The Optimal Rate of Second-Order Generalized-Covering Codes

Dor Elimelech and Moshe Schwartz,
School of Electrical and Computer Engineering
Ben-Gurion University of the Negev, Beer Sheva 8410501, Israel
doreli@post.bgu.ac.il, schwartz@ee.bgu.ac.il

2023 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-7554-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISIT54713.2023.10206841

***Abstract*—The generalized-covering radius was recently proposed as a fundamental property of linear codes. We consider a natural extension of this property to general (not necessarily linear) codes, and provide an asymptotic solution to our problem by finding the optimal rate function of second-order covering codes given a fixed normalized covering radius. We also prove that the fraction of second-order covering codes among codes of sufficiently large rate tends to 1 as the code length tends to ∞.**

I. Introduction

The covering problem is a fundamental problem in metric spaces: given a non-negative number r, find a set of points in the space that is of minimal size, such that the balls of radius r centered those points cover the entire space. Such sets, often referred to as covering codes, have been thoroughly studied due to their fascinating relations with various topics in pure and applied mathematics, such as finite fields, discrete geometry, linear algebra, communication and algorithms. We refer to the excellent book [1] for further reading on covering codes and their applications.

The generalized covering radius was recently introduced as a fundamental property of linear codes, shown to characterize a trade-off between access-complexity, storage and latency in linear data-querying protocols (commonly used in PIR schemes, as an example). In [3], the case of linear codes was studied: some fundamental properties of the generalized covering radii were examined, and asymptotic bounds on the optimal rates of linear covering codes were derived. An interesting relation between the generalized covering radius and generalized Hamming weights of linear codes (see [9]) was also observed. In another paper [5], the generalized covering radii of Reed-Muller codes were examined.

In this work, we focus on the generalized covering radii of general codes, i.e., codes which are not necessarily linear. The main result in the paper is the derivation of the exact value of the minimal asymptotic rate of second-order covering codes with a fixed normalized second covering radius over an arbitrary finite alphabet. For a normalized radius $\rho \in [0,1]$, denoting the second-order optimal rate function over an alphabet of size q by $\kappa_2(\rho,q)$, we prove in Theorem 6 that

$$\kappa_2(\rho,q) = \begin{cases} 1 - H_{q^2}(\rho) & \rho \in [0, 1-\frac{1}{q^2}), \\ 0 & \rho \in [1-\frac{1}{q^2}, 1], \end{cases}$$

where $H_{q^2}(\cdot)$ denotes the q^2-ary entropy function. This result is an improvement upon the best known upper bound on the minimal asymptotic rate of linear binary second-order covering codes, given in [3, Theorem 22]. Thus, while a gap still remains for linear codes, our main result for general codes completely finds $\kappa_2(\rho,q)$, while also extending to general finite alphabets.

Another important result in this paper is given in Theorem 17, where we prove that second-order covering codes are very common among codes of sufficiently large rate. For $\rho \in [0, 1-\frac{1}{q^2})$ let $\alpha_q(n,\rho,M)$ denote the fraction of codes of length n over an alphabet of size q with normalized second covering radius at most ρ in the set of $(n,M)_q$ codes. In Theorem 17 we prove that for any $\varepsilon > 0$

$$\lim_{n\to\infty} \alpha_q\left(n,\rho,q^{n(1-H_{q^2}(\rho)+\varepsilon)}\right) = 1.$$

The paper is organized as following: In Section II we provide the exact definitions and notation used throughout the paper, and we survey the relevant known results. In Section III we give the main results. We conclude in Section IV with a short discussion and open problems. Due to the page limitation, proofs are omitted and may be found in [4].

II. Preliminaries

We consider codes over finite Abelian groups. We use G_q to denote an Abelian group of size $q \in \mathbb{N}$ and $+$ for the group operation. Naturally, G_q^n denotes the set of vectors of length n with entries from G_q, and $G_q^{t\times n}$ denotes the set of $t \times n$ matrices with entries from G_q. We also consider G_q^n and $G_q^{t\times n}$ as Abelian groups with the entry-wise group operation. We use lower-case letters, v, to denote scalars and group elements. Overlined lower-case letters, $\overline{v}$, shall be used to denote vectors, and bold lower-case letters, $\mathbf{v}$, to denote matrices.

For a vector $\overline{v} = (v_1, \dots, v_n) \in G_q^n$, the support of $\overline{v}$ is defined as $\mathrm{supp}(\overline{v}) \triangleq \{1 \leqslant i \leqslant n \,|\, v_i \neq 0\}$, and its Hamming weight is defined as $\mathrm{wt}(\overline{v}) \triangleq |\mathrm{supp}(\overline{v})|$. The Hamming distance between two vectors $\overline{v}, \overline{v}' \in G_q^n$ is then defined as $d(\overline{v},\overline{v}') \triangleq \mathrm{wt}(\overline{v}' - \overline{v})$.

