

Article

Not peer-reviewed version

PSO-Guided Construction of MRD Codes for Rank Metrics

Behnam Dehghani^{*}, Amineh Sakhaie, [João Pedro Mendonça Assunção Silva](#)

Posted Date: 29 April 2025

doi: 10.20944/preprints202504.0883.v2

Keywords: Maximum Rank-Distance Codes; Particle Swarm Optimization; Rank Metrics; Error-Correcting Codes; Combinatorial Optimization



Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Article

PSO-Guided Construction of MRD Codes for Rank Metrics

Behnam Dehghani ^{1,*}, Amineh Sakhaie ^{2,†}, and João Pedro Mendonça Assunção Silva ¹

¹ Minho University

² Lisbon University

* Correspondence: pg41104@alunos.uminho.pt; Tel.: +351932297030

† These authors contributed equally to this work.

Abstract: Maximum Rank-Distance (MRD) codes are a class of optimal error-correcting codes that achieve the Singleton-like bound for rank metric, making them invaluable in applications such as network coding, cryptography, and distributed storage. While algebraic constructions of MRD codes (e.g., Gabidulin codes) are well-studied for specific parameters, a comprehensive theory for their existence and structure over arbitrary finite fields remains an open challenge. This paper introduces a computational optimization framework for constructing MRD codes using Particle Swarm Optimization (PSO), a bio-inspired metaheuristic algorithm adept at navigating high-dimensional, non-linear search spaces. Unlike traditional algebraic methods, our approach does not rely on prescribed algebraic structures; instead, it systematically explores the space of possible generator matrices to identify MRD configurations—particularly in cases where theoretical constructions are unknown. Key contributions include: (1) a tailored PSO formulation that encodes rank-metric constraints into the optimization process, ensuring feasible code candidates; (2) empirical evidence supporting the existence of MRD codes beyond classical families, with analysis of their properties; and (3) an open-source Python toolkit for MRD code discovery, enabling reproducibility and extension to other code parameters. Our experiments demonstrate the efficacy of PSO in identifying MRD codes with novel parameters, bridging gaps in the algebraic literature. The proposed method not only complements theoretical approaches but also opens avenues for machine learning-aided code design in future research.

Keywords: maximum rank-distance codes; particle swarm optimization; rank metrics; error-correcting codes; combinatorial optimization

1. Introduction

Maximum Rank-Distance (MRD) codes are a class of error-correcting codes that achieve the Singleton-like bound for rank distance, providing optimal performance for rank-metric error correction. Since their introduction by Delsarte in 1978 [1], and further development by Gabidulin in 1985 [2], MRD codes have become an essential tool in areas such as network coding, cryptography, and storage systems [3].

Despite their importance, the construction of MRD codes remains challenging and open-ended. Classical constructions such as Gabidulin codes are well understood, but recent discoveries [4] have shown the existence of other inequivalent MRD codes, demonstrating the potential for more comprehensive explorations.

However, most known MRD codes are obtained through algebraic constructions that do not always generalize well across all parameters. Moreover, recent works [5,6] have demonstrated that codes with desirable properties, such as higher generalized rank weights, can be constructed beyond the classical setting, motivating the search for new MRD codes.

In this paper, we propose a novel approach to constructing MRD codes using Particle Swarm Optimization (PSO). PSO is a population-based metaheuristic algorithm that excels at solving high-

dimensional, complex optimization problems [7]. By applying PSO to the combinatorial space of MRD codes [8], we aim to discover new codes and provide a systematic framework for their construction.

The remainder of this paper is organized as follows: Section 2 reviews related work on MRD codes and optimization techniques. Section 3 presents the necessary algebraic background. Section 4 details the theoretical framework underlying our approach. Section 5 introduces our PSO-guided construction method. Section 6 discusses the results and limitations of our approach, and Section 7 concludes the paper.

