Constant-Rank Codes and Their Connection to Constant-Dimension Codes

Maximilien Gadouleau, *Member, IEEE*, and Zhiyuan Yan, *Senior Member, IEEE*

Abstract—Constant-dimension codes have recently received attention due to their significance to error control in noncoherent random linear network coding. What the maximal cardinality of any constant-dimension code with finite dimension and minimum distance is and how to construct the optimal constant-dimension code (or codes) that achieves the maximal cardinality both remain open research problems. In this paper, we introduce a new approach to solving these two problems. We first establish a connection between constant-rank codes and constant-dimension codes. Via this connection, we show that optimal constant-dimension codes correspond to optimal constant-rank codes over matrices with sufficiently many rows. As such, the two aforementioned problems are equivalent to determining the maximum cardinality of constant-rank codes and to constructing optimal constant-rank codes, respectively. To this end, we then derive bounds on the maximum cardinality of a constant-rank code with a given minimum rank distance, propose explicit constructions of optimal or asymptotically optimal constant-rank codes, and establish asymptotic bounds on the maximum rate of a constant-rank code.

Index Terms—Constant-dimension codes, constant-weight codes, error control codes, injection metric, network coding, random linear network coding, rank metric codes, subspace codes, subspace metric.

I. INTRODUCTION

W HILE random linear network coding [1]–[3] has proved to be a powerful tool for disseminating information in networks, it is highly susceptible to errors caused by various sources, such as noise, malicious or malfunctioning nodes, or insufficient min-cut. If received packets are linearly combined at random to deduce the transmitted message, even a single error in one erroneous packet could render the entire transmission useless. Thus, error control for random linear network coding is critical and has received growing attention recently. Error control schemes proposed for random linear network coding assume two types of transmission models: some [4]–[8] depend on and take advantage of the underlying network topology or the particular linear network coding operations performed at various network nodes; others [9], [10] assume that the transmitter and receiver have no knowledge of such channel transfer characteristics. The contrast is similar to that between coherent and noncoherent communication systems.

Error control for noncoherent random linear network coding was first considered in [9].[1] Motivated by the property that random linear network coding is vector-space preserving, an operator channel that captures the essence of the noncoherent transmission model was defined in [9]. Similar to codes defined in complex Grassmannians for noncoherent multiple-antenna channels, codes defined in Grassmannians over a finite field [12], [13] play a significant role in error control for noncoherent random linear network coding. We refer to these codes as constant-dimension codes (CDCs) henceforth. These codes can use either the subspace metric [9] or the injection metric [14]. The standard advocated approach to random linear network coding (see, e.g., [2]) involves transmission of packet headers used to record the particular linear combination of the components of the message present in each received packet. From coding theoretic perspective, the set of subspaces generated by the standard approach may be viewed as a **suboptimal** CDC with minimum injection distance 1 in a Grassmannian, because the whole Grassmannian forms a CDC with minimum injection distance 1 [9]. Hence, studying random linear network coding from coding theoretic perspective results in better error control schemes.

General studies of subspace codes started only recently (see, for example, [15] and [16]). On the other hand, there is a steady stream of works related to codes in Grassmannians. For example, Delsarte [12] proved that a Grassmannian endowed with the injection distance forms an association scheme, and derived its parameters. The nonexistence of perfect codes in Grassmannians was proved in [13] and [17]. In [18], it was shown that Steiner structures yield diameter-perfect codes in Grassmannians; properties and constructions of these structures were studied in [19]; in [20], it was shown that Steiner structures result in optimal CDCs. Related work on certain intersecting families and on byte-correcting codes can be found in [21] and [22], respectively. An application of codes in Grassmannians

[1]A related work [11] considers security issues in noncoherent random linear network coding.

to linear authentication schemes was considered in [23]. In [9], a Singleton bound for CDCs and a family of codes that are **nearly** Singleton-bound-achieving are proposed, a recursive construction of CDCs which outperform the codes in [9] was given in [24], while a class of codes with even greater cardinality was given in [25]. Despite the **asymptotic optimality** of the Singleton bound and the codes proposed in [9], neither is optimal in finite cases: upper bounds tighter than the Singleton bound exist and can be achieved in some special cases [20]. Thus, two research problems about CDCs remain open: the **maximal cardinality** of a CDC with **finite** dimension and minimum distance is yet to be determined, and it is not clear how to construct an optimal code that achieves the maximal cardinality.

In this paper, we introduce a novel approach to solving the two aforementioned problems. Namely, we aim to solve these problems via constant-rank codes (CRCs), which are the counterparts in rank metric codes of constant Hamming weight codes. There are several reasons for our approach. First, it is difficult to solve the two problems above directly based on CDCs since projective spaces lack a natural group structure [10]. Also, the rank metric is very similar to the Hamming metric in many aspects, and hence, familiar results from the Hamming space can be readily adapted. Furthermore, existing results for rank metric codes in the literature are more extensive than those for CDCs. Finally, the rank metric has been shown relevant to error control for both noncoherent [10] and coherent [14] random linear network coding.

Based on our approach, this paper makes two main contributions. Our first main contribution is that we establish a connection between CRCs and CDCs. Via this connection, we show that optimal CDCs correspond to optimal CRCs over matrices with sufficiently many rows. This connection converts the aforementioned open research problems about CDCs into research problems about CRCs, thereby allowing us to take advantage of existing results on rank metric codes in general to tackle such problems. Despite previous works on rank metric codes, constant-rank codes per se unfortunately have received little attention in the literature. Our second main contribution is our investigation of CRCs. In particular, we derive upper and lower bounds on the maximum cardinality of a CRC, propose explicit constructions of optimal or asymptotically optimal CRCs, and establish asymptotic bounds on the maximum rate of CRCs. Our investigation of CRCs not only is important for our construction of CDCs, but also serves as a powerful tool to study CDCs and rank metric codes.

The rest of the paper is organized as follows. Section II reviews some necessary background. In Section III, we determine the connection between optimal CRCs and optimal CDCs. In Section IV, we study the maximum cardinality of CRCs, and present our results on the asymptotic behavior of the maximum rate of a CRC.

II. PRELIMINARIES

A. Rank Metric Codes

Error correction codes with the rank metric [26]–[28] have been receiving steady attention in the literature due to their applications in storage systems [28], public-key cryptosystems [29], space-time coding [30], and network coding [9], [10]. Below, we review some important properties of rank metric codes established in [26]–[28].

For all $\mathbf{X}, \mathbf{Y} \in \mathrm{GF}(q)^{m \times n}$, it is easily verified that $d_{\mathrm{R}}(\mathbf{X}, \mathbf{Y}) \stackrel{\mathrm{def}}{=} \mathrm{rk}(\mathbf{X} - \mathbf{Y})$ is a metric over $\mathrm{GF}(q)^{m \times n}$, referred to as the *rank metric* henceforth. Please note that the rank metric for the vector representation of rank metric codes is defined differently [27]. Since the connection between the matrix representation of rank metric codes and CDCs is more natural, we consider the matrix representation of rank metric codes henceforth. We denote the number of matrices of rank $r (0 \leq r \leq \min\{m, n\})$ in $\mathrm{GF}(q)^{m \times n}$ as $N_{\mathrm{R}}(q, m, n, r) = \begin{bmatrix} n \\ r \end{bmatrix} \alpha(m, r)$ [27], where $\alpha(m, 0) \stackrel{\mathrm{def}}{=} 1$, $\alpha(m, r) \stackrel{\mathrm{def}}{=} \prod_{i=0}^{r-1}(q^m - q^i)$, and $\begin{bmatrix} n \\ r \end{bmatrix} \stackrel{\mathrm{def}}{=} \alpha(n, r)/\alpha(r, r)$ for $r \geq 1$. The term $\begin{bmatrix} n \\ r \end{bmatrix}$ is often referred to as a Gaussian binomial [31], and satisfies

$$q^{r(n-r)} \leq \begin{bmatrix} n \\ r \end{bmatrix} < K_q^{-1} q^{r(n-r)} \tag{1}$$

for all $0 \leq r \leq n$, where $K_q = \prod_{j=1}^{\infty}(1 - q^{-j})$ [32]. K_q^{-1} decreases with q and satisfies $1 < K_q^{-1} \leq K_2^{-1} < 4$. We denote the volume (i.e., the number of points) of the intersection of two **spheres** in $\mathrm{GF}(q)^{m \times n}$ of radii r and s and with rank distance d between their centers as $J_{\mathrm{R}}(q, m, n, r, s, d)$. A closed-form formula for $J_{\mathrm{R}}(q, m, n, r, s, d)$ is determined in [33].

A rank metric code is a subset of $\mathrm{GF}(q)^{m \times n}$, and its *minimum rank distance*, denoted as d_{R}, is simply the minimum rank distance over all possible pairs of distinct codewords. It is shown in [26]–[28] that the minimum rank distance of a code of cardinality M in $\mathrm{GF}(q)^{m \times n}$ satisfies $d_{\mathrm{R}} \leq n - \log_{q^m} M + 1$. In this paper, we refer to this bound as the Singleton bound for rank metric codes and codes that attain the equality as maximum rank distance (MRD) codes. We refer to the subclass of MRD codes introduced in [34] as generalized Gabidulin codes. These codes are based on the vector view of rank metric codes, described as follows. The columns of a matrix $\mathbf{X} \in \mathrm{GF}(q)^{m \times n}$ can be mapped into elements of the field $\mathrm{GF}(q^m)$ according to a basis B_m of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$. Hence, $\mathbf{X}$ can be mapped into the vector $\mathbf{x} \in \mathrm{GF}(q^m)^n$, and the rank of $\mathbf{X}$ is equal to the maximum number of linearly independent coordinates of $\mathbf{x}$. Generalized Gabidulin codes are linear MRD codes over $\mathrm{GF}(q^m)$ for $m \geq n$. For all $q, 1 \leq d \leq r \leq n \leq m$, the number of codewords of rank r in an $(n, n - d + 1, d)$ linear MRD code over $\mathrm{GF}(q^m)$ is denoted by $M(q, m, n, d, r)$, and it is known that [27]

$$M(q, m, n, d, r) = \begin{bmatrix} n \\ r \end{bmatrix} \sum_{j=d}^{r}(-1)^{r-j} \begin{bmatrix} r \\ j \end{bmatrix}$$
$$\times q^{(r-j)(r-j-1)/2} \left(q^{m(j-d+1)} - 1 \right). \tag{2}$$

We will omit the dependence of the quantities defined above on q, m, and n when there is no ambiguity in some proofs.

