On the Generalized Covering Radii of Reed-Muller Codes

Dor Elimelech, *Graduate Student Member, IEEE*, Hengjia Wei, and Moshe Schwartz, *Senior Member, IEEE*

***Abstract*— We study generalized covering radii, a fundamental property of linear codes that characterizes the trade-off between storage, latency, and access in linear data-query protocols such as PIR. We prove lower and upper bounds on the generalized covering radii of Reed-Muller codes, as well as finding their exact value in certain extreme cases. With the application to linear data-query protocols in mind, we also construct a covering algorithm that gets as input a set of points in space, and find a corresponding set of codewords from the Reed-Muller code that are jointly not farther away from the input than the upper bound on the generalized covering radius of the code. We prove that the algorithm runs in time that is polynomial in the code parameters.**

***Index Terms*— Reed-Muller codes, generalized covering radius, covering algorithm.**

I. Introduction

THE generalized covering radius has recently been proposed [10] as a new fundamental property of linear codes, generalizing the classical notion of a covering radius. As a motivating application, these radii characterize a trade-off between storage, latency, and access complexities in linear data-query protocols, a prime example of which is the PIR (Private Information Retrieval) protocol. Several equivalent definitions of the generalized covering radii were given in [10], showing their combinatorial, geometric, and algebraic aspects. It has also been observed that there is an intriguing similarity between the generalized covering radii and the well known generalized Hamming weights of linear codes [29], hinting at a deeper theory and perhaps additional applications of these parameters that are yet to be revealed.

A crucial part in our understanding of any fundamental parameter of codes, is the values that it takes in specific examples and in parametric families of codes. In [10], the generalized covering radius hierarchy was found only for Hamming codes and shortened Hamming codes, whereas the remaining results did not pertain to specific code families. The Hamming code, in its extended version, is a specific case of the famous family of Reed-Muller codes, which is one of the most studied families of linear error-correcting codes. Reed-Muller codes have been extensively studied in the recent decades due to their practical applications and fascinating relations with various mathematical objects. Reed-Muller codes were recently proved to achieve asymptotically the capacity of erasure channels [17]. They have long been conjectured to achieve Shannon's capacity on symmetric channels, and a recent paper [3] took a step towards a proof of this conjecture, by showing a polarization property in Reed-Muller codes. Other applications of Reed-Muller codes include locally decodable codes [30], probabilistic proof systems [1], sequence design for wireless communications [8], [9], [23], [26], and Boolean functions [4], [18], [21]. For a recent survey, the readers are referred to [2].

While many aspects of Reed-Muller codes have been investigated, of particular interest to us is the (regular) covering radius. Its relation to the maximum nonlinearity of Boolean functions motivated many of the papers on the subject. The covering radius of Reed-Muller codes has been studied in different settings [5], [7], [13]–[16], [20], [22], [24], [25]. However, despite decades of research on the subject, the exact covering radius of Reed-Muller codes is mostly unknown, except for a handful of specific cases, and many papers resorted to finding lower and upper bounds.

The goal of this paper is to explore the *generalized covering radii* of Reed-Muller codes. Our main contributions are the following:

1) We prove lower and upper bounds on the generalized covering radii of Reed-Muller codes, $\mathrm{RM}(r,m)$, in various asymptotic regimes of its parameters: constant r, constant $m-r$, constant r/m, and constant rate, where $r=\frac{m}{2}+\Theta(\sqrt{m})$. We also find the exact t-th generalized covering radius of (r,m) in simple cases, $r\in\{0,m-2,m-1,m\}$. These results are summarized in Table I and Table II.
2) Motivated by the application for linear data-querying protocols, we construct a t-covering algorithm for Reed-Muller codes. Loosely speaking, given t vectors in the space, the algorithm finds t codewords that are jointly not farther away from the given points than the best upper bound that we have on the t-th generalized covering radius of the code. We analyze the run-time

Manuscript received July 21, 2021; revised January 6, 2022; accepted March 4, 2022. Date of publication March 10, 2022; date of current version June 15, 2022. The work of Dor Elimelech was supported in part by the Israel Science Foundation (ISF) under Grant 1052/18. The work of Hengjia Wei and Moshe Schwartz was supported in part by the German Israeli Project Cooperation (DIP) under Grant PE2398/1-1. An earlier version of this paper was presented in part at the IEEE International Symposium on Information Theory (ISIT) 2022. *(Corresponding author: Hengjia Wei.)*

Dor Elimelech and Moshe Schwartz are with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Be'er Sheva 8410501, Israel (e-mail: doreli@post.bgu.ac.il; schwartz@ee.bgu.ac.il).

Hengjia Wei is with the Peng Cheng Laboratory, Shenzhen 518000, China (e-mail: hjwei05@gmail.com).

Communicated by C. Xing, Associate Editor for Coding and Decoding.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2022.3158762.

Digital Object Identifier 10.1109/TIT.2022.3158762

complexity of the algorithm and show it is polynomial in the code parameters.

The paper is organized as follows: Preliminaries and notations are presented in Section II. Section III is devoted to the derivation of bounds on the generalized covering radii of Reed-Muller codes. In Section IV we discuss the implications of the bounds on Reed-Muller codes to bounds on general codes. The construction of our covering algorithm and its analysis are in Section V. We conclude with a discussion of the results and some open questions in Section VI.

II. Preliminaries

We use lower-case letters, v, to denote scalars, overlined lower-case letters, $\overline{v}$, to denote vectors, and either bold lower-case letters, $\mathbf{v}$, or upper-case letter, V, to denote matrices. Whether vectors are row vectors or column vectors is deduced from context.

Let $\mathbb{F}_q$ denote the finite field of size q. For $n \in \mathbb{N}$, we define $[n] \triangleq \{1, \dots, n\}$, and denote by $\binom{[n]}{t}$ the set of all subsets of $[n]$ of size t. For a vector $\overline{v} = (v_1, \dots, v_n) \in \mathbb{F}_q^n$, the support of $\overline{v}$ is defined as $\operatorname{supp}(\overline{v}) \triangleq \{i \in [n] | v_i \neq 0\}$, and its Hamming weight is defined as $\operatorname{wt}(\overline{v}) \triangleq |\operatorname{supp}(\overline{v})|$. The Hamming distance between $\overline{v}, \overline{v}' \in \mathbb{F}_q^n$ is then defined as $d(\overline{v}, \overline{v}') \triangleq \operatorname{wt}(\overline{v}' - \overline{v})$.

We say C is an $[n, k, d]_q$ linear code if $C \subseteq \mathbb{F}_q^n$ is a k-dimensional vector space, and the minimum Hamming distance between distinct codewords is d. The code C may be specified using a $k \times n$ generator matrix $G \in \mathbb{F}_q^{k \times n}$, whose row space is C, or by an $(n-k) \times n$ parity-check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$, whose null space is C. The dual code of C, denoted $C^\perp$, is the code whose generator matrix is H, and parity-check matrix is G, namely,

$$C^\perp \triangleq \left\{ \overline{v} \in \mathbb{F}_q^n \middle| \forall \overline{c} \in C, \overline{v} \cdot \overline{c} = 0 \right\}.$$

The dual code, $C^\perp$, is an $[n, n-k, d']_q$ code. We say d' is the *dual distance* of C.

For any vector $\overline{v} \in \mathbb{F}_q^n$, the distance between $\overline{v}$ and the code C is defined as

$$d(\overline{v}, C) \triangleq \min_{\overline{c} \in C} d(\overline{c}, \overline{v}).$$

The covering radius of C, denoted $R(C)$, is then defined as

$$R(C) \triangleq \max_{\overline{v} \in \mathbb{F}_q^n} d(\overline{v}, C).$$

It is therefore the minimum radius at which balls centered at the codewords of C cover the entire space $\mathbb{F}_q^n$. A generalization of this property will be presented shortly when we introduce the generalized covering radii of C. Later, we shall also make use of a connection between the covering radius of C, and the dual distance of C. To that end we recall the definition of Krawtchouk polynomials,

$$K_k(x; n, q) \triangleq \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j},$$

where

$$\binom{x}{j} \triangleq \frac{x(x-1)\dots(x-j+1)}{j!}. \tag{1}$$

We further denote the minimal root of $K_k(x; n, q)$ by

$$x(k, n; q) \triangleq \min\{x \in \mathbb{R} | K_k(x; n, q) = 0\}.$$

Lemma 1: [28, Theorem 3.3] Let C be an $[n, k]_q$ code with dual distance d'. Then

$$R(C) \leqslant \begin{cases} x(u, n-1; q) & d' = 2u - 1, \\ x(u, n; q) & d' = 2u. \end{cases}$$

A. The Generalized Covering Radii

The generalized covering radii of a linear code were introduced in [10]. They have several equivalent definitions, which we bring here and use interchangeably. We begin with a geometric definition. Consider the set of matrices $\mathbb{F}_q^{t \times n}$, in which we have a generalized notion for the Hamming weights. For a matrix $\mathbf{v} \in \mathbb{F}_q^{t \times n}$, with row vectors denoted by $\overline{v}_i$, the t-weight is defined to be

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

The t-weight naturally induces a metric on $\mathbb{F}_q^{t \times n}$ by

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

for all $\mathbf{v}, \mathbf{u} \in \mathbb{F}_q^{t \times n}$. Let $B_r^{(t)}(\mathbf{v})$ denote the ball of radius r centered in $\mathbf{v} \in \mathbb{F}_q^{t \times n}$, with respect to the metric $d^{(t)}$, namely

$$B_r^{(t)}(\mathbf{v}) \triangleq \left\{ \mathbf{v}' \in \mathbb{F}_q^{t \times n} \middle| d^{(t)}(\mathbf{v}, \mathbf{v}') \leqslant r \right\}.$$

Since this metric is translation invariant, the volume of the ball does not depend on the choice of its center. We denote this volume by

$$V_{q^t, n, r} \triangleq \left| B_r^{(t)}(\mathbf{v}) \right| = \sum_{i=0}^{r} \binom{n}{i} (q^t - 1)^i, \tag{2}$$

which is exactly the size of a ball of radius r in $\mathbb{F}_{q^t}^n$ using the Hamming metric. We now have the following definition for the t-th generalized radius:

Definition 2: Let C be an $[n, k]_q$ linear code. Then for every $t \in \mathbb{N}$, we define the t-th generalized covering radius, denoted by $R_t(C)$, to be the minimal integer r such that the balls of radius r centered at

$$C^t \triangleq \left\{ \begin{bmatrix} \overline{c}_1 \\ \vdots \\ \overline{c}_t \end{bmatrix} \in \mathbb{F}_q^{t \times n} \middle| \forall i \in [t], \overline{c}_i \in C \right\}, \tag{3}$$

cover $\mathbb{F}_q^{t \times n}$, i.e.,

$$\bigcup_{\mathbf{c} \in C^t} B_r^{(t)}(\mathbf{c}) = \mathbb{F}_q^{t \times n}.$$

One can easily see that $R_1(C) = R(C)$ is indeed the regular covering radius of the code C. Let us now turn to an equivalent definition via the parity-check matrix of a code. Assume C is a linear $[n, k]_q$ code with a (full-rank) parity-check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$. Let the columns of H be denoted by $\overline{h}_1, \dots, \overline{h}_n$. Then for $I \in \binom{[n]}{t}$, $1 \leqslant t \leqslant n$, we denote the linear span of

$\{\overline{h}_i\}_{i\in I}$ by $\langle H_I\rangle$. We have the following equivalent definition for the t-th generalized covering radius of C:

Definition 3: The t-th covering radius of C, denoted by $R_t(C)$, is the smallest integer r such that for any t vectors $\overline{v}_1,\dots,\overline{v}_t \in \mathbb{F}_q^{n-k}$, there exists $I \in \binom{[n]}{r}$ such that $\{v_1,\dots,v_t\} \subseteq \langle H_I\rangle$.

