2022 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-2159-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISIT50566.2022.9834598

Berman Codes: A Generalization of Reed-Muller Codes that Achieve BEC Capacity

Lakshmi Prasad Natarajan and Prasad Krishnan

***Abstract*—We identify a family of binary codes whose structure is similar to Reed-Muller (RM) codes and which include RM codes as a strict subclass. The codes in this family are denoted as $\mathcal{C}_n(r,m)$, and their duals are denoted as $\mathcal{B}_n(r,m)$. The length of these codes is n^m, where $n \geq 2$, and r is their 'order'. When $n = 2$, $\mathcal{C}_n(r,m)$ is the RM code of order r and length 2^m. The special case of these codes corresponding to n being an odd prime was studied by Berman (1967) and Blackmore and Norton (2001). Following the terminology introduced by Blackmore and Norton, we refer to $\mathcal{B}_n(r,m)$ as the *Berman code* and $\mathcal{C}_n(r,m)$ as the *dual Berman* code. We identify these codes using a recursive Plotkin-like construction, and we show that these codes have a rich automorphism group. Applying a result of Kumar et al. (2016) to this set of automorphisms, we show that these codes achieve the capacity of the binary erasure channel (BEC) under bit-MAP decoding.**

I. Introduction

Reed-Muller (RM) codes [1], [2] form one of the important and well studied code families in coding theory, and have a rich algebraic structure. In [3], Kudekar et al. showed that RM codes achieve the capacity of the Binary Erasure Channel (BEC). Furthermore, Reeves and Pfister [4] have recently showed the exciting result that RM codes achieve the capacity of binary-input memoryless symmetric (BMS) channels.

In the present work, we identify a family of binary linear codes (along with its dual family) which includes the RM codes as a strict subclass. These codes are defined using a recursive construction that is similar to the Plotkin construction for RM codes. This family contains a code for each choice of three integer parameters:

- (i) integers $n \geq 2$ and $m \geq 1$, which determine the length of the code, and
- (ii) an integer r, with $0 \leq r \leq m$, that determines the 'order' of the code.

We will denote the code with parameters n, r and m by $\mathcal{C}_n(r,m)$. The dual code, $\mathcal{C}_n(r,m)^{\perp}$, will be denoted by $\mathcal{B}_n(r,m)$. The length, dimension and minimum distance of $\mathcal{C}_n(r,m)$ are

$$\left[n^m,\, \textstyle\sum_{w=0}^{r} \binom{m}{w}(n-1)^w,\, n^{m-r}\right]. \tag{1}$$

The dual code $\mathcal{B}_n(r,m)$ has code parameters

$$\left[n^m,\, \textstyle\sum_{w=r+1}^{m} \binom{m}{w}(n-1)^w,\, 2^{r+1}\right]. \tag{2}$$

If we substitute $n = 2$ in (1) and (2) we obtain the parameters of the r^{th} order RM code of length 2^m, i.e., $\mathrm{RM}(r,m)$, and its dual $\mathrm{RM}(r,m)^{\perp} = \mathrm{RM}(m-r-1,m)$. Indeed, we see that the code $\mathcal{C}_2(r,m)$ is identical to $\mathrm{RM}(r,m)$, and by duality $\mathcal{B}_2(r,m) = \mathrm{RM}(m-r-1,m)$.

We study various basic properties of $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$ in this work. A sub-class of these codes, corresponding to the case $n = p$ with p being an odd prime, was studied by Berman [5], and Blackmore and Norton [6] using a group algebra framework. To the best of our knowledge, Berman [5] introduced and investigated the code $\mathcal{B}_p(r,m)$ and showed that its minimum distance 2^{r+1} is better than cyclic codes of the same length (for large values of m). Later, Blackmore and Norton [6] showed that the minimum distance of $\mathcal{C}_p(r,m)$ is p^{m-r} and analyzed the state complexity of this code. Blackmore and Norton refer to $\mathcal{B}_p(r,m)$, the code originally designed by Berman in [5], as the *Berman code*. We will follow this precedence, and we will refer to $\mathcal{B}_n(r,m)$ as the *Berman code* with parameters n, r and m, and $\mathcal{C}_n(r,m)$ as the *dual Berman code*.

We comment briefly on the differences with RM codes when $n \geq 3$. While RM codes are either self-orthogonal or dual-containing, Berman codes have complementary duals when n is odd. Also, RM codes are known to be doubly transitive; however, Berman codes with $n \geq 3$ are not. Further, the minimum distances of Berman and dual Berman codes grow slowly with block length N compared to RM codes. For any choice of $n \geq 2$ and any rate in $(0,1)$, long Berman codes and their duals have $\frac{r}{m} \approx \frac{(n-1)}{n}$. Now fixing n and letting $m \to \infty$, using (1), (2) and the fact $r \approx m(n-1)/n$, we see that the minimum distance $d_{\min}$ grows with the block length N as

$$d_{\min}\left(\mathcal{C}_n(r,m)\right) \sim N^{\frac{1}{n}},\ d_{\min}\left(\mathcal{B}_n(r,m)\right) \sim N^{\frac{(n-1)}{n\log_2 n}}.$$

In contrast, the minimum distance of RM codes (i.e., the case $n = 2$) grows approximately as the square root of N.

In the current work, we define the Berman and dual Berman codes using a recursive construction similar to the $(\boldsymbol{u}\,|\,\boldsymbol{u}+\boldsymbol{v})$ Plotkin construction. We provide a patterned basis for the dual Berman codes, and use this basis to identify some automorphisms of Berman codes and their duals (Section II). Finally, we utilize these automorphisms along with a result from Kumar et al. [7] to show that these codes are capacity achieving in the BEC under bit-MAP decoding (Section III).

The work of Lakshmi Prasad Natarajan was supported by SERB-DST via grant MTR/2019/001454. Prasad Krishnan acknowledges support from SERB-DST project CRG/2019/005572.

