Constructing MRD codes by switching

Minjia Shi1 | Denis S. Krotov2 | Ferruh Özbudak3

1Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, Anhui, China
2Sobolev Institute of Mathematics, Novosibirsk, Russia
3Faculty of Engineering and Natural Sciences, Sabancı University, Istanbul, Turkey

Correspondence
Minjia Shi, Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, Anhui 230601, China.
Email: smjwcl.good@163.com

Funding information
the National Natural Science Foundation of China, Grant/Award Number: 12071001; the Sobolev Institute of Mathematics, Grant/Award Number: FWFN-2022-0017; the METU Scientific Research Projects Coordination Unit, Grant/Award Number: GAP-101-2021

Abstract
Maximum rank-distance (MRD) codes are (not necessarily linear) maximum codes in the rank-distance metric space on $m$-by-$n$ matrices over a finite field $\mathbb{F}_q$. They are diameter perfect and have the cardinality $q^{m(n-d+1)}$ if $m \geq n$. We define switching in MRD codes as the replacement of special MRD subcodes by other subcodes with the same parameters. We consider constructions of MRD codes admitting switching, such as punctured twisted Gabidulin codes and direct-product codes. Using switching, we construct a huge class of MRD codes whose cardinality grows doubly exponentially in $m$ if the other parameters ($n$, $q$, the code distance) are fixed. Moreover, we construct MRD codes with different affine ranks and aperiodic MRD codes.

KEYWORDS
bilinear forms graph, MRD codes, rank distance, switching

AMS CLASSIFICATION
94B25

1 | INTRODUCTION

Maximum rank-distance (MRD) codes are a rank-metric analog of MDS (i.e., attaining the Singleton bound) codes in the Hamming metric or index-1 orthogonal arrays. Unlike MDS codes, MRD codes are shown to exist for all code distances and all parameters of the rank-metric space. The first such codes were constructed by Delsarte [7] and later by Gabidulin [10], who further developed the theory of rank-metric codes, see [11]. Much of the literature refers to that first class of MRD codes as Gabidulin codes.

In [5], de la Cruz et al. studied the algebraic structure of linear MRD codes, explained the automorphism group and asked whether one can construct an MRD code that is not equivalent...
to a Gabidulin code (in particular, in the full-rank case $d = n = m$ they showed their connection with quasi-fields and spreads and hence they proved the existence of such codes). In ALCOMA‘2015 conference, two groups solved this problem independently. Otal and Özbudak [23] solved this problem for some specific parameters. Sheekey [29] solved the problem for a larger class of parameters. Both solutions have similar ideas. In [24], these results were extended to additive MRD codes. Constructions of nonadditive MRD codes can be found in [4, 8, 25]. Actually, there are other constructions for linear MRD codes; the most recent survey is due to Sheekey [30].

Almost all known constructions are for $n$-by-$n$ MRD (and mainly for linear) codes. For $m$-by-$n$ MRD codes for $m \neq n$, the main technique is a kind of puncturing; nice exceptions are the interleaving construction, see for example, [31], and the construction of $m \times (n + 1)$ MRD codes with minimum rank distance $n - h$ from so-called maximum $h$-scattered $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$, see [35] and references there. For nonlinear MRD codes, there are only a few sporadic constructions (like in [25]). We should also mention a very special case, the $m$-by-2 MRD codes over $\mathbb{F}_2$, which are equivalent to the transversals in the Cayley table of the group $\mathbb{Z}_2^m$ (for a survey on transversals of Latin squares, see [34]). The number of such objects is rather well studied [9, theorem 7.2] and applied in other combinatorial problems [27].

In the current paper, we construct nonlinear MRD codes using switching. Switching technique for codes and designs is well known and based on changing a part of the code (design) in such a way that the parameters do not change. Some special cases of switching, see, for example, [22], are constructive and are used effectively in both computational and theoretical studies. However, the general switching approach does not specify how to find changeable parts of codes and needs to be concretized for each class of codes, which can be done in different ways and result in a variety of techniques. We use the switching technique close to that for MDS codes studied in [26]. The key of the approach is the possibility to switch MRD subcodes of a given MRD code, if such subcodes exist. We study known constructions of MRD codes for the existence of such subcodes and propose variations of the constructions with subcodes of different parameters. Starting with these codes and applying switching, we construct a large variety of MRD codes, including codes with different values of characteristics of nonlinearity, such as the affine rank and the dimension of the kernel.

The structure of the paper is as follows. The next section contains definitions and preliminary results; in particular, we describe switching MRD subcodes in MRD codes. For such switching to be possible, we need MRD codes with MRD subcodes. Such codes are considered in Sections 3 and 4, which use different techniques and can be read independently from each other. Section 3 deals with twisted Gabidulin codes and shows that under certain conditions, they admit MRD subcodes. In Section 4, we consider a variant of the Cartesian product for MRD codes, which also provides a family of codes admitting switching. Sections 5 and 6 contain important corollaries: a lower bound on the number of MRD codes and the possibility to construct MRD codes with different affine ranks and MRD codes with trivial kernels. Section 7 concludes the article.

2 | PRELIMINARIES

The vertex set of the bilinear forms graph $B_q(m, n)$ is the set of $m \times n$ matrices over $\mathbb{F}_q$; two vertices $X$ and $Y$ are adjacent in $B_q(m, n)$ if and only if rank($Y - X$) = 1. The minimum-path distance in $B_q(m, n)$ coincides with the rank distance $d(X, Y) = \text{rank}(Y - X)$, and the
corresponding metric space is known as the rank metric space; we also denote it by $B_q(m, n)$ in this paper. We assume $n \leq m$, so the diameter of $B_q(m, n)$ is $n$. The all-zero matrix, the size of which is always clear from the context, is denoted by $0$.

If $n < m$, then the isometry group $\text{Aut}(B_q(m, n))$ of the rank metric space (automorphism group of the bilinear forms graph) $B_q(m, n)$ is the product of $\text{GL}(m)$ (multiplication by nonsingular $m \times m$ matrices in the left), $\mathbb{F}_q^{m+1}$ (translations, addition of $m \times n$ matrices), and $\text{Aut}(\mathbb{F}_q)$ (field automorphism, acting simultaneously in all $mn$ entries of the matrix), see for example, [2, th. 9.5.1]. Taking into account that the instances of $\text{GL}(m)$ and $\text{GL}(n)$ above intersect in a subgroup isomorphic to $\mathbb{F}_q^\times$ (multiplication by a nonzero scalar), the order of $\text{Aut}(B_q(m, n))$ is

$$[m]_q! \cdot [n]_q! \cdot (q - 1)^{n+m-1} \cdot q^{m+1} \cdot \log_p q,$$

where $[m]_q! = \prod_{i=0}^{m-1} (q^i - 1)$ and $p$ is the prime divisor of $q$. In the case $m = n$, $\text{Aut}(B_q(m, n))$ also includes the matrix transposition.

**Definition 2.1** ($n'$-anticode). If, for $n' < n$, we fix (say, by 0s) the values of the elements in $n - n'$ columns, then we obtain a set of $q^{mn'}$ matrices that induces a subspace isometric to (a subgraph isomorphic to) $B_q(m, n')$. This set is a maximum set of diameter $n'$ in $B_q(m, n)$ (see Lemma 2.3 below), and it will be called an $n'$-anticode, as well as any other set that is equivalent to it under $\text{Aut}(B_q(m, n))$. Note that since $\text{Aut}(B_q(m, n))$ contains translations, an $n'$-anticode does not necessarily contain $0$.

**Remark 2.2.** In the literature related to the code–anticode bound, “an anticode” usually means “a set of diameter not larger than the given constant.” By $n'$-antcodes, defined above, we mean a special explicit class of antcodes of diameter $n'$, which is sufficient for our purposes. We do not imply that there are no other maximum sets (antcodes, in the general meaning) of diameter $n'$. It is known [19] that any linear or affine maximum set of diameter $n'$ is an $n'$-anticode according to our definition (or the transpose of an $n'$-anticode if $m = n$), but for unrestricted sets the similar characterization has not been proven, according to the author’s knowledge.

**Lemma 2.3.** An $n'$-anticode is a maximum set of diameter $n'$ in $B_q(m, n)$, $n' < n$. Moreover, every two vertices at a distance at most $n'$ from each other are included in at least one $n'$-anticode.

**Proof.** Since a matrix with $n', n' < n$, non-zero rows has rank at most $n'$, the diameter of an $n'$-anticode is $n'$.

The cardinality of an $n'$-anticode is obviously $q^{mn'}$.

The Delsarte code–anticode bound [6, theorem 3.9] says that if $C$ is a distance-$d$ code and $A$ is a set of a diameter smaller than $d$, then $|C| \cdot |A|$ cannot be larger than the space size (the graph order) $q^{mn}$. Since codes of distance $n' + 1$ and cardinality $q^{mn} / q^{mn'}$ exist, for example, Gabidulin codes [10], we conclude that $n'$-antcodes defined above are maximum sets of diameter $n'$.
To prove the last claim of the lemma, assume that two vertices $X$ and $Y$ are at distance at most $n'$ from each other. This means that their difference $Z = Y - X$ has rank at most $n'$. By a nonsingular linear transformation $\varphi$ of the row space, $Z$ can be converted to a matrix with zero last $n - n'$ columns. By definition, the set $A$ of all matrices with zero last $n - n'$ columns is an $n'$-anticode; moreover, it contains $\varphi(Z)$ and the all-zero matrix $0$. Now, $\varphi^{-1}(A) + X$ is an $n'$-anticode containing both $X$ and $Y$.