2. Related Work

2.1. Evolution and Recent Advances in Rank Metric and MRD Code Constructions

The theory of rank-metric codes began with the foundational work of Delsarte in 1978, who introduced the concept of a rank metric on matrices and defined rank-metric codes as sets of matrices over a finite field with distance measured by the rank of their difference [1]. In the same work, Delsarte also provided the first construction of MRD codes—those meeting the Singleton-like bound for the rank metric—via bilinear forms. This insight drew a parallel between MRD codes in the rank metric and MDS codes in the Hamming metric, establishing the existence of rare optimal codes under rank distance [9].

Building on this foundation, E. M. Gabidulin independently introduced in 1985 a general family of MRD codes now known as Gabidulin codes [2]. His construction employed evaluations of linearized polynomials of the form x^{q^i} over extension fields, closely analogous to how Reed–Solomon codes use regular polynomials. These codes were shown to be MRD for all feasible parameters $n \leq m$, thereby generalizing Reed–Solomon codes to the rank-metric setting.

In 2005, Kshevetskiy and Gabidulin introduced a generalized version of Gabidulin codes, extending their structure and enhancing their suitability for cryptographic applications while retaining optimality and providing additional algebraic flexibility [10]. Gabidulin codes have long been the most extensively studied family of MRD codes due to their q -linearized-polynomial construction, which achieves the Singleton-like bound $d = \min\{m, n\} - k + 1$. This construction guarantees provably optimal rank-distance and dimension along with efficient algebraic decoding algorithms [3].

For decades, it was widely believed that Gabidulin codes encompassed all practically relevant MRD codes. However, this perception shifted dramatically in 2016 when John Sheekey introduced *twisted Gabidulin codes*, a groundbreaking infinite family of linear MRD codes *inequivalent* to classical Gabidulin codes [4]. By incorporating a twisting term into the linearized polynomial structure, Sheekey uncovered deep connections between MRD codes and semifield theory, significantly broadening the landscape of MRD code constructions and demonstrating that these codes can arise from fundamentally distinct algebraic foundations.

Subsequent research from 2018 onward has focused on expanding the catalog of MRD codes and understanding their structure in new parameter regimes. One significant direction has been the study of scattered subspaces (linear sets) in projective geometries, which correspond bijectively to rank-metric codes. In 2017, Csajbók et al. established that maximum scattered linear sets yield MRD codes, leading to new constructions beyond the classical $n \leq m$ limitation [11]. Following this, Bartoli et al. (2018) constructed a 3-dimensional MRD code for the case $n = \frac{3m}{2}$ with even m , covering a previously inaccessible region in the parameter space not covered by Gabidulin codes [5,12].

In 2019, Sheekey proposed a generalized MRD code construction using skew polynomial rings, integrating both classical and twisted Gabidulin codes into a unified framework [13]. This approach significantly expanded the known families of MRD codes, enabling new constructions for many parameter sets by leveraging the algebraic structure of non-commutative polynomials and semifields.

More recently, Alfarano et al. (2022/2023) introduced a new family of \mathbb{F} -linear MRD codes of length $2m$ that are not direct sums of smaller MRD codes [6]. These codes also demonstrated strictly larger generalized rank weights than known MRD codes, highlighting new structural richness and correcting the misconception that all MRD codes exhibit similar rank weight distributions.

Together, these developments represent a significant evolution in MRD code theory—from initial bilinear constructions to modern algebraic and geometric frameworks—and continue to open new pathways for theoretical advancement and practical applications in coding and cryptography.

2.2. Heuristic and Automated Searches for MRD codes

Given the complexity of defining MRD codes algebraically, researchers have increasingly employed computational methods to find or verify new codes. For example, the classification of MRD codes with $n \leq 9$ by Csajbók et al. (2020) combined theoretical insights with computational searches [14].

Despite these efforts, the use of heuristic algorithms, particularly PSO, for MRD code discovery remains largely unexplored. Genetic Algorithms (GA), however, have shown success in evolving block codes in the Hamming metric domain, suggesting that similar strategies might be effective for rank-metric code construction [15,16].