Lakshmi Prasad Natarajan is with the Department of Electrical Engineering, Indian Institute of Technology Hyderabad, Sangareddy 502 284, India (email: lakshminatarajan@iith.ac.in).

Prasad Krishnan is with the Signal Processing and Communications Research Center, International Institute of Information Technology, Hyderabad 500032, India (email: prasad.krishnan@iiit.ac.in).

In the full version of this paper [8], we provide the proofs of various results that are not included in this present shorter version as well as a number of additional results including identifying natural generator matrices of these codes, efficient decoding algorithms up to half the minimum distance, a discrete Fourier transform (DFT) based approach to study a subclass of these codes, and further simulation results. Furthermore, except double transitivity, we also show that they satisfy all the code properties used by Reeves and Pfister in [4] to show that RM codes achieve the capacity of binary-input memoryless symmetric channels.

Notation: For any positive integer ℓ, let $[\![\ell]\!]$ denote the set $\{0, 1, \ldots, \ell-1\}$. The notation $\mathbf{0}$ denotes a zero-vector or a zero-matrix of appropriate size. For two vectors $\boldsymbol{a}, \boldsymbol{b}$ their concatenation is denoted by $(\boldsymbol{a}|\boldsymbol{b})$. We denote an n-length vector $\boldsymbol{a}$ by its components as $\boldsymbol{a} = (a_i : i \in [\![n]\!])$. For some $S \subset [\![n]\!]$, we denote the vector with components $a_i : i \in S$ as $\boldsymbol{a}_S$. If $\boldsymbol{a}$ is a n^m-length vector for some $m \geq 1$, we also use the concatenation representation $\boldsymbol{a} = (\boldsymbol{a}_0|\boldsymbol{a}_1|\ldots|\boldsymbol{a}_{n-1})$, where $\boldsymbol{a}_l : l \in [\![n]\!]$ are subvectors of length n^{m-1}. The individual components of $\boldsymbol{a}_l$ would be then denoted as $a_{l,i} : i \in [\![n^{m-1}]\!]$.

II. Berman Codes and their Duals

A. Recursive Definition of Berman & Dual Berman Codes

We now proceed to give the definitions of the codes presented in this work. For some positive integers $n \geq 2$ and m, for some non-negative integer r such that $0 \leq r \leq m$, define the family of codes $\mathcal{B}_n(r,m) \subseteq \mathbb{F}_2^{n^m}$ recursively as follows.

$$\mathcal{B}_n(m,m) \triangleq \{\mathbf{0}\}, \quad \mathcal{B}_n(0,m) \triangleq \{\boldsymbol{c} \in \mathbb{F}_2^{n^m} : \sum_i c_i = 0\}.$$

For $m \geq 2$ and $1 \leq r \leq m-1$,

$$\mathcal{B}_n(r,m) \triangleq \{(\boldsymbol{v}_0|\boldsymbol{v}_1|\ldots|\boldsymbol{v}_{n-1}) : \boldsymbol{v}_l \in \mathcal{B}_n(r-1,m-1) \; \forall l \in [\![n]\!], \sum_{l \in [\![n]\!]} \boldsymbol{v}_l \in \mathcal{B}_n(r,m-1)\}.$$

We refer to the code $\mathcal{B}_n(r,m)$ as *the Berman code with parameters $n, m,$ and r*. We similarly define the code family $\mathcal{C}_n(r,m) \subseteq \mathbb{F}_2^{n^m}$ recursively.

$$\mathcal{C}_n(m,m) \triangleq \mathbb{F}_2^{n^m}, \quad \mathcal{C}_n(0,m) \triangleq \{(0,\ldots,0),(1,\ldots,1)\}.$$

For $m \geq 2$ and $1 \leq r \leq m-1$,

$$\mathcal{C}_n(r,m) \triangleq \{(\boldsymbol{u}+\boldsymbol{u}_0|\boldsymbol{u}+\boldsymbol{u}_1|\ldots|\boldsymbol{u}+\boldsymbol{u}_{n-2}|\boldsymbol{u}) : \boldsymbol{u}_l \in \mathcal{C}_n(r-1,m-1) \; \forall l \in [\![n-1]\!], \boldsymbol{u} \in \mathcal{C}_n(r,m-1)\}.$$

We shall refer to $\mathcal{C}_n(r,m)$ as the *dual Berman code with parameters n, m and r* (this nomenclature will be validated in Theorem II.1, where we show that the codes $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$ are dual to each other). Also, observe that when $n = 2$, the code $\mathcal{C}_2(r,m)$ is then defined as $\mathcal{C}_2(r,m) = \{(\boldsymbol{u}+\boldsymbol{u}_0|\boldsymbol{u}) : \boldsymbol{u}_0 \in \mathcal{C}_n(r-1,m-1), \boldsymbol{u} \in \mathcal{C}_n(r,m-1)\}$, which coincides with $\mathrm{RM}(r,m)$. Thus the class of codes $\mathcal{C}_n(r,m)$ includes the Reed-Muller codes.

Example II.1. We give some specific examples of the codes defined above.

- By the recursive definition, the single parity check code is used as the building block along with a global parity to obtain the following code for $n = 3, m = 2, r = 1$,

$$\begin{aligned}\mathcal{B}_3(1,2) &= \{(\boldsymbol{v}_0|\boldsymbol{v}_1|\boldsymbol{v}_0+\boldsymbol{v}_1) : \boldsymbol{v}_0, \boldsymbol{v}_1 \in \mathcal{B}_3(0,1)\} \\ &= \{(v_{00}, v_{01}, v_{00}+v_{01}|v_{10}, v_{11}, v_{10}+v_{11}| \\ &\qquad v_{00}+v_{10},\ v_{01}+v_{11},\ v_{00}+v_{01}+v_{10}+v_{11}) : \\ &\qquad v_{ij} \in \mathbb{F}_2, \forall i,j \in \{0,1\}\}.\end{aligned}$$

