On the Generalized Covering Radii of Reed-Muller Codes

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

Hengjia Wei
Peng Cheng Laboratory
Shenzhen 518000, China
Email: hjwei05@163.com

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

***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 find the exact value of the generalized covering radii of Reed-Muller codes in certain extreme cases, as well as proving lower and upper bounds in various scenarios.**

I. Introduction

THE generalized covering radius has recently been proposed [9] 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 [9], 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 [27], 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 [9], 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 [15] and binary memoryless symmetric channels [23]. Other applications of Reed-Muller codes include locally decodable codes [28], probabilistic proof systems [1], sequence design for wireless communications [7], [8], [21], [25], and Boolean functions [3], [16], [19]. For a recent survey, the readers are referred to [2].

The work of D. Elimelech was supported in part by an Israel Science Foundation (ISF) Grant under Grant 1052/18. The work of H. Wei and M. Schwartz was supported in part by a German Israeli Project Cooperation (DIP) Grant under Grant PE2398/1-1.

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 [4], [6], [11]–[14], [18], [20], [22], [24]. 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 $r = \frac{m}{2} + \Theta(\sqrt{m})$. These results are summarized in Table I.
2) We find the exact t-th generalized covering radius of $\mathrm{RM}(r,m)$ in simple cases, $r \in \{0, m-2, m-1, m\}$. These results are summarized in Table II.
3) In the full version of this work (see [10]), motivated by an application to 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 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. Due to space limitations, proofs are omitted or sketched. For the full proofs the reader is referred to [10].

978-1-6654-2159-1/22/$31.00 ©2022 IEEE

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

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. We also define the *dual distance* of C to be the minimal distance of the dual code, $C^{\perp}$.

For any vector $\overline{v} \in \mathbb{F}_q^n$, the distance between $\overline{v}$ and the code C, denoted $d(\overline{v}, C)$, and then the covering radius of the code, denoted $R(C)$, are defined as

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

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

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

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

Lemma 1 *[26, 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 [9]. They have several equivalent definitions, which we bring here and use interchangeably. We begin with an definition via the parity check matrix. Assume that 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 $\overline{h}_1, \ldots, \overline{h}_n$. 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 definition for the t-th generalized covering radius of C:

Definition 2 *The t-th covering radius of C, denoted by $R_t(C)$, is the smallest integer r such that for any t vectors $\overline{v}_1, \ldots, \overline{v}_t \in \mathbb{F}_q^{n-k}$, there exists $I \in \binom{[n]}{r}$ such that $\{v_1, \ldots, v_t\} \subseteq \langle H_I \rangle$.*

One can easily see that $R_1(C) = R(C)$ is indeed the regular covering radius of the code C. An equivalent definition for the generalized covering radius is algebraic in nature:

Definition 3 *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,*

$$C_t \triangleq \left\{ \overline{u}G \,\middle|\, \overline{u} \in \mathbb{F}_{q^t}^k \right\} = \left\{ \overline{v} \in \mathbb{F}_{q^t}^n \,\middle|\, H\overline{c}^{\intercal} = \overline{0}^{\intercal} \right\}. \quad (1)$$

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 3, 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 $\mathbb{F}_{q^t}$. It is worth noting that, unlike the covering radius, the minimum distance of C_t does not change.

The generalized covering radius has a subadditivity property that proves to be useful for establishing many results:

Lemma 4 *[9, 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 ball-covering argument proves the following lemma.

Lemma 5 *For an $[n, k]_q$ code C and $t \in \mathbb{N}$,*

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

where $V_{q,n,r}$ denotes the volume of the Hamming ball of radius r in $\mathbb{F}_q^n$.

Proof: Recalling (1), 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 [5, Theorem 6.2.1]),

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

By Definition 3, $R_1(C_t) = R_t(C)$, and we conclude. ∎

B. Reed-Muller codes

Reed-Muller codes have been extensively studied (e.g., see [17], 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 $n = 2^m$, and $k = \sum_{i=0}^{r} \binom{m}{i}$. 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

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

As a base for the recursion, we define

$$\mathrm{RM}(0,m) \triangleq \{\overline{0}, \overline{1}\}, \qquad \mathrm{RM}(m,m) \triangleq \mathbb{F}_2^{2^m}.$$

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 $1 \leqslant r \leqslant m$,

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

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

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

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 6 *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 [9, 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 [6] and using the subadditivity formula from Lemma 4. The second strategy involves the use of the recursive formula from Proposition 6 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 7 *For all $m,t \in \mathbb{N}$,*

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

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 8 *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 [17, Ch. 13]), and hence the dual distance of C is $d' = 4$. Clearly, $d' = 4$ is the dual distance of C_t of (1) 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 $K_2(x; 2^m, 2^t)$. A simple calculation shows that

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

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

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

Theorem 9 *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.