PSO, widely regarded for its efficiency in high-dimensional optimization, offers a promising avenue for MRD code discovery. While PSO has been adapted for combinatorial problems [8], it has not yet been applied directly to MRD code construction. The adaptability of PSO to discrete and combinatorial problems suggests that it could be a powerful tool for exploring the space of MRD codes.

This paper builds upon these works by proposing a PSO-guided approach to MRD code construction, aiming to bridge the gap between algebraic theory and computational search techniques.

3. Algebraic Background

This section reviews the concepts and notation that underlie maximum-rank-distance (MRD) codes and their construction.

3.1. Rank Metric

The *rank metric* measures the distance between two matrices—or, equivalently, between vectors over an extension field—by the rank of their difference (the minimum number of rank-1 increments needed to transform one into the other) [3]. A *rank-metric code* \mathcal{C} is a subset of $\mathbb{F}_q^{m \times n}$ used for error detection and correction when this metric is applied.

According to Gabidulin [3], the error-correcting capability of a matrix code depends on the minimum *rank distance*

$$d(A, B) = \text{rank}_{\mathbb{F}_q}(A - B), \quad A, B \in \mathbb{F}_q^{m \times n}. \quad (1)$$

For $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ the global distance is

$$d_r = \min_{A, B \in \mathcal{C}, A \neq B} \text{rank}_{\mathbb{F}_q}(A - B). \quad (2)$$

The code \mathcal{C} is called \mathbb{F}_q -linear if it is a k -dimensional subspace of $\mathbb{F}_q^{m \times n}$ with $k \in \{1, \dots, mn\}$.

If \mathcal{C} is \mathbb{F}_q -linear it admits the *generator-matrix form*

$$\mathcal{C} = \{G\mathbf{u} : \mathbf{u} \in \mathbb{F}_q^{k \times 1}\}, \quad G \in \mathbb{F}_q^{k \times n}. \quad (3)$$

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}, \quad \mathbf{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}, \quad \mathbf{c} = G\mathbf{u} \in \mathcal{C}.$$

Each $\mathbf{c} \in \mathcal{C}$ is a *codeword*, viewed either as a vector over \mathbb{F}_q or, via a fixed \mathbb{F}_q -linear isomorphism, as an $m \times n$ matrix over the base field.

3.2. Singleton Bound and Singleton-Like Bound

Classical Hamming case. For a Hamming-metric block code of length n , dimension k , and minimum distance d , the classical Singleton bound is [9]

$$d \leq n - k + 1. \quad (4)$$

Rank-metric analogue. For $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ with minimum rank distance d and \mathbb{F}_q -dimension k , Delsarte and Gabidulin [1–3] proved the Singleton-type bounds

$$|\mathcal{C}| \leq q^{m(n-d+1)}, \quad (5)$$

$$k \leq m(n-d+1), \quad (6)$$

$$d \leq \min\{m, n\} - k + 1. \quad (7)$$

3.3. Maximum Rank-Distance (MRD) Codes

A code $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ is a *maximum rank-distance* (MRD) code when it achieves equality in the Singleton-like bound:

$$|\mathcal{C}| = q^{m(n-d+1)} \iff k = m(n-d+1) \iff d = \min\{m, n\} - k + 1. \quad (8)$$

Lemma 1. Let $G \in \mathbb{F}_q^{k \times n}$ generate a \mathbb{F}_q -linear code \mathcal{C} . Then \mathcal{C} is MRD iff

$$\text{rank}_{\mathbb{F}_q}(YG) = k \quad \text{for every } Y \in \mathbb{F}_q^{k \times n} \text{ with } \text{rank}_{\mathbb{F}_q}(Y) = k.$$

Hence an MRD code can be identified by the full-rank preservation of its generator matrix under premultiplication by any full-rank $k \times n$ matrix over the base field ([3] Lemma 2.2).