- The code $\mathcal{C}_3(1,2)$ is shown below as per the recursive construction. It is easy to verify that it is dual to $\mathcal{B}_3(1,2)$.

$$\begin{aligned}\mathcal{C}_3(1,2) = \{&(u_{00}, u_{00}, u_{00}|u_{10}, u_{10}, u_{10}|0,0,0)+ \\ &(u_0,\ u_1,\ u_2|u_0,\ u_1,\ u_2|u_0, u_1, u_2) : \\ &u_{00}, u_{10}, u_0, u_1, u_2 \in \mathbb{F}_2\}.\end{aligned}$$

□

It is clear that the codes $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$ are linear. We shall now provide various properties of these codes. The techniques involved in the proofs (available in [8]) are similar to those for RM codes, mainly involving induction on the parameter m. The parameters of $\mathcal{C}_n(r,m)$ were previously derived in [6, Remark 2.4], and the parameters of $\mathcal{B}_p(r,m)$ for odd prime p were derived in [5, Theorem 2.2], both using a group algebra framework.

Theorem II.1. *(Basic properties of $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$.)*

1) *Containment property: For $1 \leq r \leq m$,*
   a) $\mathcal{B}_n(r,m) \subset \mathcal{B}_n(r-1,m)$.
   b) $\mathcal{C}_n(r-1,m) \subset \mathcal{C}_n(r,m)$.
2) *Dimension:*

$$\dim(\mathcal{B}_n(r,m)) = \sum_{w=r+1}^{m} \binom{m}{w}(n-1)^w,$$

$$\dim(\mathcal{C}_n(r,m)) = \sum_{w=0}^{r} \binom{m}{w}(n-1)^w.$$

3) *Duality:* $\mathcal{C}_n(r,m)^\perp = \mathcal{B}_n(r,m)$.
4) *Minimum Distance:*

$$d_{\min}(\mathcal{B}_n(r,m)) = 2^{r+1}, \forall 0 \leq r \leq m-1,$$
$$d_{\min}(\mathcal{C}_n(r,m)) = n^{m-r}, \forall 0 \leq r \leq m.$$

B. A Patterned Basis for the Berman Code

Our next goal is to obtain a special patterned basis for $\mathcal{B}_n(r,m)$. Towards that end, we now give some notation to work with the indices of vectors in $\mathbb{F}_2^{n^m}$. This notation will also be used in the forthcoming section. Let $G = [\![n]\!] = \{0,1,\ldots,n-1\}$. We then identify the n^m coordinates of an arbitrary vector $\boldsymbol{v} \in \mathbb{F}_2^{n^m}$ using the m-tuples in G^m, i.e., $\boldsymbol{v} = (v_{\boldsymbol{i}} : \boldsymbol{i} \in G^m)$. We also write $\boldsymbol{v}$ as a concatenation of n vectors from $\mathbb{F}_2^{n^{m-1}}$, denoted by $\boldsymbol{v} = (\boldsymbol{v}_0|\ldots|\boldsymbol{v}_{n-1})$. The subvector $\boldsymbol{v}_l \in \mathbb{F}_2^{n^{m-1}}$ is then recursively identified as follows.

- For any $\boldsymbol{i}' \in G^{m-1}$, the component of $\boldsymbol{v}_l$ indexed by $\boldsymbol{i}'$ is identified as $v_{l,\boldsymbol{i}'} = v_{(\boldsymbol{i}'|l)}$ which is the component of $\boldsymbol{v}$ indexed by $(\boldsymbol{i}' \,|\, l) \in G^m$.

We also need the following definition of a patterned-vector in $\mathbb{F}_2^{n^m}$. For $m \geq 1$ and some $\boldsymbol{i}' \in G^m$, define the vector $\boldsymbol{c}_m(\boldsymbol{i}') \in \mathbb{F}_2^{n^m}$ as consisting of the entries

$$c_m(\boldsymbol{i}')_{\boldsymbol{i}} = \begin{cases} 1 & \text{if } \mathsf{supp}(\boldsymbol{i}) \subseteq \mathsf{supp}(\boldsymbol{i}') \text{ and } \boldsymbol{i}_{\mathsf{supp}(\boldsymbol{i})} = \boldsymbol{i}'_{\mathsf{supp}(\boldsymbol{i})} \\ 0 & \text{otherwise,} \end{cases}$$

$\forall \boldsymbol{i} \in G^m$, where $\mathsf{supp}(\boldsymbol{i}) \triangleq \{l \in [\![m]\!] : i_l \neq 0\}$ is the support set. That is, the vector $\boldsymbol{c}_m(\boldsymbol{i}')$ has 1 exactly in those coordinates $\boldsymbol{i} \in G^m$ which satisfy $i_l = i'_l$ for all $l : i_l \neq 0$. We give an example to illustrate the definition of $\boldsymbol{c}_m(\boldsymbol{i}')$.

Example II.2. Consider $m = 3, n = 3$, and $G = \{0, 1, 2\}$. Let $\boldsymbol{i}' = (1, 2, 0) \in G^3$. The components of the vector $\boldsymbol{c}_3(\boldsymbol{i}') \in \mathbb{F}_2^{27}$ are as follows.

$$\boldsymbol{c}_3(\boldsymbol{i}')_{\boldsymbol{i}} = \begin{cases} 1 & \text{for } \boldsymbol{i} \in \{(0,0,0), (1,0,0), (0,2,0), (1,2,0)\}, \\ 0 & \text{otherwise.} \end{cases}$$

□

We are now ready to show a patterned basis for $\mathcal{B}_n(r, m)$. Let $w_H(\boldsymbol{i}) \triangleq |\mathsf{supp}(\boldsymbol{i})|$ be the Hamming weight of $\boldsymbol{i}$.