The final equivalent definition that we recall for the generalized covering radius is algebraic in nature:

Definition 4: Let $C \subseteq \mathbb{F}_q^n$ be a linear code with a generator matrix $G \in \mathbb{F}_q^{k\times n}$ and a parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$. Let C_t be the code over $\mathbb{F}_{q^t}$, with generator matrix G and parity-check matrix H, namely,

$$C_t \triangleq \left\{ \overline{u}G \,\middle|\, \overline{u} \in \mathbb{F}_{q^t}^k \right\} = \left\{ \overline{v} \in \mathbb{F}_{q^t}^n \,\middle|\, H\overline{c}^\intercal = \overline{0}^\intercal \right\}. \tag{4}$$

The t-th covering radius is defined to be

$$R_t(C) \triangleq R_1(C_t),$$

where $R_1(C_t)$ is the (regular, first) covering radius of C_t.

According to Definition 4, the problem of finding the t-th covering radius of a code $C \subseteq \mathbb{F}_q^n$, is equivalent to finding the regular covering radius of C_t defined over $\mathbb{F}_{q^t}$. Since the code C_t will be used many times, we briefly show that, unlike the covering radius, its minimum distance does not change.

Lemma 5: Let C be an $[n,k,d]_q$ code. Then for any $t \in \mathbb{N}$, the code C_t of (4) is an $[n,k,d]_{q^t}$ code.

Proof: The fact that C_t has length n is trivial. Let $H \in \mathbb{F}_q^{(n-k)\times n}$ be parity-check matrix for C. Since a set of vectors from $\mathbb{F}_q^n$ is linearly independent over $\mathbb{F}_q$ if and only if it is linearly independent over $\mathbb{F}_{q^t}$, the matrix H has the same rank over $\mathbb{F}_{q^t}$, and its null-space, C_t, has dimension k. Finally, it is well known that the minimum distance d of C is the minimal number of columns of H that are linearly dependent. By the same argument as before, this number does not change when considering columns of H and linear dependence over $\mathbb{F}_{q^t}$. Hence, the minimum distance of C_t is also d. ■

The generalized covering radius has a subadditivity property that proves to be useful for establishing many of the results in this work:

Lemma 6: [10, Proposition 15] Let C be an $[n,k]_q$ code. Then for all $t_1, t_2 \in \mathbb{N}$,

$$R_{t_1+t_2}(C) \leqslant R_{t_1}(C) + R_{t_2}(C).$$

In particular, $R_t(C) \leqslant tR_1(C)$ for all $t \in \mathbb{N}$.

A simple ball-covering argument is used in the following lemma.

Lemma 7: For an $[n,k]_q$ code C and $t \in \mathbb{N}$,

$$\log_{q^t}\left(V_{q^t,n,R_t(C)}\right) \geqslant n-k.$$

Proof: Recalling (4), consider the code C_t over $\mathbb{F}_{q^t}$, generated by the same generator matrix as C. Clearly, C_t has the same dimension and length as C. By the standard ball-covering argument (see [6, Theorem 6.2.1]),

$$\log_{q^t}\left(V_{q^t,n,R_1(C_t)}\right) \geqslant n-k.$$

By Definition 4, $R_1(C_t) = R_t(C)$, and we conclude. ■

Since we shall be interested in asymptotic results, we recall facts about the asymptotics of binomial coefficients as well as the volume of balls in the Hamming metric. Let $H_q(x)$ denote the q-ary entropy function,

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

A useful Taylor expansion near the entropy function's maximum was presented in [12, Proposition 3.3.5], showing that, as $\epsilon \to 0$,

$$H_q\left(1-\frac{1}{q}-\epsilon\right) = 1 - \frac{\epsilon^2 q^2}{2(q-1)\ln q}(1+o(1)). \tag{5}$$

For any real $0<\alpha<1$, such that $\alpha n \in \mathbb{N}$, it is known (e.g., see [19, Ch. 10, Lemma 7]) that

$$\frac{1}{\sqrt{8n\alpha(1-\alpha)}}2^{nH_2(\alpha)} \leqslant \binom{n}{\alpha n} \leqslant \frac{1}{\sqrt{2\pi n\alpha(1-\alpha)}}2^{nH_2(\alpha)}, \tag{6}$$

and this holds for $n \in \mathbb{R}$, $n>1$ (recall the definition of the binomial in (1), and see [11, p. 482]). As for the Hamming ball, it is well known (see [19, Ch. 10, Corollary 9] and [12, Proposition 3.3.1]) that for $q \geqslant 2$, and $\alpha \leqslant 1-\frac{1}{q}$,

$$\frac{1}{\sqrt{8n\alpha(1-\alpha)}}q^{nH_q(\alpha)} \leqslant V_{q,n,\alpha n} \leqslant q^{nH_q(\alpha)}. \tag{7}$$

B. Reed-Muller Codes

Reed-Muller codes have been extensively studied (e.g., see [19], and the many references therein). We recall the relevant definitions and properties needed for this paper. For $m \in \mathbb{N}$ and $0 \leqslant r \leqslant m$, the r-th order Reed-Muller code, denoted by $\mathrm{RM}(r,m)$, is a binary linear $[n,k]$ code with parameters

$$n = 2^m, \quad k = \sum_{i=0}^{r}\binom{m}{i}. \tag{8}$$

Reed-Muller codes have multiple equivalent definitions, and one that will be useful for our needs is a recursive definition, given by the $(u,u+v)$ construction. Assume C_1 and C_2 are $[n,k_1]_q$ and $[n,k_2]_q$ codes, respectively. The $(u,u+v)$ construction uses C_1 and C_2 to produce a code

$$C = \left\{ (\overline{u}, \overline{u}+\overline{v}) \,\middle|\, \overline{u} \in C_1, \overline{v} \in C_2 \right\}.$$

As a base for the recursion, we define

$$\mathrm{RM}(0,m) \triangleq \left\{\overline{0}, \overline{1}\right\},$$

i.e., the repetition code. Additionally, we define

$$\mathrm{RM}(m,m) \triangleq \mathbb{F}_2^{2^m},$$

i.e., the entire set of binary vectors of length 2^m. Finally, for $1 \leqslant r \leqslant m-1$, we define $\mathrm{RM}(r,m)$ to be the code produced by the $(u,u+v)$ construction using $\mathrm{RM}(r,m-1)$ and $\mathrm{RM}(r-1,m-1)$.

Reed-Muller codes are nested, namely, for all $1 \leqslant r \leqslant m$,

$$\mathrm{RM}(r-1,m) \subseteq \mathrm{RM}(r,m). \tag{9}$$

Additionally, the family of Reed-Muller code is closed under code duality, and in particular

$$\mathrm{RM}(r,m)^\perp = \mathrm{RM}(m-r-1,m).$$

This implies that

$$\dim\left(\mathrm{RM}(r,m)\right)=2^m-\dim\left(\mathrm{RM}(m-r-1,m)\right). \quad (10)$$

To avoid cumbersome notation, we denote the t-th generalized covering radius of the r-th order Reed-Muller code by

$$R_t(r,m)\triangleq R_t(\mathrm{RM}(r,m)).$$

The following fundamental property of $R_t(r,m)$ will be used frequently in this work:

Proposition 8: For all $m,t\in\mathbb{N}$, and $1\leqslant r\leqslant m-1$,

$$R_t(r,m)\leqslant R_t(r-1,m-1)+R_t(r,m-1).$$

Proof: The claim follows from the $(u,u+v)$ construction of Reed-Muller codes. In [10, Proposition 24] it is proved that if a code C is produced using the $(u,u+v)$ construction with C_1 and C_2, then $R_t(C)\leqslant R_t(C_1)+R_t(C_2)$. ■

III. Bounds

Our main results are presented in this section. We prove bounds on the generalized covering radii of Reed-Muller codes, $\mathrm{RM}(r,m)$, in different asymptotic regimes, as $m\to\infty$:

- r is constant.
- $m-r$ is constant.
- r/m is constant.
- $\sum_{i=0}^{r}\binom{m}{i}/2^m$ is constant.

Upper bounds will be derived using two main strategies: The first is by considering the upper bounds from [7] and using the subadditivity formula from Lemma 6. The second strategy involves the use of the recursive formula from Proposition 8 and analysis of the base cases. Our lower bounds will essentially be the well known ball-covering lower bound (over the field $\mathbb{F}_{2^t}$), analyzed separately for each of the different cases.

A. The Case Where r Is Constant

In this parameter regime, the Reed-Muller codes have vanishing asymptotic rate, and high covering radius. We first consider the extreme case of $\mathrm{RM}(0,m)$, which is none other than the repetition code. In this simple case we can determine the generalized covering radii exactly.

Proposition 9: For all $m,t\in\mathbb{N}$,

$$R_t(0,m)=2^m-\lceil 2^{m-t}\rceil.$$

Proof: The Reed-Muller code $C=\mathrm{RM}(0,m)$ is the binary repetition code of length 2^m, namely, its generator matrix is $G=(1,1,\dots,1)$. Thus, C_t of (4) is just the 2^t-ary repetition code of the same length. Given a vector $\overline{v}\in\mathbb{F}_{2^t}^{2^m}$, the closest codeword of C_t to $\overline{v}$ is $\overline{c}=(c,c,\dots,c)\in C_t$ where $c\in\mathbb{F}_{2^t}$ is the symbol appearing the most times in $\overline{v}$. By simple averaging, there exists a symbol appearing at least $\lceil 2^{m-t}\rceil$ times in $\overline{v}$, giving us $R_t(0,m)\leqslant 2^m-\lceil 2^{m-t}\rceil$. For the lower bound, define $\ell\triangleq\min\{t,m\}$, and let $\overline{v}\in\mathbb{F}_{2^t}^{2^m}$ be a vector with 2^ℓ different symbols, such that each symbol appears exactly $2^{m-\ell}$ times. Clearly, we have

$$d(\overline{v},\mathrm{RM}(0,m))=2^m-2^{m-\ell}\geqslant 2^m-\lceil 2^{m-t}\rceil.$$

This proves the lower bound. ■

For the more general cases of $\mathrm{RM}(r,m)$ with $r\geqslant 1$, we provide separate upper and lower bound on the generalized covering radii. The upper bounds are proved by induction on r. The base case of $\mathrm{RM}(1,m)$ is proved first.

Lemma 10: For all $m,t\in\mathbb{N}$,

$$R_t(1,m)\leqslant\left(1-\frac{1}{2^t}\right)2^m-\frac{\sqrt{2^t-1}}{2^t}2^{m/2}.$$

Proof: Denote $C=\mathrm{RM}(1,m)$. It is well known that $C^\perp=\mathrm{RM}(m-2,m)$ is the extended binary Hamming code (see [19, Ch. 13]), and hence the dual distance of C is $d'=4$. By Lemma 5, $d'=4$ is the dual distance of C_t of (4) as well. By Lemma 1, the covering radius of C_t is upper bounded by

$$R_t(C)=R_1(C_t)\leqslant x(2,2^m;2^t),$$

i.e., the smallest root of the Krawtchouk polynomial $K_2(x;2^m,2^t)$. Since

$$K_2(x;q,n)=\frac{1}{2}\Big(q^2x^2-q(2qn-q-2n+2)x \\ +(q-1)^2n(n-1)\Big),$$

it follows that

$$x(2,n;q)=\left(1-\frac{1}{q}\right)n-\frac{1}{2}+\frac{1}{q}-\frac{\sqrt{(4q-4)n+(q-2)^2}}{2q} \\ \leqslant\left(1-\frac{1}{q}\right)n-\frac{\sqrt{(q-1)n}}{q}.$$

Plugging in $n=2^m$ and $q=2^t$, we obtain the desired result. ■

We can now prove the general upper bound on $R_t(r,m)$ for $r\geqslant 1$.

