Bounds on Minimum Rank Distances of Array Codes

Zhiyuan Yan
Dept. of ECE
Lehigh University
Bethlehem, PA 18015 USA
Email: yan@lehigh.edu

Abstract—Various bounds on minimum rank distances of linear block codes have been proposed. In this paper, we derive a Singleton bound on minimum rank distances of \( m \)-by-\( n \) array codes. Our Singleton bound not only applies to nonlinear codes, but also implies several previously proposed bounds as special cases. In addition, we derive one upper bound and one lower bound on the size of array codes which parallel the sphere-packing bound and the Gilbert bound. Finally, we propose a construction that leads to maximum rank distance codes that do not require large fields as their alphabets.

I. INTRODUCTION

Error-control codes with the rank metric \( [4], [14] \) have recently received some attention due to their application to space-time coding \([12] ,\) storage applications \([14] ,\) and cryptography \([5] .\) Bounds on the parameters of codes indicate how good codes are, and also provide guidelines to the design of good codes. Various bounds on minimum rank distances have been proposed. These bounds are derived based on two different definitions of the rank distance. One definition is due to Gabidulin \([4] :\) For a fixed basis set, each finite field element of \( \text{GF}(q^m) \) has a one-to-one correspondence with an \( m \)-dimensional column vector over \( \text{GF}(q) \), and thus any row vector of length \( n \) over \( \text{GF}(q^m) \) corresponds to an \( m \)-by-\( n \) matrix over \( \text{GF}(q) \). Using this correspondence, Gabidulin \([4] \) defined the rank distance for an \( (n, k) \) linear code over \( \text{GF}(q^m) \) and derived a Singleton bound on minimum rank distances for \( (n, k) \) linear block codes over \( \text{GF}(q^m) \)

\[
d, \leq (n - k) + 1, \tag{1}
\]

where \( d \) denotes the minimum rank distance of the code. Another bound \( (\text{see, for example,} \ [9]) \) on the minimum rank distance of a (linear or nonlinear) block codes over \( \text{GF}(q^m) \) of length \( n \) and cardinality \( N \) is given by

\[
d, \leq \frac{m}{n} (n - \log_{q^m} N) + 1. \tag{2}
\]

Clearly, the upper bound in (2) is tighter than that in (1) when \( m < n \), and vice versa when \( m \geq n \). Obviously, the minimum rank distance also satisfies \( d, \leq m \). These bounds jointly determine the optimal minimum rank distance achievable for a linear block code over \( \text{GF}(q^m) \), and we refer to \( (\text{linear or nonlinear}) \) codes that achieve the optimality as maximum rank distance (MRD) codes henceforth. MRD codes for different cases have been studied. Codes that satisfy \( d = m \) are referred to as full rank distance codes and studied in \([11] \). When \( m \geq n \), an explicit construction for MRD codes has been proposed by Gabidulin \([4] \), and this construction was generalized in \([8] \). These codes are called Gabidulin codes, and they are used in the Gabidulin-Paramonov-Trejtakov (GPT) public-key cryptosystem \([5] \) and even space-time coding \([10] \). If \( n = rm \) where \( r \geq 1 \) is an integer, cartesian product of \( r \) Gabidulin codes of \( m = n \) gives an MRD code of length \( n \) over \( \text{GF}(q^m) \) \([9] \). However, the general question of existence and construction of MRD codes when \( m < n \) are unsolved research problems to the best of our knowledge. The other definition of the rank distance is with respect to codematrices over \( \text{GF}(q) \). Roth \([14] \) considered square array codes which consist of \( n \)-by-\( n \) codematrices over \( \text{GF}(q) \), derived a bound on the minimum rank distance, and proposed a family of array codes with the maximum rank distance, which are equivalent to Gabidulin codes.