B. Constant-Dimension Codes

We refer to the set of all subspaces of $\mathrm{GF}(q)^n$ with dimension r as the Grassmannian of dimension r and denote it as $E_r(q, n)$,

where $|E_r(q,n)| = \begin{bmatrix} n \\ r \end{bmatrix}$; we refer to $E(q,n) = \bigcup_{r=0}^{n} E_r(q,n)$ as the projective space. For $U, V \in E(q,n)$, their intersection $U \cap V$ is also a subspace in $E(q,n)$, and we denote the smallest subspace containing the union of U and V as $U + V$. Both the *subspace metric* [9, (3)] $d_{\mathrm{S}}(U,V) \stackrel{\mathrm{def}}{=} \dim(U+V) - \dim(U \cap V) = 2\dim(U+V) - \dim(U) - \dim(V)$ and *injection metric* [14, Def.1] $d_{\mathrm{I}}(U,V) \stackrel{\mathrm{def}}{=} \frac{1}{2}d_{\mathrm{S}}(U,V) + \frac{1}{2}|\dim(U) - \dim(V)| = \dim(U+V) - \min\{\dim(U), \dim(V)\}$ are metrics over $E(q,n)$.

The Grassmannian $E_r(q,n)$ endowed with either the subspace metric or the injection metric forms an association scheme [9], [12]. Since $d_{\mathrm{S}}(U,V) = 2d_{\mathrm{I}}(U,V)$ for all $U, V \in E_r(q,n)$ and the injection distance provides a more natural distance spectrum, i.e., $0 \leq d_{\mathrm{I}}(U,V) \leq r$ for all $U, V \in E_r(q,n)$, we consider only the injection metric for Grassmannians and CDCs henceforth. We denote the number of subspaces in $E_r(q,n)$ at distance d from a given subspace as $N_{\mathrm{C}}(d) = q^{d^2} \begin{bmatrix} r \\ d \end{bmatrix} \begin{bmatrix} n-r \\ d \end{bmatrix}$ [9].

A subset of $E_r(q,n)$ is called a constant-dimension code (CDC). We denote the **maximum** cardinality of a CDC in $E_r(q,n)$ with minimum distance d as $A_{\mathrm{C}}(q,n,r,d)$. Constructions of CDCs and bounds on $A_{\mathrm{C}}(q,n,r,d)$ have been given in [9], [16], [20], [24], [25], [35]. In particular, $A_{\mathrm{C}}(q,n,r,1) = \begin{bmatrix} n \\ r \end{bmatrix}$ and it is shown [9], [20] for $r \leq \lfloor \frac{n}{2} \rfloor$ and $2 \leq d \leq r$

$$q^{(n-r)(r-d+1)} \leq A_{\mathrm{C}}(q,n,r,d) \leq \frac{\begin{bmatrix} n \\ r-d+1 \end{bmatrix}}{\begin{bmatrix} r \\ r-d+1 \end{bmatrix}}. \qquad (3)$$

III. CONNECTION BETWEEN CONSTANT-DIMENSION CODES AND CONSTANT-RANK CODES

In this section, we first establish some connections between the rank metric and the injection metric. We then define constant-rank codes and we show how optimal constant-rank codes can be used to construct optimal CDCs.

Let us denote the row space and the column space of $\mathbf{X} \in \mathrm{GF}(q)^{m \times n}$ over $\mathrm{GF}(q)$ as $R(\mathbf{X})$ and $C(\mathbf{X})$, respectively. Following the convention of coding theory, a generator matrix of a subspace U is any full rank matrix whose row space is the subspace U. The notations introduced above are naturally extended to codes as follows: for $\mathcal{C} \subseteq \mathrm{GF}(q)^{m \times n}$, $C(\mathcal{C}) \stackrel{\mathrm{def}}{=} \{U \in E(q,m) : \exists \mathbf{M} \in \mathcal{C}, C(\mathbf{M}) = U\}$ and $R(\mathcal{C}) \stackrel{\mathrm{def}}{=} \{V \in E(q,n) : \exists \mathbf{M} \in \mathcal{C}, R(\mathbf{M}) = V\}$.

Lemma 1: For $U \in E_r(q,m)$, $V \in E_r(q,n)$, and $\mathbf{X} \in \mathrm{GF}(q)^{m \times n}$ with rank r, $C(\mathbf{X}) = U$ and $R(\mathbf{X}) = V$ if and only if there exist a generator matrix $\mathbf{G} \in \mathrm{GF}(q)^{r \times m}$ of U and a generator matrix $\mathbf{H} \in \mathrm{GF}(q)^{r \times n}$ of V such that $\mathbf{X} = \mathbf{G}^T\mathbf{H}$.

The proof of Lemma 1 is straightforward and hence omitted. We remark that $\mathbf{X} = \mathbf{G}^T\mathbf{H}$ is referred to as a rank factorization [36]. We now derive a relation between the rank distance between two matrices and the injection distances between their respective row and column spaces.

Theorem 1: For all $\mathbf{X}, \mathbf{Y} \in \mathrm{GF}(q)^{m \times n}$

$$d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})) + d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y}))$$
$$- |\mathrm{rk}(\mathbf{X}) - \mathrm{rk}(\mathbf{Y})|$$
$$\leq d_{\mathrm{R}}(\mathbf{X}, \mathbf{Y})$$
$$\leq \min\{d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})), d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y}))\}$$

$$+ \min\{\mathrm{rk}(\mathbf{X}), \mathrm{rk}(\mathbf{Y})\}.$$

Proof: By Lemma 1, we have $\mathbf{X} = \mathbf{C}^T\mathbf{R}$ and $\mathbf{Y} = \mathbf{D}^T\mathbf{S}$, where $\mathbf{C} \in \mathrm{GF}(q)^{\mathrm{rk}(\mathbf{X}) \times m}$, $\mathbf{R} \in \mathrm{GF}(q)^{\mathrm{rk}(\mathbf{X}) \times n}$, $\mathbf{D} \in \mathrm{GF}(q)^{\mathrm{rk}(\mathbf{Y}) \times m}$, $\mathbf{S} \in \mathrm{GF}(q)^{\mathrm{rk}(\mathbf{Y}) \times n}$ are generator matrices of $C(\mathbf{X}), R(\mathbf{X}), C(\mathbf{Y})$, and $R(\mathbf{Y})$, respectively. Hence, $\mathbf{X} - \mathbf{Y} = (\mathbf{C}^T| - \mathbf{D}^T)(\mathbf{R}^T|\mathbf{S}^T)^T$ and $\mathrm{rk}(\mathbf{X} - \mathbf{Y}) \leq \min\{\mathrm{rk}(\mathbf{C}^T| - \mathbf{D}^T), \mathrm{rk}(\mathbf{R}^T|\mathbf{S}^T)\}$. Sylvester's law of nullity in [37, Corollary 6.1] or in [38, 0.4.5 (c)], states that $\mathrm{rk}(\mathbf{AB}) \geq \mathrm{rk}(\mathbf{A}) + \mathrm{rk}(\mathbf{B}) - n$ for any matrices $\mathbf{A}$ with n columns and $\mathbf{B}$ with n rows. Therefore

$$\mathrm{rk}(\mathbf{C}^T| - \mathbf{D}^T) + \mathrm{rk}(\mathbf{R}^T|\mathbf{S}^T) - \mathrm{rk}(\mathbf{X}) - \mathrm{rk}(\mathbf{Y})$$
$$\leq \mathrm{rk}(\mathbf{X} - \mathbf{Y})$$
$$\leq \min\{\mathrm{rk}(\mathbf{C}^T| - \mathbf{D}^T), \mathrm{rk}(\mathbf{R}^T|\mathbf{S}^T)\}.$$

Since $\mathrm{rk}(\mathbf{C}^T| - \mathbf{D}^T) = d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y})) + \min\{\mathrm{rk}(\mathbf{X}), \mathrm{rk}(\mathbf{Y})\}$ and $\mathrm{rk}(\mathbf{R}^T|\mathbf{S}^T) = d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})) + \min\{\mathrm{rk}(\mathbf{X}), \mathrm{rk}(\mathbf{Y})\}$, we obtain the claim. ∎

A *constant-rank code* (CRC) of constant rank r in $\mathrm{GF}(q)^{m \times n}$ is a nonempty subset of $\mathrm{GF}(q)^{m \times n}$ such that all elements have rank r. Proposition 1 below shows how a CRC leads to two CDCs with their minimum injection distance related to the minimum rank distance of the CRC.

Proposition 1: Let $\mathcal{C}$ be a CRC of constant rank r and minimum distance d_{R} in $\mathrm{GF}(q)^{m \times n}$. Then $R(\mathcal{C}) \subseteq E_r(q,n)$ and $C(\mathcal{C}) \subseteq E_r(q,m)$ have minimum distances at least $d_{\mathrm{R}} - r$.

Proposition 1 follows directly from Theorem 1, and hence, its proof is omitted. When the minimum rank distance of a CRC is greater than its constant rank, Proposition 2 below shows how the CRC leads to two CDCs with the **same cardinality**, and the relations between their distances can be further strengthened.

Proposition 2: If $\mathcal{C}$ is a CRC of constant rank r and minimum rank distance $d + r (1 \leq d \leq r)$ in $\mathrm{GF}(q)^{m \times n}$, then $R(\mathcal{C}) \subseteq E_r(q,n)$ and $C(\mathcal{C}) \subseteq E_r(q,m)$ have cardinality $|\mathcal{C}|$ and their minimum injection distances satisfy $d_{\mathrm{I}}(C(\mathcal{C})) + d_{\mathrm{I}}(R(\mathcal{C})) \leq d + r$.