Lemma II.1. *For $m \geq 1$, and $0 \leq r \leq m-1$, consider the collection of elements in $\mathbb{F}_2^{n^m}$ given by*

$$B_{\mathcal{B}_n}(r, m) = \{\boldsymbol{c}_m(\boldsymbol{i}') : \forall \boldsymbol{i}' \in G^m \text{ such that } r+1 \leq w_H(\boldsymbol{i}') \leq m\}. \quad (3)$$

Then the collection $B_{\mathcal{B}_n}(r, m)$ is a basis for $\mathcal{B}_n(r, m)$.

Proof: We first show that the vectors in $B_{\mathcal{B}_n}(r, m)$ are linearly independent. Let B' be any non-empty subset of vectors from $B_{\mathcal{B}_n}(r, m)$. Note that each vector in B' is of the form $\boldsymbol{c}_m(\boldsymbol{i}')$ for some unique $\boldsymbol{i}' \in G^m$ with $w_H(\boldsymbol{i}') \geq r+1$, by the construction of set $B_{\mathcal{B}_n}(r, m)$.

We will show that the $\mathbb{F}_2$-sum of the vectors from B' cannot be zero, which suffices to show that $B_{\mathcal{B}_n}(r, m)$ is a linearly independent set of vectors.

Let $\boldsymbol{c}_m(\boldsymbol{i}_d) \in B'$ be such that $w_H(\boldsymbol{i}_d) \geq w_H(\boldsymbol{i}')$ for any $\boldsymbol{c}_m(\boldsymbol{i}') \in B'$. Thus, $\boldsymbol{c}_m(\boldsymbol{i}_d)$ is a maximal element in B' in this sense. Note that such a maximal element $\boldsymbol{c}_m(\boldsymbol{i}_d)$ will always exist for any non-empty $B' \subseteq B_{\mathcal{B}_n}(r, m)$.

We observe the following by the definition of the vectors $\boldsymbol{c}_m(\boldsymbol{i}') \in B_{\mathcal{B}_n}(r, m)$. For any $\boldsymbol{c}_m(\boldsymbol{i}') \in B'$, if $c_m(\boldsymbol{i}')_{\boldsymbol{i}_d} = 1$, we must have $\mathsf{supp}(\boldsymbol{i}_d) \subseteq \mathsf{supp}(\boldsymbol{i}')$ and $\boldsymbol{i}'_{\mathsf{supp}(\boldsymbol{i}_d)} = (\boldsymbol{i}_d)_{\mathsf{supp}(\boldsymbol{i}_d)}$. By the maximality of $\boldsymbol{c}_m(\boldsymbol{i}_d)$, we must have $w_H(\boldsymbol{i}_d) = w_H(\boldsymbol{i}')$. Hence, by these observations, we must have that $\boldsymbol{i}' = \boldsymbol{i}_d$. Thus, the sum of vectors in B' cannot be $\mathbf{0}$ (as the $\boldsymbol{i}_d^{th}$ coordinate in the sum cannot be 0). Thus, the vectors in $B_{\mathcal{B}_n}(r, m)$ are linearly independent.

Also, we see that $|B_{\mathcal{B}_n}(r, m)| = \sum_{w=r+1}^{m} \binom{m}{w}(n-1)^w = \dim(\mathcal{B}_n(r, m))$. Thus, showing that $B_{\mathcal{B}_n}(r, m) \subset \mathcal{B}_n(r, m)$ will conclude the proof. The rest of the proof is devoted to showing this statement.

Consider an arbitrary $\boldsymbol{c}_m(\boldsymbol{i}') \in B_{\mathcal{B}_n}(r, m)$. Note that $w_H(\boldsymbol{c}_m(\boldsymbol{i}')) = 2^{w_H(\boldsymbol{i}')} \geq 2^{r+1}$, by definition. Thus, $\boldsymbol{c}_m(\boldsymbol{i}') \in \mathcal{B}_n(0, m)$ has even weight. Thus the statement holds for $r = 0$ for any m. Thus, the statement holds for $m = 1$.

Now we prove the statement for $r \geq 1, m \geq 2$ assuming it holds for $m-1$. Recall that we can use the concatenation representation for $\boldsymbol{c}_m(\boldsymbol{i}')$ as $\boldsymbol{c}_m(\boldsymbol{i}') = (\boldsymbol{c}_m(\boldsymbol{i}')_0 | \boldsymbol{c}_m(\boldsymbol{i}')_1 | \ldots | \boldsymbol{c}_m(\boldsymbol{i}')_{n-1})$. We consider two cases.

Case (a): $m-1 \in \mathsf{supp}(\boldsymbol{i}')$. Let $i'_{m-1} = l' \in G \setminus \{0\}$. Thus, for some $\boldsymbol{i} \in G^m$, if $i_{m-1} \in G \setminus \{l', 0\}$, then $\boldsymbol{c}_m(\boldsymbol{i}')_{\boldsymbol{i}} = 0$. This means $\boldsymbol{c}_m(\boldsymbol{i}')_l = \mathbf{0} \in \mathbb{F}_2^{n^{m-1}}$ if $l \notin \{l', 0\}$. Further if $l \in \{l', 0\}$, then we can observe that $\boldsymbol{c}_m(\boldsymbol{i}')_l = \boldsymbol{c}_{m-1}(\boldsymbol{i}'_{[\![m-1]\!]}) \in \mathbb{F}_2^{n^{m-1}}$, where we recall the notation $\boldsymbol{i}'_{[\![m-1]\!]} = (i'_l : l \in [\![m-1]\!])$. As $\mathsf{supp}(\boldsymbol{i}'_{[\![m-1]\!]}) = \mathsf{supp}(\boldsymbol{i}') \setminus \{m-1\}$, thus $r \leq w_H(\boldsymbol{i}'_{[\![m-1]\!]}) \leq m-1$, which means $\boldsymbol{c}_{m-1}(\boldsymbol{i}'_{[\![m-1]\!]}) \in B_{\mathcal{B}_n}(r-1, m-1)$. By the induction hypothesis, we thus have $\boldsymbol{c}_{m-1}(\boldsymbol{i}'_{[\![m-1]\!]}) \in \mathcal{B}_n(r-1, m-1)$. Further, $\sum_{l \in [\![n]\!]} \boldsymbol{c}_m(\boldsymbol{i}')_l = \boldsymbol{c}_m(\boldsymbol{i}')_0 + \boldsymbol{c}_m(\boldsymbol{i}')_{l'} = \mathbf{0} \in \mathcal{B}_n(r, m-1)$. Thus the two conditions in the definition of $\mathcal{B}_n(r, m)$ are satisfied, and thus $\boldsymbol{c}_m(\boldsymbol{i}') \in \mathcal{B}_n(r, m)$.