**Definition 2.4** (MRD code). A set $C$ of vertices of $B_q(m, n)$, $n \leq m$, is called a distance-$d$ MRD code (maximum rank-distance code) if $|C \cap A| = 1$ for every $(d - 1)$-anticode $A$.

By the definition, every MRD code is a diameter-perfect code, according to [1]. The following simple theorem shows that Definition 2.4 is equivalent to the classic definition of MRD codes. It is worth noting that although our definition of MRD codes is not standard, it is not actually an innovation to define optimal codes in a “design manner.” For example, $e$-perfect codes are often defined as intersecting every radius-$e$ ball (in the ambient metric space) in exactly one point, rather than to define them by the code distance and cardinality.

**Theorem 2.5** (Equivalent definition). A code $C$ in $B_q(m, n)$, is a distance-$d$ MRD code if and only if $|C| = q^{m(n-d+1)}$ and the rank distance between any two codewords from $C$ is at least $d$.

**Proof.** Consider a code $C$ of cardinality $q^{m(n-d+1)}$ and minimum distance-$d$ between codewords. Consider an arbitrary $(d - 1)$-anticode $A$. By the definition, $A$ is a coset of some linear $(d - 1)$-anticode $A_0$ of dimension $m(d - 1)$. The whole space is partitioned into $q^{m(n-d+1)}$ cosets of $A_0$, each of which is a $(d - 1)$-anticode by definition. Since the diameter of a $(d - 1)$-anticode is $d - 1$ and the code distance of $C$ is $d$, we see that a $(d - 1)$-anticode cannot contain more than 1 codeword of $C$. On the other hand, the cardinality of $C$ coincides with the number of cosets of $A_0$, and we conclude that every coset of $A_0$ contains exactly one element of $C$. In particular, $|C \cap A| = 1$, and $C$ is an MRD code by the definition.

Now consider an MRD code $C$. If $C$ contains two different codewords at distance less than $d$ from each other, then by Lemma 2.3 there is a $(d - 1)$-anticode $A$ containing these two codewords. In particular, $|C \cap A| \geq 2$, which contradicts the definition of an MRD code. Hence, the distance between codewords of $C$ is not less than $d$. It remains to confirm the cardinality. Consider a linear $(d - 1)$-anticode $A_0$ and the partition of the space into its cosets. By definition, $C$ has exactly 1 codeword in every coset (which is also a $(d - 1)$-anticode); hence $|C|$ is the number of cosets, that is, $q^{m(n-d+1)}$.

**Lemma 2.6.** Let $S$ be the set of $q^{m' n}$ matrices of $B_q(m, n)$ with fixed $m - m'$ rows, $n \leq m' \leq m$ (so, the induced metric space (graph) is $B_q(m', n)$). For every $n'$-anticode $B$, $n' < n$, the set $B \cap S$ is either empty or an $n'$-anticode in the graph $B_q(m', n)$ induced by $S$.

**Proof.** If $m' = m$, then the claim is trivial because $B \cap S = B$.

If $n \leq m' < m$, then $B_q(m, n)$ does not admit a matrix-transposition automorphism. In particular, up to a nonsingular linear transformation of the row space (note that this transformation fixes $S$), we can assume that the $n'$-anticode $B$ is obtained by fixing the values in $n - n'$ columns. The claim is now also trivial.
Theorem 2.7 (Switching MRD). Let $S$ be the set of $q^{m'n}$ matrices of $B_q(m, n)$ with fixed (say, by 0s) values in $m - m'$ rows, $n \leq m' \leq m$. Assume that $C$ is a distance-$d$ MRD code in $B_q(m, n)$ such that $|S \cap C| = q^{m'(n-d+1)}$ (i.e., $S \cap C$ is MRD in $B_q(m', n)$). Then for every other distance-$d$ MRD code $R$ in $B_q(m', n)$ (corresponding to $S$), the set

$$C_R := (C \setminus (S \cap C)) \cup R = (C \setminus S) \cup R$$

is a distance-$d$ MRD code in $B_q(m, n)$ (obtained by switching).

**Proof.** We consider a $(d - 1)$-anticode $M$. By the definition of MRD codes, $|M \cap C| = 1$. If $M \cap S = \emptyset$, then $M \cap C_R = M \cap C$ and so $|M \cap C_R| = 1$ as well. Otherwise, by Lemma 2.6 $M \cap S$ is a $(d - 1)$-anticode in $B_q(m', n)$. Since $S \cap C$ is MRD in $B_q(m', n)$, we have $|(M \cap S) \cap (C \cap S)| = 1$, and hence $M \cap C = (M \cap S) \cap (C \cap S)$. After replacing $(C \cap S)$ by $R$, we get $M \cap C_R = (M \cap S) \cap R$. Since $R$ is MRD in $B_q(m', n)$, the last intersection consists of a single vertex, and hence $|M \cap C_R|$ is also 1. By the definition, $C_R$ is MRD. □

Remark 2.8. Considering the subcode with some fixed values in some fixed rows (or columns) is similar to the operation known as shortening for codes in the Hamming metric space. So the main condition in the theorem above can be informally treated as follows: the code $C$ can be row-shortened to a distance-$d$ MRD code in $B_q(m', n)$.

In the next two sections, we consider constructions of MRD codes that satisfy the hypothesis of Theorem 2.7 and hence admit switching.

3 | Gabidulin-like Codes with Gabidulin-like Subcodes

In this section, we construct MRD codes with MRD subcodes in the class of punctured twisted Gabidulin codes. We provide two constructions (Constructions 3.1 and 3.4) and related results, which, in particular, explain the limitations and advantages of the constructions. We begin with a paragraph aiming to illustrate the main idea by a special case of classic Gabidulin codes, without using a more advanced technique related to the representation of matrices by linearized polynomials.

Let $n, m', m, k$ be positive integers such that $0 < k \leq n \leq m' < m$. In the classical construction of Gabidulin codes, the columns of $m'$-by-$n$ matrices over $\mathbb{F}_q$ are identified with elements of the field $\mathbb{F}_{q^m}$, written in some fixed basis over $\mathbb{F}_q$. The Gabidulin MRD code $C'$ of distance $d = n - k + 1$ in $B_q(m', n)$ is defined as the linear span, over $\mathbb{F}_{q^m}$, of the $k$ vectors $(g_{1i}, g_{2i}, \ldots, g_{ni})$, $i = 0, \ldots, k - 1$, where $g_i, \ldots, g_n$ is an arbitrary collection of $n$ linearly independent (over $\mathbb{F}_q$) elements of $\mathbb{F}_{q^m}$. If we define another Gabidulin code $C$ as the span of the same basis over the larger field $\mathbb{F}_{q^m}, \mathbb{F}_{q^m} \subset \mathbb{F}_{q^{m'}}$, then we have $C' \subset C$. With a properly chosen basis of $\mathbb{F}_{q^m}$, the code $C$ satisfies the hypothesis of Theorem 2.7, which shows that $m$-by-$n$ Gabidulin codes admit switching if $m$ has a proper divisor $m'$ such that $m' \geq n$. 
To describe more general constructions, we recall the definition of the following two functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$:

\[
\begin{align*}
\text{Norm}_{q^m/q}(x) &= x \cdot x^q \cdot \cdots \cdot x^{q^{m-1}} = x^{q^{m-1}}, \\
\text{Trace}_{q^m/q}(x) &= x + x^q + \cdots + x^{q^{m-1}}.
\end{align*}
\]

**Construction 3.1.** Let $n$, $m_1$, $m$, and $d$ be positive integers such that $2 \leq d \leq n \leq m_1 < m$ and $m|m_1$. Let $W_1 \subseteq \mathbb{F}_{q^m}$ be the kernel of the $\mathbb{F}_{q^m}$-linear map $\text{Trace}_{q^m/q} : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$. Note that $\dim_{\mathbb{F}_q}W_1 = m - m_1$. Let $W, W_1 \subseteq W \subseteq \mathbb{F}_{q^n}$, be an $\mathbb{F}_q$-linear intermediate subspace such that $\dim W = m - n$. Put $A(x) = \prod_{w \in W}(x - w) = x^{q^{m-n}} + \text{m.o.t.} + \alpha_0 x$, where $\text{m.o.t.}$ stands for middle-order terms here and throughout the paper. Let $\eta \in \mathbb{F}_{q^m}$ such that $\text{Norm}_{q^m/q}(\alpha_0) \neq (-1)^{m(m-d+1)}(\text{Norm}_{q^m/q}(\eta))^{\frac{m}{2}}$. Let

\[\mathcal{P}(W, \eta) = \{A(x) \circ (a_0 x + a_1 x^q + \cdots + a_{n-d} x^{q^{n-d}} + \eta a_0 x^{q^{n-d+1}}) : a_0, a_1, \ldots, a_{n-d} \in \mathbb{F}_{q^n}\}.\]

Here and throughout the paper $\circ$ stands for the functional composition. Let $\mathcal{P}_0(W, W_1, \eta)$ be the $\mathbb{F}_q$-linear subspace of $\mathcal{P}(W, \eta)$ defined as

\[\mathcal{P}_0(W, W_1, \eta) = \{A(x) \circ (a_0 x + a_1 x^q + \cdots + a_{n-d} x^{q^{n-d}} + \eta a_0 x^{q^{n-d+1}}) : a_0, a_1, \ldots, a_{n-d} \in \mathbb{F}_{q^n}\}.\]

$\mathcal{P}(W, \eta)$ corresponds to a punctured MRD Gabidulin twisted code and $\mathcal{P}_0(W, W_1, \eta)$ corresponds to an MRD subcode of it as explained in Theorem 3.2 below. In particular, the code $C = \mathcal{P}(W, \eta)$ satisfies the hypothesis of Theorem 2.7 and can be used for the construction of new MRD codes by switching.