Proof: Let $\mathbf{X}$ and $\mathbf{Y}$ be **any** two distinct codewords in $\mathcal{C}$. By Theorem 1, $d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})) \geq d_{\mathrm{R}}(\mathbf{X}, \mathbf{Y}) - r \geq d > 0$, and hence, $d_{\mathrm{I}}(R(\mathcal{C})) \geq d$ and $|R(\mathcal{C})| = |\mathcal{C}|$. Similarly, $d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y})) \geq d > 0$, and thus $d_{\mathrm{I}}(C(\mathcal{C})) \geq d$ and $|C(\mathcal{C})| = |\mathcal{C}|$. Furthermore, if $d_{\mathrm{R}}(\mathbf{X}, \mathbf{Y}) = d + r$, then by Theorem 1, $d + r \geq d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y})) + d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})) \geq d_{\mathrm{I}}(C(\mathcal{C})) + d_{\mathrm{I}}(R(\mathcal{C}))$. ∎

We remark that the requirement of having a minimum distance greater than the constant rank is a strong condition on the CRC. Indeed, any codeword of a linear code has rank at least equal to the minimum distance of a code. Therefore, no set of codewords of a linear code (and, in particular, a linear MRD code) satisfies this condition. Therefore, while CRCs with minimum distance no more than their constant-rank will be directly constructed from linear MRD codes in Section IV-B, designing CRCs with minimum distance greater than their constant-rank will require translates of codes instead, which are not as easy to manipulate.

Propositions 1 and 2 show how to construct CDCs from a CRC. Alternatively, Proposition 3 below shows that we can construct a CRC from a pair of CDCs.

Proposition 3: Let $\mathcal{M}$ be a CDC in $E_r(q, m)$ and $\mathcal{N}$ be a CDC in $E_r(q, n)$ such that $|\mathcal{M}| = |\mathcal{N}|$. Then there exists a CRC $\mathcal{C} \subseteq \mathrm{GF}(q)^{m \times n}$ with constant rank r and cardinality $|\mathcal{M}|$ satisfying $C(\mathcal{C}) = \mathcal{M}$ and $R(\mathcal{C}) = \mathcal{N}$. Furthermore, its minimum distance d_{R} satisfies $d_{\mathrm{I}}(\mathcal{N}) + d_{\mathrm{I}}(\mathcal{M}) \leq d_{\mathrm{R}} \leq \min\{d_{\mathrm{I}}(\mathcal{N}), d_{\mathrm{I}}(\mathcal{M})\} + r$.

Proof: Denote the generator matrices of the component subspaces of $\mathcal{M}$ and $\mathcal{N}$ as $\mathbf{G}_i$ and $\mathbf{H}_i$, respectively, and define the code $\mathcal{C}$ formed by the codewords $\mathbf{X}_i = \mathbf{G}_i^T \mathbf{H}_i$ for $0 \leq i \leq |\mathcal{M}| - 1$. Then $C(\mathcal{C}) = \mathcal{M}$ and $R(\mathcal{C}) = \mathcal{N}$ by Lemma 1 and the lower bound on d_{R} follows from Theorem 1. Let $\mathbf{X}_i$ and $\mathbf{X}_j$ be distinct codewords in $\mathcal{C}$ such that $d_{\mathrm{I}}(C(\mathbf{X}_i), C(\mathbf{X}_j)) = d_{\mathrm{I}}(\mathcal{M})$. By Theorem 1, we obtain $d_{\mathrm{R}} \leq d_{\mathrm{R}}(\mathbf{X}_i, \mathbf{X}_j) \leq d_{\mathrm{I}}(\mathcal{M}) + r$. Similarly, we also obtain $d_{\mathrm{R}} \leq d_{\mathrm{I}}(\mathcal{N}) + r$. ∎

The connections between general CRCs and CDCs derived above naturally imply relations between optimal CRCs and optimal CDCs. We denote the maximum cardinality of a CRC in $\mathrm{GF}(q)^{m \times n}$ with constant rank r and minimum rank distance d as $A_{\mathrm{R}}(q, m, n, d, r)$. If $\mathcal{C}$ is a CRC in $\mathrm{GF}(q)^{m \times n}$ with constant rank r, then its transpose code $\mathcal{C}^T$ forms a CRC in $\mathrm{GF}(q)^{n \times m}$ with the same constant rank, minimum distance, and cardinality. Therefore, $A_{\mathrm{R}}(q, m, n, d, r) = A_{\mathrm{R}}(q, n, m, d, r)$, and henceforth in this paper, we assume $n \leq m$ without loss of generality. We further observe that $A_{\mathrm{R}}(q, m, n, d, r)$ is a nondecreasing function of m and n, and a nonincreasing function of d, and that $A_{\mathrm{C}}(q, n, r, d)$ is a nondecreasing function of n and a nonincreasing function of d.

Proposition 4: For all q, $1 \leq d \leq r \leq n \leq m$, and any $0 \leq p \leq r$

$$\min\{A_{\mathrm{C}}(q, n, r, d + p), A_{\mathrm{C}}(q, m, r, r - p)\}$$
$$\leq A_{\mathrm{R}}(q, m, n, d + r, r) \leq A_{\mathrm{C}}(q, n, r, d). \quad (4)$$

Proof: Using the monotone properties of $A_{\mathrm{R}}(q, m, n, d_{\mathrm{R}}, r)$ and $A_{\mathrm{C}}(q, n, r, d)$ above, the upper bound follows from Proposition 2, while the lower bound follows from Proposition 3 for $d_{\mathrm{I}}(\mathcal{M}) = r - p$ and $d_{\mathrm{I}}(\mathcal{N}) = d + p$. ∎

We remark that the lower bound in (4) is trivial for $d + p > \min\{r, n - r\}$ or $r - p > \min\{r, m - r\}$. Therefore, the lower bound in (4) is nontrivial when $\max\{0, 2r - m\} \leq p \leq \min\{r - d, n - r - d\}$.

Combining the bounds in (4), we obtain that the cardinalities of optimal CRCs over matrices with sufficiently many rows equal the cardinalities of CDCs with related distances. Furthermore, we show that optimal CDCs can be constructed from such optimal CRCs.

Theorem 2: For all q, $2r \leq n \leq m$, and $1 \leq d \leq r$, $A_{\mathrm{R}}(q, m, n, d + r, r) = A_{\mathrm{C}}(q, n, r, d)$ if either $d = r$ or $m \geq m_0$, where $m_0 = (n - r)(r - d + 1) + r + 1$. Furthermore, if $\mathcal{C}$ is an optimal CRC in $\mathrm{GF}(q)^{m \times n}$ with constant rank r and minimum distance $d + r$ for $m \geq m_0$ or $d = r$, then $R(\mathcal{C})$ is an optimal CDC in $E_r(q, n)$ with minimum distance d.

Proof: First, the case where $d = r$ directly follows from (4) for $p = 0$. Second, if $d < r$ and $m \geq m_0$, by (3) we obtain $A_{\mathrm{C}}(q, m, r, r) \geq q^{m-r} \geq q^{m_0 - r}$. Also, by [32, Lemma 1], we obtain $q^{r(r-d+1)-1} < \alpha(r, r - d + 1) \leq q^{r(r-d+1)}$ for all $2 \leq d < r$, and hence, (3) yields $A_{\mathrm{C}}(q, n, r, d) < q^{(n-r)(r-d+1)+1} = q^{m_0 - r} \leq A_{\mathrm{C}}(q, m, r, r)$. Thus, when $p = 0$, the lower bound in (4) simplifies to $A_{\mathrm{R}}(q, m, n, d + r, r) \geq A_{\mathrm{C}}(q, n, r, d)$. Combining with the upper bound in (4), we obtain $A_{\mathrm{R}}(q, m, n, d + r, r) = A_{\mathrm{C}}(q, n, r, d)$.

The second claim immediately follows from Proposition 2. ∎

Theorem 2 implies that to determine $A_{\mathrm{C}}(q, n, r, d)$ and to construct optimal CDCs, it is sufficient to determine $A_{\mathrm{R}}(q, m, n, d + r, r)$ and to construct optimal CRCs over matrices with sufficiently many rows. We observe that this implies that $A_{\mathrm{R}}(q, m, n, d + r, r)$ remains constant for all $m \geq m_0$. When $d = r$, $A_{\mathrm{R}}(q, m, n, 2r, r)$ remains constant for $m \geq n$. When $d = 1$, $m_0 = (n - r + 1)r + 1$, but $A_{\mathrm{R}}(q, m, n, r + 1, r)$ remains constant for $m \geq n$, and this is shown in Section IV-B.

In comparison to existing constructions of CDCs [9], [10], [15], [20], [24], [35], our construction based on CRCs has two advantages. **First** and foremost, by Theorem 2, our construction leads to optimal CDCs for all parameter values. In contrast, none of previously proposed constructions lead to optimal CDCs for all parameter values. For example, the construction based on liftings of rank metric codes [9], [10] leads to suboptimal CDCs (though sometimes they may be nearly optimal). This is because CDCs of dimension r based on liftings of rank metric codes have the highest possible covering radius r [39], which implies there exists a subspace that can be added to such CDCs without decreasing the minimum distance. The CDCs constructed in similar approaches [24] are not optimal for the same reason. The optimality for some constructions [15], [25] are not clear. The construction based on Steiner structures [20] and that based on computational techniques [35] lead to optimal CDCs, but are applicable to special cases only. The **second** advantage of our construction is an additional degree of freedom, which is the number m of rows of the matrices. By Theorem 2, optimal CRCs lead to optimal CDCs provided that $m \geq m_0$, and hence, the parameter m may vary anywhere above the lower bound m_0. On the other hand, the constructions in the literature use fixed dimensions and do not introduce any new parameter. For instance, in order to obtain a CDC in $E_r(q, n)$ by lifting a rank metric code, the original code must be in $\mathrm{GF}(q)^{r \times (n-r)}$. This additional degree of freedom is significant for code design, as it may be easier to construct optimal CRCs with larger m. Thus, our construction is a very promising approach to solving the two open research problems mentioned in Section I.

IV. CONSTANT-RANK CODES

Having proved that optimal CRCs over matrices with sufficiently many rows lead to optimal CDCs, in this section we investigate the properties of CRCs.

A. Bounds

We now derive bounds on the maximum cardinality of CRCs. We first remark that the bounds on $A_{\mathrm{R}}(q, m, n, d, r)$ derived in Section III can be used in this section. Also, since

$A_{\mathrm{R}}(q,m,n,1,r) = N_{\mathrm{R}}(q,m,n,r)$ and $A_{\mathrm{R}}(q,m,n,d,r) = 1$ for $d > 2r$, we shall assume $2 \leq d \leq 2r$ henceforth.[2]

We first derive the counterparts of the Gilbert and the Hamming bounds for CRCs in terms of intersections of spheres with rank radii.