A set $C \subseteq G_q^n$ is called an $(n,M)_q$ code if it has cardinality M. The elements in a code C shall also be called codewords. For an $(n,M)_q$ code, $\log_q(M)$ is called the dimension of the code. In the case where G_q is as also a field, we say that C is a linear code if it is a linear subspace of G_q^n over G_q.

978-1-6654-7554-9/23/$31.00 ©2023 IEEE

Authorized licensed use limited to: McMaster University. Downloaded on August 25,2023 at 17:05:57 UTC from IEEE Xplore. Restrictions apply.

In that case, C is said to be an $[n,k]_q$ linear code, where $k=\log_q(M)$ is its dimension (which is also the dimension of C as a vector space).

For an $(n,M)_q$ code C, the covering radius of C, denoted $R(C)$, is the distance of the farthest point in G_q^n to the code, with respect to the Hamming distance. That is,

$$R(C) \triangleq \max_{\overline{v}\in G_q^n} \min_{\overline{c}\in C} d(\overline{c},\overline{v}).$$

Equivalently, the covering radius of the code is the minimum radius at which balls centered at the codewords of C cover the entire space G_q^n. Here, a ball of radius r (not necessarily an integer) centered at $\overline{v}\in G_q^n$ is defined as the set of vectors in G_q^n that are at distance no more than r from $\overline{v}$, i.e.,

$$B_r(\overline{v}) \triangleq \left\{\overline{u}\in G_q^n \,\middle|\, d(\overline{v},\overline{u})\leqslant r\right\}.$$

The normalized covering radius of C is denoted by $\rho(C)$, and is defined to be

$$\rho(C)\triangleq \frac{R(C)}{n}.$$

The generalized covering radius was introduced in [3] as a fundamental property of linear codes. While [3] only studied linear codes, we extend our view to general codes, i.e., codes which are not necessarily linear. We begin by recalling the definition of the t-metric, also known as the block metric, on the space of matrices $G_q^{t\times n}$.

Definition 1 *Let $\mathbf{v}\in G_q^{t\times n}$ be a matrix with rows denoted by $\overline{v}_1,\dots,\overline{v}_t$. The t-weight of $\mathbf{v}$ is defined by*

$$\mathrm{wt}^{(t)}(\mathbf{v}) \triangleq \left|\bigcup_{i\in[t]} \operatorname{supp}\overline{v}_i\right|.$$

The t-distance between two matrices $\mathbf{v}$ and $\mathbf{u}$ in $G_q^{t\times n}$ is defined to be

$$d^{(t)}(\mathbf{v},\mathbf{u}) \triangleq \mathrm{wt}^{(t)}(\mathbf{u}-\mathbf{v}).$$

The t-Ball is defined in the usual manner, with respect to the t-metric:

$$B_r^{(t)}(\mathbf{v}) \triangleq \left\{\mathbf{u}\in G_q^{t\times n} \,\middle|\, d^{(t)}(\mathbf{v},\mathbf{u})\leqslant r\right\}.$$

We remark that for $t=1$, we get the well known Hamming metric. Thus, notationally, when $t=1$ we may omit the superscript $^{(1)}$. Next we define the t-th power of a code.

Definition 2 *Let C be an $(n,M)_q$ code and $t\in\mathbb{N}$. We define $C^t\subseteq G_q^{t\times n}$ to be the set of $t\times n$ matrices over G_q such that their rows are codewords in C. That is,*

$$C^t \triangleq \left\{ \begin{bmatrix}\overline{c}_1\\ \vdots\\ \overline{c}_t\end{bmatrix} \in G_q^{t\times n} \,\middle|\, \forall i\in[t], \overline{c}_i\in C \right\}.$$

We can now define the t-th-covering radius of a code.

Definition 3 *Let C be an $(n,M)_q$ code and $t\in\mathbb{N}$. The t-th-covering radius of C is defined to be the (regular) covering radius of C^t inside $G_q^{t\times n}$ with respect to the t-metric. That is,*

$$R_t(C) \triangleq \max_{\mathbf{u}\in G_q^{t\times n}} \min_{\mathbf{c}\in C^t} d^{(t)}(\mathbf{c},\mathbf{u}).$$

Once again, we note that for $t=1$, the t-th-covering radius of a code is the regular well known covering radius of the code (with respect to the Hamming metric).

Remark 4 *The definition of the t-th-covering radius depends on the t-metric, which is defined using the group operation. However, it is easy to check that the t-metric is invariant to a change of the group operation. Thus, the t-th-covering radius may be considered as a property of codes over arbitrary finite alphabets (by considering a finite alphabet of size q as a cyclic group of order q). Nevertheless, for convenience and simplification of notation, we think of all codes as codes over finite Abelian groups.*

The fundamental problem in any coverings-type setting is to find the minimal size of a set with a covering radius which is at most r. Thus, we are interested in the minimal size (or equivalently, dimension or rate) of a code $C\subseteq G_q^n$ such that $R_t(C)\leqslant r$.