Theorem 11: For all $m,t\in\mathbb{N}$, $1\leqslant r\leqslant m$,

$$R_t(r,m)\leqslant\left(1-\frac{1}{2^t}\right)2^m-\frac{\sqrt{2^t-1}}{2^t}(1+\sqrt{2})^{r-1}2^{m/2} \\ +O(m^{r-2}).$$

where we consider r and t to be constants.

Proof: We prove the claim by induction on r. Lemma 10 shows the claim holds for $r=1$, and for all $m\in\mathbb{N}$. Assume that the claim holds for all $\ell\leqslant r-1$, and all $m\in\mathbb{N}$. We now show that it holds for r as well. By repeatedly using Proposition 8 and the induction hypothesis, we have,

$$\begin{aligned}
&R_t(r,m)\\
&\leqslant R_t(r,m-1)+R_t(r-1,m-1)\\
&\leqslant R_t(r,m-1)+\left(1-\frac{1}{2^t}\right)2^{m-1}\\
&\quad-\frac{\sqrt{2^t-1}}{2^t}(1+\sqrt{2})^{r-2}2^{(m-1)/2}+O(m^{r-3})\\
&\vdots\\
&\leqslant R_t(r,r)+\sum_{i=r}^{m-1}\Bigg(\left(1-\frac{1}{2^t}\right)2^i\\
&\quad-\frac{\sqrt{2^t-1}}{2^t}(1+\sqrt{2})^{r-2}2^{i/2}+O(m^{r-3})\Bigg)
\end{aligned}$$

$$\begin{aligned}
&\leqslant R_t(r,r) + \left(1-\frac{1}{2^t}\right)\sum_{i=0}^{m-1} 2^i \\
&\quad - \frac{\sqrt{2^t-1}}{2^t}(1+\sqrt{2})^{r-2}\sum_{i=r}^{m-1} 2^{i/2} + O(m^{r-2}) \\
&= \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}(1+\sqrt{2})^{r-1}\left(2^{m/2}-2^{r/2}\right) \\
&\quad + O(m^{r-2}) \\
&= \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}(1+\sqrt{2})^{r-1}2^{m/2} + O(m^{r-2}).
\end{aligned}$$

Here we also use the fact $R_t(r,r)=0$, since $\mathrm{RM}(r,r)=\mathbb{F}_2^{2^r}$, and so[1] $\mathrm{RM}(r,r)_t = \mathbb{F}_{2^t}^{2^r}$, whose covering radius is 0. ■

The corresponding lower bound on $R_t(r,m)$ is proved next. It is obtained by carefully considering both a ball-covering argument, and the upper bound we just proved.

Theorem 12: For all $m,t\in\mathbb{N}$, $1\leqslant r\leqslant m$,

$$R_t(r,m) \geqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2t(2^t-1)\ln 2}}{2^t\sqrt{r!}} m^{r/2}2^{m/2}(1+o(1)), \tag{11}$$

where we consider r and t to be constants.

Proof: By Lemma 7, we have that

$$\begin{aligned}
\log_{2^t}\left(V_{2^t,2^m,R_t(r,m)}\right) &\geqslant 2^m - \sum_{i=0}^{r}\binom{m}{i} \\
&= 2^m - \frac{m^r}{r!}(1+o(1)).
\end{aligned}$$

According to Theorem 11,

$$\frac{R_t(r,m)}{2^m} = 1 - \frac{1}{2^t} - o(1), \tag{12}$$

and in particular, for all large enough m,

$$\frac{R_t(r,m)}{2^m} < 1 - \frac{1}{2^t}.$$

Using (7),

$$\log_{2^t}\left(V_{2^t,2^m,R_t(r,m)}\right) \leqslant 2^m H_{2^t}\left(\frac{R_t(r,m)}{2^m}\right).$$

Combining the two inequalities above, we have

$$2^m H_{2^t}\left(\frac{R_t(r,m)}{2^m}\right) \geqslant 2^m - \frac{m^r}{r!}(1+o(1)). \tag{13}$$

Denote $y \triangleq 1-1/2^t-R_t(r,m)/2^m$. Then $y=o(1)$ by (12), and $y>0$ for all large enough m. Thus, by (5) we have

$$H_{2^t}\left(\frac{R_t(r,m)}{2^m}\right) = H_{2^t}\left(1-\frac{1}{2^t}-y\right) = 1-cy^2(1+o(1)),$$

where $c=\frac{2^{2t}}{2t(2^t-1)\ln 2}$. Hence,

$$1-cy^2(1+o(1)) \geqslant 1 - \frac{m^r}{2^m r!}(1+o(1)),$$

and so,

$$y \leqslant \frac{m^{r/2}}{2^{m/2}\sqrt{r!\cdot c}}(1+o(1)).$$

The conclusion follows since $R_t(r,m)=(1-1/2^t-y)2^m$. ■

The lower and upper bounds from Theorem 11 and Theorem 12 show that for fixed r, where the rate tends to 0 when $m\to\infty$, the normalized t-covering radius tends to $1-\frac{1}{2^t}$ (with respect to the length of the code). Furthermore, it follows that $R_t(r,m)$ is smaller than $\left(1-\frac{1}{2^t}\right)2^m$ by an amount of $2^{m/2(1+o(1))}$, where the $o(1)$ in the exponent represents the gap between our lower and upper bounds.

B. The Case Where $m-r$ Is Constant

The opposite case to the one studied in the previous section, is that of Reed-Muller codes $\mathrm{RM}(r,m)$ with $m-r$ being constant. These codes have a high rate and a vanishing normalized covering radius. As we show shortly, in this asymptotic regime, the t-th generalized covering radius is approximately linear in t. We begin, however, with the two extreme cases of $\mathrm{RM}(m-1,m)$ and $\mathrm{RM}(m-2,m)$.

Proposition 13: For all $m,t\in\mathbb{N}$,

$$\begin{aligned}
R_t(m,m) &= 0, \\
R_t(m-1,m) &= 1, \\
R_t(m-2,m) &= \min\{t,m\}+1.
\end{aligned}$$

Proof: The case of $R_t(m,m)$ is trivial since $\mathrm{RM}(m,m)=\mathbb{F}_2^{2^m}$. For the next case, $\mathrm{RM}(m-1,m)$ is the binary $[2^m,2^m-1,2]$ parity code. Its parity-check matrix is $H_1=(1,1,\dots,1)$. Then, by directly using Definition 3, we get that for all $t\in\mathbb{N}$, $R_t(m-1,m)=1$.

Finally, $\mathrm{RM}(m-2,m)$ is the binary $[2^m,2^m-m-1,4]$ extended Hamming code. A parity-check matrix for this code is the $(m+1)\times 2^m$ matrix H_2 containing all the binary column vectors that start with a 1. Let $\overline{e}_i$ denote the i-th standard unit column vector. We again use Definition 3 directly: for any $1\leqslant t\leqslant m$, we contend that the set $\{\overline{e}_2,\overline{e}_3,\dots,\overline{e}_{t+1}\}$ cannot be spanned by t columns of H_2. That is because $\langle\overline{e}_2,\dots,\overline{e}_{t+1}\rangle$ is a t-dimensional vector space, all of whose vectors contain a 0 in the first coordinate. However, the span of any t columns from H_2 is, at best, a t-dimensional vector space, but whose vectors' first coordinate is not always 0. Thus, $R_t(m-2,m)\geqslant t+1$. However, given any set of t column vectors of length $m+1$, $\{\overline{v}_1,\dots,\overline{v}_t\}$, the set is spanned by the $t+1$ vectors $\{\overline{v}'_1,\overline{v}'_2,\dots,\overline{v}'_t,\overline{e}_1\}$ where $\overline{v}'_i=\overline{v}_i$ if the first coordinate of $\overline{v}_i$ is 1 and $\overline{v}'_i=\overline{v}_i+\overline{e}_1$ otherwise. Clearly, $\{\overline{v}'_1,\overline{v}'_2,\dots,\overline{v}'_t,\overline{e}_1\}$ are all columns of H, and therefore, $R_t(m-2,m)\leqslant t+1$. Combining the two bounds we get that $R_t(m-2,m)=t+1$, for all $t\leqslant m$. Finally, for $t>m$ the claim is trivial since $\mathrm{rank}(H_2)=m+1$, and any set of column vectors of length $m+1$ can be spanned by $m+1$ linearly independent columns of H_2. ■

Turning to the more general case of $\mathrm{RM}(m-s,m)$, we first prove a technical lemma. The proof of this lemma is primarily based on the estimation of binomial coefficients by Stirling's approximation.

[1] Recall that $\mathrm{RM}(r,m)_t$ is the code over $\mathbb{F}_{2^t}$ that is generated by the generating matrix of $\mathrm{RM}(r,m)$ (see Definition 4).

Lemma 14: Let $t \in \mathbb{N}$ be a constant, and $r = o\left(2^m\right)$. Then

$$\log_{2^t}\left(V_{2^t,2^m,r}\right) = \frac{mr}{t} - O(r\log(r)).$$

Proof: Since $r = o\left(2^m\right)$, for sufficiently large m we have that $r < 2^{m-1}$, and therefore

$$\binom{2^m}{i}(2^t-1)^i \leqslant \binom{2^m}{i+1}(2^t-1)^{i+1},$$

for all $0 \leqslant i \leqslant r$. It follows that

$$\begin{aligned}\binom{2^m}{r}2^{r(t-1)} &\leqslant V_{2^t,2^m,r} \qquad (14)\\ &= \sum_{i=0}^{r}\binom{2^m}{i}(2^t-1)^i \leqslant (r+1)\binom{2^m}{r}2^{rt}.\end{aligned}$$

By Stirling's approximation (e.g., see [11, p. 251]),

$$\left(\frac{2^m}{r}\right)^r \leqslant \binom{2^m}{r} \leqslant \left(e\frac{2^m}{r}\right)^r.$$

Applying $\log_{2^t}$ and simplifying we obtain,

$$\frac{mr}{t} - r\log_{2^t}(r) \leqslant \log_{2^t}\binom{2^m}{r} \leqslant \frac{mr}{t} - r\log_{2^t}\left(\frac{r}{e}\right). \qquad (15)$$

Combining (14) and (15) we have

$$\begin{aligned}\log_{2^t}\left(V_{2^t,2^m,r}\right) &\leqslant \log_{2^t}\left((r+1)\binom{2^m}{r}2^{rt}\right)\\ &\leqslant \log_{2^t}(r+1) + \frac{mr}{t} - r\log_{2^t}\left(\frac{r}{e}\right) + r\\ &= \frac{mr}{t} - O(r\log(r)).\end{aligned}$$

Similarly,

$$\begin{aligned}\log_{2^t}\left(V_{2^t,2^m,r}\right) &\geqslant \log_{2^t}\left(\binom{2^m}{r}2^{r(t-1)}\right)\\ &\geqslant \frac{mr}{t} - r\log_{2^t}(r) + \frac{r(t-1)}{t}\\ &= \frac{mr}{t} - O(r\log(r)).\end{aligned}$$

■

We can now state the main bounds for this asymptotic regime.

Theorem 15: For all $m, t \in \mathbb{N}$, $3 \leqslant s \leqslant m$,

$$\begin{aligned}&\frac{t}{(s-1)!}m^{s-2} + O(m^{s-3}\log(m))\\ &\qquad\leqslant R_t(m-s,m)\\ &\qquad\leqslant \frac{t}{(s-2)!}m^{s-2} + O(m^{s-3}),\end{aligned}$$

where we consider s and t to be constants.