Proposition 5: For all q, $1 \leq r, d \leq n \leq m$, and $t = \lfloor \frac{d-1}{2} \rfloor$

$$\frac{N_{\mathrm{R}}(q,m,n,r)}{\sum_{i=0}^{d-1} J_{\mathrm{R}}(q,m,n,i,r,r)}$$

$$\leq A_{\mathrm{R}}(q,m,n,d,r)$$

$$\leq \min_{1 \leq s \leq n} \left\{ \frac{N_{\mathrm{R}}(q,m,n,s)}{\sum_{i=0}^{t} J_{\mathrm{R}}(q,m,n,i,s,r)} \right\}.$$

Proof: The proof of the lower bound is straightforward and hence omitted. Let $\mathcal{C} = \{\mathbf{c}_k\}_{k=0}^{K-1}$ be a CRC with constant rank r and minimum distance d in $\mathrm{GF}(q)^{m \times n}$. For all $0 \leq k \leq K-1$ and $0 \leq s \leq n-1$, if we denote the set of matrices in $\mathrm{GF}(q)^{m \times n}$ with rank s and distance $\leq t$ from $\mathbf{c}_k$ as $R_{k,s}$, then $|R_{k,s}| = \sum_{i=0}^{t} J_{\mathrm{R}}(i,s,r)$ for all k. Clearly, $R_{k,s} \cap R_{l,s} = \emptyset$ for all $k \neq l$, and hence, $N_{\mathrm{R}}(s) \geq |\bigcup_{k=0}^{K-1} R_{k,s}| = K|R_{k,s}|$, which yields the upper bound. ∎

We now derive upper bounds on $A_{\mathrm{R}}(q,m,n,d,r)$. We begin by proving the counterpart in rank metric codes of a well-known bound on constant-weight codes proved by Johnson in [40].

Proposition 6 (Johnson Bound for Rank Metric Codes): For all q, $1 \leq r, d < n \leq m$, $A_{\mathrm{R}}(q,m,n,d,r) \leq \frac{q^n-1}{q^{n-r}-1} A_{\mathrm{R}}(q,m,n-1,d,r)$.

Proof: Let $\mathcal{C}$ be an optimal CRC in $\mathrm{GF}(q)^{m \times n}$ with constant rank r and minimum distance d. For all $\mathbf{C} \in \mathcal{C}$ and all $V \in E_{n-1}(q,n)$, we define $f(V,\mathbf{C}) = 1$ if $R(\mathbf{C}) \subseteq V$ and $f(V,\mathbf{C}) = 0$, otherwise. For any $\mathbf{C}$, the row space of $\mathbf{C}$ is contained in $\begin{bmatrix} n-r \\ 1 \end{bmatrix}$ subspaces in $E_{n-1}(q,n)$, and hence, $\sum_{V \in E_{n-1}(q,n)} f(V,\mathbf{C}) = \begin{bmatrix} n-r \\ 1 \end{bmatrix}$; for all V, $\sum_{\mathbf{C} \in \mathcal{C}} f(V,\mathbf{C}) = |\{\mathbf{C} \in C : R(\mathbf{C}) \subseteq V\}|$. Summing over all possible pairs, we obtain

$$\sum_{V \in E_{n-1}(q,n)} \sum_{\mathbf{C} \in \mathcal{C}} f(V,\mathbf{C})$$

$$= \sum_{V \in E_{n-1}(q,n)} |\{\mathbf{C} \in C : R(\mathbf{C}) \subseteq V\}|,$$

$$\sum_{\mathbf{C} \in \mathcal{C}} \sum_{V \in E_{n-1}(q,n)} f(V,\mathbf{C})$$

$$= \begin{bmatrix} n-r \\ 1 \end{bmatrix} A_{\mathrm{R}}(q,m,n,d,r).$$

Hence, there exists $U \in E_{n-1}(q,n)$ such that $|\{\mathbf{C} \in C : R(\mathbf{C}) \subseteq U\}| = \sum_{\mathbf{C} \in \mathcal{C}} f(U,\mathbf{C}) \geq \frac{\begin{bmatrix} n-r \\ 1 \end{bmatrix}}{\begin{bmatrix} n \\ 1 \end{bmatrix}} A_{\mathrm{R}}(q,m,n,d,r)$. By Lemma 1, all the codewords $\mathbf{C}_i$ with $R(\mathbf{C}_i) \subseteq U$ can be expressed as $\mathbf{C}_i = \mathbf{G}_i^T \mathbf{H}_i \mathbf{U}$, where $\mathbf{H}_i \in \mathrm{GF}(q)^{r \times (n-1)}$ and

$\mathbf{U} \in \mathrm{GF}(q)^{(n-1) \times n}$ is a generator matrix of U. Therefore, the code $\{\mathbf{G}_i^T \mathbf{H}_i\}$ forms a CRC in $\mathrm{GF}(q)^{m \times (n-1)}$ with constant rank r, minimum distance d, and cardinality $|\{\mathbf{C} \in C : R(\mathbf{C}) \subseteq U\}|$, and hence, $\frac{q^{n-r}-1}{q^n-1} A_{\mathrm{R}}(q,m,n,d,r) \leq |\{\mathbf{C} \in C : R(\mathbf{C}) \subseteq U\}| \leq A_{\mathrm{R}}(q,m,n-1,d,r)$. ∎

The Singleton bound for rank metric codes yields upper bounds on $A_{\mathrm{R}}(q,m,n,d,r)$. For any $I \subseteq \{0,1,\ldots,n\}$, let $A_{\mathrm{R}}(q,m,n,d,I)$ denote the maximum cardinality of a code in $\mathrm{GF}(q)^{m \times n}$ with minimum rank distance d such that all codewords have ranks belonging to I. Then $A_{\mathrm{R}}(q,m,n,d,r) \leq q^{m(n-d+1)} - A_{\mathrm{R}}(q,m,n,d,P_r)$, where $P_r \stackrel{\text{def}}{=} \{i : 0 \leq i \leq n, |i-r| \geq d\}$. We now determine the counterpart of the Singleton bound for CRCs.

Proposition 7 (Singleton Bound for CRCs): For all $0 \leq i \leq \min\{d-1,r\}$, $A_{\mathrm{R}}(q,m,n,d,r) \leq A_{\mathrm{R}}(q,m,n-i,d-i,J_i)$, where $J_i = \{r-i, r-i+1, \ldots, \min\{n-i,r\}\}$.

Proof: Let $\mathcal{C}$ be an optimal CRC in $\mathrm{GF}(q)^{m \times n}$ with constant rank r and minimum distance d, and consider the code $\mathcal{C}_i$ obtained by puncturing i coordinates of the codewords in $\mathcal{C}$. Since $i \leq r$, the codewords of $\mathcal{C}_i$ all have ranks between $r-i$ and $\min\{n-i,r\}$. Also, since $i < d$, any two codewords have distinct puncturings, and we obtain $|\mathcal{C}_i| = |\mathcal{C}|$ and $d_{\mathrm{R}}(\mathcal{C}_i) \geq d - i$. Hence, $A_{\mathrm{R}}(q,m,n,d,r) = |\mathcal{C}| = |\mathcal{C}_i| \leq A_{\mathrm{R}}(q,m,n-i,d-i,J_i)$. ∎

We now combine the counterpart of the Johnson bound in Proposition 6 and that of the Singleton bound in Proposition 7 in order to obtain an upper bound on $A_{\mathrm{R}}(q,m,n,d,r)$ for $d \leq r$.

Proposition 8: For all q, $1 \leq d \leq r \leq n \leq m$, $A_{\mathrm{R}}(q,m,n,d,r) \leq \begin{bmatrix} n \\ r \end{bmatrix} \alpha(m,r-d+1)$.

Proof: Applying Proposition 6 $n-r$ times successively, we obtain $A_{\mathrm{R}}(q,m,n,d,r) \leq \begin{bmatrix} n \\ r \end{bmatrix} A_{\mathrm{R}}(q,m,r,d,r)$. For $n = r$ and $i = d-1$, $J_i = \{r-d+1\}$ and hence, Proposition 7 yields $A_{\mathrm{R}}(q,m,r,d,r) \leq A_{\mathrm{R}}(q,m,r-d+1,1,r-d+1) = N_{\mathrm{R}}(q,m,r-d+1,r-d+1) = \alpha(m,r-d+1)$. Thus, $A_{\mathrm{R}}(q,m,n,d,r) \leq \begin{bmatrix} n \\ r \end{bmatrix} \alpha(m,r-d+1)$. ∎

We now derive the counterpart in rank metric codes of the Bassalygo–Elias bound [41] and we also tighten the bound when $d > r+1$. For a code $\mathcal{C} \subseteq \mathrm{GF}(q)^{l \times k} (k \leq l)$, $A_i \stackrel{\text{def}}{=} |\{\mathbf{C} \in \mathcal{C} : \mathrm{rk}(\mathbf{C}) = i\}|$ for $0 \leq i \leq l$; we refer to A_i's as the rank distribution of $\mathcal{C}$.

Proposition 9 (Bassalygo–Elias Bound for Rank Metric Codes): For $\max\{r,d\} \leq k \leq n$, $0 \leq s \leq k$, $k \leq l \leq m$, and any code $\mathcal{C} \subseteq \mathrm{GF}(q)^{l \times k}$ with minimum rank distance d and rank distribution A_i's

$$A_{\mathrm{R}}(q,m,n,d,r) \geq \max_{s,\{A_i\},k,l} \frac{\sum_{i=0}^{n} A_i J_{\mathrm{R}}(q,l,k,s,r,i)}{N_{\mathrm{R}}(q,l,k,s)}. \quad (5)$$

Furthermore, if $r+1 < d \leq 2r$, then see (6), shown at the bottom of the next page.

The proof of Proposition 9 is given in Appendix I-A.

Although the RHS of (5) and (6) can be maximized over $\{A_i\}$, it is difficult to do so since $\{A_i\}$ is not available for most rank metric codes with the exception of linear MRD codes.

---

[2]Since the minimum distance of a code is defined using pairs of distinct codewords, the minimum distance for a code of cardinality one is defined to be zero sometimes.

Thus, we derive a bound using the rank weight distribution of linear MRD codes.

Corollary 1: For all q, $1 \leq r, d \leq n \leq m$, $A_{\mathrm{R}}(q, m, n, d, r) \geq N_{\mathrm{R}}(q, m, n, r) q^{m(-d+1)}$.