Definition 5 *Let $n,t,q\in\mathbb{N}$, and $0\leqslant r\leqslant n$. The optimal dimension function, denoted by $k_t(n,r,q)$, is the minimal dimension of a code of length n over a group of size q with t-th-covering radius at most r. Namely,*

$$k_t(n,r,q)\triangleq \min\left\{\log_q|C| \,\middle|\, C\subseteq G_q^n, R_t(C)\leqslant r\right\}.$$

For $\rho\in[0,1]$, the asymptotic optimal rate is then defined as

$$\kappa_t(\rho,q)\triangleq \liminf_{n\to\infty}\frac{k_t(n,\rho n,q)}{n}.$$

We remark that the group G_q is omitted from the notation, as by Remark 4, k_t and κ_t only depend on the size q.

A restriction to linear codes of the above functions was studied in [3]. Similarly to the general case, if $G_q=\mathbb{F}_q$ is the finite field of size q, then k_t^{Lin} and κ_t^{Lin} are defined to be

$$k_t^{\mathrm{Lin}}(n,r,q)\triangleq \min\left\{\log_q|C| \,\middle|\, {\scriptstyle C\subseteq\mathbb{F}_q^n, R_t(C)\leqslant r \atop C \text{ is linear}}\right\},$$

and

$$\kappa_t^{\mathrm{Lin}}(\rho,q)\triangleq \liminf_{n\to\infty}\frac{k_t^{\mathrm{Lin}}(n,\rho n,q)}{n}.$$

Obviously, for all n,t,r,ρ and prime power q we have

$$k_t(n,r,q)\leqslant k_t^{\mathrm{Lin}}(n,r,q) \quad\text{and}\quad \kappa_t(\rho,q)\leqslant\kappa_t^{\mathrm{Lin}}(\rho,q).$$

It is well known [2] that in the case of $t=1$,

$$\kappa_1(\rho,q)=\kappa_1^{\mathrm{Lin}}(\rho,q)=\begin{cases}1-H_q(\rho) & \rho\in[0,1-\frac{1}{q}),\\ 0 & \rho\in[1-\frac{1}{q},1],\end{cases} \qquad (1)$$

where H_q is the q-ary entropy function defined by

$$H_q(x)\triangleq x\log_q(q-1)-x\log_q(x)-(1-x)\log_q(1-x),$$

Authorized licensed use limited to: McMaster University. Downloaded on August 25,2023 at 17:05:57 UTC from IEEE Xplore. Restrictions apply.

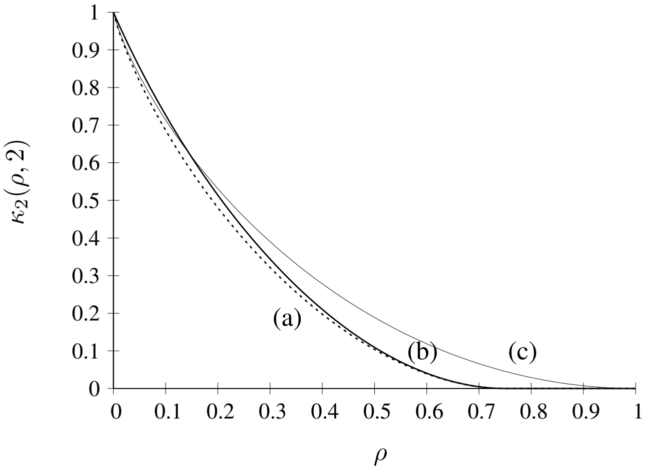

Fig. 1. A comparison of the bounds on $\kappa_2(\rho, 2)$: (a) the ball-covering lower bound of (2), (b) the upper bound of (4), and (c) the upper bound of (3).

and for continuity, $H_q(0) \triangleq 0$.

At this point, our knowledge of $\kappa_t(\rho, q)$ becomes severely limited, and we restrict ourselves to the first unresolved case, i.e., $t = 2$. The lower bound from [3, Proposition 12] is:

$$\kappa_2(\rho, q) \geqslant \begin{cases} 1 - H_{q^2}(\rho) & \rho \in [0, 1 - \frac{1}{q^2}), \\ 0 & \rho \in [1 - \frac{1}{q^2}, 1]. \end{cases} \tag{2}$$