Case (b): $m-1 \notin \mathsf{supp}(\boldsymbol{i}')$. In this case, a necessary condition for $\boldsymbol{c}_m(\boldsymbol{i}')_{\boldsymbol{i}} = 1$ is that $m-1 \notin \mathsf{supp}(\boldsymbol{i})$. This means we have $\boldsymbol{c}_m(\boldsymbol{i}')_l = \mathbf{0}$ if $l \neq 0$, and $\boldsymbol{c}_m(\boldsymbol{i}')_l = \boldsymbol{c}_{m-1}(\boldsymbol{i}'_{[\![m-1]\!]}) \in \mathbb{F}_2^{n^{m-1}}$ for $l = 0$. Now, as $\mathsf{supp}(\boldsymbol{i}'_{[\![m-1]\!]}) = \mathsf{supp}(\boldsymbol{i}')$, this means that $r+1 \leq w_H(\boldsymbol{i}'_{[\![m-1]\!]}) = w_H(\boldsymbol{i}') \leq m-1$. Hence, $\boldsymbol{c}_{m-1}(\boldsymbol{i}'_{[\![m-1]\!]}) \in B_{\mathcal{B}_n}(r, m-1)$ and thus $\boldsymbol{c}_{m-1}(\boldsymbol{i}'_{[\![m-1]\!]}) \in \mathcal{B}_n(r, m-1)$ by the induction hypothesis. By Theorem II.1 (part 1), this means $\boldsymbol{c}_{m-1}(\boldsymbol{i}'_{[\![m-1]\!]}) \in \mathcal{B}_n(r-1, m-1)$. It is thus clear that the conditions in the definition of $\mathcal{B}_n(r, m)$ are satisfied by the vector $\boldsymbol{c}_m(\boldsymbol{i}')$. This concludes the proof. ■

Example II.3. For the code $\mathcal{B}_3(1, 3)$, with the coordinates indexed by $\{0, 1, 2\}^3$, Lemma II.1 shows that the following collection $B_{\mathcal{B}_3}(1, 3)$ consisting of 20 vectors is a basis.

$$\bigcup_{a,b,c \in \{1,2\}} \{\boldsymbol{c}_3((a,b,0)), \boldsymbol{c}_3((0,a,b)), \boldsymbol{c}_3((a,0,b)), \boldsymbol{c}_3((a,b,c))\}$$

□

C. Some useful automorphisms of $\mathcal{B}_n(r, m)$ and $\mathcal{C}_n(r, m)$

The results in this sub-section specify some automorphisms of the code $\mathcal{B}_n(r, m)$ (and hence for $\mathcal{C}_n(r, m)$, by duality).

Lemma II.2. *Let σ be any permutation of the set G. The following permutation $\pi_{m-1,\sigma}$ on the m-tuples in G^m is an automorphism of $\mathcal{B}_n(r, m)$.*

$$\pi_{m-1,\sigma} : (i_0, \ldots, i_{m-2}, i_{m-1}) \mapsto (i_0, \ldots, i_{m-2}, \sigma(i_{m-1})).$$

Proof: Let $\boldsymbol{v} = (\boldsymbol{v}_0 | \ldots | \boldsymbol{v}_{n-1})$ be an arbitrary codeword in $\mathcal{B}_n(r, m)$. We want to show that the vector $\boldsymbol{v}'$, with coordinates $v'_{\boldsymbol{i}} = v_{\pi_{m-1,\sigma}(\boldsymbol{i})}$, also lies in $\mathcal{B}_n(r, m)$.

To see this, observe that if we write $\boldsymbol{v}'$ as $(\boldsymbol{v}'_0 | \ldots | \boldsymbol{v}'_{n-1})$, for any $l \in [\![n]\!]$ we have that $\boldsymbol{v}'_l = \boldsymbol{v}_{l'}$ for precisely that unique l' such that $\sigma(l') = l$. Thus, the subvectors of $\boldsymbol{v}'$ are precisely the same as those in $\boldsymbol{v}$, only their positions are permuted. Thus $\boldsymbol{v}'$ satisfies the two conditions in the definition of $\mathcal{B}_n(r, m)$. Hence $\boldsymbol{v}' \in \mathcal{B}_n(r, m)$, which completes the proof. ■

Lemma II.3. *For any $t \in [\![m-1]\!]$, the permutation β_t on G^m defined below is an automorphism of $\mathcal{B}_n(r,m)$.*

$$\beta_t \colon (i_0, \ldots, i_{m-1}) \mapsto (i_0, \ldots, i_{t-1}, i_{m-1}, i_{t+1}, \ldots, i_{m-2}, i_t).$$

Proof: Clearly, the statement is true for $r = m$. Hence we assume $r \leq m-1$. Recalling the definition of the set $B_{\mathcal{B}_n}(r,m)$ in (3), to show the lemma, it is sufficient to show that for each $\boldsymbol{c}_m(\boldsymbol{i}') \in B_{\mathcal{B}_n}(r,m)$, the permuted vector $\boldsymbol{c}'$ defined below is also in $B_{\mathcal{B}_n}(r,m)$.

$$c'_{\boldsymbol{i}} = c_m(\boldsymbol{i}')_{\beta_t(\boldsymbol{i})}, \ \forall \boldsymbol{i} \in G^m. \tag{4}$$

We shall in fact prove that $\boldsymbol{c}' = \boldsymbol{c}_m(\beta_t(\boldsymbol{i}')))$. The proof will then be complete as β_t is a one-one map.

