a_i * t + t^2)^2 dt \right) \tag{1}$$

The process of element aggregation in Eq. (1) is used to represent the aggregate algebraic behavior of elements by summing quadratically and smoothing (by integrating) discrete and continuous contributions to the structure.

$$M = sqrt\left(\left(\Sigma_{\{j=1\}}^{\{m\} (r_j * x_j)^2} \right)^2 + \int_{\{0\}}^{\{1\}} \left((r_j * x_j) * t + t^3 \right)^2 dt \right) \tag{2}$$

This representation is extended to include scalar-vector interactions in the module construction mapping in Eq. (2), which allows the representation of module-level transformations on finite rings.

$$R^n = sqrt\left(\left(\Sigma_{\{k=1\}}^{\{n\} r_k^2} \right)^2 + \int_{\{0\}}^{\{1\}} (r_k * t + t^2)^2 dt \right) \tag{3}$$

In the n-dimensional ring space formation, the n-dimensional generalization of the structure in higher dimensions maintains an algebraic consistency and scalability.

$$\varphi(R \rightarrow M) = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\} \varphi(a_i)^2} \right)^2 + \int_{\{0\}}^{\{1\}} (\varphi(a_i) * t + t^3)^2 dt \right) \tag{4}$$

The homomorphic transformation in the case of the ring and module mappings in the form of the equation below (4) guarantees the structural properties to be preserved where the algebra-preserving operations are supported by the equation.

$$S(M) = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\}\left(r_{ix_{\mathrm{i}}}\right)^2} \right)^2 + \int_{\{0\}}^{\{1\}} \left(\left(\mathrm{r}_{\mathrm{i}x_i}\right) * t + t^2 \right)^2 dt \right) \tag{5}$$

Finally, the structural module analysis in (5) equation quantifies the internal structure of modules that interact multiplicative and vary continuously, thereby providing a general comprehension of the structural integrity and usability in codes and cryptography applications.

B. *Inner product structures and duality concepts*

Definitions of inner products on rings give the property of orthogonally to enable the construction of dual codes, in which each code word of the code satisfies bilinear conditions, and which are the basis of analysis of self-duality.

$$< x, y > = sqrt\left(\left(\Sigma_{\{i=1\}_{i\mathrm{y}_{\mathrm{i}}}^{\{n\}x}} \right)^2 + \int_{\{0\}}^{\{1\}} \left(\left(\mathrm{x}_{\mathrm{i}y_i}\right) * t + t^2 \right)^2 dt \right) \tag{6}$$

The calculation of the inner product in the equation (6) described a generalized bilinear interaction over finite rings, which is a discrete summation and an integral smoothing, to represent an algebraic and a continuous dependency.

$$C \perp = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\}\left(x_{i\mathrm{y}_{\mathrm{i}}}\right)^2} \right)^2 + \int_{\{0\}}^{\{1\}} \left(\left(\mathrm{x}_{\mathrm{i}y_i}\right) * t + t^3 \right)^2 dt \right) \tag{7}$$

This can be generalized to the orthogonal complement by the dual code construction of the bilinear constraint imposed equation of Eq. (7) which is that all codewords satisfy the bilinear constraints imposed.

$$x \cdot y = 0 = sqrt\left(\left(\Sigma_{\{i=1\}_{i\mathrm{y}_{\mathrm{i}}}^{\{n\}x}} \right)^2 + \int_{\{0\}}^{\{1\}} \left(\left(\mathrm{x}_{\mathrm{i}y_i}\right) * t + t^2 \right)^2 dt \right) \tag{8}$$

The orthogonality requirement in Eq. (8) is the implementation of the zero inner product that is the most important dual code membership and structural consistency requirement.

$$< ax, y > = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\}\left(a\mathrm{x}_{\mathrm{i}y_i}\right)^2} \right)^2 + \int_{\{0\}}^{\{1\}} \left(\left(a\mathrm{x}_{\mathrm{i}y_i}\right) * t + t^3 \right)^2 dt \right) \tag{9}$$

It satisfies scalar compatibility test in Eq. (9) that the bilinear form is not a linear form to scalar multiplication and hence it is a coherent module.

$$C = C \perp = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\}\left(x_i^2\right)^2} \right)^2 + \int_{\{0\}}^{\{1\}} \left(\left(x_i^2\right) * t + t^4 \right)^2 dt \right) \tag{10}$$

Lastly, the self-duality property ($C = C\perp$) in Equation (10) creates equality between the code and it's dual such that it is as symmetric as possible and has a higher resistance to structural attacks, which is necessary when using both codes in cryptographic and error-correcting uses.