This bound is based on a simple ball-covering argument. We also remark that while [3] only considered linear codes, the proof for the bound does not use the linearity of the code in any way, and thus the bound applies not only to $\kappa_2^{\mathrm{Lin}}(\rho, q)$, but also to $\kappa_2(\rho, q)$. In the other direction, [3] only managed to handle the further restricted case of $q = 2$, and thus [3, Proposition 14 and Theorem 22] proved two upper bounds which give us:

$$\kappa_2(\rho, 2) \leqslant \kappa_2^{\mathrm{Lin}}(\rho, 2) \leqslant 1 - H_2\left(\frac{\rho}{2}\right), \tag{3}$$

$$\kappa_2(\rho, 2) \leqslant \kappa_2^{\mathrm{Lin}}(\rho, 2) \leqslant \begin{cases} 1 - (4H_4(\rho) - f(\rho)) & \rho \in [0, \frac{3}{4}), \\ 0 & \rho \in [\frac{3}{4}, 1], \end{cases} \tag{4}$$

where, for all $\rho \in [0, \frac{3}{4})$ we define

$$f(\rho) \triangleq H_2(s(\rho)) + 2s(\rho) + 2(1 - s(\rho))H_2\left(\frac{\rho - s(\rho)}{1 - s(\rho)}\right),$$
$$s(\rho) \triangleq \frac{1}{10}\left(1 + 8\rho - \sqrt{1 + 16\rho - 16\rho^2}\right).$$

The bounds of [3] are depicted in Figure 1, and a gap between the lower and upper bounds is evident. Our main theorem, proved in the following section, closes the gap completely, while extending the setting to a general alphabet of size q, giving us the exact value of $\kappa_2(\rho, q)$.

A key component in the proofs ahead is an estimate of the size of balls. Let $V_{r,n,q}^{(t)}$ denote the size of a t-ball of radius r in $G_q^{t \times n}$ with respect to $d^{(t)}$, $V_{r,n,q}^{(t)} \triangleq \left|B_r^{(t)}(\mathbf{v})\right|$, which does not depend on the center, $\mathbf{v}$, as the metric is translation invariant. By choosing $\mathbf{v} = \mathbf{0}$, one can easily see that $V_{r,n,q}^{(t)}$ counts the number of $t \times n$ matrices with at most r non-zero columns. Thus, after conveniently denoting $\rho = \frac{r}{n}$,

$$V_{\rho n,n,q}^{(t)} = \sum_{i=0}^{\lfloor \rho n \rfloor} \binom{n}{i} (q^t - 1)^i = V_{\rho n,n,q^t}^{(1)}.$$

By a standard use of Stirling's approximation (e.g., see [6, Chapter 3]) it is well known that for $\rho \in [0, 1 - \frac{1}{q^t}]$

$$q^{tn(H_{q^t}(\rho) - o(1))} \leqslant V_{\rho n,n,q^t}^{(1)} \leqslant q^{tnH_{q^t}(\rho)}, \tag{5}$$

and therefore

$$\begin{aligned} V_{\rho n,n,q}^{(t)} &= \sum_{i=0}^{\lfloor \rho n \rfloor} \binom{n}{i} (q^t - 1)^i = V_{\rho n,n,q^t}^{(1)} \\ &= \begin{cases} q^{tn(H_{q^t}(\rho) + o(1))} & \rho \in [0, 1 - \frac{1}{q^t}), \\ q^{tn(1 - o(n))} & \rho \in [1 - \frac{1}{q^t}, 1]. \end{cases} \end{aligned} \tag{6}$$

Using the same approximation, we also mention that for $0 \leqslant m \leqslant n$, $n > 0$,

$$\binom{n}{m} (q - 1)^m = q^{n(H_q(m/n) + o(1))}. \tag{7}$$

Finally, here in (6)-(7) and throughout the paper, we use $o(1)$ to denote a function of n whose limit is 0 as $n \to \infty$. Then, given a continuous real function $f(x)$, we shall often use the fact that $f(x + o(1)) = f(x) + o(1)$.

III. The second-order optimal rate

The purpose of this section is to prove the following main theorem:

Theorem 6

$$\kappa_2(\rho, q) = \begin{cases} 1 - H_{q^2}(\rho) & \rho \in [0, 1 - \frac{1}{q^2}), \\ 0 & \rho \in [1 - \frac{1}{q^2}, 1]. \end{cases}$$

Since the proof of Theorem 6 is long and involved, we first describe the overall strategy in brief. We start by noting that the lower bound of (2) matches the claim of Theorem 6. Additionally, the upper bound of (4) matches the claim of Theorem 6 in the range $[1 - \frac{1}{q^2}, 1]$. Furthermore, the case of $\rho = 0$ is trivial. Hence, it remains to prove an upper bound matching Theorem 6 in the interval $(0, 1 - \frac{1}{q^2})$.

In order to show that $\kappa_2(\rho, q)$ is upper bounded by some number γ, we are required to find a sequence of codes with lengths that tend to infinity, whose normalized second covering radius is no more then ρ, and whose rate (asymptotically) does not exceed γ.