In the following theorem, we prove that MRD codes from Construction 3.1 satisfy the hypothesis of Theorem 2.7 and hence admit switching.

**Theorem 3.2.** We keep the notation and assumptions of Construction 3.1. We choose an ordered basis $(e_1, \ldots, e_m)$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that the last $m - m_1$ entries form a basis of $W_1$ over $\mathbb{F}_q$. Note that $\text{Im}(A)$ is an $\mathbb{F}_q$-linear subspace of dimension $n$ in $\mathbb{F}_{q^n}$. We choose an ordered basis $(f_1, \ldots, f_n)$ of $\text{Im}(A)$ over $\mathbb{F}_q$. We note that both $\mathcal{P}(W, \eta)$ and $\mathcal{P}_0(W, W_1, \eta)$ depend on the given integer $2 \leq d \leq n$.

For each $L \in \mathcal{P}(W, \eta)$, let $M(L)$ denote the $m \times n$ matrix representing the evaluation map $L : \mathbb{F}_{q^m} \to \text{Im}(A)$ defined as $x \mapsto L(x)$ with respect to the bases $(e_1, \ldots, e_m)$ and $(f_1, \ldots, f_n)$. Let $C(W, \eta)$ be the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^{mn}}$ consisting of $M(L)$ as $L$ runs through $\mathcal{P}(W, \eta)$. Similarly, let $C_0(W, W_1, \eta)$ be the $\mathbb{F}_q$-linear subspace of $C(W, \eta)$ consisting of $M(L)$ as $L$ runs through $\mathcal{P}_0(W, W_1, \eta)$.

Then we have the following:

- $C(W, \eta)$ is an MRD code of minimum rank distance $d$. 


• If $M \in C_0(W, W_1, \eta)$, then the last $m - m_1$ rows of $M$ are the zero rows. Considering $C_0(W, W_1, \eta)$ in $\mathbb{F}_q^{m \times n}$ by ignoring the last $m - m_1$ zero rows, we obtain an MRD code of minimum rank distance $d$.

Proof. Let $a_0, a_1, ..., a_{n-d} \in \mathbb{F}_q^n$, not all zero. As $A(x) = x^{q^{m-n}} + \alpha_{m-n-1}x^{q^{m-n-1}} + \text{m.o.t.} + \alpha_0x$, by definition of functional composition, we have that $A(x) \circ (a_0x + a_1x^q + \cdots + a_{n-d}x^{q^{n-d}} + \eta a_0x^{q^{n-d+1}})$ is equal to

$$
\eta^{q^{m-n}}a_0^{q^{m-n}}x^{q^{n-d}+1} + \left(a_0^{q^{n-d}} + \alpha_{m-n-1} \eta a_0^{q^{m-n-1}} a_0^{q^{m-n}}\right)x^{q^{n-d}} + \text{m.o.t.} + \alpha_0 a_0x. \quad (1)
$$

Note that $A(x) \circ (a_0x + a_1x^q + \cdots + a_{n-d}x^{q^{n-d}} + \eta a_0x^{q^{n-d+1}})$ is an additive polynomial and its solution set in $\mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear subspace. Using $(1)$ and [12], we conclude that its solution set has dimension at most $m - d$ over $\mathbb{F}_q$. This implies that the corresponding evaluation map has rank at least $d$. Note that $\dim_{\mathbb{F}_q} C(W, \eta) = \dim_{\mathbb{F}_q} \mathcal{P}(W, \eta)$ by definition. Moreover, if $a_0, a_1, ..., a_{n-d} \in \mathbb{F}_q^n$, then the polynomial $A(x) \circ (a_0x + a_1x^q + \cdots + a_{n-d}x^{q^{n-d}} + \eta a_0x^{q^{n-d+1}})$ has degree at most $q^{m-n+n-d+1} = q^{m-d} < q^m$. This implies that, for $a_0, b_0, a_1, b_1, ..., a_{n-d}, b_{n-d} \in \mathbb{F}_q^n$, the corresponding mappings defined by $A(x) \circ (a_0x + a_1x^q + \cdots + a_{n-d}x^{q^{n-d}} + \eta a_0x^{q^{n-d+1}})$ and $A(x) \circ (b_0x + b_1x^q + \cdots + b_{n-d}x^{q^{n-d}} + \eta b_0x^{q^{n-d+1}})$ are the same if and only if $a_0 = b_0$, $a_1 = b_1$, ..., $a_{n-d} = b_{n-d}$. Consequently, we have $\dim_{\mathbb{F}_q} C(W, \eta) = \dim_{\mathbb{F}_q} \mathcal{P}(W, \eta) = m(n - d + 1)$. We conclude that $C(W, \eta)$ is an MRD code of minimum rank distance $d$ in $\mathbb{F}_q^{m \times n}$.

Put $A_1(x) = \text{Trace}_{q^n/q^m}(x)$. We have the property that $A_1(\alpha x) = \alpha A_1(x)$ for any $\alpha \in \mathbb{F}_q^n$. We also have the property that $A_1(x^q) = A_1(x)^q$ for any $x \in \mathbb{F}_q^n$. Using [21], we obtain that there exists an $\mathbb{F}_q$-linear polynomial $B(x) \in \mathbb{F}_q[x]$ such that $A(x) = B(x) \circ A_1(x)$. Hence, for $a_0, a_1, ..., a_{n-d} \in \mathbb{F}_q^n$ and $w_1 \in W_1$ we obtain that

$$
A_1\left(a_0 w_1 + a_1 w_1^q + \cdots + a_{n-d} w_1^{q^{n-d}} + \eta a_0 w_1^{q^{n-d+1}}\right) = a_0 A_1(w_1) + a_1 A_1(w_1)^q + \cdots + a_{n-d} A_1(w_1)^{q^{n-d}} + \eta a_0 A_1(w_1)^{q^{n-d+1}} = 0.
$$

Note that $\dim_{\mathbb{F}_q} \mathcal{P}_0(W, W_1 \eta) = m_1(n - d + 1)$. We conclude that $C_0(W, W_1, \eta)$ is an MRD code of minimum rank distance $d$ when considered in $\mathbb{F}_q^{m_1 \times n}$.

In some cases, it is impossible to generalize Construction 3.1 directly to the situation $m_1 \not\mid m$ in some cases. Namely, we have the following proposition.

**Proposition 3.3.** As in Construction 3.1, apart from the statement $m_1 
 m$, we have similar assumptions, but for some special parameters as follows. Namely, let $n$, $m_1$, $m$ be positive integers such that $n = m_1 < m$, $m_1 \mid m$, and let $d = n$. Let $W \subseteq \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear subspace such that $\dim_{\mathbb{F}_q} W = m - n$. Put $A(x) = \prod_{w \in W} (x - w) = x^{q^{m-n}} + \text{m.o.t.} + \alpha_0 x$.

Let $\eta \in \mathbb{F}_q^n$ such that $\text{Norm}_{q^n/q}(\eta) \not\in \{-1\}^m \cup \{-1\}^m \text{Norm}_{q^n/q}(\alpha_0)$. Let $\mathcal{P}(W, \eta) = \{A(x) \circ (a_0 x + \eta a_0 x^q) : a_0 \in \mathbb{F}_q^n\}$.
Let \((e_1, ..., e_m)\) be an ordered basis of \(\mathbb{F}_q^n\) over \(\mathbb{F}_q\). Let \((f_1, ..., f_n)\) be an ordered basis of \(\text{Im}(A)\) over \(\mathbb{F}_q\). Provided that these bases are chosen, for each \(L \in \mathcal{P}(W, \eta)\), let \(M(L)\) denote the \(m \times n\) matrix representing the evaluation map \(L : \mathbb{F}_q^n \rightarrow \text{Im}(A)\) defined as \(x \mapsto L(x)\) with respect to the bases \((e_1, ..., e_m)\) and \((f_1, ..., f_n)\). Let \(C(W, \eta)\) be the \(\mathbb{F}_q\)-linear subspace of \(\mathbb{F}_q^{m \times n}\) consisting of \(M(L)\) as \(L\) runs through \(\mathcal{P}(W, \eta)\).