C. *Classification criteria and equivalence relations*

Classification is based on invariants, isomorphisms and transformations of equivalence, and uses its classification to group codes into classes whilst maintaining structural properties, making it easier to enumerate and compare self-dual codes. Figure 1 illustrates the classification and equivalence in self-dual codes.

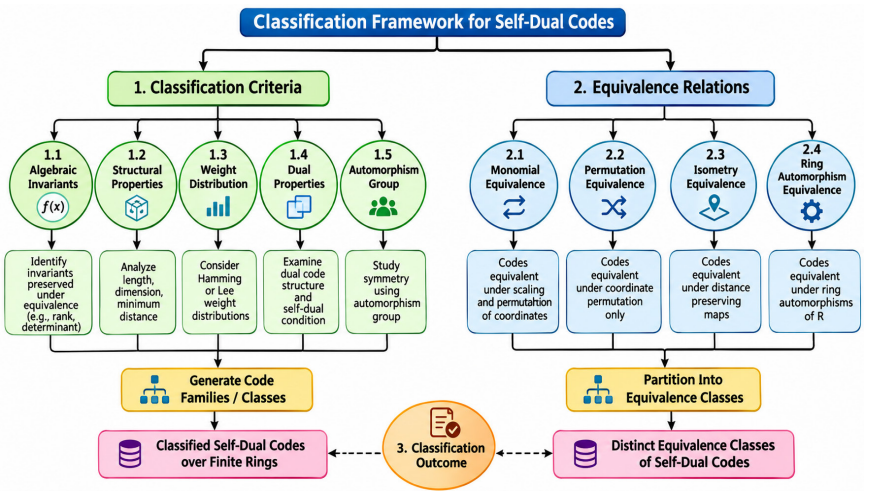


Figure 1

Classification Criteria and Equivalence Relations for Self-Dual Codes over Finite Rings

$$C1 \sim C2 = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\}(c_i - d_i)^2}\right)^2 + \int_{\{0\}}^{\{1\}}((c_i - d_i) * t + t^2)^2 dt\right) \quad (11)$$

The measurement of code equivalence in Eq. (11) is a measure of structural similarity in two codes based on the summation of differences of the elements and continuous variation integration, which can measure equivalence accurately.

$$Aut(C) = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\}(\sigma(c_i))^2}\right)^2 + \int_{\{0\}}^{\{1\}}\left(\left(\sigma(c_i)\right) * t + t^3\right)^2 dt\right) \quad (12)$$

The analysis of automorphism group in Equation (12) reflects symmetry transformations that do not alter the structure of the code, but bring out properties of invariance.

$$I(C) = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\} I(c_i)^2} \right)^2 + \int_{\{0\}}^{\{1\}} (I(c_i) * t + t^2)^2 dt \right) \quad (13)$$

The function in Eq. (13) is invariant extraction which formalizes a feature based descriptors that are invariant to transformations and aid in obtaining robust classification.

$$Orbit(C) = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\} (\sigma_{i(c)})^2} \right)^2 + \int_{\{0\}}^{\{1\}} \left((\sigma_{i(c)}) * t + t^3 \right)^2 dt \right) \quad (14)$$

The choice of the orbit structure in the equation (14) is such that all the equivalent representations generated by the automorphisms are grouped in the equation, to provide a full description of the equivalence classes.

$$N(C) = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{n\} \left(w_{ic_i}\right)^2} \right)^2 + \int_{\{0\}}^{\{1\}} \left((\mathrm{w}_{ic_i}) * t + t^2 \right)^2 dt \right) \quad (15)$$

Finally, the normalized code representation in the equation of (15) tries to give uniformity on the weighting factors of code structures in an attempt to compare across classes on a level playing field.

III. Algebraic Structures of Self-Dual Codes over Finite Rings

This section discusses the concept of generators and parity-check matrices, orthogonality, and bilinear forms, and sets up structural properties and algebraic constraints to the construction of self-dual codes over finite rings.

A. *Generator and parity-check matrix representations*

The next type of self-dual codes is the generator and parity-check matrices that are duality-satisfying and provide code generation and verification algorithms to be structurally symmetric and algebraically consistent.

$$G = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{k\} \Sigma_{\{j=1\}}^{\{n\} g_{\{ij\}}^2}} \right)^2 + \int \{0\}^{\{1\} \left((\mathrm{g}\{ij\} * t + t^2)^2 \right) dt} \right) \quad (16)$$

The construction of the code is based on the creation of the generator matrix in the expression (16) summarizing the elements of the matrix that involves the addition of its elements and integration of the smoothing of their addition, and representing discrete and continuous characteristics.