In order to find such codes, we take a probabilistic approach. We generate random codes using a carefully chosen distribution. Then, we prove that the event of obtaining a second-order covering code with a normalized radius not bigger than ρ, is non-zero for a large-enough length. We then make sure that some of these codes have a sufficiently low rate. This will imply that the desired codes exist and the upper bound holds.

Authorized licensed use limited to: McMaster University. Downloaded on August 25,2023 at 17:05:57 UTC from IEEE Xplore. Restrictions apply.

From now on, we fix some $\rho \in (0, 1 - \frac{1}{q^2})$. Let $\{\chi_{\overline{v}}\}_{\overline{v} \in G_2^n}$ be a set of i.i.d $\mathrm{Ber}(p)$ random variables. We consider the random code C which consists of all the vectors $\overline{v} \in G_q^n$ such that $\chi_{\overline{v}} = 1$, i.e.,

$$C \triangleq \left\{\overline{v} \in G_q^n \,\middle|\, \chi_{\overline{v}} = 1\right\}.$$

Let $\overline{u}_1, \overline{u}_2 \in G_q^n$ be two vectors, and assume $\mathbf{v} \in G_q^{2\times n}$. We say that the unordered pair $\{\overline{u}_1, \overline{u}_2\}$ covers $\mathbf{v}$, denoted $\{\overline{u}_1, \overline{u}_2\} \mathrel{⋺} \mathbf{v}$, if $\mathbf{v}$ is contained in at least one of the two balls of radius ρn centered at $\left[\begin{smallmatrix}\overline{u}_1\\ \overline{u}_2\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}\overline{u}_2\\ \overline{u}_1\end{smallmatrix}\right]$. That is,

$$\{\overline{u}_1, \overline{u}_2\} \mathrel{⋺} \mathbf{v} \text{ iff } \mathbf{v} \in B_{\rho n}^{(2)}(\left[\begin{smallmatrix}\overline{u}_1\\ \overline{u}_2\end{smallmatrix}\right]) \cup B_{\rho n}^{(2)}(\left[\begin{smallmatrix}\overline{u}_2\\ \overline{u}_1\end{smallmatrix}\right]) \text{ and } \overline{u}_1 \neq \overline{u}_2.$$

Equivalently,

$$\{\overline{u}_1, \overline{u}_2\} \mathrel{⋺} \mathbf{v} \text{ iff } \left\{\left[\begin{smallmatrix}\overline{u}_1\\ \overline{u}_2\end{smallmatrix}\right], \left[\begin{smallmatrix}\overline{u}_2\\ \overline{u}_1\end{smallmatrix}\right]\right\} \cap B_{\rho n}^{(2)}(\mathbf{v}) \neq \emptyset \text{ and } \overline{u}_1 \neq \overline{u}_2.$$

Then, for any matrix $\mathbf{v} \in G_q^{2\times n}$ we define the random variable

$$X_{\mathbf{v}} \triangleq \sum_{\{\overline{u}_1, \overline{u}_2\} \mathrel{⋺} \mathbf{v}} \chi_{\overline{u}_1} \cdot \chi_{\overline{u}_2}.$$

We observe that if $X_{\mathbf{v}} > 0$ then $\mathbf{v}$ is 2-covered by at least one matrix from C^2 with distinct rows.

Aiming for a lower bound on $\mathbb{P}[X_{\mathbf{v}} = 0]$, we use the Janson-type concentration inequality given as follows:

Theorem 7 ([8, Theorem 11]) *Let $\{\chi_i\}_{i\in\Omega}$ be a finite set of independent Boolean random variables, and let $\mathcal{A} \subseteq 2^{\Omega}$ be a family of non-empty subsets. Let X be the random variable defined by*

$$X \triangleq \sum_{A\in\mathcal{A}} I_A, \quad I_A \triangleq \prod_{i\in A} \chi_i,$$

and for each $A \in \mathcal{A}$ let us define

$$X_A \triangleq I_A + \sum_{\substack{A\neq B\in\mathcal{A}\\ A\cap B\neq\emptyset}} I_B, \quad \textit{and} \quad p_A \triangleq \mathbb{P}[I_A = 1].$$

Then,

$$\mathbb{P}[X = 0] \leqslant \exp\left(-\sum_{A\in\mathcal{A}} p_A \,\mathrm{E}\left[\frac{1}{X_A} \,\middle|\, I_A = 1\right]\right). \tag{8}$$

One can easily see that for any $\mathbf{v} \in G_q^{2\times n}$, our probabilistic model exactly fits the setting of Theorem 7 with $X = X_{\mathbf{v}}$, $\Omega = G_q^n$, and $\mathcal{A} = \{\{\overline{u}_1, \overline{u}_2\} \,|\, \overline{u}_1 \neq \overline{u}_2 \text{ and } \{\overline{u}_1, \overline{u}_2\} \mathrel{⋺} \mathbf{v}\}$.