Firstly we observe that the following two statements are equivalent for any $\boldsymbol{i} \in G^m$, because β_t is a self-inverse permutation.

- $\mathsf{supp}(\beta_t(\boldsymbol{i})) \subseteq \mathsf{supp}(\boldsymbol{i}')$ and $\beta_t(\boldsymbol{i})_{\mathsf{supp}(\beta_t(\boldsymbol{i}))} = \boldsymbol{i}'_{\mathsf{supp}(\beta_t(\boldsymbol{i}))}$, are both true.
- $\mathsf{supp}(\boldsymbol{i}) \subseteq \mathsf{supp}(\beta_t(\boldsymbol{i}'))$ and $\boldsymbol{i}_{\mathsf{supp}(\boldsymbol{i})} = \beta_t(\boldsymbol{i}')_{\mathsf{supp}(\boldsymbol{i})}$, are both true.

Now, using the above equivalence and (4), we have,

$$c'_{\boldsymbol{i}} = \begin{cases} 1 & \text{if } \mathsf{supp}(\boldsymbol{i}) \subseteq \mathsf{supp}(\beta_t(\boldsymbol{i}')) \ \&\ \boldsymbol{i}_{\mathsf{supp}(\boldsymbol{i})} = \beta_t(\boldsymbol{i}')_{\mathsf{supp}(\boldsymbol{i})}, \\ 0 & \text{otherwise,} \end{cases} \tag{5}$$

for all $\boldsymbol{i} \in G^m$. Clearly, by (5), we see that $\boldsymbol{c}'$ is precisely the vector $\boldsymbol{c}_m(\beta_t(\boldsymbol{i}'))$. Since $w_H(\beta_t(\boldsymbol{i}')) = w_H(\boldsymbol{i}') \geq r+1$, we have that $\boldsymbol{c}_m(\beta_t(\boldsymbol{i}')) \in B_{\mathcal{B}_n}(r,m)$ as well. This completes the proof. ∎

We now summarize the results from the above two lemmas. We use $\mathcal{S}_m$ to denote the symmetric group of degree m, i.e., $\mathcal{S}_m$ is the group of all permutations on $[\![m]\!]$.

Theorem II.2. *Let $\sigma_0, \ldots, \sigma_{m-1}$ be any permutations of the set G, and let $\gamma \in \mathcal{S}_m$. The following permutations on G^m are automorphisms of $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$.*

$$(i_0, \ldots, i_{m-1}) \to (\sigma_0(i_0), \ldots, \sigma_{m-1}(i_{m-1})),$$
$$(i_0, \ldots, i_{m-1}) \to (i_{\gamma(0)}, \ldots, i_{\gamma(m-1)}).$$

Proof: It is sufficient to show that the permutations in the statement are automorphisms of $\mathcal{B}_n(r,m)$ because of the duality of $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$.

Part 1): For any $t \in [\![m-1]\!]$, the permutation

$$(i_0, \ldots, i_{m-1}) \to (i_0, \ldots, i_{t-1}, \sigma_t(i_t), i_{t+1}, \ldots, i_{m-1}),$$

is identical with the composition $\beta_t \pi_{m-1,\sigma_t} \beta_t$, where π_{m-1,σ_t} and β_t are as defined in Lemma II.2 and Lemma II.3 respectively. Thus, the permutation

$$(i_0, \ldots, i_{m-1}) \to (\sigma_0(i_0), \ldots, \sigma_{m-1}(i_{m-1})), \tag{6}$$

is identical with the composition $\pi_{m-1,\sigma_{m-1}} \left(\prod_{t \in [\![m-1]\!]} \beta_t \pi_{m-1,\sigma_t} \beta_t \right)$. Since the set of automorphisms of $\mathcal{B}_n(r,m)$ form a group under composition, by Lemmas II.2 and II.3, we have that (6) is an automorphism of $\mathcal{B}_n(r,m)$.

Part 2): It is known (see, for example, [9]) that any permutation $\gamma \in \mathcal{S}_m$ can be generated by a composition of transpositions, where a transposition refers to a permutation which interchanges one element of $[\![m]\!]$ with another, and leaves the other elements as is. Observe that β_t as in Lemma II.3 is precisely the transposition that interchanges t with $m-1$. Further, a transposition that interchanges two distinct elements $t_1, t_2 \in [\![m-1]\!]$ can be obtained as the composition $\beta_{t_2} \beta_{t_1} \beta_{t_2}$. This completes the proof following Lemma II.3 and because the automorphisms of $\mathcal{B}_n(r,m)$ form a group. ∎

III. Capacity-Related Properties

A. Rate of $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$

The rate of $\mathcal{C}_n(r,m)$ is $R_n(r,m) \triangleq \frac{\sum_{w=0}^{r} \binom{m}{w} (n-1)^w}{n^m}$, which is equal to the fraction of vectors in G^m with weight at the most r. Similar to RM codes [4], the rate of $\mathcal{C}_n(r,m)$ can be seen to be equal to the cumulative distribution function of a binomial random variable with m trials and probability of success $(n-1)/n$ (please see [8] for more details). The *Berry-Esseen inequality* [10] can be used to approximate this distribution function with that of the standard Gaussian. Let $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-t^2/2} \mathrm{d}t$ be the tail probability of the standard Gaussian distribution. The Berry-Esseen inequality guarantees that there exists a constant $\kappa > 0$, that depends only on n, such that

$$\left| R_n(r,m) - \left(1 - Q\left(\tfrac{r - m\mu}{\sqrt{m\sigma^2}}\right)\right) \right| \leq \tfrac{\kappa}{\sqrt{m}}, \tag{7}$$

where $\mu = (n-1)/n$ and $\sigma^2 = (n-1)/n^2$. We also note that $1 - R_n(r,m)$ is the rate of $\mathcal{B}_n(r,m)$. Hence, from (7), we deduce that the rate of $\mathcal{B}_n(r,m)$ is $Q\left(\frac{r-m\mu}{\sqrt{m\sigma^2}}\right) + O\left(\frac{1}{\sqrt{m}}\right)$.