3.4. Gabidulin Codes

Let q be a prime power and $m, n, k \in \mathbb{N}$ with $k \leq n \leq m$ (since for Gabidulin codes, the code length n must not exceed the field extension degree m ($n \leq m$), and the dimension k must not exceed the length ($k \leq n$)) [3]. Choose

$$\alpha = (\alpha_1 \quad \alpha_2 \quad \cdots \quad \alpha_n) \in \mathbb{F}_q^{1 \times n}, \quad \text{with entries } \mathbb{F}_q\text{-linearly independent.} \quad (9)$$

For a q -linearised polynomial

$$P(x) = \sum_{i=0}^{k-1} a_i x^{[i]}, \quad x^{[i]} := x^{q^i}, \quad a_i \in \mathbb{F}_q, \quad (10)$$

define the evaluation map explicitly as a matrix:

$$\text{Ev}_\alpha(P) = \begin{pmatrix} P(\alpha_1) & P(\alpha_2) & \cdots & P(\alpha_n) \end{pmatrix} \in \mathbb{F}_q^{1 \times n}. \quad (11)$$

The *Gabidulin code* is then given by the set of matrix evaluations:

$$\text{Gab}_q(n, k, m) = \{\text{Ev}_\alpha(P) : \deg_q(P) < k\}, \quad (12)$$

forming an \mathbb{F}_q -linear $[n, k, d]_{q^m}$ code with parameters:

$$d = n - k + 1, \quad |\text{Gab}_q(n, k, m)| = q^{mk}. \quad (13)$$

Its generator matrix appears explicitly as a Moore (or σ -Vandermonde) matrix:

$$G_{\text{Gab}} = \begin{pmatrix} \alpha_1^{[0]} & \alpha_2^{[0]} & \cdots & \alpha_n^{[0]} \\ \alpha_1^{[1]} & \alpha_2^{[1]} & \cdots & \alpha_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{[k-1]} & \alpha_2^{[k-1]} & \cdots & \alpha_n^{[k-1]} \end{pmatrix} \in \mathbb{F}_q^{k \times n}. \quad (14)$$

Since G_{Gab} satisfies Lemma 1, $\text{Gab}_q(n, k, m)$ attains the Singleton-like bound and is an MRD code.

4. Theoretical Framework

This section lays out the foundations for using PSO to construct MRD codes. We first summarise PSO and then formulate code construction as a combinatorial optimisation problem.

4.1. Particle Swarm Optimisation

Particle swarm optimisation (PSO) is a population-based metaheuristic inspired by the collective motion of biological swarms [7,8]. A swarm of S particles explores the search space; particle i keeps track of its position \mathbf{x}_i , velocity \mathbf{v}_i , personal best \mathbf{p}_i , and the global best \mathbf{g} found so far.

The standard updates are

$$\mathbf{v}_i(t+1) = w \mathbf{v}_i(t) + c_1 r_{1,i}(t) (\mathbf{p}_i - \mathbf{x}_i(t)) + c_2 r_{2,i}(t) (\mathbf{g} - \mathbf{x}_i(t)), \quad (15)$$

$$\mathbf{x}_i(t+1) = \mathbf{x}_i(t) + \mathbf{v}_i(t+1), \quad (16)$$

where $r_{1,i}(t), r_{2,i}(t) \stackrel{\text{i.i.d.}}{\sim} \mathcal{U}(0,1)$ are independent scalars (or component-wise vectors) drawn anew each iteration, w is the inertia weight, and c_1, c_2 are the cognitive and social acceleration coefficients.