Proof: Applying (5) to an $(n, n - d + 1, d)$ MRD code over $\mathrm{GF}(q^m)$, we obtain $N_{\mathrm{R}}(s) A_{\mathrm{R}}(d, r) \geq \sum_{i=0}^{n} M(d, i) J_{\mathrm{R}}(s, r, i)$. Summing for all $0 \leq s \leq n$, we obtain $A_{\mathrm{R}}(d, r) \geq N_{\mathrm{R}}(r) q^{m(-d+1)}$ since $\sum_{s=0}^{n} J_{\mathrm{R}}(s, r, i) = N_{\mathrm{R}}(r)$. ∎

The RHS of (5) and (6) decrease rapidly with increasing d, rendering the bounds in (5) and (6) trivial for d approaching $2r$.

Proposition 10 below shows that the bound in Corollary 1 is tight up to a scalar for $d \leq r$. To measure the tightness, we introduce a ratio $C(q, m, n, d, r) \stackrel{\text{def}}{=} A_{\mathrm{R}}(q, m, n, d, r) / [N_{\mathrm{R}}(q, m, n, r) q^{m(-d+1)}]$ for $2 \leq d \leq r \leq n \leq m$.

Proposition 10: For all q, $2 \leq d \leq r \leq n \leq m$, $C(q, m, n, d, r) \leq \frac{q^2}{q^2 - 1}$ for $r + d - 1 \leq m$ and $C(q, m, n, d, r) < \frac{q-1}{q} K_q^{-1}$ otherwise.

Proof: By Proposition 8, $C(d, r) \leq q^{m(d-1)} \alpha(m, r - d + 1) / \alpha(m, r) = q^{(m-r+d-1)(d-1)} / \alpha(m - r + d - 1, d - 1)$. Since $\alpha(n, l) > \frac{q}{q-1} K_q q^{nl}$ for all $1 \leq l \leq n - 1$ [32, Lemma 1], we obtain $C(d, r) < \frac{q-1}{q} K_q^{-1}$. Finally, $\alpha(n, l) \geq \frac{q^2 - 1}{q^2} q^{nl}$ for $l \leq n - l$ [32, Lemma 1] yields $C(d, r) \leq \frac{q^2}{q^2 - 1}$ for $r + d - 1 \leq m$. ∎

The proof of Proposition 10 indicates that the upper bound in Proposition 8 is also tight up to a scalar for $d \leq r$. However, these bounds are not constructive. Below we derive constructive bounds on $A_{\mathrm{R}}(q, m, n, d, r)$.

B. Constructions of CRCs

We first give a construction of asymptotically optimal CRCs when $d \leq r$. We assume the matrices in $\mathrm{GF}(q)^{m \times n}$ are mapped into vectors in $\mathrm{GF}(q^m)^n$ according to a fixed basis B_m of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$.

Proposition 11: For all q, $2 \leq d \leq r \leq n \leq m$, $A_{\mathrm{R}}(q, m, n, d, r) \geq M(q, m, n, d, r) > \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d)}$.

Proof: The codewords of rank r in an $(n, n - d + 1, d)$ linear MRD code over $\mathrm{GF}(q^m)$ form a CRC in $\mathrm{GF}(q)^{m \times n}$ with constant rank r and minimum distance d. Thus, $A_{\mathrm{R}}(d, r) \geq M(d, r)$.

We now prove the lower bound on $M(d, r)$. First, for $d = r$, $M(r, r) = \begin{bmatrix} n \\ r \end{bmatrix} (q^m - 1) > \begin{bmatrix} n \\ r \end{bmatrix}$. Second, suppose $d < r$. By (2),

$M(d, r)$ can be expressed as $M(d, r) = \begin{bmatrix} n \\ r \end{bmatrix} \sum_{j=d}^{r} (-1)^{r-j} \mu_j$, where $\mu_j \stackrel{\text{def}}{=} q^{(r-j)(r-j-1)/2} \begin{bmatrix} r \\ j \end{bmatrix} (q^{m(j-d+1)} - 1)$. It can be easily shown that $\mu_j > \mu_{j-1}$ for $d + 1 \leq j \leq r$, and hence, $M(d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix} (\mu_r - \mu_{r-1})$. Therefore, $M(d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix} [(q^{m(r-d+1)} - 1) - \begin{bmatrix} r \\ 1 \end{bmatrix} (q^{m(r-d)} - 1)] > \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d)}$. ∎

Corollary 2: For all q, $1 \leq r \leq n \leq m$, $A_{\mathrm{R}}(q, m, n, r, r) = \begin{bmatrix} n \\ r \end{bmatrix} (q^m - 1)$.

Proof: By Proposition 8, $A_{\mathrm{R}}(r, r) \leq \begin{bmatrix} n \\ r \end{bmatrix} (q^m - 1)$, and by Proposition 11, $A_{\mathrm{R}}(r, r) \geq M(r, r) = \begin{bmatrix} n \\ r \end{bmatrix} (q^m - 1)$. ∎

By Corollary 2, the codewords of rank r in an $(n, n - r + 1, r)$ linear MRD code are **optimal** CRCs with minimum distance r. Proposition 12 shows that for all but one case, the codewords of rank r in an $(n, n - d + 1, d)$ MRD code form a code whose cardinality is close to that of an optimal CRC up to a scalar which tends to 1 for large q. To measure the optimality, we introduce a ratio $B(q, m, n, d, r) \stackrel{\text{def}}{=} A_{\mathrm{R}}(q, m, n, d, r) / M(q, m, n, d, r)$ for $1 \leq d < r \leq n \leq m$.

Proposition 12: For all q, $1 \leq d < r \leq n \leq m$ and $m \geq 3$, see (7)–(11), shown at the bottom of the next page.

The proof of Proposition 12 is given in Appendix I-B.

We now construct CRCs for $d > r$ using generalized Gabidulin codes [34]. Let $\mathbf{g} \in \mathrm{GF}(q^m)^n$ have rank n, and for $0 \leq i \leq m - 1$, denote the vector in $\mathrm{GF}(q^m)^n$ obtained by raising each coordinate of $\mathbf{g}$ to the q^{ai}th power, $\mathbf{g}^{[i]}$, where a and m are coprime. Let $\mathcal{C}$ be the $(n, n - d + 1, d)$ generalized Gabidulin code over $\mathrm{GF}(q^m)$ generated by $\left(\mathbf{g}^{[0]T}, \mathbf{g}^{[1]T}, \ldots, \mathbf{g}^{[n-d]T} \right)^T$, and $\mathcal{C}'$ be the $(n, d - r, n - d + r + 1)$ generalized Gabidulin code generated by $\left(\mathbf{g}^{[n-d+1]T}, \mathbf{g}^{[n-d+2]T}, \ldots, \mathbf{g}^{[n-r]T} \right)^T$. We consider the coset $\mathcal{C} + \mathbf{c}'$, where $\mathbf{c}' \in \mathcal{C}'$, and we denote the number of codewords of rank r in $\mathcal{C} + \mathbf{c}'$ as $\sigma_r(\mathbf{c}')$.

Lemma 2: For all $d > r$, there exists $\mathbf{c}' \in \mathcal{C}'$ such that $\sigma_r(\mathbf{c}') \geq \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}$.

Proof: Any codeword $\mathbf{c}' \in \mathcal{C}'$ can be expressed as $\mathbf{c}' = c_{n-d+1} \mathbf{g}^{[n-d+1]} + c_{n-d+2} \mathbf{g}^{[n-d+2]} + \cdots + c_{n-r} \mathbf{g}^{[n-r]}$, where $c_i \in \mathrm{GF}(q^m)$ for $n - d + 1 \leq i \leq n - r$. If $c_{n-r} = 0$, then $(\mathcal{C} + \mathbf{c}') \subset \mathcal{D}$, where $\mathcal{D}$ is the $(n, n - r, r + 1)$ generalized Gabidulin code generated by $\left(\mathbf{g}^{[0]T}, \mathbf{g}^{[1]T}, \ldots, \mathbf{g}^{[n-r-1]T} \right)^T$. Therefore, $\sigma_r(\mathbf{c}') = 0$ if $c_{n-r} = 0$.

Denote the number of codewords of rank r in $\mathcal{C} \oplus \mathcal{C}'$ as τ_r. Since $\bigcup_{\mathbf{c}' \in \mathcal{C}'} (\mathcal{C} + \mathbf{c}') = \mathcal{C} \oplus \mathcal{C}'$, we have $\tau_r = \sum_{\mathbf{c}' \in \mathcal{C}'} \sigma_r(\mathbf{c}')$. Also, $\mathcal{C} \oplus \mathcal{C}'$ forms an $(n, n - r + 1, r)$ MRD code, and hence, $\tau_r = M(q, m, n, r, r) = \begin{bmatrix} n \\ r \end{bmatrix} (q^m - 1)$. Suppose that for all $\mathbf{c}' \in$

$$A_{\mathrm{R}}(q, m, n, d, r) \geq \max_{s, \{A_i\}, k, l} \frac{\sum_{i=0}^{n} A_i J_{\mathrm{R}}(q, l, k, s, r, i)}{N_{\mathrm{R}}(q, l, k, s) - \sum_{i=0}^{n} A_i \sum_{t=0}^{d-r-1} J_{\mathrm{R}}(q, l, k, s, t, i)} \tag{6}$$

$\mathcal{C}'$, $\sigma_r(\mathbf{c}') < \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}$. Then $\tau_r = \sum_{\mathbf{c}':c_{n-r}\neq 0} \sigma_r(\mathbf{c}') < \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$, which contradicts $\tau_r = \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$. ∎

Although Lemma 2 proves the existence of a vector $\mathbf{c}'$ for which the translate $\mathcal{C} + \mathbf{c}'$ has high cardinality, it does not indicate how to choose $\mathbf{c}'$. For $d = r + 1$, it can be shown that all $\mathbf{c}' \in \mathcal{C}'$ satisfy the bound, and that they all lead to optimal codes.

Corollary 3: If $d = r + 1$, then $\sigma_r(\mathbf{c}') = \begin{bmatrix} n \\ r \end{bmatrix}$ for all $\mathbf{c}' \in \mathcal{C}'$.