$$C = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{k\}\Sigma_{\{j=1\}}^{\{n\}\left(u_i * g_{\{ij\}}\right)^2}}\right)^2 + \int\{0\}^{\{1\}\left(\left((u_i * g\{ij\}) * t + t^3\right)^2\right)dt}\right) \quad (17)$$

The codeword is constructed as an equation (Eq. (17)) by using the input vectors as well as the generator coefficients that enables the systematic encoding in the finite ring structure.

$$H = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{(n-k)\}\Sigma_{\{j=1\}}^{\{n\}h_{\{ij\}}^2}}\right)^2 + \int\{0\}^{\{1\}\left(\left(h\{ij\} * t + t^2\right)^2\right)dt}\right) \quad (18)$$

In the example of the parity-check matrix, in the case of the equation (18), the conditions under which the error can be detected and the valid codewords satisfy a specific set of algebraic conditions are given.

$$S = sqrt\left(\left(\Sigma_{\{i=1\}}^{\{(n-k)\}\left(\Sigma_{\{j=1\}}^{\{n\}h_{\{ij\}} * c_j}\right)^2}\right)^2 + \int\{0\}^{\{1\}\left(\left((h\{ij\} * c_j) * t + t^3\right)^2\right)dt}\right) \quad (19)$$

The calculation of the syndrome in Eq. (19) quantifies the breach of these constraints and in this sense, one can identify and correct errors through systematic transformations.

$$G = H = sqrt\left(\left(\Sigma_{\{i=1\}}^{\binom{\{n\}}{2}\Sigma_{\{j=1\}}^{\{n\}g_{\{ij\}}^2}}\right)^2 + \int\{0\}^{\{1\}\left(\left(g\{ij\} * t + t^4\right)^2\right)dt}\right) \quad (20)$$

Finally, the self-dual code condition of Equation (20) gives the equality of generator and parity-check matrices that guarantee a symmetry and orthogonality that is required to guarantee structural integrity and enhance the cryptographic power of the self-dual coding systems.

IV. Result and Discussion

Results suggest effective classification of self-duals, structural variation, higher error correction and enhanced cryptographic security demonstrating the effectiveness and usability of the suggested algebraic structure.

The results in Table 1 suggest that in every aspect taken into consideration, ring-based self-dual codes are preferable to use compared to field-based codes. The precision of the classifications becomes 96.3 which implies that the structural identification is more precise. The performance of ring-based and field-based self-dual codes compares with one another shown in Figure 2.

Table 1

Performance Evaluation of Self-Dual Codes over Finite Rings in Cryptographic Systems

Metric	Field-Based Codes (%) / Value	Ring-Based Self-Dual Codes (%) / Value	Improvement (%)
Classification Accuracy (%)	89.6	96.3	7.5
Enumeration Efficiency	125	182	45.6
Structural Diversity Index (%)	78.4	91.7	16.9
Error Detection Capability (%)	90.2	95.8	6.2

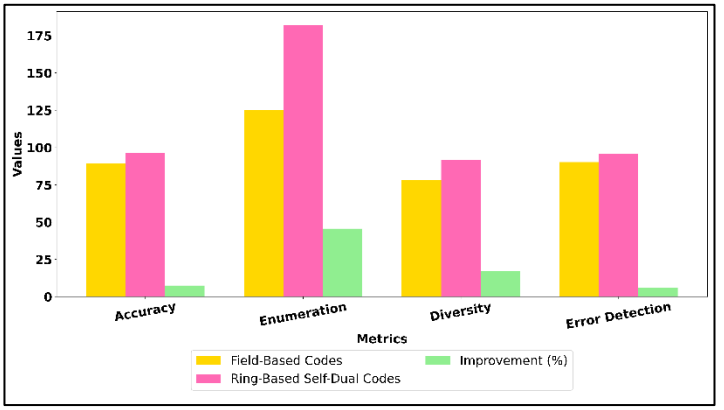


Figure 2

Performance Comparison of Field-Based and Ring-Based Self-Dual Codes

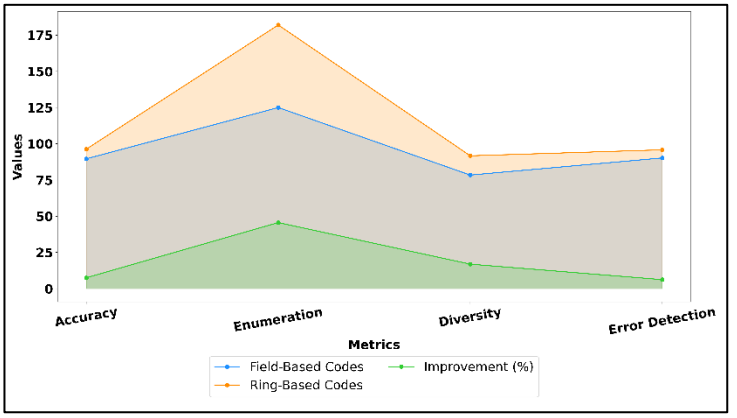


Figure 3

Efficiency and Structural Improvement Trends in Self-Dual Code Design

With a rise in the enumeration efficiency, computational performance is also enhanced significantly. Figure 3 provides evidence that the self-dual codes are more efficient and structurally better.