4.2. Problem Formulation

Let $[n, k, d]_{q^m}$ be the target parameters of an MRD vector code. We seek a generator matrix $G \in \mathbb{F}_q^{k \times n}$ such that the \mathbb{F}_q -linear code \mathcal{C} given by the generator-matrix form (2)-(3) attains minimum rank distance

$$d_{\min}(\mathcal{C}) = \min_{\mathbf{u} \in \mathbb{F}_q^k \setminus \{0\}} \text{rank}_{\mathbb{F}_q}(\Phi(G\mathbf{u})) \geq d, \quad (17)$$

where $\Phi: \mathbb{F}_{q^m}^n \rightarrow \mathbb{F}_q^{m \times n}$ is the fixed \mathbb{F}_q -linear isomorphism that converts each length- n vector over the extension field into its $m \times n$ matrix representation [3]. The rank in (17) is therefore taken over \mathbb{F}_q on this unfolded matrix.

To search for such a G we vectorise every $k \times n$ matrix into a particle position in $\mathbb{F}_q^{k \times n}$. The PSO fitness function is the left-hand side of (17), so particles with larger minimum rank distance are rewarded, guiding the swarm toward matrices that realise MRD codes.

4.3. Objective Function

To guide PSO we require a fitness that rewards generator matrices whose codes meet the MRD criterion. By (8), a linear rank-metric code is MRD precisely when its minimum rank distance attains the Singleton-like bound. Consequently we maximise that minimum distance.

Let $\Phi: \mathbb{F}_{q^m}^n \rightarrow \mathbb{F}_q^{m \times n}$ be the fixed \mathbb{F}_q -linear isomorphism used in (17). For a candidate generator matrix G we define

$$F(G) = \min_{\mathbf{u} \in \mathbb{F}_{q^m}^k \setminus \{0\}} \text{rank}_{\mathbb{F}_q}(\Phi(G\mathbf{u})). \quad (18)$$

The optimisation goal is $\max F(G)$ subject to $F(G) \geq d$. If this primary target is reached, secondary terms—such as larger generalised rank weights—may be added to the score to refine the search [17].

4.4. Search Space and Constraints

The search domain comprises all full-rank $k \times n$ matrices over \mathbb{F}_q . Constraint handling is enforced by **i- a penalty on particles with $F(G) < d$** and **ii- a repair routine that restores full rank if a velocity update introduces dependence**. Details are given in Section 5.

4.5. Representation and Initialisation

Each PSO particle encodes a generator matrix G (see (18)). Positions are initialised either purely at random or as low-rank perturbations of Gabidulin generators [8,15,16], ensuring broad coverage of the search space.

4.6. PSO Algorithm for MRD Code Construction

At every iteration the swarm updates velocities and positions via (15)–(16). After each move the fitness (18) is evaluated; personal and global bests are updated accordingly, steering the particles toward matrices that realise MRD codes.

This completes the theoretical basis. Section 5 turns the framework into a concrete PSO-guided construction algorithm.

5. Proposed PSO-Guided Construction Method

This section presents the proposed PSO-guided method for constructing MRD codes. The algorithm leverages PSO's global search capabilities to explore the space of rank-metric codes effectively.

5.1. Initialisation

The swarm starts with N particles, each encoding a candidate generator matrix $G^{(j)} \in \mathbb{F}_q^{k \times n}$ (particle $j = 1, \dots, N$). Two complementary strategies create a diverse yet feasible initial pool.

(i) Purely random sampling. For roughly half of the particles we draw each entry of G independently and uniformly from \mathbb{F}_q . Because rank-deficient matrices are unusable, we resample until $\text{rank}_{\mathbb{F}_q}(G) = k$. A convenient implementation is:

- Fix a normal basis $\{\beta, \beta^{[q]}, \dots, \beta^{[q^{m-1}]}\}$ of \mathbb{F}_q .
- Generate a random $k \times n$ array over \mathbb{F}_q .
- Map each m -tuple of \mathbb{F}_q -coefficients to the field element $\sum_{i=0}^{m-1} a_i \beta^{[q^i]} \in \mathbb{F}_q$.
- If the resulting matrix has full \mathbb{F}_q -rank, accept; otherwise repeat.