Proof: First, by Proposition 4, $\sigma_r(\mathbf{c}') \leq A_{\mathrm{R}}(q, m, n, r + 1, r) \leq A_{\mathrm{C}}(q, n, r, 1) = \begin{bmatrix} n \\ r \end{bmatrix}$ for all $\mathbf{c}' \in \mathcal{C}'$. Suppose there exists $\mathbf{c}'$ such that $\sigma_r(\mathbf{c}') < \begin{bmatrix} n \\ r \end{bmatrix}$. Then $\tau_r < \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$, which contradicts $\tau_r = \begin{bmatrix} n \\ r \end{bmatrix}(q^m - 1)$. ∎

Proposition 13: For all q, $1 \leq r < d \leq n \leq m$, $A_{\mathrm{R}}(q, m, n, d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix} q^{n(r-d+1)}$, and a class of codes that satisfy this bound can be constructed from Lemma 2.

Proof: The codewords of rank r in a code considered in Lemma 2 form a CRC in $\mathrm{GF}(q)^{m \times n}$ with constant rank r, minimum distance d, and cardinality $\geq \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}$. Therefore, $A_{\mathrm{R}}(q, m, n, d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}$. The proof is concluded by noting that $A_{\mathrm{R}}(q, m, n, d, r) \geq A_{\mathrm{R}}(q, n, n, d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix} q^{n(r-d+1)}$. ∎

Corollary 4: For all q, $1 \leq r < n \leq m$, $A_{\mathrm{R}}(q, m, n, r + 1, r) = \begin{bmatrix} n \\ r \end{bmatrix} = A_{\mathrm{C}}(q, n, r, 1)$.

This can be shown by combining Propositions 4 and 13. We note that $\begin{bmatrix} n \\ r \end{bmatrix}$ is independent of m. We also remark that the lower bound in Proposition 13 is also trivial for d approaching $2r$. Since the proof is only partly constructive, computer search can be used to help find better results for small parameter values.

By Proposition 4, the lower bounds on $A_{\mathrm{R}}(q, m, n, d, r)$ derived in this section for $d > r$ can be viewed as lower bounds on the maximum cardinality of a corresponding CDC. Although in Corollary 4, we obtain a tight bound for $d = r + 1$, we remark that the bound in Proposition 13 does not improve on the lower bounds on $A_{\mathrm{C}}(q, n, r, d - r)$ previously derived in the literature when $d > r + 1$. However, the construction of good CDCs from CRCs is an interesting topic for future work.

C. Asymptotic Results

We study the asymptotic behavior of CRCs using the following set of normalized parameters: $\nu = \frac{n}{m}$, $\rho = \frac{r}{m}$, and $\delta = \frac{d}{m}$. By definition, $0 \leq \rho$, $\delta \leq \nu$, and since we assume $n \leq m$, $\nu \leq 1$. We consider the asymptotic rate defined as $a_{\mathrm{R}}(\nu, \delta, \rho) \stackrel{\mathrm{def}}{=} \lim_{m \to \infty} \sup \left[\log_{q^{m^2}} A_{\mathrm{R}}(q, m, n, d, r) \right]$. We now investigate how $A_{\mathrm{R}}(q, m, n, d, r)$ behaves as the parameters tend to infinity. Without loss of generality, we only consider the case where $0 \leq \delta \leq \min\{\nu, 2\rho\}$, since $a_{\mathrm{R}}(\nu, \delta, \rho) = 0$ for $\delta > 2\rho$.

Proposition 14: For $0 \leq \delta \leq \rho$, $a_{\mathrm{R}}(\nu, \delta, \rho) = \rho(1 + \nu - \rho) - \delta$. For $\rho \leq \delta$, we have to distinguish three cases. First, for $2\rho \leq \nu$

$$\max\left\{ \frac{(1 - \rho)(\nu - \rho)}{1 + \nu - 2\rho}(2\rho - \delta), \rho(2\nu - \rho) - \nu\delta \right\}$$
$$\leq a_{\mathrm{R}}(\nu, \delta, \rho) \leq (\nu - \rho)(2\rho - \delta). \quad (12)$$

Second, for $\nu \leq 2\rho \leq 1$

$$\max\left\{ \rho(1 - \rho)(\nu - \delta), \rho(2\nu - \rho) - \nu\delta \right\}$$
$$\leq a_{\mathrm{R}}(\nu, \delta, \rho) \leq \rho(\nu - \delta). \quad (13)$$

Third, for $2\rho \geq 1$

$$\max\left\{ \frac{\rho}{2}(1 + \nu - 2\rho - \delta), \rho(2\nu - \rho) - \nu\delta, 0 \right\}$$
$$\leq a_{\mathrm{R}}(\nu, \delta, \rho) \leq \rho(\nu - \delta). \quad (14)$$

The proof of Proposition 14 is given in Appendix I-C.

Proposition 12 indicates that the codewords of a given rank in a linear MRD code form asymptotically optimal CRCs. In particular, Proposition 14 shows that the set of codewords with rank n in an $(n, n - d + 1, d)$ linear MRD code constitutes a CRC of rank n and asymptotic rate of $\nu - \delta$, which is equal to the asymptotic rate of an optimal rank metric code [42].

We can split the range of δ into two regions: when $\delta \leq \rho$, the asymptotic rate of CRCs is determined due to the construction of good CRCs when $d \leq r$; when $\delta \geq \rho$, we only have bounds on the asymptotic rate of CRCs. Also, the lower bounds based on the connection between CDCs and CRCs (the first lower bound in the LHS of (12)–(14) are tighter for $2\rho \leq \nu$ and on the other hand become trivial for ρ approaching 1. The bounds on $a_{\mathrm{R}}(\nu, \delta, \rho)$ in the three cases in (12)–(14) are illustrated in Figs. 1–3 for $\nu = 3/4$ and $\rho = 1/5, 2/5, 3/5$, respectively.

V. CONCLUSION

Rank metric codes and CDCs have been considered for error control in noncoherent random linear network coding. It has

$$B(2, m, m, m - 1, m) \leq 2^{m-1} - 1 \tag{7}$$

$$B(q, m, m, m - 1, m) < \frac{q - 1}{q - 2} \quad \text{for } q > 2 \tag{8}$$

$$B(q, m, m, m - 2, m) < \frac{(q^2 - 1)(q - 1)}{(q^2 - 1)(q - 2) + 1} \tag{9}$$

$$B(q, m, m, d, m) < \frac{(q^3 - 1)(q^2 - 1)(q - 1)}{(q^3 - 1)(q^2 - 1)(q - 2) + q^3 - 2} \quad \text{for } d < m - 2 \tag{10}$$

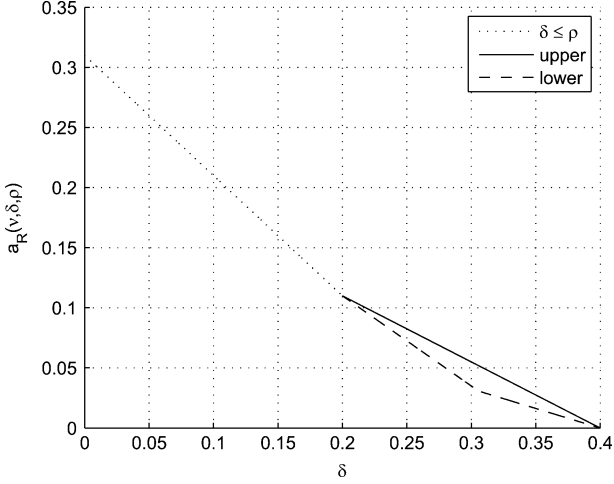$$B(q, m, n, d, r) < \frac{q}{q - 1} \quad \text{for } r < m \tag{11}$$

Fig. 1. Asymptotic bounds on the maximal rate of a CRC as a function of δ, with $\nu = 3/4$ and $\rho = 1/5$.
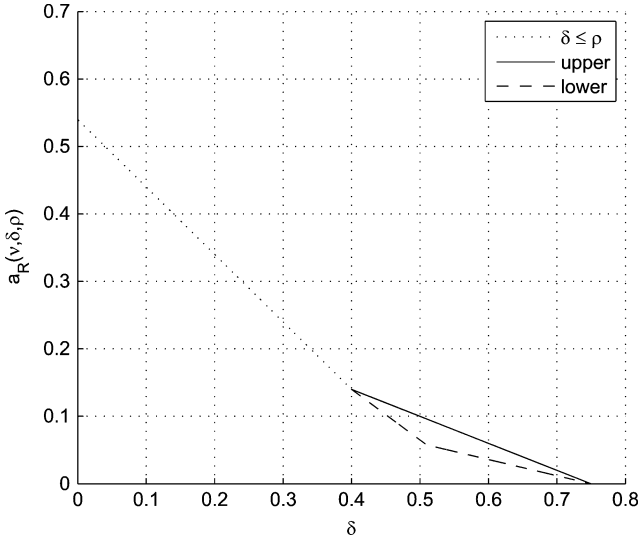

Fig. 2. Asymptotic bounds on the maximal rate of a CRC as a function of δ, with $\nu = 3/4$ and $\rho = 2/5$.

been shown that these two classes of codes are related by the lifting operation, which turns an optimal rank metric code into a nearly optimal constant-dimension code. However, liftings of rank metric codes are not optimal constant-dimension codes. In this paper, we first established a novel connection between CRCs and CDCs, by showing that optimal CRCs over matrices with sufficiently many rows lead to optimal CDCs with a related minimum injection distance. In comparison to previously proposed constructions of CDCs, our construction based on CRCs guarantees the optimality of CDCs, and hence is a promising approach. Despite previous works on rank metric codes in general, CRCs have received little attention in the literature. We hence investigated the properties of CRCs, derived bounds on their cardinalities, and proposed explicit constructions of CRCs in some cases. Although we have not been able to propose constructions of optimal CRCs in all cases, we hope our novel connection between CRCs and CDCs and investigation of CRCs can lead to constructions of optimal CDCs, which is the topic of our future work.
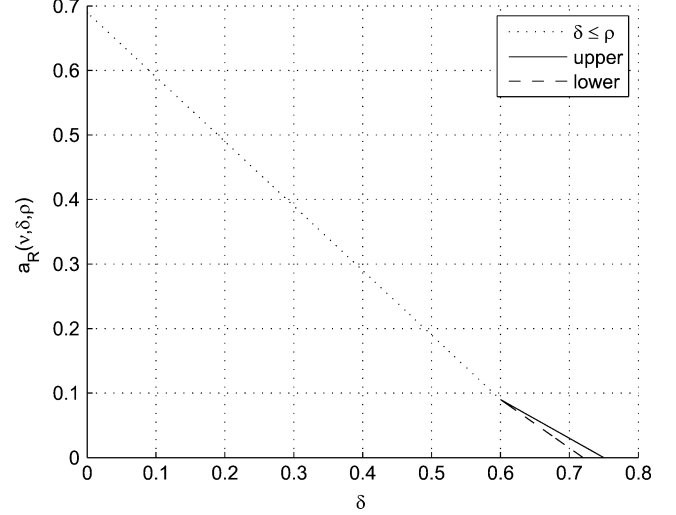

Fig. 3. Asymptotic bounds on the maximal rate of a CRC as a function of δ, with $\nu = 3/4$ and $\rho = 3/5$.