In this paper, we consider \( m \)-by-\( n \) array codes over \( \text{GF}(q) \) and derive a Singleton bound on minimum rank distances of array codes over \( \text{GF}(q) \). Our Singleton bound has a similar form to that for the minimum Hamming distance of codes, and is slightly more general than that in \([14] \). Since \( (n, k) \) linear codes over \( \text{GF}(q^m) \) correspond to a subclass of \( m \)-by-\( n \) linear array codes, our Singleton bound implies the four bounds mentioned above as special cases. We also propose two bounds on the size of array codes that parallel the sphere-packing bound and the Gilbert bound \([1] \). Finally, we propose an explicit construction of MRD codes over \( \text{GF}(q^m) \) provided \( mk \) is a multiple of \( n \) \( (m < n) \). Our construction is less restrictive on the parameters of the MRD codes than
the cartesian product construction. However, the MRD codes obtained by our new construction are group codes and not necessarily linear. Unlike Gabidulin codes, the MRD codes obtained via our new construction do not require \( m \geq n \) and do not need large fields as their alphabets.

The rest of the paper is organized as follows. In Section II, the rank distance of array codes is defined and our Singleton bound on the minimum distance of array codes is derived. Section III presents two other bounds we derived for array codes. In Section IV, we show that our Singleton bound unifies the previously proposed bounds, and illustrate our new construction of MRD codes over \( \text{GF}(q^m) \) when \( m < n \) and \( mk \) is a multiple of \( n \). Potential applications of our Singleton bound are also discussed in Section IV.

II. Singleton Bounds on the Minimum Rank Distance

In order to make this paper self-contained, we first introduce the important concepts of array codes, and then establish our Singleton bound.

A. Definitions

To avoid confusion, we refer to the codes that consist of (row or column) vectors as vector codes henceforth. Let \( M_{m,n}(\text{F}) \) denote the set of all \( m \)-by-\( n \) matrices over \( \text{F} \), where \( \text{F} \) is a finite field \( \text{GF}(q) \). Clearly, \( M_{m,n}(\text{F}) \) constitutes an \((mn)\)-dimensional vector space over \( \text{F} \). An \( m \)-by-\( n \) array code \( \mathbb{C} \) over the alphabet \( \text{F} \), linear or nonlinear, is defined as a size-\( N \) subset of \( M_{m,n}(\text{F}) \). That is,

\[
\mathbb{C} \triangleq \{ X_1, X_2, \ldots, X_N \in M_{m,n}(\text{F}) \}.
\]

As in the case of vector codes, a linear \( m \)-by-\( n \) array code over \( \text{F} \) is a subspace of \( M_{m,n}(\text{F}) \), and we call it an \((m, n, k)\) linear array code where \( k \) is the dimension of the subspace. A sufficient and necessary condition for linearity of an array code \( \mathbb{C} \) is that for any two codemats \( X_1 \) and \( X_2 \) in \( \mathbb{C} \) and any two scalars \( a_1 \) and \( a_2 \) in \( \text{F} \), \( a_1 X_1 + a_2 X_2 \) is also a codematrix in \( \mathbb{C} \). This sufficient and necessary condition can be used as an alternative definition for linear array codes. For an \((m, n, k)\) linear array code \( \mathbb{C} \), clearly \( N = q^k \).

For any matrix \( X \in M_{m,n}(\text{F}) \), the rank of \( X \), \( \text{rank}(X) \), is defined to be the maximum number of linearly independent rows (or columns) of \( X \). One can verify that the mapping \( M_{m,n}(\text{F}) \rightarrow \text{R} \) given by \( X \mapsto \text{rank}(X) \) verifies all the axioms of a vector norm [7]. Hence, we denote this mapping as the rank norm \( \| \cdot \| \). The rank norm induces a rank metric on \( M_{m,n}(\text{F}) \):

\[
d_d(X, Y) \triangleq \| X - Y \|, \quad \text{for } X, Y \in M_{m,n}(\text{F}).
\]

The minimum rank distance of an array code \( \mathbb{C} \), denoted as \( d_r(\mathbb{C}) \), is defined as:

\[
d_r(\mathbb{C}) \triangleq \min_{X, Y \in \mathbb{C}, X \neq Y} d_d(X, Y).
\]

The minimum rank distance for a linear array code is the minimum rank norm among the nonzero codemats. That is, for an \((m, n, k)\) linear array code, we have

\[
d_r(\mathbb{C}) = \min_{X \in \mathbb{C}, X \neq 0} \text{rank}(X).
\]

For a linear array code \( \mathbb{C} \) of dimension \( k \), there exists a basis set \( \{ G_0, G_1, \ldots, G_{k-1} \} \) of size \( k \) such that any codematrix \( X \in \mathbb{C} \) can be uniquely expressed as

\[
X = \sum_{i=0}^{k-1} u_i G_i \text{ where } u_i \in \text{F} \text{ are the data symbols.}
\]

We call the \( k \)-by-\( m \)-by-\( n \) 3-D array \( G \) that is formed by stacking \( G_0, G_1, \ldots, G_{k-1} \) a generator array of the array code. Thus, we also call \( G_i \)'s as the layer matrices of \( G \). Hence, \( X \) can be written as \( X = uG \), where the row vector \( u = (u_0, u_1, \ldots, u_{k-1}) \) is the data word.