(ii) Perturbed Gabidulin seeds. The remaining particles are produced by adding a low-rank perturbation to a known Gabidulin generator matrix G_{Gab} :

$$G^{(j)} = G_{\text{Gab}} + R^{(j)}, \quad \text{rank}_{\mathbb{F}_q}(R^{(j)}) \leq r, \quad (19)$$

where $r \ll k$ (typically $r = 1$ or 2). Perturbations are generated by sampling $R^{(j)} = \mathbf{a}^{(j)} \mathbf{b}^{(j)\top}$ with random $\mathbf{a}^{(j)} \in \mathbb{F}_q^{k \times 1}$ and $\mathbf{b}^{(j)} \in \mathbb{F}_q^{n \times 1}$. This seeding injects useful structure while still encouraging exploration.

For every particle we assign a velocity matrix $\mathbf{v}^{(j)}(0) \in \mathbb{F}_q^{k \times n}$ by the same uniform procedure as in 5.1-(i), ensuring that the initial momentum is uncorrelated with the starting position.

Together, these two sampling schemes give the swarm a wide coverage of the search space while guaranteeing that every particle begins with a valid full-rank generator matrix.

5.2. Fitness Evaluation

Each particle is scored with the objective in (18). A particle is *feasible* if its minimum rank distance satisfies $F(G) \geq d$. Among feasible particles we break ties lexicographically:

- maximise $F(G)$ itself;
- subject to (a), maximise the second-smallest rank (a proxy for the second generalised rank weight);

- c. subject to (a)–(b), minimise the Hamming weight of the generator (promoting sparse descriptions).

The composite score is used both for personal–best and global–best updates, so the swarm is steered toward MRD codes and, secondarily, toward codes with stronger weight hierarchies.

5.3. Velocity and Position Update

Updates follow (15)–(16). Here $\mathbf{x}_i(t)$ is the vectorised form of a generator matrix and $\mathbf{v}_i(t)$ is a *difference matrix* of the same size.

Because additions in \mathbb{F}_q replace the usual Euclidean operations, the update $\mathbf{x}_i(t) + \mathbf{v}_i(t+1)$ is interpreted as component-wise field addition. The random coefficients $r_{1,i}, r_{2,i}$ modulate the probability that a given entry of \mathbf{v}_i is flipped; concretely, we draw $r_{1,i}, r_{2,i}$ from $\mathcal{U}(0, 1)$ and apply the corresponding term to each entry with that probability.

Matrix-level “velocity clamping” is enforced by limiting $\text{rank}_{\mathbb{F}_q}(\mathbf{v}_i(t)) \leq r_{\max}$, preventing excessively disruptive jumps.

5.4. Constraint Handling

Two complementary mechanisms keep the search inside the feasible region:

- Penalty.** If $F(G) < d$ we subtract $\lambda[d - F(G)]$ from the fitness, with an adaptive penalty weight λ that grows once every ten iterations.
- Repair.** After every position update we test $\text{rank}_{\mathbb{F}_q}(G)$. If $\text{rank} < k$ we replace the shortest set of dependent rows with random full-rank rows, repeating until full rank is restored.

This hybrid strategy keeps the swarm from stagnating on invalid matrices while allowing an occasional escape into promising infeasible regions.

5.5. Termination Criteria

The algorithm stops when any of the following holds:

- the iteration counter reaches T_{\max} ;
- a particle achieves $F(G) = d$ and all secondary criteria (a)–(c) in the fitness hierarchy;
- the global-best score has not improved for τ consecutive iterations, where $\tau \approx 0.1T_{\max}$.

These criteria balance run-time control with a high probability of discovering an MRD generator matrix.

5.6. Algorithm Summary

The proposed algorithm can be summarized as follows:

Algorithm 1 **PSO**-Guided MRD Code Construction

- 1: Initialize population of N particles (generator matrices).
 - 2: Evaluate fitness of each particle.
 - 3: **while** termination criteria not met **do**
 - 4: **for** each particle **do**
 - 5: Update velocity and position using PSO equations.
 - 6: Evaluate fitness of the updated particle.
 - 7: Update personal and global bests if improved.
 - 8: **end for**
 - 9: **end while**
 - 10: Return the best-found generator matrix.
-

The Python implementation of this algorithm over finite fields, using the *galois* library [18], is available in the GitHub repository, which includes both the source code and documentation. The repository can be accessed at https://github.com/behnamde/pso_mrd [19].