APPENDIX

A) Proof of Proposition 9 (Bassalygo–Elias Bound for Rank Metric Codes):

Proof: For all $\mathbf{X} \in \mathrm{GF}(q)^{l \times k}$ with rank s and $\mathbf{C} \in \mathcal{C}$, we define $f_r(\mathbf{X}, \mathbf{C}) = 1$ if $d_{\mathrm{R}}(\mathbf{X}, \mathbf{c}) = r$ and $f_r(\mathbf{X}, \mathbf{C}) = 0$ otherwise. Note that $\sum_{\mathbf{X}:\mathrm{rk}(\mathbf{X})=s} f_r(\mathbf{X}, \mathbf{C}) = J_{\mathrm{R}}(q, l, k, s, r, \mathrm{rk}(\mathbf{C}))$ for all $\mathbf{C} \in \mathcal{C}$ and $\sum_{\mathbf{c} \in C} f_r(\mathbf{X}, \mathbf{C}) = |\{\mathbf{Y} \in C - \mathbf{X} : \mathrm{rk}(\mathbf{Y}) = r\}| \leq A_{\mathrm{R}}(q, l, k, d, r)$ for all $\mathbf{X} \in \mathrm{GF}(q)^{l \times k}$. We obtain

$$\sum_{\mathbf{C} \in \mathcal{C}} \sum_{\mathbf{X}:\mathrm{rk}(\mathbf{X})=s} f_r(\mathbf{X}, \mathbf{C}) = \sum_{i=0}^{n} A_i J_{\mathrm{R}}(q, l, k, s, r, i) \qquad (15)$$

$$\sum_{\mathbf{X}:\mathrm{rk}(\mathbf{X})=s} \sum_{\mathbf{C} \in \mathcal{C}} f_r(\mathbf{X}, \mathbf{C}) \leq N_{\mathrm{R}}(q, l, k, s) A_{\mathrm{R}}(q, l, k, d, r). \qquad (16)$$

Combining (15) and (16), we obtain

$$A_{\mathrm{R}}(q, l, k, d, r) \geq \frac{\sum_{i=0}^{n} A_i J_{\mathrm{R}}(q, l, k, s, r, i)}{N_{\mathrm{R}}(q, l, k, s)}. \qquad (17)$$

Suppose $d > r + 1$. For all $\mathbf{C} \in \mathcal{C}$, let us denote the set of matrices with rank s at distance at most $d - r - 1$ from $\mathbf{C}$ as $S_{\mathbf{C}}$, and $S \overset{\text{def}}{=} \bigcup_{\mathbf{C} \in \mathcal{C}} S_{\mathbf{C}}$. For $\mathbf{X} \in S_{\mathbf{C}}$, we have $d_{\mathrm{R}}(\mathbf{X}, \mathbf{C}) \leq d - r - 1 < r$. We have for $\mathbf{C}' \in \mathcal{C}$ and $\mathbf{C}' \neq \mathbf{C}$, $d_{\mathrm{R}}(\mathbf{X}, \mathbf{C}') \geq d_{\mathrm{R}}(\mathbf{C}, \mathbf{C}') - d_{\mathrm{R}}(\mathbf{X}, \mathbf{C}) \geq r + 1$; and hence, $f_r(\mathbf{X}, \mathbf{C}') = 0$ for all $\mathbf{C}' \in \mathcal{C}$. Therefore, $\sum_{\mathbf{C} \in \mathcal{C}} f_r(\mathbf{X}, \mathbf{C}) = 0$ for all $\mathbf{X} \in S$ and

$$\sum_{\mathbf{X}:\mathrm{rk}(\mathbf{X})=s} \sum_{\mathbf{C} \in \mathcal{C}} f_r(\mathbf{X}, \mathbf{C})$$
$$= \sum_{\mathbf{X} \in S} \sum_{\mathbf{C} \in C} f_r(\mathbf{X}, \mathbf{C}) + \sum_{\substack{\mathbf{X} \notin S \\ \mathrm{rk}(\mathbf{X})=s}} \sum_{\mathbf{C} \in \mathcal{C}} f_r(\mathbf{X}, \mathbf{C})$$
$$\leq [N_{\mathrm{R}}(q, l, k, s) - |S|] A_{\mathrm{R}}(q, l, k, d, r). \qquad (18)$$

Since $d - r - 1 < \frac{d}{2}$, the balls with radius $d - r - 1$ around the codewords are disjoint, and hence, $|S| =$

$\sum_{i=0}^{n} A_i \sum_{t=0}^{d-r-1} J_{\mathrm{R}}(q,l,k,s,t,i)$. Combining (15) and (18), we obtain

$$
A_{\mathrm{R}}(q,l,k,d,r)
$$

$$
\geq \frac{\sum_{i=0}^{n} A_i J_{\mathrm{R}}(q,l,k,s,r,i)}{N_{\mathrm{R}}(q,l,k,s) - \sum_{i=0}^{n} A_i \sum_{t=0}^{d-r-1} J_{\mathrm{R}}(q,l,k,s,t,i)}. \quad (19)
$$

Note that (17) and (19) both hold for any s and rank spectrum $\{A_i\}$. Furthermore, since $A_{\mathrm{R}}(q,l,k,d,r)$ is a nondecreasing function of l and k, $A_{\mathrm{R}}(q,m,n,d,r) \geq A_{\mathrm{R}}(q,l,k,d,r)$ for all $\max\{r,d\} \leq k \leq n$ and $k \leq l \leq m$. Thus, we have (5) and (6). ∎

B) Proof of Proposition 12:

Proof: By Proposition 8, we obtain $A_{\mathrm{R}}(q,m,m,d,m) \leq \alpha(m,m-d+1)$ for $r = n = m$ and $A_{\mathrm{R}}(q,m,n,d,r) \leq \begin{bmatrix} n \\ r \end{bmatrix} \alpha(m,r-d+1) < \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}$ otherwise. We now derive lower bounds on $M(q,m,n,d,r)$. Again, $M(q,m,n,d,r) = \begin{bmatrix} n \\ r \end{bmatrix} \sum_{j=d}^{r} (-1)^j \mu_j$ where $\mu_j > \mu_{j-1}$ for $d+1 \leq j \leq r$. Therefore, when needed, we shall only consider the last terms in the summation.

First, $M(q,m,m,m-1,m) = (q^{2m}-1) - \frac{q^m-1}{q-1}(q^m-1) > \frac{q-2}{q-1}(q^{2m}-1) > \frac{q-2}{q-1}\alpha(m,2)$, which leads to (8). For $q = 2$, $M(2,m,m,m-1,m) = 2(2^m-1) = (2^{m-1}-1)^{-1}\alpha(m,2)$, which results in (7). Second, when $r = n = m$ and $d = m-2$

$$
M(q,m,m,m-2,m)
$$
$$
= (q^{3m}-1) - \frac{\alpha(m,1)}{q-1}(q^{2m}-1)
$$
$$
+ \frac{\alpha(m,2)}{(q^2-1)(q-1)}(q^m-1)
$$
$$
> \frac{q-2}{q-1}\alpha(m,1)(q^{2m}-1)
$$
$$
+ \frac{1}{(q^2-1)(q-1)}\alpha(m,2)(q^m-1)
$$
$$
> \frac{(q^2-1)(q-2)+1}{(q^2-1)(q-1)}\alpha(m,1)
$$

which leads to (9). Third, when $r = n = m$ and $d < m-2$, by considering the last four terms in the summation, we obtain

$$
M(q,m,m,d,m)
$$
$$
> (q^{m(m-d+1)}-1) - \frac{\alpha(m,1)}{q-1}(q^{m(m-d)}-1)
$$
$$
+ \frac{\alpha(m,2)}{(q^2-1)(q-1)}(q^{m(m-d-1)}-1)
$$
$$
- \frac{\alpha(m,3)}{(q^3-1)(q^2-1)(q-1)}(q^{m(m-d-2)}-1)
$$
$$
> \left\{ \frac{q-2}{q-1} + \frac{q^3-2}{(q^3-1)(q^2-1)(q-1)} \right\}
$$
$$
\times \alpha(m,m-d+1)
$$

which results in (10). Fourth, when $d < r < m$, by considering the last two terms in the summation, we obtain

$$
M(q,m,n,d,r)
$$
$$
\geq \begin{bmatrix} n \\ r \end{bmatrix} \left((q^{m(r-d+1)}-1) - \begin{bmatrix} r \\ 1 \end{bmatrix}(q^{m(r-d)}-1) \right)
$$
$$
\geq \begin{bmatrix} n \\ r \end{bmatrix} \left(q^{m(r-d+1)} - 1 - q^{m(r-d)+r} + q^r \right)
$$
$$
\geq \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)}(1 - q^{r-m}).
$$

Therefore, since $r < m$, $B(q,m,n,d,r) < (1-q^{r-m})^{-1} \leq \frac{q}{q-1}$, which leads to (11). ∎

C) Proof of Proposition 14:

Proof: We first derive a lower bound on $a_{\mathrm{R}}(\nu,\delta,\rho)$. For $d \leq r$, Proposition 11 yields $A_{\mathrm{R}}(d,r) \geq q^{r(n-r)+m(r-d)}$, which asymptotically becomes $a_{\mathrm{R}}(\nu,\delta,\rho) \geq \rho(1+\nu-\rho) - \delta$ for $\delta \leq \rho$. Similarly, for $d > r$, Proposition 13 yields $A_{\mathrm{R}}(q,m,n,d,r) \geq q^{r(n-r)+n(r-d+1)}$, which asymptotically becomes $a_{\mathrm{R}}(\nu,\delta,\rho) \geq \rho(2\nu-\rho) - \nu\delta$ for $\delta \geq \rho$.