To define the parity check matrix for a linear array code, we need to first define the inner product on \( M_{m,n}(\text{F}) \), \( \langle \cdot, \cdot \rangle : M_{m,n}(\text{F}) \times M_{m,n}(\text{F}) \rightarrow \text{F} \). Let \( \langle X, Y \rangle \triangleq \text{trace} \{ XY^T \} \) for any \( X \) and \( Y \) in \( M_{m,n}(\text{F}) \). Furthermore, \( X \) and \( Y \) are said to be orthogonal to each other in the vector space \( M_{m,n}(\text{F}) \) if and only if \( \langle X, Y \rangle \equiv 0 \) (mod \( q \)). Since the dimension of the array code generated by \( G \) is \( k \), its null space has a dimension of \( mn - k \) with a basis set \( \{ H_0, H_1, \ldots, H_{mn-k-1} \} \) where \( H_i \in M_{m,n}(\text{F}) \) \((i = 0, 1, \ldots, mn-k-1)\) verifies

\[
\langle H_j, G_j \rangle \equiv 0 \pmod{q} \text{ for } j = 0, 1, \ldots, k - 1.
\]

If we stack all \( H_j \)'s, call it \( H \), and define the product \( HX^T \) of \( H \), an \((mn - k)\)-by-\( m \)-by-\( n \) 3-D array, and the transpose of an \( m \)-by-\( n \) matrix \( X \) as

\[
H X^T \triangleq ((H_0, X), (H_1, X), \ldots, (H_{mn-k-1}, X))^T,
\]

then \( H \) verifies \( HX^T = 0 \) for all \( X \in \mathbb{C} \). We call \( H \) a parity check array for the linear array code \( \mathbb{C} \). Clearly, a linear array code can also be defined as the null space of \( H \).

We define the blocklength of an array code to be the product of its numbers of rows and columns. We also define the rate \( R \) of an array code to be the ratio \( \frac{\log_2 N}{mn} \). When the array code is linear with dimension \( k \), \( R = \frac{k}{mn} \). The rate of the array code indicates how redundant the code is.
There are mainly two categories of vector codes: block vector codes and convolutional vector codes. Similarly, we can distinguish block array codes and convolutional array codes in the same way. In the following, we will focus on block array codes, and thus for simplicity “array codes” refer to block array codes henceforth.

B. Singleton Bounds

We will first establish the following key lemma about the size of any array code.

Lemma 1: If an \( m \)-by-\( n \) array code \( C \) over \( \text{GF}(q) \) with minimum rank distance \( d \) consists of \( N \) codematri-ces, then \( N \leq q^{mn - \max\{m,n\}(d-1)} \).

The proof of Lemma 1 is omitted here due to limited space. Using Lemma 1, the Singleton bound on minimum rank distances of array codes below can be derived.

Theorem 1: (Singleton bound) For an \( m \)-by-\( n \) array code of rate \( R \), its minimum rank distance satisfies \( d \leq \min\{m, n\} (1 - R) + 1 \).

Proof: Since \( N \leq q^{mn - \max\{m,n\}(d-1)} \), we have \( \frac{\log_q N}{\max\{m,n\}} \leq \min\{m, n\} - d + 1 \). Rearranging the inequality, we have

\[
d \leq \min\{m, n\} \left( 1 - \frac{\log_q N}{mn} \right) + 1 = \min\{m, n\} \cdot (1 - R) + 1.
\]

(3)

Note that the Singleton bound applies to both linear and nonlinear array codes. We also remark that the Singleton bound for an array codes has a form that is similar to the Singleton bound on the minimum Hamming distance of vector codes \( d \leq n(1 - R) + 1 \). Fix the blocklength \( mn \) and rate \( R \), different factorizations of \( mn \) lead to different array codes. Among these array codes, the array codes with \( m = n \) maximize the right hand side of (3). Thus, for given blocklength \( mn \) and rate \( R \) we have the following bound:

\[
d \leq \sqrt{mn} \cdot (1 - R) + 1.
\]

Let the blocklength of the matrix goes to infinity, we can see that asymptotically the minimum rank distance of the array codes is proportional to the square root of the blocklength. Following the convention of vector codes, we call the codes that achieve the Singleton bound with equality maximum distance separable (MDS) array codes.