B. Achieving the BEC Capacity

Kumar, Calderbank and Pfister [7, Theorem 19] use code automorphisms to provide a sufficient condition for a code to achieve the capacity of BEC under bit-MAP decoding. This condition is less demanding than requiring double transitivity, which was the property used in [3] to prove RM codes achieve BEC capacity. To use this result on a sequence of codes with increasing block lengths, we require the following

1) the rates of the sequence of codes must converge to a value in $(0,1)$,
2) each code in this sequence must be transitive,
3) for each code the orbit of the coordinates under a subgroup of automorphisms (those automorphisms that fix an arbitrarily chosen coordinate) must be sufficiently large.

We will now apply this result to the family of codes $\{\mathcal{C}_n(r,m)\}$. A similar result holds for $\{\mathcal{B}_n(r,m)\}$.

1) Code Sequence with Converging Rate: For a given $n \geq 2$ and $R^* \in (0,1)$, consider a sequence of codes $\{\mathcal{C}_n(r_l, m_l)\}$ with $m_l \to \infty$ and $r_l = m_l\mu + Q^{-1}(1-R^*)\sqrt{m_l\sigma^2} + o(\sqrt{m_l})$. Using (7) we note that the rate $R_n(r_l, m_l) \to R^*$ as $m_l \to \infty$. Hence, for any $R^* \in (0,1)$ there exists a sequence of $\mathcal{C}_n(r,m)$ codes with increasing lengths, and rates converging to R^*.

2) Transitivity: We now use Theorem II.2 to observe that for any choice of parameters n, r, m, the code $\mathcal{C}_n(r,m)$ is transitive. Consider any choice of coordinates $\boldsymbol{i}, \boldsymbol{j} \in G^m$. We need to show that there is a code automorphism that maps $\boldsymbol{i}$ to $\boldsymbol{j}$. Let $\sigma_0, \ldots, \sigma_{m-1}$ be permutations of the set G such that

$$\sigma_0(i_0) = j_0, \ldots, \sigma_{m-1}(i_{m-1}) = j_{m-1}.$$

Applying Theorem II.2 for this choice of $\sigma_0, \ldots, \sigma_{m-1}$ shows that $\mathcal{C}_n(r,m)$ is indeed transitive.

3) Orbits Under a Subgroup of Automorphisms: Let $\mathcal{G}_0$ be the subgroup of automorphisms of $\mathcal{C}_n(r,m)$ that fixes the coordinate $\mathbf{0} \in G^m$. We want a lower bound on the size of the orbits of $\boldsymbol{i} \in G^m \setminus \{\mathbf{0}\}$ under the action of $\mathcal{G}_0$, which is

$$\mathcal{O}_{r,m}(\boldsymbol{i}) \triangleq \{\pi(\boldsymbol{i}) : \pi \in \mathcal{G}_0\}.$$

We will identify a subset of $\mathcal{O}_{r,m}(\boldsymbol{i})$ to obtain this lower bound.

Consider any $\boldsymbol{i} \neq \mathbf{0}$ and any $\boldsymbol{j} \in G^m$ such that $\mathsf{supp}(\boldsymbol{i}) = \mathsf{supp}(\boldsymbol{j})$. There exist m permutations of G, $\sigma_0, \ldots, \sigma_{m-1}$, such that

$$\sigma_l(i_l) = j_l \text{ and } \sigma_l(0) = 0 \text{ for all } l \in [\![m]\!].$$

Using Theorem II.2, we see that the map $(k_0, \ldots, k_{m-1}) \to (\sigma_0(k_0), \ldots, \sigma_{m-1}(k_{m-1}))$ is an automorphism of $\mathcal{C}_n(r,m)$ that fixes $\mathbf{0}$ and sends $\boldsymbol{i}$ to $\boldsymbol{j}$. We thus conclude that $\mathcal{O}_{r,m}(\boldsymbol{i})$ contains all $\boldsymbol{j}$ such that $\mathsf{supp}(\boldsymbol{j}) = \mathsf{supp}(\boldsymbol{i})$.

Now, for a given $\boldsymbol{i} \neq \mathbf{0}$, consider any $\boldsymbol{j}$ such that $w_H(\boldsymbol{j}) = w_H(\boldsymbol{i})$. Clearly, there exists a permutation $\gamma \in \mathcal{S}_m$ such that $\mathsf{supp}(\boldsymbol{j}) = \mathsf{supp}(\gamma(\boldsymbol{i}))$. From our argument in the previous paragraph, $\boldsymbol{j} \in \mathcal{O}_{r,m}(\gamma(\boldsymbol{i}))$. Since γ is a code automorphism that fixes $\mathbf{0}$, we see that $\gamma(\boldsymbol{i})$ itself belongs to $\mathcal{O}_{r,m}(\boldsymbol{i})$, and therefore, $\boldsymbol{j} \in \mathcal{O}_{r,m}(\boldsymbol{i})$. We have thus showed that for any $\boldsymbol{i} \neq \mathbf{0}$, $\mathcal{O}_{r,m}(\boldsymbol{i}) \supseteq \{\boldsymbol{j} \in G^m : w_H(\boldsymbol{j}) = w_H(\boldsymbol{i})\}$. Hence,

$$|\mathcal{O}_{r,m}(\boldsymbol{i})| \geq \binom{m}{w_H(\boldsymbol{i})} (n-1)^{w_H(\boldsymbol{i})}.$$

Note that for any $n \geq 3$, and any $\boldsymbol{i} \in G^m \setminus \{\mathbf{0}\}$, we have

$$|\mathcal{O}_{r,m}(\boldsymbol{i})| \geq 2m.$$

We are now ready to apply [7, Theorem 19]. Let $n \geq 3$. Consider a sequence of codes $\{\mathcal{C}_n(r_l, m_l)\}$ with $m_l \to \infty$ and rates converging to $R^* \in (0,1)$. All the codes in this sequence are transitive, and they satisfy

$$\min_{\boldsymbol{i} \in G^{m_l} \setminus \{\mathbf{0}\}} |\mathcal{O}_{r_l,m_l}(\boldsymbol{i})| \to \infty \text{ as } l \to \infty.$$

These are precisely the sufficient conditions identified in [7] to guarantee that this sequence of codes has a vanishing bit erasure probability under bit-MAP decoding in the BEC for any channel erasure probability $\epsilon < (1 - R^*)$. Note that a similar result holds for Berman codes $\{\mathcal{B}_n(r,m)\}$.