Then we have the following:

- For any choice of \((e_1, ..., e_m)\), the set \(C(W, \eta)\) is an MRD code of minimum rank distance \(d\).
- Recall that \(d = m_1\). It is impossible to choose an ordered basis \((e_1, ..., e_m)\) and a suitable \(\mathbb{F}_q\)-linear subspace \(C_0(W, \eta)\) of \(C(W, \eta)\) such that the last \(m - m_1\) rows of each matrix in \(C_0(W, \eta)\) are the zero rows and ignoring the last \(m - m_1\) zero rows, \(C_0(W, \eta)\) becomes an MRD code of minimum rank distance \(d\).

**Proof.** The proof of the first item is similar to that of Theorem 3.2. It remains to prove the second item. Assume the contrary and let \((e_1, ..., e_m)\) be such an ordered basis. Let \(W_1\) be the \(\mathbb{F}_q\)-span of the last \(m - m_1\) entries in the ordered basis \((e_1, ..., e_m)\). Note that \(\dim_{\mathbb{F}_q} W_1 = m - m_1\).

Let \(\Psi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n\) be the map \(x \mapsto x + \eta x^d\). As \(\text{Norm}_{\mathbb{F}_q}(\eta) \neq (-1)^m\), using [12], we conclude that \(\Psi\) is a permutation. Put \(\tilde{W}_1 = \{w_1 + \eta w_1^d : w_1 \in W_1\}\); we have \(\dim_{\mathbb{F}_q} \tilde{W}_1 = m - m_1\).

As we ignore the last \(m - m_1\) rows, \(n = m_1\), and \(d = m_1\), the code \(C_0(W, \eta)\) becomes an MRD code on \(m_1 \times m_1\) matrices of minimum rank distance \(m_1\). Using the Singleton-like bound, we get \(\dim_{\mathbb{F}_q} C_0(W, \eta) = m_1(m_1 - m_1 + 1) = m_1\).

Let \(S\) be the subset of \(\mathbb{F}_q^n\) consisting of the elements \(a_0\) such that \(A(x) \circ (a_0(x + \eta x^d))\) corresponds to a matrix in \(C_0(W, \eta)\). Note that there is an \(\mathbb{F}_q\)-linear isomorphism between \(S\) and \(C_0(W, \eta)\). Therefore \(S\) is an \(\mathbb{F}_q\)-linear space with \(\dim_{\mathbb{F}_q} S = m_1\). Moreover let \(a_0 \in S \setminus \{0\}\). Then by the definition of \(W_1\), the evaluation of the additive polynomial \(A(x) \circ (a_0(x + \eta x^d))\) at \(w_1\) is zero for all \(w_1 \in W_1\). This means that \(a_0(w_1 + \eta w_1^d)\) is a root of the polynomial \(A(x)\) for all \(w_1 \in W_1\). Recall that \(W\) is the set of the roots of \(A(x)\). Therefore, if \(a_0 \in S \setminus \{0\}\), then \(a_0 \tilde{w}_1 \in W\) for all \(\tilde{w}_1 \in \tilde{W}_1\). As \(|W| = |\tilde{W}_1|\), we conclude that if \(a_0 \notin S \setminus \{0\}\), then \(a_0 \tilde{w}_1 = W\) for all \(\tilde{w}_1 \in \tilde{W}_1\). The converse holds as well. These arguments imply that for \(a_0 \in \mathbb{F}_q^n\), we have \(a_0 \in S \iff a_0 \tilde{W}_1 = W\).

As \(m_1 > 0\), let \(a_0^\ast\) be an element in \(S \setminus \{0\}\). Let \(\hat{S} = \{a_0/a_0^\ast : a_0 \in S\}\). Note that \(\hat{S}\) is an \(\mathbb{F}_q\)-linear subspace of \(\mathbb{F}_q^n\) with the properties that \(1 \in \hat{S}\) and the statement that if \(a \in \hat{S}\), then \(a \tilde{W}_1 = \tilde{W}_1\).

Let \(\hat{S} \subseteq \mathbb{F}_q^n\) be the largest subset consisting of \(a \in \mathbb{F}_q^n\) such that \(a \tilde{W}_1 = \tilde{W}_1\). It follows from the definition that \(\hat{S} \subseteq \hat{S}\). It also follows from the definition that \(\hat{S}\) is not only additive but also closed under multiplication. This implies that \(\hat{S}\) is a finite integral domain, and hence \(\hat{S}\) is an intermediate field \(\mathbb{F}_q \subseteq \hat{S} \subseteq \mathbb{F}_q^n\) (see also Wedderburn's Theorem, for example, in [17, theorem 2.55]). Put \(\dim_{\mathbb{F}_q} \hat{S} = \rho\). As \(\hat{S}\) is an intermediate field we obtain that \(\rho \mid m\). Note that this also implies that \(\tilde{W}_1\) is a linear space over \(\hat{S}\). As \(\dim_{\mathbb{F}_q} \tilde{W}_1 = m - m_1\) we conclude that \(\rho(m - m_1)\) and hence
Note that $\bar{S} \subseteq \bar{S}$ and $\bar{S}$ is an $F_q$-linear space of dimension $m_1$. This immediately implies that

$$m_1 \leq \rho.$$  \hfill (3)

Combining (2) and (3), we conclude that $m_1 = \rho$. This is a contradiction as $m_1 \nmid m$. \hfill $\square$

In some cases, it is possible to extend Construction 3.1 to cover the case $m_1 \nmid m$. We present such an extension below.

**Construction 3.4.** Let $n, m_1, m$, and $d$ be positive integers such that $2 \leq d \leq n \leq m_1 < m$ (we do not assume $m_1 \mid m$). Take $\eta \in F_q^m$ such that $\|\eta\| \neq (-1)^m(m-d+1)$. Assume the existence of $F_q$-linear subspaces $W, W_1 \subseteq F_q^n$, and $S \subseteq F_q^n \times \cdots \times F_q^n$ with the following properties:

P.1. We have $\dim_{F_q} W = m - n$, $\dim_{F_q} W_1 = m - m_1$, and $\dim_{F_q} S = m_1(n - d + 1)$.

P.2. For each $(a_0, \ldots, a_{n-d}) \in S$ and for each $w_1 \in W_1$ we have that

$$a_0 w_1 + a_1 w_1^q + \cdots + a_{n-d} w_1^{q^{n-d}} + \eta a_0 w_1^{q^{n-d+1}} \in W.$$

Put $A(x) = \prod_{w \in W} (x - w) = x^{q^{m-n}} + \text{m.o.t} + a_0 x$.

Let

$$P(W, W_1, \eta) = \{ A(x) \circ (a_0 x + a_1 x^q + \cdots + a_{n-d} x^{q^{n-d}} + \eta a_0 x^{q^{n-d+1}}) : a_0, a_1, \ldots, a_{n-d} \in F_q^m \}.$$  \hfill (4)

Let $P_0(W, W_1, \eta)$ be the $F_q$-linear subspace of $P(W, W_1, \eta)$ defined as

$$P_0(W, W_1, \eta) = \{ A(x) \circ (a_0 x + a_1 x^q + \cdots + a_{n-d} x^{q^{n-d}} + \eta a_0 x^{q^{n-d+1}}) : (a_0, a_1, \ldots, a_{n-d}) \in S \}.$$  \hfill (5)

As in Construction 3.1, $P(W, W_1, \eta)$ corresponds to a punctured MRD Gabidulin twisted code, and $P_0(W, W_1, \eta)$ corresponds to an MRD subcode of it as explained in Theorem 3.5 below. In particular, the code $C = P(W, W_1, \eta)$ satisfies the hypothesis of Theorem 2.7 and can be used for the construction of new MRD codes by switching.

**Theorem 3.5.** We keep the notation and assumptions of Construction 3.4. We choose an ordered basis $(e_1, \ldots, e_m)$ of $F_q^m$ over $F_q$ such that the last $m - m_1$ entries form a basis of $W_1$ over $F_q$. We choose an ordered basis $(f_1, \ldots, f_n)$ of $\text{Im}(A)$ over $F_q$. We note that both $P(W, W_1, \eta)$ and $P_0(W, W_1, \eta)$ depend on the given integer $d$, $2 \leq d \leq n$.  \hfill $\square$
For each \( L \in \mathcal{P}(W, W_1, \eta) \), let \( M(L) \) denote the \( m \times n \) matrix representing the evaluation map \( L : \mathbb{F}_q^m \to \text{Im}(A) \) defined as \( x \mapsto L(x) \) with respect to the bases \((e_1, \ldots, e_m)\) and \((f_1, \ldots, f_n)\). Let \( \mathcal{C}(W, W_1, \eta) \) be the \( \mathbb{F}_q \)-linear subspace of \( \mathbb{F}_q^{m \times n} \) consisting of \( M(L) \) as \( L \) runs through \( \mathcal{P}(W, W_1, \eta) \). Similarly let \( \mathcal{C}_0(W, W_1, \eta) \) be the \( \mathbb{F}_q \)-linear subspace of \( \mathcal{C}(W, W_1, \eta) \) consisting of \( M(L) \) as \( L \) runs through \( \mathcal{P}_0(W, W_1, \eta) \).

Then we have the following:

\( \mathcal{C}(W, W_1, \eta) \) is an MRD code of minimum rank distance \( d \).