Given $A = \{\overline{u}_1, \overline{u}_2\}$, with $\overline{u}_1, \overline{u}_2 \in G_q^n$, and given $\mathbf{v} = \left[\begin{smallmatrix}\overline{v}_1\\ \overline{v}_2\end{smallmatrix}\right] \in G_q^{2\times n}$, we shall conveniently define

$$w_A \triangleq \min_{i,j\in\{1,2\}} d(\overline{u}_i, \overline{v}_j), \tag{9}$$

where the dependence on $\mathbf{v}$ is implicit in the notation w_A.

Lemma 8 *With the notation above, for any $\mathbf{v} = \left[\begin{smallmatrix}\overline{v}_1\\ \overline{v}_2\end{smallmatrix}\right] \in G_q^{2\times n}$ and $A = \{\overline{u}_1, \overline{u}_2\} \in \mathcal{A}$, we have that*

$$\frac{1}{2} \cdot \frac{1 - (1-p)^{n_A+1}}{p(n_A+1)} \leqslant \mathrm{E}\left[\frac{1}{X_A} \,\middle|\, I_A = 1\right] \leqslant \frac{1 - (1-p)^{n_A+1}}{p(n_A+1)}$$

where n_A is an integer satisfying

$$q^{w_A} \cdot V^{(1)}_{\rho n - w_A, n - w_A, q} \leqslant n_A \leqslant 4 \cdot q^{w_A} \cdot V^{(1)}_{\rho n - w_A, n - w_A, q}.$$

By further analyzing the function $\frac{1-(1-p)^{n_A+1}}{p(n_A+1)}$ from Lemma 8, we immediately arrive at the following corollary:

Corollary 9 *For any $\left[\begin{smallmatrix}\overline{v}_1\\ \overline{v}_2\end{smallmatrix}\right] = \mathbf{v} \in G_q^{2\times n}$ and $A = \{\overline{u}_1, \overline{u}_2\} \in \mathcal{A}$, with $w_A = m = \mu n \leqslant \rho n$ we have that*

$$\mathrm{E}\left[\frac{1}{X_A} \,\middle|\, I_A = 1\right] \geqslant \frac{1}{2} \cdot \frac{1 - (1-p)^{q^{n\cdot(f(\mu)+o(1))}}}{p \cdot q^{n\cdot(f(\mu)+o(1))}},$$

where

$$f(\mu) \triangleq \begin{cases} 1 & \mu \in [0, 1 - q(1-\rho)], \\ \mu + (1-\mu) H_q\!\left(\frac{\rho-\mu}{1-\mu}\right) & \mu \in (1 - q(1-\rho), \rho]. \end{cases}$$

We now turn towards an asymptotic analysis of $\mathbb{P}[X_{\mathbf{v}} = 0]$. Our strategy is to show, using the Janson-type inequality given in Theorem 7, that for an appropriate choice of p, this probability decreases rapidly to 0 for all the matrices in $G_q^{2\times n}$. Let $A = \{\overline{u}_1, \overline{u}_2\}$ be such that $w_A = m = \mu n \leqslant \rho n$. As we continue, we shall find the case of $\mu = \frac{q}{q+1}\rho$ of particular interest. In the following lemma we show the existence of a large subset $\mathcal{A}' \subseteq \mathcal{A}$ such that for all $A \in \mathcal{A}'$ we have $w_A = n(\mu + o(1))$.

Lemma 10 *Let $\left[\begin{smallmatrix}\overline{v}_1\\ \overline{v}_2\end{smallmatrix}\right] = \mathbf{v} \in G_q^{2\times n}$ be any matrix, $\rho \in (0, 1 - \frac{1}{q^2})$, and $\mu = \frac{q}{q+1}\rho$. Then there exists a subset $\mathcal{A}' \subseteq \mathcal{A}$ with*

$$|\mathcal{A}'| \geqslant q^{n\left(H_q(\mu) + \mu + (1-\mu)H_q\left(\frac{\rho-\mu}{1-\mu}\right) + o(1)\right)},$$

such that for all $A \in \mathcal{A}'$ we have

$$\mu n - 11 \leqslant w_A \leqslant \mu n.$$

Another technical result we shall need is the following entropy identity.

Lemma 11 *For any $\rho \in (0, 1 - \frac{1}{q^2})$ and $\mu = \frac{q}{q+1}\rho$,*

$$H_q(\mu) + \mu + (1-\mu) H_q\left(\frac{\rho-\mu}{1-\mu}\right) = 2H_{q^2}(\rho).$$

Lemma 12 *For any integer $q \geqslant 2$ and $\rho \in (0, 1 - \frac{1}{q^2})$,*

$$H_q\left(\frac{q}{q+1}\rho\right) - H_{q^2}(\rho) > 0.$$

We now have all the technical lemmas needed to bound $\mathbb{P}[X_{\mathbf{v}} = 0]$.