Proof: In [7, Section 3] it is proved for the (first) covering radius that

$$R_1(m-s,m) \leqslant \frac{m^{s-2}}{(s-2)!} + O(m^{s-3}).$$

Combining this with Lemma 6, the upper bound follows immediately.

Having proven the upper bound, we see that $R_t(m-s,m) = o(2^m)$. Thus, by Lemma 14,

$$\begin{aligned}\log_{2_t}\left(V_{2^t,2^m,R_t(m-s,m)}\right) = &\frac{mR_t(m-s,m)}{t}\\ &- O(m^{s-2}\log(m)).\end{aligned}$$

Combining this with the ball-covering argument from Lemma 7 and (10), it follows that

$$\begin{aligned}&\frac{mR_t(m-s,m)}{t} - O(m^{s-2}\log(m))\\ &\quad= \log_{2_t}\left(V_{2^t,2^m,R_t(m-s,m)}\right)\\ &\quad\geqslant 2^m - \dim\left(\mathrm{RM}(m-s,m)\right)\\ &\quad= \dim\left(\mathrm{RM}(s-1,m)\right) = \sum_{i=0}^{s-1}\binom{m}{i}\\ &\quad\geqslant \binom{m}{s-1} \geqslant \frac{m^{s-1}}{(s-1)!} - O(m^{s-2}).\end{aligned}$$

After rearranging we get the claim. ■

We note that the ratio between the upper and lower bounds from Theorem 15 tends to $s-1$ when m tends to infinity. In particular, this implies that for fixed s, $R_t(m-s,m) = \Theta(m^{s-2})$.

C. The Case Where r/m Is Constant

The next asymptotic regime we study is when $r/m = \alpha$ is constant. For technical reasons, we divide the discussion into two different cases: $\frac{1}{2} < \alpha < 1$, and $0 < \alpha < \frac{1}{2}$. We begin with the range $\frac{1}{2} < \alpha < 1$.

Theorem 16: For all $m, t \in \mathbb{N}$ and $\frac{1}{2} < \alpha < 1$,

$$\begin{aligned}&t\cdot\sqrt{\frac{1-\alpha}{8(\alpha m)^3}}\cdot 2^{mH_2(\alpha)}\cdot(1+o(1))\\ &\qquad\leqslant R_t(\alpha m, m)\\ &\qquad\leqslant t\cdot 4^{H_2(\alpha)}\cdot 2^{mH_2(\alpha)}\cdot(1+o(1)),\end{aligned}$$

where we consider t and α to be constants.

Proof: In [6, Theorem 9.4.25] it is proved that for $\frac{1}{2} < \alpha < 1$, the (first) covering radius satisfies

$$R_1(\alpha m, m) \leqslant 4^{H_2(\alpha)}\cdot 2^{mH_2(\alpha)}\cdot(1+o(1)).$$

By applying the subadditivity property from Lemma 6 we immediately obtain the claimed upper bound.

For the lower bound, as in the proof of Theorem 15,

$$\begin{aligned}&\log_{2^t}\left(V_{2^t,2^m,R_t(\alpha m,m)}\right)\\ &\quad\geqslant \dim\left(\mathrm{RM}((1-\alpha)m-1,m)\right) = \sum_{i=0}^{(1-\alpha)m-1}\binom{m}{i}\\ &\quad\geqslant \binom{m}{(1-\alpha)m-1} = \frac{(1-\alpha)m}{\alpha m+1}\binom{m}{(1-\alpha)m}\\ &\quad= \frac{1-\alpha}{\alpha}\binom{m}{(1-\alpha)m}(1+o(1))\\ &\quad\geqslant \sqrt{\frac{1-\alpha}{8m\alpha^3}}\cdot 2^{mH_2(\alpha)}\cdot(1+o(1)),\end{aligned}$$

where the last inequality follows from (6). By the upper bound presented above, $R_t(\alpha m, m) = o(2^m)$, and Lemma 14 may be applied to obtain

$$\begin{aligned}\frac{mR_t(\alpha m,m)}{t}(1+o(1)) &= \log_{2^t}(V_{2^t,2^m,R_t(\alpha m,m)}) \\ &\geqslant \sqrt{\frac{1-\alpha}{8m\alpha^3}}\cdot 2^{mH_2(\alpha)}\cdot(1+o(1)).\end{aligned}$$

By rearranging we obtain the desired lower bound. ■

The upper bound and the lower bound from Theorem 16 differ from one another by a factor of $\Theta(m^{2/3})$, and therefore the ratio between them tends to infinity. Despite that, much of the asymptotic behavior is revealed, as it shows that the t-covering radius in this case is $2^{m(H_2(\alpha)+o(1))}$. In particular, the relative t-covering radius with respect to the length of the code vanishes as $m \to \infty$.

We now move on to the range $0 < \alpha < \frac{1}{2}$. We begin with two lemmas, laying the groundwork for the bounds. The first lemma is a weaker, more general version of an upper bound on $R_t(r,m)$.

Lemma 17: For all $m,t \in \mathbb{N}$, $1 \leqslant r \leqslant m$,

$$R_t(r,m) \leqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}\binom{m}{r}.$$

Proof: We prove the claim by induction on m. We first observe that the claim holds in the extreme cases where $r = 1$ and $r = m$. Since $2^{m/2} \geqslant m = \binom{m}{1}$ for any $m \in \mathbb{N}$, by Lemma 10 we have

$$\begin{aligned}R_t(1,m) &\leqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}2^{\frac{m}{2}} \\ &\leqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}\binom{m}{1}.\end{aligned}$$

In the case where $r = m$, $\mathrm{RM}(m,m) = \mathbb{F}_2^{2^m}$, and thus $R_t(m,m) = 0$ and the claim holds. In particular, this proves the claim for $m = 1, 2$, serving as the induction base.

Assume the claim holds for $m-1$, and we now prove it holds for m. We already know the claim holds for $R_t(1,m)$ and $R_t(m,m)$. Thus, we only need to show it holds for $2 \leqslant r \leqslant m-1$. By Proposition 8 and the induction hypothesis,

$$\begin{aligned}R_t(r,m) &\leqslant R_t(r-1,m-1) + R_t(r,m-1) \\ &\leqslant \left(1-\frac{1}{2^t}\right)2^{m-1} - \frac{\sqrt{2^t-1}}{2^t}\binom{m-1}{r-1} \\ &\quad + \left(1-\frac{1}{2^t}\right)2^{m-1} - \frac{\sqrt{2^t-1}}{2^t}\binom{m-1}{r} \\ &= \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}\binom{m}{r},\end{aligned}$$

thus completing the induction step. ■

The next technical lemma proves the limit of $R_t(\alpha m,m)/2^m$.

Lemma 18: Let $0 < \alpha < \frac{1}{2}$ be a constant. Then

$$\lim_{m\to\infty}\frac{R_t(\alpha m,m)}{2^m} = 1-\frac{1}{2^t}.$$

Proof: Using Lemma 7 and (7), we have

$$\begin{aligned}\log_{2^t}\left(V_{2^t,2^m,R_t(\alpha m,m)}\right) &\geqslant 2^m - \sum_{i=0}^{\alpha m}\binom{m}{i} \qquad (16)\\ &\geqslant 2^m - 2^{mH_2(\alpha)} \\ &= 2^m\left(1-2^{-m(1-H_2(\alpha))}\right).\end{aligned}$$

Assume to the contrary that $R_t(\alpha m,m) \leqslant \mu 2^m$ for some $\mu < 1-\frac{1}{2^t}$ and infinitely many values of m. In that case, by (16) and (7),

$$\begin{aligned}H_{2^t}(\mu)2^m &\geqslant \log_{2^t}\left(V_{2^t,2^m,R_t(r,m)}\right) \\ &\geqslant 2^m\left(1-2^{-m(1-H_2(\alpha))}\right).\end{aligned}$$

That is,

$$H_{2^t}(\mu) \geqslant 1-2^{-m(1-H_2(\alpha))}.$$

Since $\alpha < \frac{1}{2}$, we have $H_2(\alpha) < 1$, and therefore taking $m \to \infty$ we get $H_{2^t}(\mu) \geqslant 1$. That is a contradiction as $\mu < 1-\frac{1}{2^t}$. This proves that

$$\liminf_{m\to\infty}\frac{R_t(\alpha m,m)}{2^m} \geqslant 1-\frac{1}{2^t}.$$

From the upper bound presented in Lemma 17 we have

$$\limsup_{m\to\infty}\frac{R_t(\alpha m,m)}{2^m} \leqslant 1-\frac{1}{2^t}.$$

Combining these two inequalities we have claim. ■

Using the previous two lemmas, we can now state the bound on $R_t(\alpha m,m)$.

Theorem 19: For all $m,t \in \mathbb{N}$, and $0 < \alpha < \frac{1}{2}$,

$$\begin{aligned}&\left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2t(2^t-1)\ln 2}}{2^t}\cdot 2^{\frac{m}{2}(1+H_2(\alpha))}\cdot(1+o(1)) \\ &\leqslant R_t(\alpha m,m) \\ &\leqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}\cdot\frac{1}{\sqrt{8m\alpha(1-\alpha)}}\cdot 2^{mH_2(\alpha)},\end{aligned}$$

where t and α are constants.

Proof: The upper bound follows immediately from (6) and Lemma 17. We turn to prove the lower bound. By Lemma 7 and (7) again,

$$\begin{aligned}2^m H_{2^t}\left(\frac{R_t(\alpha m,m)}{2^m}\right) &\geqslant \log_{2^t}\left(V_{2^t,m,R_t(\alpha m,m)}\right) \qquad (17)\\ &\geqslant 2^m - 2^{mH_2(\alpha)}.\end{aligned}$$

Since Lemma 17 implies $R_t(\alpha m,m) < \left(1-\frac{1}{2^t}\right)2^m$, we denote $y \triangleq 1-1/2^t - R_t(\alpha m,m)/2^m > 0$. By Lemma 18, $y = o(1)$. In a similar fashion to the proof of Theorem 12, by (5) we have

$$H_{2^t}\left(\frac{R_t(\alpha m,m)}{2^m}\right) = 1-cy^2(1+o(1)),$$

where $c = \frac{2^{2t}}{2t(2^t-1)\ln 2}$. Substituting this back into (17) we get

$$1-cy^2(1+o(1)) \geqslant 1-2^{m(H_2(\alpha)-1)},$$

and therefore,

$$y \leqslant c^{-\frac{1}{2}} 2^{\frac{m}{2}(H_2(\alpha)-1)}(1+o(1)).$$

Since $R_t(\alpha m, m) = (1 - 1/2^t - y)2^m$, we reach the claimed lower bound. ■

In the region $0 < \alpha \leqslant 1 - \frac{1}{\sqrt{2}}$, we follow a similar procedure to that of [7], in order to improve the upper bound of Theorem 19. The following lemma is a sharpening of Lemma 17, requiring more involved work.

Lemma 20: For all $m, t \in \mathbb{N}$, $2 \leqslant r \leqslant \frac{m}{2+\sqrt{2}}$, and $m \geqslant 3$,

$$\begin{aligned} R_t(r,m) \leqslant{} & \left(1 - \frac{1}{2^t}\right) 2^m - \frac{\sqrt{2^t-1}}{2^t}\left(1+\sqrt{2}\right)^{r-1} 2^{\frac{m-1}{2}} \\ & + \frac{\sqrt{2^t-1}}{2^t\sqrt[4]{2}} r \binom{m}{r}. \end{aligned}$$

Proof: Like the proof of Lemma 17, we proceed by induction on m. Throughout this proof we denote the constant $\frac{\sqrt{2^t-1}}{2^t}$ by c. As base cases we shall consider both the case of $m = \lceil (2+\sqrt{2})r \rceil$ and $r \geqslant 2$, as well as the case of $r = 2$ for all m.