If \( M \in \mathcal{C}_0(W, W_1, \eta) \), then the last \( m_1 - 1 \) rows of \( M \) are the zero rows. Considering \( \mathcal{C}(W, W_1, \eta) \) in \( \mathbb{F}_q^{m \times n} \) by ignoring the last \( m_1 - 1 \) zero rows, we obtain an MRD code of minimum rank distance \( d \).

Moreover, Construction 3.4 generalizes Construction 3.1.

**Proof.** If \( a_0, \ldots, a_{n-d} \in \mathbb{F}_q^m \), not all zero, then the arguments of the proof of Theorem 3.2 imply that the rank of the map \( A(x) \circ (a_0 x + a_1 x^q + \cdots + a_{n-d} x^{q^{n-d}} + \eta_0 x^{q^{n-d+1}}) \) is at least \( d \). Similarly, we obtain that \( \dim_{\mathbb{F}_q} \mathcal{C}(W, W_1, \eta) = m(n - d + 1) \). Using Singleton-like bound we conclude that \( \mathcal{C}(W, W_1, \eta) \) is an MRD code of minimum rank distance \( d \).

If \( w_1 \in W_1 \) and \( (a_0, \ldots, a_{n-d}) \in S \), then using property P.2 of Construction 3.4 we obtain that \( A(x) \circ (a_0 w_1 + a_1 w_1^q + \cdots + a_{n-d} w_1^{q^{n-d}} + \eta_0 w_1^{q^{n-d+1}}) = 0 \). As \( \dim_{\mathbb{F}_q} S = m_1(n - d + 1) \) we complete the proof. \( \square \)

Next, we present an application of a slight modification of Construction 3.4. The following result cannot be obtained using Construction 3.1 or the product construction of Section 4 below. For integers \( \mu \geq 1 \) and \( \ell \geq 2 \), put \( m = \mu \ell \), \( n = \mu (\ell - 1) \), and \( m' = m_1 = \mu \).

The following is a construction an \( m \times n \) MRD code having an \( m' \times n \) MRD subcode where \( m > n \) and \( m' < n \). This looks as an interesting unusual case of shortening MRD codes, although it cannot be used for switching as it does not meet the hypothesis of Theorem 2.7.

**Proposition 3.6.** Let \( \mu \geq 1 \) and \( \ell \geq 2 \) be integers. Put \( n = \mu (\ell - 1) \) and \( m = \mu \ell \) so that \( n < m \). Moreover, put \( m_1 = \mu \). Let \( W = \mathbb{F}_q^m \). Let \( W_1 = \{w_1 \in \mathbb{F}_q^m : \text{Trace}_{q^n/q^m}(w_1) = 0\} \). Note that \( W, W_1 \) are \( \mathbb{F}_q \)-linear subspaces of \( \mathbb{F}_q^m \) with \( \dim_{\mathbb{F}_q} W = \mu \) and \( \dim_{\mathbb{F}_q} W_1 = m - \mu \).

Let \( S \) be the set defined as

\[
S = \left\{ (a_0, a_1, \ldots, a_{\mu(\ell-2)}) \in \mathbb{F}_q^m \times \cdots \times \mathbb{F}_q^m : 
\begin{align*}
    a_i &= 0 \text{ if } \mu \nmid i, \\
    a_0 &= a_1 \\
    a_\mu &= a_0 + a_0^{q^\mu}, \\
    a_{2\mu} &= a_0 + a_0^{q^\mu} + a_0^{q^{2\mu}}, \\
    &\vdots \\
    a_{\mu(\ell-2)} &= a_0 + a_0^{q^\mu} + a_0^{q^{2\mu}} + \cdots + a_0^{q^{(\ell-2)\mu}} \right\}.
\right.
\]
Let $$\mathcal{P}(W) = \{ A(x) \circ (a_0 x + a_1 x^q + \cdots + a_{\mu(\ell-2)} x^{q^{\mu(\ell-2)}}) : a_0, a_1, \ldots, a_{\mu(\ell-2)} \in \mathbb{F}_q^n \}.$$ 

Let $$\mathcal{P}_0(W, W_1, S)$$ be the $$\mathbb{F}_q$$-linear subspace of $$\mathcal{P}(W)$$ defined as $$\mathcal{P}_0(W, W_1, S) = \{ A(x) \circ (a_0 x + a_1 x^q + \cdots + a_{\mu(\ell-2)} x^{q^{\mu(\ell-2)}}) : (a_0, a_1, \ldots, a_{\mu(\ell-2)}) \in S \}.$$ 

We choose an ordered basis $$(e_1, \ldots, e_m)$$ of $$\mathbb{F}_q^m$$ over $$\mathbb{F}_q$$ such that the last $$m - m_1$$ entries form a basis of $$W_1$$ over $$\mathbb{F}_q$$. We choose an ordered basis $$(f_1, \ldots, f_n)$$ of $$\text{Im}(A)$$ over $$\mathbb{F}_q$$.

Let $$\mathcal{C}(W)$$ be the $$\mathbb{F}_q$$-linear subspace of $$\mathbb{F}_q^{m \times n}$$ consisting of $$M(L)$$ as $$L$$ runs through $$\mathcal{P}(W)$$. Similarly, let $$\mathcal{C}_0(W_1, W, S)$$ be the $$\mathbb{F}_q$$-linear subspace of $$\mathcal{C}(W)$$ consisting of $$M(L)$$ as $$L$$ runs through $$\mathcal{P}_0(W, W_1, S)$$.

Then we have the following:

- $$\mathcal{C}(W)$$ is an MRD code of minimum rank distance $$\mu$$.
- If $$M \in \mathcal{C}_0(W_1, W, S)$$, then the last $$m - m_1$$ rows of $$M$$ are the zero rows. Considering $$\mathcal{C}_0(W_1, W, S)$$ in $$\mathbb{F}_q^{m_1 \times n}$$ by ignoring the last $$m - m_1$$ zero rows, we obtain an MRD code of minimum rank distance $$\mu$$.

Note that $$\mathcal{C}(W)$$ is in $$\mathbb{F}_q^{m \times n}$$ with $$m > n$$, while the subcode $$\mathcal{C}_0(W_1, W, S)$$ is considered in $$\mathbb{F}_q^{m_1 \times n}$$ with $$m_1 < n$$. This property is different from the earlier results in this section.

**Proof.** As $$m > n$$, an MRD code of rank $$\mu$$ in $$\mathbb{F}_q^{m \times n}$$ has $$\mathbb{F}_q$$-dimension $$m(n - \mu + 1)$$. This is the same as $$\dim_{\mathbb{F}_q} \mathcal{P}(W)$$ as $$a_i \in \mathbb{F}_q^n$$ in the definition of $$\mathcal{P}(W)$$ and the number of such coefficients is $$1 + \mu(\ell - 2) = 1 + \mu(\ell - 1) - \mu = 1 + (n - \mu)$$. Here we also use the fact that $$n = \mu(\ell - 1)$$.

As $$m_1 < n$$, an MRD code of minimum rank distance $$\mu$$ in $$\mathbb{F}_q^{m_1 \times n}$$ has $$\mathbb{F}_q$$-dimension $$n(m_1 - \mu + 1) = n = \mu(\ell - 1)$$. This is the same as $$\dim_{\mathbb{F}_q} W_1$$. Moreover if $$(a_0, a_1, \ldots, a_{\mu(\ell-2)}) \in S$$, then we have

$$\left(x^{q^\mu} - x\right) \circ \left( a_0 x + a_1 x^{q^\mu} + a_2 x^{q^{2\mu}} + \cdots + a_{\mu(\ell-2)} x^{q^{\mu(\ell-2)\mu}} \right)$$

$$= -a_0 (x + x^{q^\mu} + \cdots + x^{q^{(\ell-1)\mu}}),$$

where we use the properties of the coefficients given in (4). Hence evaluating the function in (5) at $$w_1 \in W_1$$ we obtain 0. This completes the proof.

### 4 | PRODUCT CONSTRUCTION

In this section, we describe the direct product construction for MRD codes. It is an analog of a similar construction for MDS codes (in particular, for Latin squares), which constructs an MDS code over a $$q'q^n$$-ary alphabet from MDS codes of the same length and distance over a
q'-ary alphabet and a q''-ary alphabet. Actually, MRD codes in $B_q(m, n), n \leq m$, form a subclass of q''-ary MDS codes if we treat columns of the matrices as symbols of the corresponding q''-ary alphabet. It happens that the direct product of two such codes (in the manner that corresponds to the direct product of the alphabets) keeps not only the MDS property but also the MRD one.

Remark 4.1. The product construction we consider is also known as vertical interleaving; for MRD codes, it was first suggested in [18]. The most general form was considered in [31], where the height of the matrices of the component codes are not required to be equal.

For two codes $C'$ and $C''$ in $B_{q(m', n)}$, $n \leq m'$, and $C''$ is a distance-$d$ MRD code in $B_{q(n', n)}$, respectively, we denote

$$C' \times C'' = \left\{ \begin{bmatrix} X' \\ X'' \end{bmatrix} : X' \in C', X'' \in C'' \right\}.$$

**Proposition 4.2** (Direct product). If $C'$ is a distance-$d$ MRD code in $B_{q(m', n)}$, $n \leq m'$, and $C''$ is a distance-$d$ MRD code in $B_{q(n', n)}$, $n \leq m''$, then $C = C' \times C''$ is a distance-$d$ MRD code in $B_{q(m' + n', n)}$. If, additionally, $C'$ and $C''$ are linear (over $\mathbb{F}_q$), then $C' \times C''$ is linear too.