Proposition 13 *Let $\rho \in (0, 1 - \frac{1}{q^2})$ and $\varepsilon \in (0, H_q(\frac{q}{q+1}\rho) - H_{q^2}(\rho))$ be fixed. Assume that $p = q^{-n(H_{q^2}(\rho)-\varepsilon)}$, $\left[\begin{smallmatrix}\overline{v}_1\\ \overline{v}_2\end{smallmatrix}\right] = \mathbf{v} \in G_q^{2\times n}$. Then,*

$$\mathbb{P}[X_{\mathbf{v}} = 0] \leqslant \exp\left(-q^{n(2\varepsilon + o(1))}\right),$$

where the $o(1)$ term does not depend on $\mathbf{v}$.

Authorized licensed use limited to: McMaster University. Downloaded on August 25,2023 at 17:05:57 UTC from IEEE Xplore. Restrictions apply.

The last components for the proof of Theorem 6 are the following concentration inequality for binomial random variables, and a proposition that shows that, with high probability, the cardinality of the random code C is close to its expected value of $q^{n(1-H_{q^2}(\rho)+\varepsilon)}$.

Lemma 14 ([7, Theorem 1]) *Let $X \sim \mathrm{Bin}(n,p)$ be a binomial random variable. Then for every real $a > 0$*

$$\mathbb{P}[X \geqslant \mathrm{E}[X] + a] \leqslant \exp\Big(-\frac{a^2}{2np}\Big(1-\frac{a}{3np}\Big)\Big).$$

From Lemma 14 it follows that if $X \sim \mathrm{Bin}(n,p)$, and $\gamma > 0$, then

$$\mathbb{P}[X \geqslant \mathrm{E}[X](1+\gamma)] \leqslant \exp\Big(-\frac{1}{2}\gamma^2 np\Big(1-\frac{\gamma}{3}\Big)\Big). \tag{10}$$

Proposition 15 *Under the assumptions of Proposition 13, for all sufficiently large n,*

$$\mathbb{P}\Big[\{R_2(C) \leqslant \rho n\} \cap \Big\{|C| < q^{n(1-H_{q^2}(\rho)+\varepsilon+1/n)}\Big\}\Big] \geqslant 1 - \exp\Big(-q^{n(2\varepsilon+o(1))}\Big).$$

The proof of Theorem 6 now easily follows.

Proof of Theorem 6: As explained in the beginning of Section III, the only remaining part we need to prove is that $\kappa_2(\rho, q) \leqslant 1 - H_{q^2}(\rho)$ for all $\rho \in (0, 1-\frac{1}{q^2})$. Let $\rho \in (0,1-\frac{1}{q^2}))$ and $\varepsilon \in (0, H_q(\frac{q}{q+1}\rho) - H_{q^2}(\rho))$ be fixed. By Proposition 15, for all sufficiently large n, the random code C satisfies

$$\mathbb{P}\Big[\{R_2(C) \leqslant \rho n\} \cap \Big\{|C'| < q^{n(1-H_{q^2}(\rho)+\varepsilon+1/n)}\Big\}\Big] > 0.$$

In particular, there exists at least one (deterministic) code C_n such that

$$R_2(C_n) \leqslant \rho n, \quad \text{and} \quad |C_n| < q^{n(1-H_{q^2}(\rho)+\varepsilon+1/n)}.$$

This immediately implies that,

$$k_2(n, \rho n, q) \leqslant q^{n(1-H_{q^2}(\rho)+\varepsilon+1/n)} = q^{n(1-H_{q^2}(\rho)+\varepsilon+o(1))}.$$

This proves that

$$\begin{aligned}\kappa_2(\rho,q) &= \liminf_{n\to\infty} \frac{1}{n}\log_q(k_2(n,\rho n,q)) \\ &\leqslant \liminf_{n\to\infty}\big(1 - H_{q^2}(\rho) + \varepsilon + o(1)\big) = 1 - H_{q^2}(\rho) + \varepsilon.\end{aligned}$$

Taking $\varepsilon \to 0$ we conclude the claim. ■

While for the proof of the upper-bound part of Theorem 6 it is only required to show the existence of second-order covering codes, we observe that a stronger conclusion may follow, namely, that with high probability, a random code generated according to our distribution is a second-order covering code. We use this fact in order to prove that the fraction of second-order covering codes (among the set of codes of sufficiently large size) tends to 1 as $n \to \infty$.