The proof of the claim proceeds by induction on r. Lemma 8 shows that the claim holds for $r = 1$, and for all $m \in \mathbb{N}$. The induction step is proved by repeatedly using Proposition 6, the induction hypothesis, and an analysis of the extreme case where $r = m$.

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 10 *For all $m, t \in \mathbb{N}$, $1 \leqslant r \leqslant m$,*

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

where we consider r and t to be constants.

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 11 *For all $m, t \in \mathbb{N}$,*

$$R_t(m,m) = 0, \qquad R_t(m-1,m) = 1,$$
$$R_t(m-2,m) = \min\{t,m\}+1.$$

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 $H_1 = (1,1,\ldots,1)$. Then, by directly using Definition 2, 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. In this case, the $R_t(m-2,m)$ is calculated directly by Definition 3, using the well known $(m+1)\times 2^m$ parity-check matrix for this code, containing all the binary column vectors that start with a 1. ∎

Turning to the more general case of $\mathrm{RM}(m-s,m)$, we have the following bound.

Theorem 12 *For all $m, t \in \mathbb{N}$, $3 \leqslant s \leqslant m$,*

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

where we consider s and t to be constants.

Proof: In [6, 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 4, the upper bound follows immediately. The lower bound is proven using the ball-covering argument from Lemma 5 and a careful analysis of the ball size in this regime. ∎

We note that the ratio between the upper and lower bounds from Theorem 12 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 13 *For all $m, t \in \mathbb{N}$ and $\frac{1}{2} < \alpha < 1$,*

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

where we consider t and α to be constants.

The upper bound is proved by applying the subadditivity property from Lemma 4 to [5, Theorem 9.4.25]. The lower bound is followed from the ball-covering argument presented in Lemma 5.

We now move on to the range $0 < \alpha < \frac{1}{2}$. The upper bound in Theorem 14 is a weaker, more general version of an upper bound on $R_t(r,m)$.

Theorem 14 *For all $m, t \in \mathbb{N}$, and $0 < \alpha < \frac{1}{2}$,*

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

where t and α are constants.

For the the upper bound we first prove by induction, using Lemma 8 and Proposition 6, that for all $m, t \in \mathbb{N}$, $1 \leqslant r \leqslant m$,

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

We conclude by combining it with an approximation of binomial coefficients using the binary entropy function. The lower bound, is proven using ball-covering argument and an approximation of the ball size with the binary entropy function.

In the region $0 < \alpha \leqslant 1-\frac{1}{\sqrt{2}}$, we follow a similar procedure to that of [6], in order to improve the upper bound of Theorem 14. The bound is obtained by sharpening the upper bound of Theorem 14 in this region, requiring more involved work.

Theorem 15 *For all $m, t \in \mathbb{N}$, and $0 < \alpha < 1-\frac{1}{\sqrt{2}}$,*

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

where t and α are constants.

TABLE I
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 9
	$\geqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2t(2^t-1)\ln 2}}{2^t\sqrt{r!}}m^{r/2}2^{m/2}(1+o(1))$	Theorem 10
$R_t(m-s,m)$	$\leqslant \frac{t}{(s-2)!}m^{s-2} + O(m^{s-3})$	Theorem 12
	$\geqslant \frac{t}{(s-1)!}m^{s-2} + O(m^{s-3}\log(m))$	
$R_t(\alpha m,m)$	$\leqslant \left(1-\frac{1}{2^t}\right)2^m - \frac{\sqrt{2^t-1}}{2^t(2+\sqrt{2})}2^{m\left(\frac{1}{2}+\alpha\log_2(1+\sqrt{2})\right)}(1+o(1))$	Theorem 15, 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 14, 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 13, 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 14, 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 13, 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 16, assuming $\sum_{i=0}^{r}\binom{m}{i}=\kappa 2^m$
	$\geqslant H_{2^t}^{-1}(1-\kappa)2^m(1+o(1))$	