**Proof.** If $X = \begin{bmatrix} X' \\ X'' \end{bmatrix}$ and $Y = \begin{bmatrix} Y' \\ Y'' \end{bmatrix}$ are two different codewords of $C$, then $X' \neq Y'$ or $X'' \neq Y''$. If $X'' \neq Y''$, then $\text{rank}(Y'' - X'') \geq d$ and hence $\text{rank}(Y - X) \geq d$, which confirms the code distance of $C$. If $X'' = Y''$, then $X' \neq Y'$, $\text{rank}(Y' - X') \geq d$, and again $\text{rank}(Y - X) \geq d$. The linearity is straightforward. □

For the MRD code $C$ constructed as above, we observe the following. For given $X''$ in $C''$, the set $S$ of matrices whose last $m''$ rows coincide with $X''$ satisfy the hypothesis of Theorem 2.7, that is, $S \cap C$ is MRD in $B_q(m', q)$. Such MRD subcode (actually, it is a coset of $C'$) can be switched independently for each $X''$. This results in the following switching variation of the product construction.

**Theorem 4.3.** Let $m', m'', n, d$ satisfy $1 \leq d \leq n \leq m'$, $n \leq m''$. Let $C''$ be a distance-$d$ MRD code in $B_{q(m', n)}$, and for every $X''$ in $C''$ let $C'_{X''}$ be a distance-$d$ MRD code in $B_q(m', n)$. Then the code $C$ defined as

$$C = \left\{ \begin{bmatrix} X' \\ X'' \end{bmatrix} : X'' \in C'', X' \in C'_{X''} \right\}$$

is a distance-$d$ MRD code in $B_q(m' + m'', n)$.

The proof is the same as for Proposition 4.2, taking into account that $X'$ and $Y'$ belong to the same code $C'_{X''}$ if $X'' = Y''$. In a special case, we can prove that the product construction gives linear MRD codes that are not equivalent to twisted Gabidulin codes. The following fact is straightforward from Proposition 3.3.
**Corollary 4.4.** Assume, under the notation and the hypothesis of Proposition 4.2, that \( C' \) and \( C'' \) are \( \mathbb{F}_q \)-linear, \( m' = n = d \), and \( m' \) does not divide \( m'' \). Then the code \( C = C' \times C'' \) is not equivalent to any Gabidulin or twisted Gabidulin code.

**Proof.** By construction, the product MRD code has an MRD subcode consisting of \( n \)-by-\( n \) matrices. The codes considered in Proposition 3.3 have no such subcodes. \( \square \)

## 5 | ON THE NUMBER OF INEQUIVALENT CODES

If the hypothesis of Theorem 2.7 is satisfied (which is true for twisted Gabidulin codes if \( m' \) divides \( m \) and for product MRD codes for any parameters satisfying \( 2 \leq d \leq n \leq m' \leq m - n \)), then the code \( C \) is partitioned into \( q^{(n-d+1)(m-m')} \) cosets of \( S \cap C \). Each of these cosets can be independently replaced by a coset of the MRD code \( R \) from Theorem 2.7 (or any other MRD code with the same parameters), resulting in a new MRD code with the same parameters as \( C \). So, we can obtain more than

\[
2^{q^{(n-d+1)(m-m')}}
\]

different MRD codes. To evaluate the number of inequivalent codes, we can divide this number by the maximum size of an equivalence class, which is not more than the number of automorphisms of \( B_q(m, n) \). So, we have at least

\[
\frac{2^{q^{(n-d+1)(m-m')}}}{|GL(m)| \cdot |GL(n)| \cdot |\mathbb{F}_q^m| \cdot |\text{Aut}(\mathbb{F}_q)|} \geq \frac{2^{q^{(n-d+1)(m-m')}}}{q^{m'} \cdot q^n \cdot q^{mn} \cdot \log q} = 2^{q^{(n-d+1)(m-o(m))}}
\]

inequivalent MRD codes as \( n \) and \( m' \) are fixed and \( m \to \infty \). Of course, most of them are nonlinear.

**Corollary 5.1.** If \( d \leq n \leq m \), then there are at least \( 2^{q^{(n-d+1-o(1))m}} \) inequivalent MRD codes of distance \( d \) in \( B_q(m, n) \) as \( m \to \infty \).

## 6 | CODES WITH DIFFERENT AFFINE RANKS AND APERIODIC CODES

With the switching approach, we can construct many MRD codes with the same parameters, and most of them are nonlinear. Two known numerical characteristics of codes that show how far a code is from being linear are the affine rank and the kernel size, see the definitions below. In this section, we will show how to construct MRD codes with different affine ranks and MRD codes with trivial kernel.

### 6.1 | Codes with different affine ranks

The **affine rank** of a code \( C \) in a vector space (in our case, the set of all \( m \)-by-\( n \) matrices with elements from \( \mathbb{F}_q \), forming an \( mn \)-dimensional vector space over \( \mathbb{F}_q \) ) is the dimension of the affine span of \( C \), that is, the dimension of the minimal subspace whose coset includes \( C \). Note
that this concept does not depend on the metric, and the words “rank” has different meanings in “affine rank” and “rank distance.” If the code is linear or a coset of a linear code, then its affine rank coincides with its dimension.

**Theorem 6.1** (On the affine rank of MRD codes). If $1 < d \leq n \leq m/2$ and $q$ is a prime power, then in $B_q(m, n)$ there are distance-$d$ MRD codes of each affine rank from $m(n - d + 1)$ to $m(n - d + 1) + \rho$, where

$$\rho = \max_{m' \in [n, \ldots, m]} \min\{m'(d - 1), q^{(m-m')(n-d+1)} - (m - m')(n - d + 1) - 1\}.$$ 

*Proof.* For each $m'$ in the range $[n, \ldots, m - n]$, there is a product (see Section 4) $\mathbb{F}_q$-linear distance-$d$ MRD code $C$ in $B_q(m, n)$ that is representable as the union of cosets of a $\mathbb{F}_q$-linear distance-$d$ MRD code $M$ in $B_q(m', n)$ (regarded as a subgraph of $B_q(m, n)$):

$$C = \bigcup_{x \in P} (M + x),$$

where $P$ is a set of representatives, $|P| = q^{(m-m')(n-d+1)}$, $\emptyset \in P$. By Theorem 2.7, every instance of $M$ in (6) can be replaced by another MRD code in $B_q(m', n)$, in particular, by a translation $M + y_x$ of $M$ with any vector $y_x$ from $B_q(m', n)$:

$$C' = \bigcup_{x \in P} (M + y_x + x).$$

Our goal is to choose $y_x$ in such a way that $C'$ has the required affine rank.

We now choose two collections of vectors. The first collection is a subset $P'$ of $P$ such that $|P'| = (m - m')(n - d + 1) = \log_q|P|$ and the linear span $\langle M, P' \rangle$ coincides with $C$ (in particular, the affine span of $M \cup P' \cup \{\emptyset\}$ is $C$).

The second collection $Z = \{z_1, \ldots, z_{m'(d-1)}\}$ of vectors such that the linear span $\langle M, Z \rangle$ exhausts the vertex set of $B_q(m', n)$ (this is possible because $m'n = \dim(M) + m'(d - 1)$).

In $P \setminus (P' \cup \{\emptyset\})$, we choose $k$ vectors $x_1, \ldots, x_k$, where $k \leq \min\{|P| - |P'| - 1, m'(d - 1)\}$ and set $y_{x_i} := z_i$, $i = 1, \ldots, k$. For every other vector $x$ from $P \setminus \{x_1, \ldots, x_k\}$, we set $y_x := \emptyset$. We now see that the affine span of $C'$ includes the linear code $C$ and, additionally, the vectors $z_1, \ldots, z_k$; each of them increases the affine rank by 1. So, the affine rank of $C'$ equals $\dim(C) + k$, where $k \in \{0, \ldots, \min\{|P| - |P'| - 1, m'(d - 1)\}\}$. It remains to note that we can choose the best result over all $m'$ in $[n, \ldots, m - n]$. \qed

**Remark 6.2.** The goal of this section was to demonstrate, with reasonably simple arguments, the possibility to construct MRD codes of the same parameters with wide variety of affine ranks. We are convinced that in the majority of cases, higher values of the affine rank can be achieved after developing this technique further. In particular, in the proof above, we consider only a very special variant of switching, where each coset of the MRD subcode $M$ is replaced by its translation. As a result, every such replacement contributes at most $+1$ to the affine rank. This approach can be improved if one replace a coset of $M$ by a coset of another MRD code $M'$ in the same $B_q(m', n)$ subgraph.
Depending on the dimension of the linear span $\langle M \cup M' \rangle$, each such replacement can add more than 1 to the affine rank of the resulting code. With such generalized approach, the total increase $\rho$ of the affine rank is still bounded by the value $(m - n)(d - 1)$. Increasing further the affine rank might be related to switching MRD subcodes in “nonparallel” $B_q(m', m)$ subgraphs, see the brief discussion in the conclusion part of the paper.