Assume that $m = \lceil (2+\sqrt{2})r \rceil$ and $r \geqslant 2$. We first observe that

$$H_2\left(\frac{1}{2+\sqrt{2}}\right) = \frac{1}{2} + \frac{1}{2+\sqrt{2}} \log_2\left(1+\sqrt{2}\right). \tag{18}$$

Additionally, by simply monotonicity, as well as (6) and the comment following it,

$$\begin{aligned} \binom{m}{r} &= \binom{\lceil r\left(2+\sqrt{2}\right)\rceil}{r} \\ &\geqslant \binom{r\left(2+\sqrt{2}\right)}{r} \geqslant \frac{\sqrt[4]{2}}{\sqrt{8r}} 2^{r(2+\sqrt{2})H_2\left(\frac{1}{2+\sqrt{2}}\right)}. \end{aligned} \tag{19}$$

We now have the following sequence of inequalities proving the first base case,

$$\begin{aligned} R_t(r,m) &\overset{(a)}{\leqslant} \left(1 - \frac{1}{2^t}\right) 2^m \\ &\overset{(b)}{\leqslant} \left(1 - \frac{1}{2^t}\right) 2^m \\ &\quad - c\left(\frac{1}{1+\sqrt{2}} - \frac{\sqrt{r}}{\sqrt{8}}\right) 2^{r\log_2(1+\sqrt{2}) + \frac{r}{2}(2+\sqrt{2})} \\ &\overset{(c)}{=} \left(1 - \frac{1}{2^t}\right) 2^m - \frac{c}{1+\sqrt{2}}(1+\sqrt{2})^r 2^{\frac{r}{2}(2+\sqrt{2})} \\ &\quad + \frac{cr}{\sqrt{8r}} 2^{r(2+\sqrt{2})H_2\left(\frac{1}{2+\sqrt{2}}\right)} \\ &\overset{(d)}{\leqslant} \left(1 - \frac{1}{2^t}\right) 2^m - c(1+\sqrt{2})^{r-1} 2^{\frac{m-1}{2}} + \frac{cr}{\sqrt[4]{2}}\binom{m}{r}, \end{aligned}$$

where (a) follows from Lemma 17, (b) follows since for all $r \geqslant 2$ we have $\frac{1}{1+\sqrt{2}} \leqslant \frac{\sqrt{r}}{\sqrt{8}}$, (c) follows from (18), and (d) follows since $m = \lceil (2+\sqrt{2})r \rceil$ as well as by (19).

We now check that the claim holds for the second base case, where $r = 2$. We observe that,

$$\begin{aligned} R_t(2,m) &\overset{(a)}{\leqslant} \sum_{i=2}^{m-1} R_t(1,i) \\ &\overset{(b)}{\leqslant} \left(1 - \frac{1}{2^t}\right)\left(\sum_{i=2}^{m-1} 2^i\right) - c\sum_{i=2}^{m-1}(\sqrt{2})^i \\ &\leqslant \left(1 - \frac{1}{2^t}\right) 2^m - c\sum_{i=2}^{m-1}(\sqrt{2})^i \\ &= \left(1 - \frac{1}{2^t}\right) 2^m - c\left((1+\sqrt{2})2^{\frac{m}{2}} - \frac{2}{\sqrt{2}-1}\right), \end{aligned}$$

where (a) follows by repeated application of Proposition 8 and the fact that $R_t(2,2) = 0$, and (b) follows from Lemma 10. We note that the base case is proved when

$$(1+\sqrt{2})2^{\frac{m}{2}} - \frac{2}{\sqrt{2}-1} \geqslant (1+\sqrt{2})2^{\frac{m-1}{2}} - \frac{1}{\sqrt[4]{2}} \cdot 2 \cdot \binom{m}{2}, \tag{20}$$

is satisfied. Indeed, one can easily check that (20) holds for all $m \geqslant \lceil (2+\sqrt{2})2 \rceil = 7$.

Having completed the induction base cases, assume the claim holds for $m-1$, i.e., for all $2 \leqslant r \leqslant \frac{m-1}{2+\sqrt{2}}$. We shall now prove the claim also holds for m, and all $2 \leqslant r \leqslant \frac{m}{2+\sqrt{2}}$. The two extreme cases, i.e., $r = 2$, and $m = \lceil (2+\sqrt{2})r \rceil$, have already been proved in the base cases. For the remaining values of r,

$$\begin{aligned} & R_t(r,m) \\ &\leqslant R_t(r-1,m-1) + R_t(r,m-1) \\ &\leqslant \left(1 - \frac{1}{2^t}\right) 2^{m-1} - c(1+\sqrt{2})^{r-2} 2^{\frac{m-2}{2}} \\ &\quad + \frac{c}{\sqrt[4]{2}}(r-1)\binom{m-1}{r-1} + \left(1 - \frac{1}{2^t}\right) 2^{m-1} \\ &\quad - c(1+\sqrt{2})^{r-1} 2^{\frac{m-2}{2}} + \frac{c}{\sqrt[4]{2}} r\binom{m-1}{r} \\ &\leqslant \left(1 - \frac{1}{2^t}\right) 2^m - c(1+\sqrt{2})^{r-1}\left(1 + \frac{1}{1+\sqrt{2}}\right) 2^{\frac{m-2}{2}} \\ &\quad + \frac{cr}{\sqrt[4]{2}}\left(\binom{m-1}{r} + \binom{m-1}{r-1}\right) \\ &= \left(1 - \frac{1}{2^t}\right) 2^m - c(1+\sqrt{2})^{r-1} 2^{\frac{m-1}{2}} + \frac{cr}{\sqrt[4]{2}}\binom{m}{r}, \end{aligned}$$

where the first inequality follows from Proposition 8, and then we use the induction hypothesis. ■

Theorem 21: For all $m, t \in \mathbb{N}$, and $0 < \alpha < 1 - \frac{1}{\sqrt{2}}$,

$$\begin{aligned} R_t(\alpha m, m) \leqslant{} & \left(1 - \frac{1}{2^t}\right) 2^m \\ & - \frac{\sqrt{2^t-1}}{2^t(2+\sqrt{2})} 2^{m\left(\frac{1}{2} + \alpha\log_2(1+\sqrt{2})\right)}(1+o(1)), \end{aligned}$$

where t and α are constants.

Proof: By Lemma 20,

$$\begin{aligned}
&R_t(\alpha m, m)\\
&\quad\leqslant \left(1-\frac{1}{2^t}\right)2^m\\
&\qquad - \frac{\sqrt{2^t-1}}{2^t}\left((1+\sqrt{2})^{\alpha m-1}2^{\frac{m-1}{2}} - \frac{\alpha m}{\sqrt[4]{2}}\binom{m}{\alpha m}\right)\\
&\quad= \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t(2+\sqrt{2})}2^{m\left(\frac{1}{2}+\alpha\log_2(1+\sqrt{2})\right)}\\
&\qquad + 2^{m(H_2(\alpha)+o(1))}\\
&\quad= \left(1-\frac{1}{2^t}\right)2^m\\
&\qquad - \frac{\sqrt{2^t-1}}{2^t(2+\sqrt{2})}2^{m\left(\frac{1}{2}+\alpha\log_2(1+\sqrt{2})\right)}(1+o(1)),
\end{aligned}$$

where we made use of (6), and the fact that

$$\frac{1}{2}+\alpha\log_2(1+\sqrt{2}) > H_2(\alpha).$$

■

The bounds from Theorem 19 and Theorem 21 show that for $0<\alpha<\frac{1}{2}$, the t covering radius of $\mathrm{RM}(\alpha m, m)$ is smaller than $\left(1-\frac{1}{2^t}\right)2^m$ by a number which is exponential in m. However, due to the gap between our lower and upper bounds, the dependency of that exponential term in α can only be bounded. The bound from Theorem 19 provides a bound for this exponential term for all $0<\alpha<\frac{1}{2}$:

$$\begin{aligned}
2^{m(H_2(\alpha)+o(1))} &\leqslant \left(1-\frac{1}{2^t}\right)2^m - R_t(\alpha m, m)\\
&\leqslant 2^{m\left(\frac{1}{2}+\frac{1}{2}H_2(\alpha)+o(1)\right)}.
\end{aligned}$$

In Theorem 21 we improve the upper bound for $0<\alpha<1-\frac{1}{\sqrt{2}}$ by proving that

$$2^{m\left(\frac{1}{2}+\alpha\log_2(1+\sqrt{2})+o(1)\right)} \leqslant \left(1-\frac{1}{2^t}\right)2^m - R_t(\alpha m, m).$$

In Figure 1, a comparison between the functions defining the exponential term obtained in our bounds is presented. We observe that in the point $\alpha = 1-\frac{1}{\sqrt{2}}$, we have $\frac{1}{2}+\alpha\log_2(1+\sqrt{2}) = H_2(\alpha)$ and the exponential coefficients in our bounds meet, namely,

$$\begin{aligned}
R_t(\alpha m, m) &\leqslant \left(1-\frac{1}{2^t}\right)2^m - 2^{m\left(\frac{1}{2}\alpha\log_2(1+\sqrt{2})+o(1)\right)}\\
&= \left(1-\frac{1}{2^t}\right)2^m - 2^{m(H_2(\alpha)+o(1))}.
\end{aligned}$$

D. The Case Where $r=\frac{m}{2}+\Theta(\sqrt{m})$

We observe that whenever $r=\frac{m}{2}$, the rate of $\mathrm{RM}(r,m)$ is exactly $\frac{1}{2}$. Being able to track the dependence of the generalized covering radius on the rate of the code is very interesting, especially since the case of constant rate is perhaps the most important regime for communications. Therefore, we now focus on the case where the code rate is constant, i.e., $r=\frac{m}{2}+\Theta(\sqrt{m})$.

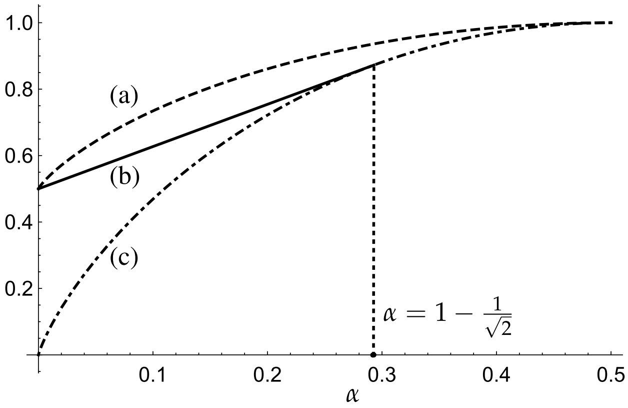

Fig. 1. A comparison of the exponential term in the bounds from Theorem 19 and Theorem 21: (a) $=\frac{1}{2}+\frac{1}{2}H_2(\alpha)$, (b) $=\frac{1}{2}+\alpha\log_2(1+\sqrt{2})$, and (c) $=H_2(\alpha)$.