6. Discussion

The proposed PSO-guided construction method offers a metaheuristic route to discovering maximum-rank-distance codes by exploiting the global-search capabilities of particle swarm optimisation (PSO). In contrast to purely algebraic methods—such as Gabidulin’s construction—that rely on explicit theoretical derivations, PSO provides a flexible, data-driven framework that can be applied even when no closed-form constructions are known.

6.1. Advantages of the PSO Approach

- **Generality:** The algorithm is applicable to a broad range of MRD parameters, including regimes beyond classical Gabidulin families.
- **Scalability:** Larger dimensions can be tackled by increasing the swarm size or by tuning the fitness-evaluation schedule.
- **Adaptability:** Domain insight—e.g. seeding particles with Gabidulin-like structures—can be injected seamlessly to accelerate convergence.
- **Exploratory power:** The population nature of PSO balances exploration and exploitation, a desirable trait for navigating highly irregular search landscapes.

6.2. Limitations and Challenges

- **Curse of dimensionality:** The search space grows exponentially with the generator-matrix size, making convergence slower for large instances.
- **Expensive fitness:** Computing the minimum rank distance for every particle is costly, especially when k or m is large.
- **No optimality guarantee:** PSO finds high-quality—but not provably optimal—solutions; post-processing heuristics may be required.
- **Initialization sensitivity:** Swarm quality depends heavily on the diversity and structure of the initial population.

6.3. Future Work

- **Hybrid heuristics:** Combine PSO with algebraic insights or other metaheuristics (e.g., genetic algorithms) to improve robustness.
- **Richer fitness:** Incorporate generalised rank weights or decoding complexity into the objective.
- **Parallelisation:** Leverage GPUs and distributed architectures to accelerate particle updates and fitness checks.
- **Applications:** Deploy the discovered codes in network coding, cryptography, and distributed storage to assess real-world gains.
- **Quantum computation:** Investigate quantum-inspired PSO variants and explore how MRD codes can support quantum error-correction or other quantum-information tasks.

7. Conclusion

We have framed MRD-code construction as a combinatorial optimisation problem and introduced a PSO-based algorithm to explore the corresponding search space of generator matrices. By harnessing PSO’s balance of exploration and exploitation, our method can recover MRD codes in parameter regimes where traditional algebraic constructions are unavailable or unwieldy.

Although promising, the approach still faces scalability bottlenecks and relies on carefully crafted fitness functions. Ongoing work will integrate algebraic structure more deeply into the PSO update rules, refine constraint-handling strategies, and benchmark the resulting codes in practical settings.

Overall, this study shows that metaheuristic techniques such as PSO can complement algebraic theory and open new pathways for advancing rank-metric coding. Continued research along these lines is likely to yield further insights and expand the toolbox for modern coding-theory applications.