Proposition 4 and (3) yield $\log_q A_{\mathrm{R}}(d,r) \geq \min\{(n-r)(2r-d-p+1), (m-r)(p+1)\}$ for $d > r$ and $2r \leq n$. Treating the two terms as functions and assuming that p is real, the lower bound is maximized when $p = \frac{(n-r)(2r-d+1)-m+r}{m+n-2r}$. Using $p = \left\lfloor \frac{(n-r)(2r-d+1)-m+r}{m+n-2r} \right\rfloor$, asymptotically we obtain $a_{\mathrm{R}}(\nu,\delta,\rho) \geq \frac{(1-\rho)(\nu-\rho)}{1+\nu-2\rho}(2\rho-\delta)$ for $2\rho \leq \nu$.

For $d > r$ and $n \leq 2r \leq m$, Proposition 4 and (3) lead to $\log_q A_{\mathrm{R}}(d,r) \geq \min\{r(n-d-p+1), (m-r)(p+1)\}$. After maximizing this expression over p, we asymptotically obtain $a_{\mathrm{R}}(\nu,\delta,\rho) \geq \rho(1-\rho)(\nu-\delta)$ for $\nu \leq 2\rho \leq 1$.

For $d > r$ and $2r \geq m$, Proposition 4 and (3) lead to $\log_q A_{\mathrm{R}}(d,r) \geq \min\{r(n-d-p+1), r(m-2r+p+1)\}$. After maximizing this expression over p, we asymptotically obtain $a_{\mathrm{R}}(\nu,\delta,\rho) \geq \frac{\rho}{2}(1+\nu-2\rho-\delta)$ for $2\rho \geq 1$.

We now derive an upper bound on $a_{\mathrm{R}}(\nu,\delta,\rho)$. First, Proposition 8 gives $A_{\mathrm{R}}(d,r) < \begin{bmatrix} n \\ r \end{bmatrix} q^{m(r-d+1)} < K_q^{-1} q^{r(n-r)+m(r-d+1)}$ for $d \leq r$, which asymptotically becomes $a_{\mathrm{R}}(\nu,\delta,\rho) \leq \rho(1+\nu-\rho) - \delta$ for $\rho \geq \delta$. Second, by Proposition 4, we obtain $a_{\mathrm{R}}(\nu,\delta,\rho) \leq \lim_{m\to\infty}\sup\left[\log_{q^{m^2}} A_{\mathrm{C}}(q,n,r,d-r)\right] = \min\{(\nu-\rho)(2\rho-\delta), \rho(\nu-\delta)\}$ for $\rho \leq \delta \leq \min\{2\rho,\nu\}$. ∎

ACKNOWLEDGMENT

REFERENCES

[1] T. Ho, R. Koetter, M. Médard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Proc. IEEE Int. Symp. Information Theory*, Yokohama, Japan, Jun.-Jul. 2003, p. 442.

[2] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," presented at the Allerton Conf. on Comm., Control, and Computing, Monticello, IL, Oct. 2003.

[3] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[4] N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc. IEEE Information Theory Workshop*, Bangalore, India, Oct. 2002, pp. 20–25.

[5] L. Song, R. W. Yeung, and N. Cai, "Zero-error network coding for acyclic networks," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3129–3139, Dec. 2003.

[6] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 19–36, 2006.

[7] N. Cai and R. W. Yeung, "Network error correction, part II: Lower bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 37–54, 2006.

[8] Z. Zhang, "Linear network error correction codes in packet networks," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 209–218, Jan. 2008.

[9] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[10] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.

[11] S. Jaggi, M. Langberg, S. Katti, T. Ho, and D. K. Médard, "Resilient network coding in the presence of byzantine adversaries," in *Proc. IEEE Infocom*, Anchorage, AK, May 2007, pp. 616–624.

[12] P. Delsarte, "Association schemes and *t*-designs in regular semilattices," *J. Combin. Theory A*, vol. 20, no. 2, pp. 230–243, Mar. 1976.

[13] L. Chihara, "On the zeros of the askey-wilson polynomials with applications to coding theory," *SIAM J. Math. Anal.*, vol. 8, no. 1, pp. 191–207, Jan. 1987.

[14] "On metrics for error correction in network coding," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 5479–5490, Dec. 2009.

[15] T. Etzion and A. Vardy, "Error-correcting codes in projective space," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, ON, Canada, Jul. 2008, pp. 871–875.

[16] E. M. Gabidulin and M. Bossert, "Codes for network coding," in *Proc. IEEE Int. Symp. on Information Theory*, Toronto, ON, Canada, Jul. 2008, pp. 867–870.

[17] W. J. Martin and X. J. Zhu, "Anticodes for the Grassmann and bilinear forms graphs," *Designs, Codes, Cryptogr.*, vol. 6, no. 1, pp. 73–79, Jul. 1995.

[18] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, "On perfect codes and related concepts," *Designs, Codes, Cryptogr.*, vol. 22, no. 3, pp. 221–237, Jan. 2001.

[19] M. Schwartz and T. Etzion, "Codes and anticodes in the Grassmann graph," *J. Combin. Theory Ser. A*, vol. 97, no. 1, pp. 27–42, Jan. 2002.

[20] S.-T. Xia and F.-W. Fu, "Johnson type bounds on constant dimension codes," *Designs, Codes, Cryptogr.*, vol. 50, no. 2, pp. 163–172, Feb. 2009.

[21] P. Frankl and R. M. Wilson, "The Erdös-Ko-Rado theorem for vector spaces," *J. Combin. Theory A*, vol. 43, no. 2, pp. 228–236, Nov. 1986.

[22] T. Etzion, "Perfect byte-correcting codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 3140–3146, Nov. 1998.

[23] H. Wang, C. Xing, and R. Safani-Naini, "Linear authentication codes: Bounds and constructions," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 866–872, Apr. 2003.

[24] V. Skachek, "Recursive code construction for random networks," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1378–1382, Mar. 2010.

[25] T. Etzion and N. Silberstein, "Error-correcting codes in projective spaces via rank-metric codes and ferrers diagrams," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 2909–2919, Jul. 2009.

[26] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *J. Combin. Theory A*, vol. 25, no. 3, pp. 226–241, Nov. 1978.

[27] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inf. Transmission*, vol. 21, no. 1, pp. 1–12, Jan. 1985.

[28] R. M. Roth, "Maximum-rank array codes and their application to criss-cross error correction," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 328–336, Mar. 1991.

[29] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a non-commutative ring and their application in cryptology," in *Proc. Eurocrypt*, Brighton, U.K., Apr. 1991, pp. 482–489.

[30] P. Lusina, E. M. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2757–2760, Oct. 2003.

[31] G. E. Andrews, *The Theory of Partitions, ser. Encyclopedia of Mathematics and its Applications*, G.-C. Rota, Ed. Reading, MA: Addison-Wesley, 1976, vol. 2.

[32] M. Gadouleau and Z. Yan, "On the decoder error probability of bounded rank-distance decoders for maximum rank distance codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3202–3206, Jul. 2008.

[33] M. Gadouleau and Z. Yan, "Bounds on covering codes with the rank metric," *IEEE Commun. Lett.*, vol. 13, pp. 691–693, Sep. 2009.

[34] A. Kshevetskiy and E. M. Gabidulin, "The new construction of rank codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 2105–2108.

[35] A. Kohnert and S. Kurz, "Construction of large constant dimension codes with a prescribed minimum distance," *Mathematical Meth. Comput. Sci., LNCS*, vol. 5393, pp. 31–42, Dec. 2008.

[36] A. R. Rao and P. Bhimasankaram, *Linear Algebra*, 2nd ed. Guragon, India: Hindustan Book Agency, 2000.

[37] G. Marsaglia and G. P. H. Styan, "Equalities and inequalities for ranks of matrices," *Linear and Multilinear Algebra*, vol. 2, pp. 269–292, 1974.

[38] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.k.: Cambridge Univ. Press, 1985.

[39] M. Gadouleau and Z. Yan, "Construction and covering properties of constant-dimension codes," *IEEE Trans. Inf. Theory*, submitted for publication.

[40] S. M. Johnson, "A new upper bound for error-correcting codes," *IRE Trans. Inf. Theory*, vol. 8, no. 3, pp. 203–207, Apr. 1962.

[41] L. A. Bassalygo, "New upper bounds for error correcting codes," *Probl. Inf. Transmission*, vol. 1, no. 4, pp. 32–35, Oct.-Dec. 1965.

[42] M. Gadouleau and Z. Yan, "Packing and covering properties of rank metric codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3873–3883, Sep. 2008.

Maximilien Gadouleau (S'06–M'10) received an equivalent of the M.S. degree in electrical and computer engineering from Esigelec, Saint-Etienne du Rouvray, France, in 2004, and the M.S. and Ph.D. degrees in computer engineering from Lehigh University, Bethlehem, PA, in 2005 and 2009, respectively.

In 2009, he joined the Université de Reims Champagne-Ardenne, Reims, France, as a postdoctoral researcher. His current research interests are coding theory, cryptography, and network coding and their relations to combinatorics and graph theory.

Dr. Gadouleau is a member of the IEEE Information Theory Society.

Zhiyuan Yan (S'00–M'03–SM'08) received the B.E. degree in electronic engineering from Tsinghua University, Beijing, China, in 1995, and the M.S. and Ph.D. degrees, both in electrical engineering, from the University of Illinois at Urbana-Champaign, Urbana, in 1999 and 2003, respectively.

During summer 2000 and 2002, He was a Research Intern with Nokia Research Center, Irving, TX. He joined the Electrical and Computer Engineering Department, Lehigh University, Bethlehem, PA, as an Assistant Professor in August 2003. His current research interests are in coding theory, cryptography, wireless communications, and VLSI implementations of communication, and signal processing systems, and he has published over 70 technical papers in refereed journals and conference proceedings.

Dr. Yan served as technical program committee co-chair and general co-chair for ACM Great Lakes Symposium on VLSI in 2007 and 2008, respectively, and served as technical program committee member for many other key conferences. Dr. Yan has been an associate editor for the IEEE COMMUNICATIONS LETTERS since 2008 and is a member of the IEEE Information Theory, Communications, Signal Processing, and Computer Societies. He is also a member of Tau Beta Pi, Sigma Xi, and Phi Kappa Phi honor societies.