Lemma 22: Let $0<\kappa<1$ be a constant. Let r be an integer such that $\sum_{i=0}^{r}\binom{m}{i}=\kappa 2^m$. Then

$$R_t(r,m) \geqslant H_{2^t}^{-1}(1-\kappa)\,2^m.$$

Proof: Using Lemma 7, we have

$$\log_{2^t}\left(V_{2^t,2^m,R_t(r,m)}\right) \geqslant 2^m - \sum_{i=0}^{r}\binom{m}{i} = 2^m(1-\kappa). \tag{21}$$

Assume to the contrary that $R_t(r,m)\leqslant \mu 2^m$ for some $\mu < H_{2^t}^{-1}(1-\kappa)$ and some m. In that case, by (21) and (7),

$$\begin{aligned}
(1-\kappa)2^m > H_{2^t}(\mu)2^m &\geqslant \log_{2^t}\left(V_{2^t,2^m,R_t(r,m)}\right)\\
&\geqslant (1-\kappa)\,2^m,
\end{aligned}$$

which is a contradiction. ■

For an upper bound, we use an asymptotic approximation of the near central binomial coefficients, given in the following lemma:

Lemma 23: [27, Chapter 5.4] For any sequence of integers $(k_m)_m$ such that $\left|\frac{m}{2}-k_m\right| = o(m^{2/3})$,

$$\binom{m}{k_m} = \frac{2^m}{\sqrt{\frac{1}{2}m\pi}}e^{-\frac{(m-2k_m)^2}{2m}}(1+o(1)).$$

Theorem 24: Let $0<\kappa<1$ be a constant. Let r be an integer such that $\sum_{i=0}^{r}\binom{m}{i}=\kappa 2^m$. Then

$$\begin{aligned}
&H_{2^t}^{-1}(1-\kappa)\,2^m\\
&\quad\leqslant R_t(r,m)\\
&\quad\leqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}\frac{2^m}{\sqrt{\frac{1}{2}m\pi}}e^{-\frac{(m-2r)^2}{2m}}(1+o(1)).
\end{aligned}$$

Proof: The lower bound follows directly from Lemma 22. The upper bound follows from Lemma 17 and Lemma 23, as $|m-2r| = \Theta(\sqrt{m}) = o(m^{2/3})$. ■

We observe that in this case, the ratio between the lower and upper bounds from Theorem 24 does not tend to 1 as $m\to\infty$. However, our bounds show that in the case of constant rate, the t-covering radius is in some linear dependency with the

TABLE I
A SUMMARY OF EXACT VALUES

$R_t(0,m)$	$2^m - \lceil 2^{m-t} \rceil$	Proposition 9
$R_t(m-2,m)$	$\min\{t,m\}+1$	Proposition 13
$R_t(m-1,m)$	1	Proposition 13
$R_t(m,m)$	0	Proposition 13

length of the code. That is, for any sequence $(r_m)_m$ such that $\sum_{i=0}^{r_m}\binom{m}{i} = \kappa 2^m$,

$$H_{2^t}^{-1}(1-\kappa) \leqslant \liminf_{m\to\infty} \frac{R_t(r_m,m)}{2^m} \leqslant \limsup_{m\to\infty} \frac{R_t(r_m,m)}{2^m} \leqslant 1-\frac{1}{2^t}. \tag{22}$$

It remains unclear whether the limit always exists, and if it does, what is its value. We would like to remark that even in the case where $t=1$ and $r=\frac{m}{2}$, an answer to that intriguing question is still unknown. As similarly to our case, the best known lower and upper bounds (presented in [7]) exhibit an asymptotic gap between them:

$$H_2\left(\frac{1}{2}\right) \leqslant \liminf_{m\to\infty} \frac{R_1(m/2,m)}{2^m} \leqslant \frac{1}{4}.$$

Compared with (22), the upper bound above reduces from $\frac{1}{2}$ to $\frac{1}{4}$.

IV. Application of the Bounds to General Codes

In this section, we show our upper bounds on the covering radii of Reed-Muller codes may also be used for the study of the asymptotic behaviour of generalized covering radii of linear codes in general. Given the parameters $t \in \mathbb{N}$, $\rho \in [0,1]$ and a prime power q, the asymptotic minimal rate of a code over $\mathbb{F}_q$ with a normalized t-th generalized covering radius of no more than ρ, is denoted by $\kappa_t(\rho,q)$. Since the t-th generalized covering radius of a direct sum of codes is the sum of the t-th generalized covering radii of its component codes (see [10, Prop. 25]), an $[n,k]_q$ linear code with t-th generalized covering radius of r immediately creates an infinite family of codes with rate $\frac{k}{n}$ and normalized t-th generalized covering radius $\frac{r}{n}$. It then follows that $\kappa_t(r/n,q) \leqslant k/n$. By the monotonicity of $\kappa_t(\rho,q)$ in ρ, this upper bound holds for all $\rho \geqslant r/n$. Thus, our upper bounds on the generalized covering radii of Reed-Muller codes (denoted by $U_t(r,m)$) give the following upper bounds:

$$\kappa_t(\rho,2) \leqslant \frac{\dim(\mathrm{RM}(r,m))}{2^m} \text{ for all } \rho \geqslant \frac{U_t(r,m)}{2^m} \tag{23}$$

In Figure 2, we present the bound obtained by applying (23) in the range $2 \leqslant m \leqslant 20$, $1 \leqslant r \leqslant m$, in the case where $t=3$. Each pair (r,m), results in a point depicted in the graph. We observe that some of the points obtained in this way improve upon the upper bound in [10, Prop. 14], which is derived from the subadditive property, i.e.,

$$\kappa_t(\rho,q) \leqslant 1 - H_q\left(\frac{\rho}{t}\right), \tag{24}$$

where $H_q(\cdot)$ is the q-ary entropy function.

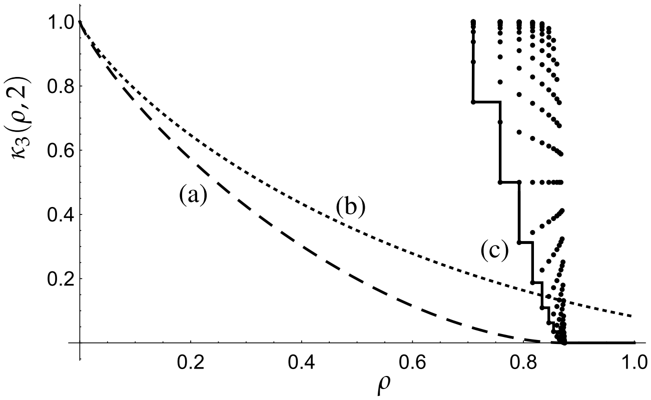

Fig. 2. A comparison of the bounds on $\kappa_3(\rho,2)$: (a) the ball-covering lower bound [10, Prop. 12], (b) the general upper bound [10, Prop. 14], and (c) our upper bound obtained from the upper bound on the t-th generalized covering radius of Reed-Muller codes.

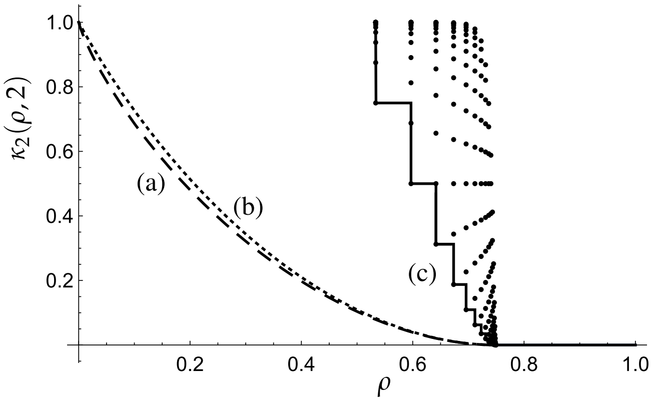

Fig. 3. A comparison of the bounds on $\kappa_2(\rho,2)$: (a) the ball-covering lower bound [10, Prop. 12], (b) the improved upper bound [10, Thm. 22], and (c) our upper bound obtained from the upper bound on the t-th generalized covering radius of Reed-Muller codes.

We remark that the upper bound of (24) may be improved using our result for general $t \geqslant 2$. Fixing some finite r, we consider the sequence of codes $(\mathrm{RM}(r,m))_{m=1}^{\infty}$. The rates of these codes obviously vanishes to 0 as $m \to \infty$. On the other hand, from Theorem 11,

$$\lim_{m\to\infty} \frac{U_t(r,m)}{2^m} = 1 - \frac{1}{2^t}.$$

Thus, the bounds obtained by applying (23) to $\mathrm{RM}(r,m)_m$ provides that

$$\kappa_t(\rho) = 0 \text{ for all } \rho > 1-2^t.$$

That is an improvement upon (24), as $H_2\left(\frac{\rho}{t}\right) > 0$ for all $1-\frac{1}{2^t} \leqslant \rho \leqslant 1$ and $t \geqslant 2$.

A similar comparison, with $t=2$, is shown in Figure 3. Note that the upper bound of [10, Theorem 22], which is tailored for $t=2$ and is derived by using the probabilistic method, is stronger than (24), and so the bound of (23) offers no improvement.

V. Covering Algorithm

In this section we describe an algorithm which receives as input a matrix $\mathbf{v} \in \mathbb{F}_2^{t\times 2^m}$, and returns a codeword matrix[2]

[2] Recall that $\mathrm{RM}(r,m)^t$ is the code in $\mathbb{F}_2^{t\times n}$ comprising of all the matrices whose rows belong in $\mathrm{RM}(r,m)$ (see Definition 2).

TABLE II

A SUMMARY OF THE BOUNDS

$R_t(r,m)$	$\leqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}(1+\sqrt{2})^{r-1}2^{m/2} + O(m^{r-2})$	Theorem 11
	$\geqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2t(2^t-1)\ln 2}}{2^t\sqrt{r!}}m^{r/2}2^{m/2}(1+o(1))$	Theorem 12
$R_t(m-s,m)$	$\leqslant \frac{t}{(s-2)!}m^{s-2} + O(m^{s-3})$	Theorem 15
	$\geqslant \frac{t}{(s-1)!}m^{s-2} + O(m^{s-3}\log(m))$	
$R_t(\alpha m,m)$	$\leqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t(2+\sqrt{2})}2^{m\left(\frac{1}{2}+\alpha\log_2(1+\sqrt{2})\right)}(1+o(1))$	Theorem 21, assuming $0<\alpha<1-\frac{1}{\sqrt{2}}$
	$\leqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}\cdot\frac{1}{\sqrt{8m\alpha(1-\alpha)}}\cdot 2^{mH_2(\alpha)}$	Theorem 19, assuming $1-\frac{1}{\sqrt{2}}\leqslant\alpha<\frac{1}{2}$
	$\leqslant t\cdot 4^{H_2(\alpha)}\cdot 2^{mH_2(\alpha)}\cdot(1+o(1))$	Theorem 16, assuming $\frac{1}{2}<\alpha<1$
	$\geqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2t(2^t-1)\ln 2}}{2^t}\cdot 2^{\frac{m}{2}(1+H_2(\alpha))}\cdot(1+o(1))$	Theorem 19, assuming $0<\alpha<\frac{1}{2}$
	$\geqslant t\cdot\sqrt{\frac{1-\alpha}{8(\alpha m)^3}}\cdot 2^{mH_2(\alpha)}\cdot(1+o(1))$	Theorem 16, assuming $\frac{1}{2}<\alpha<1$
$R_t(r,m)$	$\leqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t}\frac{2^m}{\sqrt{\frac{1}{2}m\pi}}e^{-\frac{(m-2r)^2}{2m}}(1+o(1))$	Theorem 24, assuming $\sum_{i=0}^{r}\binom{m}{i}=\kappa 2^m$
	$\geqslant H_{2^t}^{-1}(1-\kappa)2^m(1+o(1))$	

$\mathbf{c}\in\mathrm{RM}(r,m)^t$ that is no farther away from $\mathbf{v}$ than the upper bounds described in the previous section, namely

$$d^{(t)}(\mathbf{v},\mathbf{c})\leqslant U_t(r,m),$$

where $U_t(r,m)$ is any upper bound on $R_t(r,m)$ from Table II. We call this a *covering algorithm*, and it may be thought of as the analogue to a decoding algorithm for an error-correcting code.