### 6.2 Kernel

The *kernel* of a code is the set of its periods:

$$\ker(C) = \{x : C + x = C\}.$$  

For a linear code $C$, it holds $\ker(C) = C$. Conversely, if $\ker(C) = C$ then $C$ is additive (closed under addition), but, for non-prime $q$, is not necessarily linear over $\mathbb{F}_q$. If $\ker(C)$ consists of only the zero vector, then the code is said to have *trivial kernel*, or just to be *aperiodic*.

**Lemma 6.3.** Let $M$ be a linear rank-distance-$d$ code in $B_q(m, n)$, $d > 1$, $|M| > 1$, and let $x$ be a nonzero matrix in $B_q(m, n)$. Then there is a linear rank-distance-$d$ code $D$ in $B_q(m, n)$ such that $|M| = |D|$ and $x \notin D$.

**Proof.** If $x \notin D$, then we take $D = M$. Otherwise, let $i$ be the index of any nonzero row of $x$ and $j$ any other row index. Denote by $\pi_{ij}$ the transformation of matrices that add the $i$th row to the $j$th row. Obviously, $\pi_{ij}$ is an isometry of $B_q(m, n)$, and hence $D := \pi_{ij}(M)$ has the same code parameters as $M$. It remains to observe that the rank distance between $x$ and $\pi_{ij}(x)$ is 1; hence $D$, containing $\pi_{ij}(x)$, does not contain $x$. \qed

**Lemma 6.4.** Let $M$ be a linear rank-distance-$d$ code in $B_q(m, n)$, $d > 1$, $\dim(M) = r$. Then for every $k \in \{0, \ldots, r\}$, there is a collection $(M = M_0, M_1, \ldots, M_k)$ of linear codes of the same cardinality and code distance such that $\dim(M_0 \cap \cdots \cap M_k) \leq r - k$. Moreover, if $k > 0$, then $M_1 \notin \{M_0, M_2, \ldots, M_k\}$.

**Proof.** We proceed by induction on $k$. If $k = 0$, the claim is trivial. If $k > 0$, then from the inductive hypothesis we have a collection $(M = M_0, M_1, \ldots, M_{k-1})$ such that the dimension of $U := M_0 \cap \cdots \cap M_{k-1}$ is at most $r - k + 1$. If $\dim(U) = 0$, then we take $M_k = M$ (note that this can only happen if $k \geq 2$, and thus we get $M_k \neq M_i$ in this case). Otherwise, we choose a nonzero matrix $x$ in $U$ and take $M_k = D$, where $D$ is from Lemma 6.3 (since $x$ belongs to all $M_0, \ldots, M_{k-1}$ but not to $M_k$, we get $M_i \neq M_0$ if $k = 1$ and $M_k \neq M_i$ if $k > 1$; this inductively provides the last claim of the lemma). \qed

**Theorem 6.5** (Aperiodic MRD codes). If $1 < d \leq n \leq m/2$ and $q$ is a prime power, then there are aperiodic distance-$d$ MRD codes in $B_q(m, n)$.  


Proof. There is an $\mathbb{F}_q$-linear distance-$d$ MRD code $C$ in $B_q(m, n)$ that is representable as the union of cosets of an $\mathbb{F}_q$-linear distance-$d$ MRD code $M$ in $B_q(n, n)$, regarded as the subgraph of $B_q(m, n)$ induced by a linear subspace $S$ of $\mathbb{F}_q$-dimension $mn$

$$C = \bigcup_{x \in P} (x + M), \quad x + M = C \cap (x + S),$$

where $P$ is a set of representatives, $|P| = q^{(m-n)(n-d+1)} > n(n-d-1)$, $\overline{0} \in P$. By Theorem 2.7, for every $x$ in $P$, the corresponding instance of $M$ in (8) can be replaced by another MRD code $M^{(x)}$ in $B_q(n, n)$ with the same code parameters as $M$:

$$C' = \bigcup_{x \in P} (x + M^{(x)}), \quad x + M^{(x)} = C' \cap (x + S).$$

We choose distinct $x_0, \ldots, x_r$ in $P$, where $r = n(n - d - 1) = \dim(M)$, and set $M^{(x_i)} := M_i$, $i = 0, \ldots, r$, where $M_i$ are from Lemma 6.4 ($k = r$). For the remaining $|P| - r - 1$ elements $x$ of $P$, we keep $M^{(x)} := M$.

We now consider an arbitrary non-zero $y$ in $B_q(m, n)$ and show that it is not a period of $C'$. Seeking a contradiction, assume $y$ is a period. In this case, both $x_1$ and $x_1 + y$ are in $C'$. From (9), we conclude

$$x_1 + y = x_1 + M^{(x)}.$$ 

This implies $y = \overline{0}$ because $M_0 \cap \cdots \cap M_d = \{\overline{0}\}$ by Lemma 6.4.

(ii) Assume $x_1 + y \in x + M^{(x)}$ for some $x$ from $P \setminus \{x_1\}$. In this case, we have $y \in S$. In particular, for every $i$ in $\{0, \ldots, r\}$, it holds $x_i + y \in x_i + S$. On the other hand, since $y$ is a period, $x_i + y$ belongs to $C'$. From (9), we conclude $x_1 + y \in x_1 + M_i$. Therefore, $y \in M_i, i = 0, \ldots, r$. This implies $y = \overline{0}$ because $M_0 \cap \cdots \cap M_d = \{\overline{0}\}$ by Lemma 6.4.

7 | CONCLUSION

We have established a lower bound $2^q(n-d+1-o(1)m$ on the number of MRD codes of distance $d$ in $B_q(m, n)$ as $m$ grows. A trivial upper bound on the number of MRD codes ($d > 1$) is

$$(q^{(n-k)m})q^{km} = 2^{m-q^{km}(1+o(1))}, \quad k = n - d + 1$$

(indeed, the space is partitioned into $q^{km}$ anticodes of cardinality $q^{(n-k)m}$, each containing exactly 1 codeword). In particular, the proportion of the MRD codes ($d > 1$) in the set of all

$$\binom{q^{nm}}{q^{km}} = (q^{(n-k)m})q^{km} \cdot q^{km(1+o(1))}$$
unrestricted codes of the same cardinality tends to 0 as $m \to \infty$. In [14], a more advanced upper bound on the number of MRD codes was considered, with the same conclusion for $q \to \infty$. In contrast, the proportion of MRD codes in the set of all $\mathbb{F}_q^n$-linear codes of the same cardinality tends to 1 as $m \to \infty$, see [20]. In [13] (see also the references there), the “intermediate” case of $\mathbb{F}_q$-linear rank-metric codes was considered; in particular, it was shown that the proportion of MRD codes among all $\mathbb{F}_q$-linear codes of fixed dimension tends to 0 as $q \to \infty$ ($m \geq n > 2$ and $d > 1$) and is bounded by some nontrivial constant as $m \to \infty$.

The logarithm of the upper bound $(q^{(n-k)m}a^km)$ on the number of MRD codes is in $O(m \cdot q^{km})$, $m \to \infty$, while the logarithm of our lower bound is only $\text{const} \cdot q^{km}$. With the switching approach, further improvement of the lower bound is possible if one can switch “nonparallel” MRD subcodes of the initial MRD code. This strategy worked well for evaluating the number of $Q$-ary nonlinear MDS codes (equivalently, systems of $t$ strongly orthogonal latin $m$-cubes of order $Q$, where $t$ and $m$ are constants and $Q$ grows) of fixed length and distance and growing alphabet size $Q$ (an analog of our $q^m$), see [26]. To apply a similar switching strategy to constructing MRD codes, we need to start with an MRD code with different $\mathbb{F}_q$-linear MRD subcodes, corresponding to different, “nonparallel” $B_q(m', n)$-subgraphs. Developing this idea is a promising direction for further studies. While the switching approach can give a constructive way to build a huge amount of objects, we cannot ignore also a nonconstructive probabilistic approach to evaluate the number of objects of similar nature. The recent result by Keevash et al. [16] for subspace designs suggests that the number of MRD codes ($n$ fixed, $m$ grows) can be evaluated in a similar manner.

Another point we want to mention is that the subcode switching for MRD codes has some restrictions: with this method, we could only construct new MRD codes with parameters satisfying $m \geq 2n$. This is enough to obtain powerful asymptotic results, but does not allow to construct new codes with $n \leq m < 2n$. One can try to bypass this restriction with other variations of the switching technique. The most common way to construct codes by switching in some direction, see for example, [22], can also be applied to MRD codes: a code $C'$ is obtained from a code $C$ by switching in a direction $v$, where $v$ is a vector from the ambient vector space, if $C'$ is a subset of $C \cup (C + v)$. For given $C$ and $v$, finding all such $C'$ is a simple computational problem, which is good for experiments with small-parameter codes. However, developing this technique theoretically for arbitrary parameters remains an open challenging problem for MRD codes. One of the main questions here is the following: given a starting linear code $C$ and a vector $v$ (often, of weight 1, although this is not a necessary restriction), what is the minimum subspace $S$ of $C$ such that $C \cup (S + v) \setminus S$ has the same parameters as $C$? More generally, one can ask what is the minimum difference between two MRD codes of the same parameters. This question is common for many classes of optimal codes, and one of the developed methods to make lower bounds for this minimum is to study eigenspaces of the ambient graph, see [32] for a survey for different graphs and [33] for the bilinear form graphs.