For an integer $q \geqslant 2$, $\rho \in (0, 1-\frac{1}{q^2})$, $n \in \mathbb{N}$, and $0 \leqslant M \leqslant q^n$, let $\alpha_q(n,\rho,M)$ denote the fraction of codes of length n over G_q with second covering radius at most ρn in the set of $(n,M)_q$ codes. Namely,

$$\alpha_q(n,\rho,M) \triangleq \frac{|\mathcal{C}_q(n,\rho,M)|}{\binom{q^n}{M}},$$

where

$$\mathcal{C}_q(n,\rho,M) \triangleq \big\{C \subseteq G_q^n \,\big|\, R_2(C) \leqslant \rho n, |C| = M\big\}.$$

Lemma 16 *Let ρ and n be fixed. For any $0 \leqslant M \leqslant q^n - 1$,*

$$\alpha_q(n,\rho,M) \leqslant \alpha_q(n,\rho,M+1).$$

The following theorem asserts that the fraction of second-order covering codes tends to 1 as the length tends to infinity when we consider codes with rate larger then the optimal rate presented in Theorem 6 by an arbitrarily small amount.

Theorem 17 *For any $\rho \in (0, 1-\frac{1}{q^2})$ and $\varepsilon > 0$, let us denote $M(n,\rho,\varepsilon) \triangleq \lfloor q^{n(1-H_{q^2}(\rho)+\varepsilon+1/n)} \rfloor$. Then,*

$$\lim_{n\to\infty} \alpha_q(n,\rho,M(n,\rho,\varepsilon)) = 1.$$

IV. Conclusion and Further Questions

In this paper we studied the optimal rate of general second-order covering codes over finite Abelian groups. Our main result, the exact asymptotic minimal rate of second-order covering codes, was proved using a probabilistic approach. In summary, for the first-order covering radius we already know

$$\kappa_1(\rho, q^t) = \begin{cases} 1 - H_{q^t}(\rho) & \rho \in [0, 1-\frac{1}{q^t}), \\ 0 & \rho \in [1-\frac{1}{q^t}, 1]. \end{cases}$$

In the second-order case, Theorem 6 reveals that

$$\kappa_2(\rho, q) = \kappa_1(\rho, q^2) = \begin{cases} 1 - H_{q^2}(\rho) & \rho \in [0, 1-\frac{1}{q^2}), \\ 0 & \rho \in [1-\frac{1}{q^2}, 1]. \end{cases}$$

In theory, the proof strategy of Theorem 6 may be applied for higher values of t. However in practice, the analysis performed in our proof, which is already involved in the second-order case, seems not to be scalable for higher orders. We therefore leave the higher-order problem for future study:

Question 1 *Prove that for any $q, t \geqslant 2$*

$$\kappa_t(\rho, q) = \kappa_1(\rho, q^t) = \begin{cases} 1 - H_{q^t}(\rho) & \rho \in [0, 1-\frac{1}{q^t}), \\ 0 & \rho \in [1-\frac{1}{q^t}, 1]. \end{cases}$$

Another interesting direction of research involves linear codes. In the case where $G_q = \mathbb{F}_q$ is a finite field, (1) raises the suspicion that there is no different in asymptotic minimal rate between general codes and linear codes. Thus, we suggest the following open problem as well:

Question 2 *Prove or disprove that for any $q, t \geqslant 2$*

$$\kappa_t(\rho, q) = \kappa_t^{\mathrm{Lin}}(\rho, q). \tag{11}$$

Except for the first-order case, it is unknown whether (11) is true.

Authorized licensed use limited to: McMaster University. Downloaded on August 25,2023 at 17:05:57 UTC from IEEE Xplore. Restrictions apply.

References

[1] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes*. North-Holland, 1997.

[2] G. Cohen and P. Frankl, "Good coverings of Hamming spaces with spheres," *Discrete Mathematics*, vol. 56, no. 2-3, pp. 125–131, 1985.

[3] D. Elimelech, M. Firer, and M. Schwartz, "The generalized covering radii of linear codes," *IEEE Transactions on Information Theory*, vol. 67, no. 12, pp. 8070–8085, 2021.

[4] D. Elimelech and M. Schwartz, "The second-order football-pool problem and the optimal rate of generalized-covering codes," *arXiv preprint arXiv:2210.00531*, 2022.

[5] D. Elimelech, H. Wei, and M. Schwartz, "On the generalized covering radii of reed-muller codes," *IEEE Transactions on Information Theory*, 2022.

[6] V. Guruswami, A. Rudra, and M. Sudan, *Essential Coding Theory*, 2022.

[7] S. Janson, "Large deviation inequalities for sums of indicator variables," *arXiv preprint arXiv:1609.00533*, 2016.

[8] M. Schwartz and A. Vardy, "New bounds on the capacity of multidimensional run-length constraints," *IEEE transactions on information theory*, vol. 57, no. 7, pp. 4373–4382, 2011.

[9] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1412–1418, Sep. 1991.

Authorized licensed use limited to: McMaster University. Downloaded on August 25,2023 at 17:05:57 UTC from IEEE Xplore. Restrictions apply.