The bounds from Theorem 14 and Theorem 15 show that for $0<\alpha<\frac{1}{2}$, the t covering radius of $\mathrm{RM}(\alpha m,m)$ is smaller than $(1-\frac{1}{2^t})2^m$ 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 14 provides a bound for this exponential term for all $0<\alpha<\frac{1}{2}$:

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

In Theorem 15 we improve the upper bound for $0<\alpha<1-\frac{1}{\sqrt{2}}$ by showing that

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

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

We now focus on the case where the code rate is constant, i.e., $r=\frac{m}{2}+\Theta(\sqrt{m})$. Using similar techniques as in the previous cases, involving analysis of the ball-covering argument for the lower bound and (2) for the upper bound, we obtained the following lower and upper bounds:

Theorem 16 *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*

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

We observe that in this case, the ratio between the lower and upper bounds from Theorem 16 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 length of the code. That is, for any sequence $(r_m)_m$ such that $\sum_{i=0}^{r_m}\binom{m}{i}=\kappa 2^m$,

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

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 [6]) exhibit an asymptotic gap between them.

TABLE II
A SUMMARY OF EXACT VALUES

$R_t(0,m)$	$2^m - \lceil 2^{m-t}\rceil$	Proposition 7
$R_t(m-2,m)$	$\min\{t,m\}+1$	Proposition 11
$R_t(m-1,m)$	1	Proposition 11
$R_t(m,m)$	0	Proposition 11

REFERENCES

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

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

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

[4] C. Carlet and S. Mesnager, "Improving the upper bounds on the covering radii of binary Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 1, pp. 162–173, 2006.

[5] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes*. Elsevier, 1997.

[6] G. Cohen and S. Litsyn, "On the covering radius of Reed-Muller codes," *Discrete Math.*, vol. 106, pp. 147–155, 1992.

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

[8] ——, "Peak-to-mean power control and error correction for OFDM transmission using Golay sequences and Reed-Muller codes," *Electronics Letters*, vol. 33, no. 4, pp. 267–268, 1997.

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

[10] D. Elimelech, H. Wei, and M. Schwartz, "On the generalized covering radii of reed-muller codes," *arXiv preprint arXiv:2107.09902*, 2021.

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

[12] X.-D. Hou, "Further results on the covering radii of the Reed-Muller codes," *Designs, Codes and Cryptography*, vol. 3, no. 2, pp. 167–177, 1993.

[13] ——, "On the norm and covering radius of the first-order Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 43, no. 3, pp. 1025–1027, 1997.

[14] ——, "Some results on the covering radii of Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 39, no. 2, pp. 366–378, 2006.

[15] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Şaşoğlu, and R. L. Urbanke, "Reed-Muller codes achieve capacity on erasure channels," *IEEE Trans. Inform. Theory*, vol. 63, no. 7, pp. 4298–4316, 2017.

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

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Elsevier, 1977.

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

[19] Q. Meng, H. Zhang, M. Yang, and Z. Wang, "Analysis of affinely equivalent Boolean functions," *Science in China Series F: Information Sciences*, vol. 50, no. 3, pp. 299–306, 2007.

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

[21] K. G. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation," *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 104–120, 2000.

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

[23] G. Reeves and H. D. Pfister, "Reed-Muller codes achieve capacity on BMS channels," *arXiv preprint arXiv:2110.14631*, 2021.

[24] J. Schatz, "The second order Reed-Muller code of length 64 has covering radius 18," *IEEE Trans. Inform. Theory*, vol. 27, no. 4, pp. 529–530, 1981.

[25] K.-U. Schmidt, "Complementary sets, generalized Reed-Muller codes, and power control for OFDM," *IEEE Trans. Inform. Theory*, vol. 53, no. 2, pp. 808–814, 2007.

[26] A. Tietäväinen, "Covering radius and dual distance," *Designs, Codes and Cryptography*, vol. 1, pp. 31–46, 1991.

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

[28] S. Yekhanin, *Locally Decodable Codes*. Now, 2012.