Note that the roles of \( m \) and \( n \) are symmetric in the right-hand side of (3). That is, the bound is invariant with respect to the transpose operation. Let us consider an operation on an array code \( C \) that transpose all the codematri-ces of \( C \). Clearly, the resultant codematri-ces form another array code, and we call it the transpose code \( C^T \) of \( C \). If \( G \) is a generator array of \( C \), then the 3-D array obtained by stacking the transposes of the layer matrices of \( G \) is a generator array of \( C^T \), denoted as \( G^T \) henceforth. Clearly, the minimum rank distance and rate of an array code are both invariant under the transpose operation. Thus, we have:

Corollary 1: For an \( m \)-by-\( n \) array code of rate \( R \) and its transpose code, their minimum rank distance satisfies \( d \leq \min\{m, n\} (1 - R) + 1 \).

III. GILBERT AND SPHERE-PACKING BOUNDS FOR ARRAY CODES

In this section, we present two bounds on the size of array codes. Let us denote the size of an \( m \)-by-\( n \) array code over \( \text{GF}(q) \) with minimum rank distance \( d \), as \( A_q(m, n, d) \). Let us also denote the number of \( m \)-by-\( n \) matrices over \( \text{GF}(q) \) with rank \( w \) as \( N_q(m, n, w) \). It can be shown that for \( w \leq \min\{m, n\} \)

\[
N_q(m, n, w) = \prod_{i=0}^{w-1} \frac{(q^m - q^i)(q^n - q^i)}{(q^w - q^i)}.
\]

(4)

Let us denote the volume of a ball of radius \( w \) (in the rank metric) in \( M_{m,n}(\text{F}) \) by \( V_q(m, n, w) \), we obtain

\[
V_q(m, n, w) = \sum_{j=0}^{w} N_q(m, n, j).
\]

(5)

The Gilbert and sphere-packing bounds are two important bounds for codes in the Hamming metric [1]. Note that the derivations of these two bounds are transparent to the metric considered, and hence these two bounds can be easily adapted to array codes with the rank metric. Following the same approaches used to prove these two bounds for vector codes, we prove the following bounds for array codes.

Lemma 2 (Gilbert Bound): Let \( d \leq \min\{m, n\} \), there exists an \( m \)-by-\( n \) array code over \( \text{GF}(q) \) with cardinality \( A_q(m, n, d) \) and minimum rank distance \( d \), that satisfies

\[
\frac{q^{mn}}{V_q(m, n, d - 1)} \leq A_q(m, n, d).
\]

The Gilbert bound gives a lower bound to the cardinality of a “reasonably good” array code for given size and minimum rank distance.

Lemma 3 (Sphere-Packing Bound): Let \( d \leq \min\{m, n\} \), any \( m \)-by-\( n \) array code over \( \text{GF}(q) \) with cardinality \( A_q(m, n, d) \) and minimum rank distance \( d \), satisfies

\[
A_q(m, n, d) \leq \frac{q^{mn}}{V_q(m, n, t)},
\]

where \( t = \lfloor (d - 1)/2 \rfloor \).
IV. APPLICATION OF OUR NEW SINGLETON BOUND

To apply the Singleton bound on minimum rank distances of array codes, we need to clarify the connections between vector and array codes first.