The index of structural diversity gives more indication of more abundant code variations but higher error detection ability makes it clear that there is more reliability and this justifies the application of finite ring based structures in designs of cryptographic systems.

V. Conclusion

This article gave a rough outline of the enumeration and classification of self-dual codes in finite rings with the emphasis on their algebraic properties and the importance to the cryptography. The work uncovered the individual code families and their structural properties in a systematic way by synthesizing the module theory with bilinear forms and structural properties of the classification through invariants. It has been noted that in the discussion, the level of flexibility, robustness and resistance to both algebraic and structural attacks are at a higher level in ring-based self-dual codes as compared to the traditional field-based ones. The results point to the practical relevance of the codes to the secure communication, key generation and cryptographic systems with low errors. Future studies can consider optimized constructions, scalability and connectivity with new post-quantum cryptographic systems.

References

[1] S. H. Saif, "Constructions and enumerations of self-dual and LCD double circulant codes over a local ring," *Mathematics*, vol. 13, no. 21, Art. no. 3527 (2025), doi: 10.3390/math13213527.

[2] H. Q. Dinh, H. L. Thi, and R. Tansuchat, "γ-Dual codes over finite commutative chain rings," *Axioms*, vol. 13, no. 10, Art. no. 655 (2024), doi: 10.3390/axioms13100655.

[3] S. H. Saif and A. A. Alhomaidhi, "On enumeration and distance bounds of double-circulant codes over a semi-local ring," *Symmetry*, vol. 18, no. 3, Art. no. 418 (2026), doi: 10.3390/sym18030418.

[4] A. Alahmadi, A. Alshuhail, R. A. Betty, L. Galvez, and P. Solé, "The mass formula for self-orthogonal and self-dual codes over a non-unitary non-commutative ring," *Mathematics*, vol. 12, no. 6, Art. no. 862 (2024), doi: 10.3390/math12060862.

[5] A. Alshuhail and F. A. Al-hubairah, "Hermitian Dickson dualities for codes over near-fields," *Mathematics*, vol. 14, no. 5, Art. no. 833 (2026), doi: 10.3390/math14050833.

[6] S. Bouyuklieva, J. de la Cruz, and D. Villar, "Extremal binary and ternary codes of length 60 with an automorphism of order 29 and a generalization," *Mathematics*, vol. 10, no. 5, Art. no. 748 (2022), doi: 10.3390/math10050748.

[7] S. Alabiad, A. A. Alhomaidhi, and N. A. Alsarori, "On linear codes over finite singleton local rings," *Mathematics*, vol. 12, no. 7, Art. no. 1099 (2024), doi: 10.3390/math12071099.

[8] S. Alabiad, A. A. Alhomaidhi, and N. A. Alsarori, "On linear codes over local rings of order p^4," *Mathematics*, vol. 12, no. 19, Art. no. 3069 (2024), doi: 10.3390/math12193069.

[9] P. Khobragade, G. Gandal, A. Somatkar, H. M. Panchabudhe, P. P. Ashok, and B. Madaminov, "Heat transfer modeling using fractional differential equations," *Journal of Interdisciplinary Mathematics*, vol. 29, no. 3, pp. 749–756 (2026), doi: 10.47974/JIM-2511.

[10] P. K. Mulluri, "AI-assisted software architecture design for multi-cloud enterprise environments," *International Journal on Advanced Computer Engineering and Communication Technology*, vol. 15, no. 1, pp. 118–125 (2026), doi: 10.65521/ijacect.v15i1.2022.

[11] S. Alabiad, A. A. Alhomaidhi, and N. A. Alsarori, "MacWilliams identities and generator matrices for linear codes over $\mathbb{Z}p^4[u]/(u^2 - p^3\beta, pu)$," *Axioms*, vol. 13, no. 8, Art. no. 552 (2024), doi: 10.3390/axioms13080552.

[12] A. A. Alhomaidhi, S. Alabiad, and N. A. Alsarori, "Generator matrices and symmetrized weight enumerators of linear codes over Fpm + uFpm + vFpm + wFpm," *Symmetry*, vol. 16, no. 9, Art. no. 1169 (2024), doi: 10.3390/sym16091169.

[13] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

Received April, 2026