To motivate our study of a covering algorithm, we recall the motivating example described in [10]. We look at linear data querying schemes, the most prominent example of which is private information retrieval (PIR), in which the user queries a database by linear combinations. We think of the database as a sequence of elements $\overline{x}=(x_1,\dots,x_m)\in\mathbb{F}_{q^\ell}^m$. The user may query the contents of the database by providing $\overline{s}=(s_1,\dots,s_m)\in\mathbb{F}_q^m$, and getting in response the linear combination $\overline{s}\cdot\overline{x}=\sum_{i=1}^m s_ix_i$. The access complexity in such protocols is the number of database items that need to be read in order to compute the desired linear combination. In a straightforward implementation, the access complexity is the number of non-zero coefficients in $s_1,\dots,s_m$. Thus, in a typical PIR scheme, which selects random coefficients, the expected fraction of non-zero coefficients is $1-\frac{1}{q}$, resulting in a prohibitively high access complexity.

In order to reduce the access complexity one may pre-compute and store some linear combinations of data elements. If the original database is $\overline{x}=(x_1,\dots,x_m)\in\mathbb{F}_{q^\ell}^m$, the linear combinations $\overline{h}_1\cdot\overline{x},\overline{h}_2\cdot\overline{x},\dots,\overline{h}_n\cdot\overline{x}$ are pre-computed and stored instead of the original database $\overline{x}$, where $\overline{h}_1,\dots,\overline{h}_n\in\mathbb{F}_q^m$. Assume now that the database receives a query given by $\overline{s}\in\mathbb{F}_q^m$. If we can find $r\leqslant m$ vectors $\overline{h}_{i_1},\dots,\overline{h}_{i_r}$ such that $\overline{s}\in\langle\overline{h}_{i_1},\dots,\overline{h}_{i_r}\rangle$, then we may answer the query by accessing the r pre-computed linear combinations $\overline{h}_{i_1}\cdot\overline{x},\dots,\overline{h}_{i_r}\cdot\overline{x}$, instead of accessing all the m elements in the database, $x_1,\dots,x_m$. Considering the vectors $\overline{h}_1,\dots,\overline{h}_n$ as the columns of a parity-check matrix H of an $[n,n-m]_q$ linear code C, Definition 3 guarantees that $r\leqslant R_1(C)$ such vectors may always be found. Thus, by storing the n pre-computed linear combinations instead of the original database, we increased the storage, but we reduced the access complexity since we need to access at most $R_1(C)$ elements of the database. As an additional step, assume the database does not answer queries individually, but instead groups together t queries given by $\overline{s}_1,\dots,\overline{s}_t\in\mathbb{F}_q^m$. We now need the r vectors $\overline{h}_{i_1},\dots,\overline{h}_{i_r}$ to satisfy $\overline{s}_1,\dots,\overline{s}_t\in\langle\overline{h}_{i_1},\dots,\overline{h}_{i_r}\rangle$ in order to answer the queries. By Definition 3, $r\leqslant R_t(C)$ such vectors exist, and by Lemma 6, $R_t(C)\leqslant tR_1(C)$. Thus, by delaying the answers to queries, namely, increasing the latency, we have further reduced the access complexity from $tR_1(C)$ (the access complexity of treating t queries individually) to $R_t(C)$.

We translate this problem into a more convenient form. Let us write the vectors $\overline{s}_1,\dots,\overline{s}_t$ as rows of a matrix $\mathbf{s}\in\mathbb{F}_q^{t\times m}$. Since the parity-check matrix of C is a full-rank matrix, $H\in\mathbb{F}_q^{m\times n}$, by solving a set of linear equations we can efficiently find a matrix $\mathbf{v}\in\mathbb{F}_q^{t\times n}$ such that $H\mathbf{v}^\intercal=\mathbf{s}^\intercal$. We would now like to solve the following task: Given $\mathbf{v}\in\mathbb{F}_q^{t\times n}$, find $\mathbf{c}\in C^t$ such that $d^{(t)}(\mathbf{v},\mathbf{c})\leqslant r$. We observe that by finding such $\mathbf{c}$, since $H(\mathbf{v}-\mathbf{c})^\intercal=\mathbf{s}^\intercal$, the rows of $\mathbf{v}-\mathbf{c}$ describe linear combinations of the columns of H that both result in $\overline{s}_1,\dots,\overline{s}_t$, and use no more than r columns. Ideally, we would like to choose $r=R_t(C)$.

We call such an algorithm a *t-covering algorithm for C, with radius r*. It bears a resemblance to a decoding algorithm for an error-correcting code, however some crucial differences are to be noted. To guarantee unique decoding, standard decoding algorithms assume the input is a point in the space that is no more than $\lfloor\frac{d-1}{2}\rfloor$ away from a codeword, where d is the

Algorithm 1 A t-Covering Algorithm for $\mathrm{RM}(r,m)$ With Radius $U_t(r,m)$

```
Function recursive(v, r)
    Input : $\mathbf{v}\in\mathbb{F}_2^{t\times 2^m}$, $r\in\mathbb{N}$, $1\leqslant r\leqslant m$
    // Check edge cases
    if $r=m$ then return $\mathbf{v}$
    if $r=1$ then return $\mathrm{argmin}_{\mathbf{c}\in\mathrm{RM}(1,m)^t}\, d^{(t)}(\mathbf{v},\mathbf{c})$
    // Use the $(u,u+v)$ recursion
    Let $\mathbf{v}_1,\mathbf{v}_2\in\mathbb{F}_2^{t\times 2^{m-1}}$ s.t. $\mathbf{v}=(\mathbf{v}_1,\mathbf{v}_2)$
    $\mathbf{c}_1\leftarrow$ recursive($\mathbf{v}_1, r$)
    $\mathbf{c}_2\leftarrow$ recursive($\mathbf{v}_2-\mathbf{c}_1, r-1$)
    return $(\mathbf{c}_1,\mathbf{c}_1+\mathbf{c}_2)$
Function subadditive(v, r)
    Input : $\mathbf{v}\in\mathbb{F}_2^{t\times 2^m}$, $r\in\mathbb{N}$, $1\leqslant r\leqslant m$
    // Use subadditivity
    Let $\overline{v}_i$ be the $i$-th row of $\mathbf{v}$
    forall the $i\in[t]$ do
        $\overline{c}_i\leftarrow$ recursive($\overline{v}_i, r$)
    return $(\overline{c}_1^{\mathsf{T}},\dots,\overline{c}_t^{\mathsf{T}})^{\mathsf{T}}$
Function cover(v, r)
    Input : $\mathbf{v}\in\mathbb{F}_2^{t\times 2^m}$, $r\in\mathbb{N}$, $1\leqslant r\leqslant m$
    $\mathbf{c}_{\min}\leftarrow$ recursive($\mathbf{v}, r$)
    $\mathbf{c}'_{\min}\leftarrow$ subadditive($\mathbf{v}, r$)
    return $\mathrm{argmin}_{\mathbf{c}\in\{\mathbf{c}_{\min},\mathbf{c}'_{\min}\}}\, d^{(t)}(\mathbf{v},\mathbf{c})$
```

minimum distance of the code. The covering algorithm may receive as input *any* point in the metric space. Additionally, the decoding algorithm returns the closest (and only) codeword within radius of $\lfloor\frac{d-1}{2}\rfloor$ from the input point. In contrast, the covering algorithm may return *any* codeword whose distance from the input as it most r, and not necessarily the closest codeword. Thus, the covering algorithm discussed here does not perform maximum-likelihood decoding.

As we saw in Section III, computing the generalized covering radii of Reed-Muller codes is a difficult task in general. Even for the case of $t=1$, and despite having been studied for decades, the covering radius of Reed-Muller codes is still not fully known. Thus, finding an efficient t-covering algorithm for $\mathrm{RM}(r,m)$, with radius $R_t(r,m)$, poses a great challenge, if only for the fact that $R_t(r,m)$ is unknown in general. An inefficient, brute-force implementation of such an algorithm is trivial, yet, uninteresting.

Instead, in what follows, we devise an efficient t-covering algorithm for $\mathrm{RM}(r,m)$, with radius $U_t(r,m)$, where $U_t(r,m)$ is any of the upper bounds on $R_t(r,m)$ found in this paper, and summarized in Table II. Our approach stems from the fact that all the bounds in Table II are derived recursively using the $(u,u+v)$ construction (Proposition 8) and subadditivity (Lemma 6), as well as simple base cases.

Theorem 25: For any $t,r,m\in\mathbb{N}$, $r\leqslant m$, and any $\mathbf{v}\in\mathbb{F}_2^{t\times 2^m}$, running $\mathbf{c}=\texttt{cover}(\mathbf{v},r)$, from Algorithm 1, produces $\mathbf{c}\in\mathrm{RM}(r,m)^t$ such that $d^{(t)}(\mathbf{v},\mathbf{c})\leqslant U_t(r,m)$. Additionally, its run-time complexity is $O(t2^t(2^{t+1})^{m+1}(2^{t+1}-1)^{-r}+tm2^m)$.

Proof: The algorithm clearly stops since, during the recursive calls, either r or m strictly decrease, and the base cases of $r=1$ and $r=m$ are eventually reached. The returned $\mathbf{c}$ is clearly a codeword, stemming from the base cases and the $(u,u+v)$ structure of Reed-Muller codes. Finally, $d^{(t)}(\mathbf{v},\mathbf{c})\leqslant U_t(r,m)$ due to Proposition 8, Lemma 6, and the fact that all the bounds in Table II are relaxations of both (including Theorem 15 which is based on a result from [7]).

We move on to the analysis of the run-time complexity. We first analyze $\texttt{recursive}(\mathbf{v},r)$, whose running time we denote by $T(t,r,m)$. We contend that for some constant $c\in\mathbb{N}$,

$$\begin{aligned}T(t,r,m)&\leqslant f(t,r,m)\\&\triangleq c\left(t2^t(2^{t+1})^{m+1}(2^{t+1}-1)^{-r}+tm2^m\right).\end{aligned}$$

This proof is by induction. For the first simple base case of $r=m$ we have $T(t,m,m)=c'$, a constant, and indeed

$$\begin{aligned}T(t,m,m)=c'&\leqslant c\left(t2^t(2^{t+1})^{m+1}(2^{t+1}-1)^{-m}+tm2^m\right)\\&=f(t,m,m),\end{aligned}$$

for a proper choice of c. Next, we check the base case $r=1$. In this case, a brute-force distance measurement is performed between $\mathbf{v}$ and the codewords of $\mathrm{RM}(1,m)^t$. Each codeword is a $t\times 2^m$ matrix, and we have a total of $|\mathrm{RM}(1,m)^t|=2^{(m+1)t}$ such codewords. Thus, for some constant c',

$$\begin{aligned}T(t,1,m)&=c'\cdot t2^m\cdot 2^{(m+1)t}\\&\leqslant c\left(t2^t(2^{t+1})^{m+1}(2^{t+1}-1)^{-1}+tm2^m\right)\\&=f(t,1,m),\end{aligned}$$

for any $c\geqslant c'$. Moving on to the main recursion, assume the claim holds for $T(t,r,m-1)$, for all $1\leqslant r\leqslant m-1$, and we prove it also holds for $T(t,r,m)$ for all $1\leqslant r\leqslant m$. If $r=1$ or $r=m$, we have a base case which we have already proved. Otherwise, the algorithm manipulates a $t\times 2^m$ matrix and runs two recursive instances. Hence, for some constant c', and after choosing any $c\geqslant c'$, we have

$$\begin{aligned}&T(t,r,m)\\&\quad=c't2^m+T(t,r-1,m-1)+T(t,r,m-1)\\&\quad\leqslant ct2^m+c\left(t2^t(2^{t+1})^m(2^{t+1}-1)^{-r+1}+t(m-1)2^{m-1}\right)\\&\qquad+c\left(t2^t(2^{t+1})^m(2^{t+1}-1)^{-r}+t(m-1)2^{m-1}\right)\\&\quad=c\left(t2^t(2^{t+1})^{m+1}(2^{t+1}-1)^{-r}+tm2^m\right)\\&\quad=f(t,r,m).\end{aligned}$$

This completes the induction. To complete the proof as well, we note that the complexity of $\texttt{subadditive}(\mathbf{v},r)$ is always subsumed by the complexity of $\texttt{recursive}(\mathbf{v},r)$. ■

As in the previous section, we analyze three asymptotic regimes for r and m:

Corollary 26: Let $t\in\mathbb{N}$ be a constant, let $n=2^m$ be the length of the code $\mathrm{RM}(r,m)$, and denote $\beta\triangleq\log_2\sqrt[t+1]{2^{t+1}-1}$. Then the run-time complexity of Algorithm 1 is:

- $O(n^{t+1})$ when r is constant.
- $O(n^{(t+1)(1-\alpha\beta)})$ when $r=\alpha m$, and $0<\alpha<\frac{t}{(t+1)\beta}$ is a constant.