IV. Simulation Result

In our simulations we have compared codes with reasonably close rates and lengths. To account for the difference in the rates we use $\epsilon - (1-R)$, instead of ϵ, as the horizontal axis in our plots (where R is the code rate). Note that $\epsilon - (1-R)$ is the difference between the actual channel erasure probability and the capacity limit (i.e., $1 - R$ is the highest possible channel erasure probability that any code of rate R can withstand).

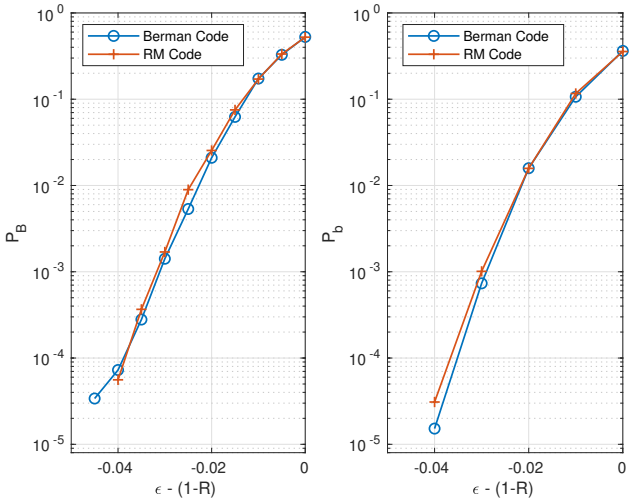

Fig. 1. The block and bit erasure rates of $\mathcal{B}_3(5,7)$ and $\mathrm{RM}(4,11)$ in BEC.

We compare the block erasure rate P_B (under block-MAP decoding) and bit erasure rate P_b (under bit-MAP decoding) of $\mathcal{B}_3(5,7)$ with $\mathrm{RM}(4,11)$ in Fig. 1. The parameters of these two codes are $[2187, 576, 64]$ and $[2048, 562, 128]$, respectively. Note the similarity in their bit erasure rate performance for $P_b \geq 10^{-5}$.

In [8], we compare the performances of the dual Berman code $\mathcal{C}_3(5,7)$ (with parameters $[2187, 1611, 9]$) and $\mathrm{RM}(6,11)$ (parameters $[2048, 1486, 32]$). While these two codes have similar P_b, the P_B curve of $\mathcal{C}_3(5,7)$ exhibits a high floor due to its small minimum distance.

V. Discussion

We identified a family of codes that includes the RM codes [1], [2] ($n = 2$) and whose properties are similar to RM codes. While the similarity of $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$ to RM codes is striking, there are some key differences as well, especially in terms of the minimum distance and the automorphism group. Our guarantees on capacity achievability in the BEC are in the sense of vanishing bit erasure probability P_b. It is not clear if these codes have vanishing block erasure probability P_B under block-MAP decoding for rates close to capacity limit. It is possible that some of the differences of $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$ with RM codes might offer advantages. For large block lengths, the minimum distance of $\mathcal{C}_n(r,m)$ is significantly smaller than that of RM codes. This implies that its dual $\mathcal{B}_n(r,m)$ has a parity check matrix that is considerably sparser than the parity-check matrix of RM codes. This sparsity might be useful in designing low complexity iterative decoders for $\mathcal{B}_n(r,m)$, see [11].

REFERENCES

[1] D. E. Muller, "Application of boolean algebra to switching circuit design and to error detection," *Transactions of the I.R.E. Professional Group on Electronic Computers*, vol. EC-3, no. 3, pp. 6–12, 1954.

[2] I. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *Transactions of the IRE Professional Group on Information Theory*, vol. 4, no. 4, pp. 38–49, 1954.

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

[4] G. Reeves and H. D. Pfister, "Reed-Muller codes achieve capacity on BMS channels," *CoRR*, vol. abs/2110.14631, 2021. [Online]. Available: https://arxiv.org/abs/2110.14631

[5] S. Berman, "Semisimple cyclic and Abelian codes. II," *Cybernetics*, vol. 3, no. 3, pp. 17–23, 1967.

[6] T. Blackmore and G. Norton, "On a family of abelian codes and their state complexities," *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 355–361, 2001.

[7] S. Kumar, R. Calderbank, and H. D. Pfister, "Beyond double transitivity: Capacity-achieving cyclic codes on erasure channels," in *2016 IEEE Information Theory Workshop (ITW)*, 2016, pp. 241–245.

[8] L. P. Natarajan and P. Krishnan, "Berman codes: A generalization of Reed-Muller codes that achieve BEC capacity," 2022. [Online]. Available: https://arxiv.org/abs/2202.09981

[9] B. R. Heap, "Permutations by Interchanges," *The Computer Journal*, vol. 6, no. 3, pp. 293–298, 11 1963. [Online]. Available: https://doi.org/10.1093/comjnl/6.3.293

[10] V. Y. Korolev and I. G. Shevtsova, "On the upper bound for the absolute constant in the Berry–Esseen inequality," *Theory of Probability & Its Applications*, vol. 54, no. 4, pp. 638–658, 2010.

[11] E. Santi, C. Hager, and H. D. Pfister, "Decoding Reed-Muller codes using minimum-weight parity checks," in *2018 IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 1296–1300.