A. Connections Between Vector and Array Codes

Array codes have various connections with vector codes. Clearly, vector codes of blocklength $n$ constitute a special subclass ($m = 1$) of array codes. It is of particular interest to consider the connection between vector codes over extension fields and array codes over base fields. Via the one-to-one correspondence between the extension field $\text{GF}(q^m)$ and all $m$-dimensional column vectors $\mathbf{F}^m$, there is an one-to-one correspondence between the $n$-dimensional row vectors over $\text{GF}(q^m)$ and all $m$-by-$n$ matrices over $\mathbf{F}$. Let us denote this correspondence as $P(\cdot) : [\text{GF}(q^m)]^\mathbf{F} \rightarrow M_{m,n}(\mathbf{F})$. Thus, any vector code of length $n$ over $\text{GF}(q^m)$ can be mapped to an $m$-by-$n$ array code via $P(\cdot)$. Also, this mapping preserves the rank distance of the vector code. If the vector code is linear with dimension $k$, then the corresponding array code is also linear with dimension $km$. Furthermore, there is also a correspondence between the generator matrix for the linear vector code and the generator array for its corresponding array code. Suppose $G = \left[ \begin{array}{c} g_0^T \\ g_1^T \\ \vdots \\ g_{k-1}^T \end{array} \right]^T$ is the $k$-by-$n$ generator matrix for an $(n, k)$ vector code over $\text{GF}(q^m)$, where $g_0, g_1, \ldots, g_{k-1}$ are the rows of $G$. Let $\{b_0, b_1, \ldots, b_{m-1}\}$ be a basis set for the elements of $\text{GF}(q^m)$ over $\mathbf{F}$. Any codeword in the vector code can be written as $\sum_{i=0}^{k-1} u_i G_i$, where $u_i$'s are in $\text{GF}(q^m)$. Using the basis set, $u_i = \sum_{j=0}^{m-1} u_j b_j$ for $i = 0, 1, \ldots, k - 1$. Any codeword $c$ in the vector code can be expanded as follows:

$$c = \sum_{i=0}^{k-1} u_i g_i = \sum_{i=0}^{k-1} \sum_{j=0}^{m-1} u_{ij} b_j g_i.$$  \hfill (6)

Projecting both sides of Eq. (6), we have

$$P(c) = \sum_{i=0}^{k-1} \sum_{j=0}^{m-1} u_{ij} P(b_j g_i).$$  \hfill (7)

From Eq. (7), it is clear that the projection of the linear vector code over $\text{GF}(q^m)$ results in an $(m, n, mk)$ array code. Stacking the $mk$ matrices $P(b_j g_i)$ for $i = 0, 1, \ldots, k - 1$ and $j = 0, 1, \ldots, m - 1$ produces a generator array of the corresponding array code. The appropriate relations for the mapping $P^{-1}(\cdot) : M_{m,n}(\mathbf{F}) \rightarrow [\text{GF}(q^m)]^\mathbf{F}$ can also be derived accordingly, and the details are omitted here.

B. Relation Between the Singleton Bounds

From the discussion above, an $(n, k)$ linear vector codes over $\text{GF}(q^m)$ corresponds to an $(m, n, mk)$ linear array code with rate $R = \frac{mk}{m} = \frac{k}{n}$. Thus, linear vector codes of length $n$ over $\text{GF}(q^m)$ correspond to a subclass of linear array codes whose dimensions are multiples of the number of rows of the codematrices. The rank distance is invariant under this correspondence. Thus, our Singleton bound (3), when restricted to this subclass of linear array codes, becomes the bound in (1) when $m \geq n$ and that in (2) when $m < n$. It is easy to verify that the bound in [14, Corollary 1] is a special case of our Singleton bound. Also, for $R \neq 0$, our Singleton bound implies $d \leq \min \{m, n\}$. Thus, our new Singleton bound implies all four previously proposed bounds mentioned in Section I as special cases. The correspondence between vector codes and array codes above implies that linear MRD codes, if exist, correspond to linear MDS array codes. Our Singleton bound is more general since it applies to any array code, whereas the bounds in (1) and (2) apply only to the subclass of linear array codes corresponding to linear vector codes.

C. New Construction of MRD Codes

Gabidulin codes require $m \geq n$, which implies that Gabidulin codes have to use very large fields as their alphabets, especially when the length of the code is large. This may not be practical or suitable for some applications.

As mentioned above, the existence of MRD codes when $n > m$ and how to construct these codes are open research problems. Below, we show that when $mk$ is a multiple of $n$, MRD codes of length $n$ ($n > m$) indeed exist and can be constructed by using the correspondence detailed in Section IV-A. The construction is described as a constructive proof of the following theorem:

Theorem 2: When $1 \leq m, k \leq n$ and $mk$ is a multiple of $n$, an MRD code over $\text{GF}(q^m)$ of length $n$ and cardinality $q^{mk}$ exists.