- $O(n \log n)$ when $r = m - s$, s is constant, or when $r = \alpha m$, and $\frac{t}{(t+1)\beta} \leqslant \alpha < 1$ is a constant.

Proof: This is a straightforward application of Theorem 25. The $\frac{t}{(t+1)\beta}$ cutoff point stems from the fact that the complexity is in fact $O(n^{(t+1)(1-\alpha\beta)} + n \log n)$. Thus, for $\alpha < \frac{t}{(t+1)\beta}$, we have that $(t+1)(1-\alpha\beta) > 1$, and $n^{(t+1)(1-\alpha\beta)}$ dominates the complexity. However, when $\alpha \geqslant \frac{t}{(t+1)\beta}$, we have that $(t+1)(1-\alpha\beta) \leqslant 1$ and $n \log n$ dominates the complexity. ■

VI. Conclusion

In this work, we studied the generalized covering radii of Reed-Muller codes, $R_t(r, m)$. In some simple cases we found the exact generalized covering radii (see Table I). For most other cases we found lower and upper bounds on the generalized covering radii (see Table II). These bounds were found in three asymptotic regimes: r constant, $m - r$ constant, and r/m constant. We also constructed a t-covering algorithm with radius no worse than the upper bounds that we found (see Algorithm 1). We analyzed the algorithm's run-time complexity and showed it is polynomial in the code parameters.

We would like to mention a couple of interesting open questions pertaining to the results of this paper. We first observe that, apart from the base cases, our bounds are obtained using the $(u, u+v)$ recursion, and subadditivity. We suspect that for improved bounds, a different approach may be needed, perhaps an approach that exploits the unique geometric and combinatorial properties of Reed-Muller codes.

Another open problem concerns Algorithm 1. The edge case of $\mathrm{RM}(1, m)$ is solved in the algorithm using a brute-force approach: the distance between the input, $\mathbf{v}$, and the codewords of $\mathrm{RM}(1, m)^t$ is measured exhaustively and naively. However, for $t = 1$, the codewords of $\mathrm{RM}(1, m)$ form a Sylvester-type Hadamard matrix and its complement. Thus, by using the Walsh-Hadamard transform, an efficient measurement of the distance from $\mathbf{v}$ to the codewords of $\mathrm{RM}(1, m)$ is possible in $O(n \log n)$ time, instead of the $\Theta(n^2)$ of a naive implementation, where $n = 2^m$ is the code length. Whether a similar approach can improve Algorithm 1 is still unknown.

Finally, and more generally, it is known that the generalized covering radii are monotone non-decreasing in t. Thus, any improvement in the bounds on $R_t(r, m)$ may perhaps bring about an improvement in the bounds on the (regular) covering radius of Reed-Muller codes, $R_1(r, m)$. These problems, and others, are left for future research.

Acknowledgment

The authors would like to thank the associate editor and the anonymous referees, whose suggestions helped to improve the paper.

References

[1] E. Abbe, A. Shpilka, and A. Wigderson, "Reed-M´uller codes for random erasures and errors," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5229–5252, Oct. 2015.

[2] E. Abbe, A. Shpilka, and M. Ye, "Reed–Müller codes: Theory and algorithms," *IEEE Trans. Inf. Theory*, vol. 67, no. 6, pp. 3251–3277, Jun. 2021.

[3] E. Abbe and M. Ye, "Reed-muller codes polarize," *IEEE Trans. Inf. Theory*, vol. 66, no. 12, pp. 7311–7332, Dec. 2020.

[4] Y. Borissov, A. Braeken, S. Nikova, and B. Preneel, "On the covering radii of binary Reed–Müller codes in the set of resilient Boolean functions," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1182–1189, Mar. 2005.

[5] C. Carlet and S. Mesnager, "Improving the upper bounds on the covering radii of binary Reed–M´uller codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 162–173, Jan. 2007.

[6] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: Elsevier, 1997.

[7] G. D. Cohen and S. N. Litsyn, "On the covering radius of reed-muller codes," *Discrete Math.*, vols. 106–107, pp. 147–155, Sep. 1992.

[8] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed–Müller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2397–2417, Nov. 1999.

[9] J. A. Davis and J. Jedwab, "Peak-to-mean power control and error correction for OFDM transmission using Golay sequences and Reed–Müller codes," *Electron. Lett.*, vol. 33, no. 4, pp. 267–268, Feb. 1997.

[10] D. Elimelech, M. Firer, and M. Schwartz, "The generalized covering radii of linear codes," *IEEE Trans. Inf. Theory*, vol. 67, no. 12, pp. 8070–8085, Dec. 2021.

[11] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*. Reading, MA, USA: Addison-Wesley, 1994.

[12] V. Guruswami, A. Rudra, and M. Sudan. (2019). *Essential Coding Theory*. [Online]. Available: https://cse.buffalo.edu/faculty/atri/courses/coding-theory/book/

[13] T. Helleseth, T. Kløve, and J. Mykkeltveit, "On the covering radius of binary codes," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 5, pp. 627–628, Sep. 1978.

[14] X.-D. Hou, "Further results on the covering radii of the reed-muller codes," *Des., Codes Cryptogr.*, vol. 3, no. 2, pp. 167–177, May 1993.

[15] X.-D. Hou, "On the norm and covering radius of the first-order Reed-M´uller codes," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 1025–1027, May 1997.

[16] X. D. Hou, "Some results on the covering radii of Reed–Müller codes," *IEEE Trans. Inf. Theory*, vol. 39, no. 2, pp. 366–378, Mar. 1993.

[17] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, and R. L. Urbanke, "Reed–Müller codes achieve capacity on erasure channels," *IEEE Trans. Inf. Theory*, vol. 63, no. 7, pp. 4298–4316, Jul. 2017.

[18] K. Kurosawa, T. Iwata, and T. Yoshiwara, "New covering radius of Reed–Müller codes for t-resilient functions," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 468–475, Mar. 2004.

[19] F. J. MacWilliams and N. J. A. Sloane, *The Theory Error-Correcting Codes*. Amsterdam, The Netherlands: Elsevier, 1977.

[20] A. M. McLoughlin, "The covering radius of the $(m-3)$rd order Reed–Müller codes and a lower bound on the $(m-4)$th order Reed–Müller codes," *SIAM J. Appl. Math.*, vol. 37, no. 2, pp. 419–422, 1979.

[21] Q. Meng, H. Zhang, M. Yang, and Z. Wang, "Analysis of affinely equivalent Boolean functions," *Sci. China F, Inf. Sci.*, vol. 50, no. 3, pp. 299–306, Jun. 2007.

[22] J. Mykkeltveit, "The covering radius of the $(128, 8)$ Reed–Müller code is 56," *IEEE Trans. Inf. Theory*, vol. IT-26, no. 3, pp. 359–362, May 1980.

[23] K. G. Paterson, "Generalized Reed-M´uller codes and power control in OFDM modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 104–120, Jan. 2000.

[24] N. J. Patterson and D. H. Wiedemann, "The covering radius of the $(215, 16)$ Reed–Müller code is at least 16276," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 3, pp. 354–355, May 1983.

[25] J. Schatz, "The second order reed-muller code of length 64 has covering radius 18 (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 4, pp. 529–530, Jul. 1981.

[26] K.-U. Schmidt, "Complementary sets, generalized Reed–M´uller codes, and power control for OFDM," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 808–814, Feb. 2007.

[27] J. Spencer, *Asymptopia*, vol. 71. Providence, RI, USA: American Mathematical Society, 2014.

[28] A. Tietäväinen, "Covering radius and dual distance," *Des., Codes Cryptograph.*, vol. 1, no. 1, pp. 31–46, May 1991.

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

[30] S. Yekhanin, "Locally decodable codes," *Found. Trends Theor. Comput. Sci.*, vol. 6, no. 3, pp. 139–255, Oct. 2012.

Dor Elimelech (Graduate Student Member, IEEE) received the B.Sc. degree in mathematics and the B.Sc. and M.Sc. *(summa cum laude)* degrees in electrical engineering from the Ben-Gurion University of the Negev, Israel, in 2018 and 2020, respectively, where he is currently pursuing the Ph.D. degree in electrical engineering. His research interests include coding theory, ergodic theory, and dynamical systems.

Hengjia Wei received the Ph.D. degree in applied mathematics from Zhejiang University, Hangzhou, China, in 2014.

He was a Post-Doctoral Fellow with Capital Normal University, Beijing, China, from 2014 to 2016; a Research Fellow with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, from 2016 to 2019; and a Post-Doctoral Fellow with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Israel, from 2019 to 2022. Currently, he is an Associate Researcher with the Peng Cheng Laboratory, Shenzhen, China. His research interests include combinatorial design theory, coding theory, and their intersections. He received the 2017 Kirkman Medal from the Institute of Combinatorics and Its Applications.

Moshe Schwartz (Senior Member, IEEE) received the B.A. *(summa cum laude)*, M.Sc., and Ph.D. degrees from the Computer Science Department, Technion—Israel Institute of Technology, Haifa, Israel, in 1997, 1998, and 2004, respectively.

He was a Fulbright Post-Doctoral Researcher with the Department of Electrical and Computer Engineering, University of California at San Diego, and a Post-Doctoral Researcher with the Department of Electrical Engineering, California Institute of Technology. While on sabbatical from 2012 to 2014, he was a Visiting Scientist at the Massachusetts Institute of Technology (MIT). He is a Professor with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Israel. His research interests include algebraic coding, combinatorial structures, and digital sequences.

Prof. Schwartz has been an Editorial Board Member of the *Journal of Combinatorial Theory, Series A* since 2021. He received the 2009 IEEE Communications Society Best Paper Award in Signal Processing and Coding for Data Storage, and the 2020 NVMW Persistent Impact Prize. He served as an Associate Editor for Coding Techniques and Coding Theory of the IEEE TRANSACTIONS ON INFORMATION THEORY from 2014 to 2021 and has been serving as an Area Editor for Coding and Decoding of the IEEE TRANSACTIONS ON INFORMATION THEORY since 2021.