As was mentioned by one of the reviewers of the present paper, $n$-by-$n$ distance-$n$ MRD codes correspond to partitions of the $2n$-dimensional vector space into $n$-dimensional subspaces that have trivial mutual intersection (see [5]). For such partitions, known as spreads, the switching technique is also studied (see, e.g., regulus switching [3]) and without doubt corresponds to switching (in general meaning) in MRD codes. It, however, requires a separate study to answer how (if), for example, regulus switching can be generalized to switching in MRD codes of rank distance smaller than $n$. In a slightly different meaning, the term “switching” is used for semifields [15, 28], which are related to additive $n$-by-$n$ distance-$n$ MRD
codes (see, e.g., see [5, th. 3]); such switching of an operation also results in changing the corresponding additive MRD code, but its treatment as subset switching is less straightforward.

ACKNOWLEDGMENTS
The authors thank Vladimir Potapov for useful discussions and the anonymous referees for detailed reviews and constructive suggestions which helped to improve the quality of the presentation of the results. The work of M. J. Shi is supported by the National Natural Science Foundation of China (12071001); the work of D. S. Krotov is supported by the state contract of the Sobolev Institute of Mathematics (FWNF-2022-0017); the work of F. Özbudak is supported by the METU Scientific Research Projects Coordination Unit (GAP-101-2021).

DATA AVAILABILITY STATEMENT
The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

ORCID
Minjia Shi  http://orcid.org/0000-0002-4990-6271
Denis S. Krotov  http://orcid.org/0000-0002-8516-755X
Ferruh Özbudak  https://orcid.org/0000-0002-1694-9283

REFERENCES
1. R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, *On perfect codes and related concepts*, Des. Codes Cryptography. **22** (2001), no. 3, 221–237. https://doi.org/10.1023/A:1008394205999
2. A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-regular graphs*, Springer-Verlag, Berlin, 1989. https://doi.org/10.1007/978-3-642-74341-2
3. A. Bruen and R. Silverman, *Switching sets in PG*(3, q), Proc. Am. Math. Soc. **43** (1974), no. 1, 176–180. https://doi.org/10.2307/2039350
4. A. Cossidente, G. Marino, and F. Pavese, *Non-linear maximum rank distance codes*, Des. Codes Cryptography. **79** (2016), no. 3, 597–609. https://doi.org/10.1007/s10623-015-0108-0
5. de la J. Cruz, M. Kiermaier, A. Wassermann, and W. Willems, *Algebraic structures of MRD codes*, Adv. Math. Commun. **10** (2016), no. 3, 499–510. https://doi.org/10.3934/amc.2016021
6. P. Delsarte, *An algebraic approach to association schemes of coding theory*, Philips Res. Rep., Supplement, vol. 10, N.V. Philips' Gloeilampenfabrieken, Eindhoven, 1973.
7. P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, J. Comb. Theory, Ser. A. **25** (1978), 226–241. https://doi.org/10.1016/0097-3165(78)90015-8
8. N. Durante and A. Siciliano, *Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries*, Electr. J. Comb. **24** (2017), no. 2, (1–18). https://doi.org/10.37236/6106
9. S. Eberhard, *More on additive triples of bijections*, E-print 1704.02407, arXiv.org, 2017. http://arxiv.org/abs/1704.02407
10. È.M. Gabidulin, *Theory of codes with maximum rank distance*, Probl. Inf. Transm. **21** (1985), no. 1, 1–12. Translation from Probl. Peredachi Inf. 21:1 (1985), 3–16.
11. E. M. Gabidulin, *Rank codes*, TUM University Press, Munich, 2021. https://doi.org/10.14459/2021md1601193
12. R. Gow and R. Quinlan, *Galois theory and linear algebra*, Linear Algebra Appl. **430** (2009), no. 7, 1778–1789. https://doi.org/10.1016/j.laa.2008.06.030
13. A. Gruica and A. Ravagnani, *Common complements of linear subspaces and the sparseness of MRD codes*, SIAM J. Appl. Algebra Geometry. **6** (2022), no. 2, 79–100. https://doi.org/10.1137/21M1428947
14. A. Gruica and A. Ravagnani, *The proportion of (non-)linear MRD codes*, WCC 2022: The Twelfth International Workshop on Coding and Cryptography. March 7–11, 2022, Rostock, Germany, 2022, p. 9.
15. X. D. Hou, F. Özbudak, and Y. Zhou, *Switchings of semifield multiplications*. Des. Codes Cryptography. **80** (2016), no. 2, 217–239. https://doi.org/10.1007/s10623-015-0081-7
16. P. Keevash, A. Sah, and M. Sawhney, *The existence of subspace designs*, E-print 2212.00870, arXiv.org, 2022.
17. R. Lidl, and H. Niederreiter, *Finite fields*, Encycl. Math. Appl., vol. 20, Cambridge University Press, Cambridge, 1997.
18. P. Loidreau and R. Overbeck, *Decoding rank errors beyond the error correction capability*, Proc. Tenth Int. Workshop on Algebraic and Combinatorial Coding Theory ACCT-10, Zvenigorod, Russia, 2006, pp. 186–190.
19. R. Meshulam, *On the maximal rank in a subspace of matrices*, Quarterly J. Math. 36 (1985), no. 2, 225–229. https://doi.org/10.1093/qmath/36.2.225
20. A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal, *On the genericity of maximum rank distance and Gabidulin codes*. Des. Codes Cryptography. 86 (2018), no. 2, 341–363. https://doi.org/10.1007/s10623-017-0354-4
21. O. Ore, *On a special class of polynomials*. Trans. Am. Math. Soc. 35 (1933), 559–584. https://doi.org/10.2307/1989849
22. P. R. J. Östergård, *Switching codes and designs*, Discrete Math. 312 (2012), no. 3, 621–632. https://doi.org/10.1016/j.disc.2011.05.016
23. K. Otal and F. Özbudak, *Explicit constructions of some non-Gabidulin linear maximum rank distance codes*, Adv. Math. Commun. 10 (2016), no. 3, 589–600. https://doi.org/10.3934/amc.2016028
24. K. Otal and F. Özbudak, *Additive rank metric codes*, IEEE Trans. Inf. Theory. 63 (2017), no. 1, 164–168. https://doi.org/10.1109/TIT.2016.2622277
25. K. Otal and F. Özbudak, *Some new non-additive maximum rank distance codes*, Finite Fields Appl. 50 (2018), 293–303. https://doi.org/10.1016/j.ffa.2017.12.003
26. V. N. Potapov, *On the number of SQSs, Latin hypercubes and MDS codes*, J. Comb. Des. 26 (2018), no. 5, 237–248. https://doi.org/10.1002/jcd.21603
27. V. N. Potapov, A. A. Taranenko, and Y. V. Tarannikov, *An asymptotic lower bound on the number of bent functions*. Des. Codes Cryptography. (2023). https://doi.org/10.1007/s10623-023-01239-z
28. A. Pott, and Y. Zhou, *Switching construction of planar functions on finite fields*, Proc. 3d Int. Workshop WAIFI 2010, Istanbul, Turkey, June 2010, Lect. Notes Comput. Sci., vol. 6087, 2010, pp. 135–150. https://doi.org/10.1007/978-3-642-13797-6_10
29. J. Sheekey, *A new family of linear maximum rank distance codes*, Adv. Math. Commun. 10 (2016), no. 3, 475–488. https://doi.org/10.3934/amc.2016019
30. J. Sheekey, *MRD codes: Constructions and connections*, Radon Ser. Comput. Appl. Math. vol., 23, De Gruyter, Berlin, 2019, pp. 255–285. https://doi.org/10.1515/9783110642094-013
31. V. Sidorenko, V. Li, and G. Kramer, *On interleaved rank metric codes*, 2020 Algebraic and Combinatorial Coding Theory (ACCT), 2020, pp. 128–134. https://doi.org/10.1109/ACCTS1235.2020.9383406
32. E. Sotnikova and A. Valyuzhenich, *Minimum supports of eigenfunctions of graphs: a survey*, Art Disc. Appl. Math. 4 (2021), no. 2, P2.09(1–34). https://doi.org/10.26493/2590-9770.1404.61e
33. E. V. Sotnikova, *Minimum supports of eigenfunctions in bilinear forms graphs*, Sib. Élektron. Mat. Izv. 16 (2019), 501–515. https://doi.org/10.33048/semi.2019.16.032
34. I. M. Wanless, *Transversals in Latin squares: a survey*, Surveys in Combinatorics 2011, London Math. Soc. Lecture Note Ser., vol. 392, Cambridge Univ. Press, Cambridge, 2011, pp. 403–437.
35. G. Zini and F. Zullo, *Scattered subspaces and related codes*, Des. Codes Cryptography. 89 (2021), no. 8, 1853–1873. https://doi.org/10.1007/s10623-021-00891-7

How to cite this article: M. Shi, D. S. Krotov and F. Özbudak, *Constructing MRD codes by switching*, J. Combin. Des. (2024), 32, 219–237. https://doi.org/10.1002/jcd.21931