References

1. Delsarte, P. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A* **1978**, *25*, 226–241. [https://doi.org/10.1016/0097-3165\(78\)90015-8](https://doi.org/10.1016/0097-3165(78)90015-8).
2. Gabidulin, E.M. Theory of codes with maximum rank distance. *Problems of Information Transmission* **1985**, *21*, 1–12.
3. Gabidulin, E.M. *Rank Codes*; TUM.University Press: Technical University of Munich, Arcisstrasse 21, 80333 Munich, 2021. Translated by Vladimir Sidorenko. Layout design, typesetting, and cover design by Vladimir Sidorenko and Caroline Ennemoser., <https://doi.org/10.14459/2021md1601193>.
4. Sheekey, J. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications* **2016**, *10*, 475–488. <https://doi.org/10.3934/amc.2016019>.
5. Bartoli, D.; Giulietti, M.; Marino, G.; Polverino, O. Maximum Scattered Linear Sets and Complete Caps in Galois Spaces. *Combinatorica* **2015**, *38*, 255–278. <https://doi.org/10.1007/s00493-016-3531-6>.
6. Alfarano, G.N.; Neri, A.; Zullo, F. Maximum Flag-Rank Distance Codes. *arXiv preprint arXiv:2303.16653* **2023**. <https://doi.org/10.48550/arXiv.2303.16653>.
7. Kennedy, J.; Eberhart, R. Particle swarm optimization. In Proceedings of the Proceedings of ICNN'95-International Conference on Neural Networks. IEEE, 1995, Vol. 4, pp. 1942–1948. <https://doi.org/10.1109/ICNN.1995.488968>.
8. van Zyl, J.P.; Engelbrecht, A.P. Set-Based Particle Swarm Optimisation: A Review. *Mathematics* **2023**, *11*, 2980. <https://doi.org/10.3390/math11132980>.
9. Hamming, R.W. Error Detecting and Error Correcting Codes. *The Bell System Technical Journal* **1950**, *29*, 147–160. <https://doi.org/10.1002/j.1538-7305.1950.tb00463.x>.
10. Kshevetskiy, A.; Gabidulin, E. The new construction of rank codes. In Proceedings of the Proceedings. International Symposium on Information Theory, 2005. ISIT 2005., 2005, pp. 2105–2108. <https://doi.org/10.1109/ISIT.2005.1523717>.
11. Csajbók, B.; Marino, G.; Polverino, O.; Zullo, F. Maximum scattered linear sets and MRD-codes. *Journal of Algebraic Combinatorics* **2017**, *46*, 193–213. <https://doi.org/10.1007/s10801-017-0762-6>.
12. Bartoli, D.; Csajbók, B.; Montanucci, M. On a conjecture about maximum scattered subspaces of $\mathbb{F}_{q^6} \times \mathbb{F}_{q^6}$. *arXiv preprint* **2021**. <https://doi.org/10.48550/arXiv.2004.13101>.
13. Sheekey, J. MRD Codes: Constructions and Connections. In *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications*; Schmidt, K.U.; Winterhof, A., Eds.; Radon Series on Computational and Applied Mathematics, De Gruyter, 2019. <https://doi.org/10.48550/arXiv.1904.05813>.
14. Csajbók, B.; Marino, G.; Polverino, O.; Zhou, Y. MRD codes with maximum idealizers. *Discrete Mathematics* **2020**, *343*, 111985. <https://doi.org/https://doi.org/10.1016/j.disc.2020.111985>.
15. Cuéllar, M.P.; Gómez-Torrecillas, J.; Lobillo, F.J.; Navarro, G. Genetic algorithms with permutation-based representation for computing the distance of linear codes. *arXiv preprint* **2020**. <https://doi.org/10.48550/arXiv.2002.12330>.
16. Azouaoui, A.; Belkasmi, M. Efficient Dual Domain Decoding of Linear Block Codes Using Genetic Algorithms. *Journal of Electrical and Computer Engineering* **2012**. <https://doi.org/10.1155/2012/503834>.
17. Lunardon, G.; Trombetti, R.; Zhou, Y. Generalized twisted Gabidulin codes. *Journal of Combinatorial Theory, Series A* **2018**, *159*, 79–106. <https://doi.org/https://doi.org/10.1016/j.jcta.2018.05.004>.
18. Hostetter, M. *Galois: A performant NumPy extension for Galois fields*, 2020. GitHub repository containing implementation and documentation. Available at <https://github.com/mhostetter/galois>.
19. Dehghani, B. *PSO-Guided Construction of MRD Codes in Rank Metric*, 2025. GitHub repository containing implementation and documentation. Available at https://github.com/behnamde/pso_mrd.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.