Proof: First consider an $(n', k')$ MRD code $\mathbb{C}_1$ with $d_1 = n' - k' + 1$ over $\text{GF}(q^{m'})$ for $m' \geq n'$. Such a code can be constructed using Gabidulin’s approach. Via the mapping $P(\cdot)$, this code corresponds to an $(n', m', m'k')$ linear MDS array code $\mathbb{C}_1'$ with the same rank distance $d_1$. Furthermore, the transpose code of $\mathbb{C}_1'$ is an $(n', m', m'k')$ linear MDS array code $\mathbb{C}_2'$ with rank distance $d_1$. Clearly $1 \leq m', k' \leq n$. Let us assume $m'k'$ is a multiple of $n'$, then via $P^{-1}(\cdot)$, $\mathbb{C}_2'$ corresponds to a vector code $\mathbb{C}_1$ over $\text{GF}(q^{m'})$ $(m = n')$ with rank distance $d_1$, blocklength $n = n'$, and cardinality $q^{mk}$.
\[ N = q^{mk} \] It is easy to check that \( C_1 \) over \( \text{GF}(q^n) \) achieves the equality of the bound (2) and is indeed an MRD code. Note that the only condition in the above construction is that \( mk \) is a multiple of \( n \). The relation between the four codes is illustrated in Figure 1.

![Connections between MRD codes and their corresponding MDS array codes in the proof](image)

Let \( C \) be an \((n, k, d) = (n - k + 1)\) MRD code over \( \text{GF}(q^n) \) \((n \leq m)\), and let \( C^l \) be the code obtained by \( l \) cartesian products of \( C \). Thus, \( C^l \) is an array code over \( \text{GF}(q^n) \), dimension \( k^l = kl \), and minimum rank distance \( d^l = d = n - k + 1 \). Note that \( C^l \) is an MRD code if and only if \( n = m \). Thus, \( k^l = m \) is a multiple of \( n^l \), i.e., these codes also satisfy the condition of our new construction. In addition, the code length \( n \) of the MRD codes based on the cartesian product construction is a multiple of the degree of the extension \( m \). Thus, our construction is less restrictive on the parameters of MRD codes than the cartesian product construction. However, it can be easily shown that codes based on our construction are group codes and not necessarily linear.

**D. Applications**

Gabidulin codes are used in the GPT public-key cryptosystem and space-time code. However, Gabidulin codes require \( m \geq n \), which often means that the codes have to use very large fields as their alphabets, especially when the length of the code is large. This may not be practical or suitable for some applications. The MRD codes obtained by our new construction (and their corresponding MDS array codes) achieve optimal rank distance, and hence they have applications in cryptography and space-time coding as well. But the MRD codes obtained via our new construction do not have the inconvenience of requiring large fields as their alphabets.

Suppose we design \( n_x \)-by-\( T \) space-time block (or trellis) codes, the codematrix of which is transmitted over \( n_x \) transmit antennas during \( T \) symbol epochs. Note that the minimum rank distance over all possible pairs of distinct codematrixes represents the transmit diversity gain achieved by a space-time code over quasi-static flat Rayleigh fading channel (see, for example, [6], [12]). Thus, we have the following corollary of Theorem 1:

**Corollary 2:** For an \( n_x \)-by-\( T \) \((n_x \leq T)\) space-time block (or trellis) codes of size \( N \) over \( \text{GF}(q) \), the maximum transmit diversity gain \( d \) over quasi-static flat Rayleigh fading channel is given by \( d \leq n_x - r + 1 \), where \( r \) denotes the ratio \( \log_q N \) and represents the number of message symbols over \( \text{GF}(q) \) transmitted during each channel usage.

Note that the quantity \( r \) is analogous to the rate of a vector code \( k/n \). In the bound above, it is clear that \( d_r \leq n_x \) for any \( \log_q N \). It is interesting to note that the tradeoff between \( d \) and \( r \) in Corollary 2 has a similar form to the fundamental tradeoff between the diversity gain and multiplexing gain given by Zheng and Tse [13]. But the two results are actually different since the diversity gain defined in [13] is different from that in [12].

**References**