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, they are generated by the minimum weight codewords, and that they can be decoded up to half the minimum distance efficiently. Using a result of Kumar et al. (2016), we show that these codes achieve the capacity of the binary erasure channel (BEC) under bit-MAP decoding. Furthermore, except double transitivity, they satisfy all the code properties used by Reeves and Pfister to show that RM codes achieve the capacity of binary-input memoryless symmetric channels. Finally, when n is odd, we identify a large class of abelian codes that includes $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$ and which achieves BEC capacity.

Index Terms

Abelian codes, binary erasure channel, capacity, Plotkin construction, Reed-Muller codes.

This paper was presented in parts at the 2022 IEEE International Symposium on Information Theory (ISIT 2022), and the 2022 National Conference on Communications (NCC 2022).

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).

CONTENTS

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

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

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

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

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 $\mathrm{RM}(r,m)^\perp = \mathrm{RM}(m-r-1,m)$, respectively. Indeed, we will 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*. Naturally, we are interested in the capacity achievability of the code families $\{\mathcal{C}_n(r,m)\}$ and $\{\mathcal{B}_n(r,m)\}$. We show that these codes achieve the capacity of the BEC under bit-MAP decoding, using a technique based on code automorphisms developed in [7] (which does not require double transitivity, which was used in [3], [4]). We also present a few simulation results that illustrate the performance of these codes, in comparison with RM codes in the BEC.

For the case of n being odd, we use a discrete Fourier transform (DFT) based framework to study the codes $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$ as abelian codes, i.e., as ideals of a group algebra $\mathbb{F}_2[G^m]$, where G is any abelian group with n elements. We also identify a large class of abelian codes, which includes the families $\{\mathcal{C}_n(r,m) : n \text{ odd}\}$ and $\{\mathcal{B}_n(r,m) : n \text{ odd}\}$, that achieves the BEC capacity. Fig. 1 shows the relationship between the code family $\{\mathcal{C}_n(r,m)\}$ presented in this work, the RM codes, the class of capacity achieving abelian codes (obtained in Theorem IV.3 of this work), and their capacity achieving nature.

A. Similarity with Reed-Muller Codes

For $n \geq 3$, the similarity of $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$ with RM codes runs deep. The likeness to RM codes was noted by Blackmore and Norton [6] for the case n being an odd prime. In the current work,

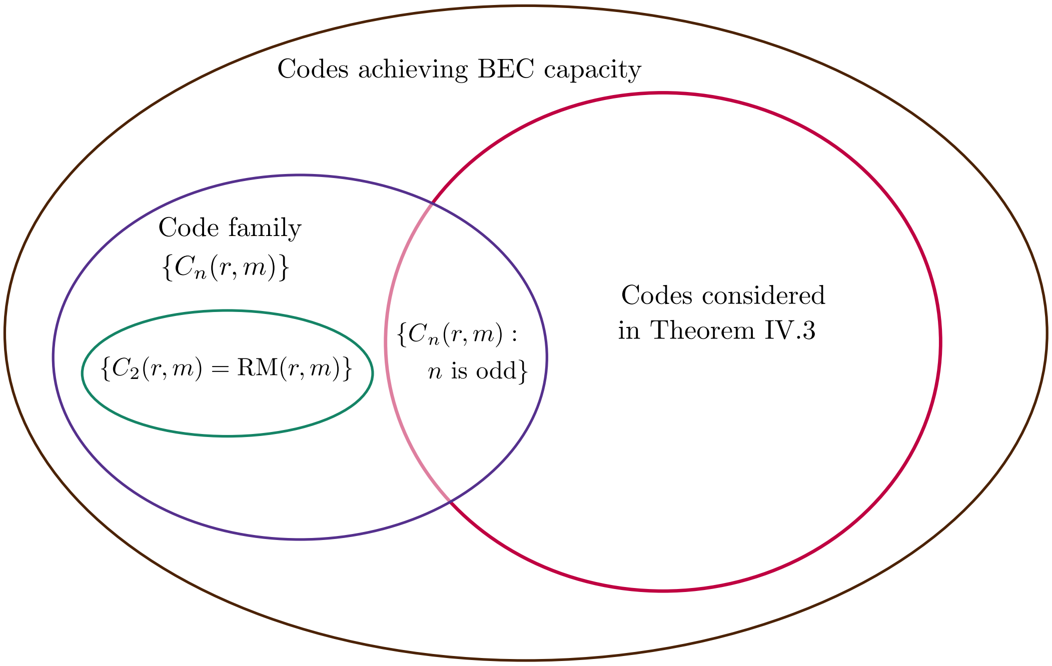

Fig. 1. The picture shows the relationship between the code family $\{\mathcal{C}_n(r,m)\}$ presented in this work, the codes considered in Theorem IV.3, and the Reed-Muller Codes. A similar picture holds for the code family $\{\mathcal{B}_n(r,m)\}$ which are dual to $\mathcal{C}_n(r,m)$. All the codes shown in the picture are capacity achieving for the BEC under bit-MAP decoding.

we define the Berman and dual Berman codes using a recursive construction similar to the $(\boldsymbol{u}\,|\,\boldsymbol{u}+\boldsymbol{v})$ Plotkin construction, and we show that their puncturing properties are similar to RM codes, they have a rich automorphism group (although they are not doubly transitive), they are generated by their minimum weight codewords, and that they can be decoded up to half the minimum distance efficiently. Furthermore, except double transitivity, Berman and dual Berman codes satisfy all the properties of RM codes exploited by Reeves and Pfister [4] to show that RM codes achieve the capacity of BMS channels.

There are also 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. The lack of double transitivity has been mentioned already. When $n \geq 3$, 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 its duals have $\frac{r}{m} \approx \frac{(n-1)}{n}$ (please see the discussion in Section III-B leading to (13)). 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 the block length.

B. Overview of the Main Results and Organization

We now summarize the main results and the organization of the present work (please see Table I).

Section II. We define $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$ recursively using an n-fold generalization of the Plotkin construction. We then identify the basic parameters of these codes, including the dimension and the minimum distance, and identify generator and parity-check matrices that are composed of minimum weight codewords of the respective codes. We also identify patterned bases for $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$, using which we then identify some automorphisms of these codes. These automorphisms will be later used in Section III to prove capacity achievability in the BEC. We then present recursive decoders, which

TABLE I
ORGANIZATION OF THIS PAPER.

Section	Title
II	**Berman Codes and their Duals**
II-A	Recursive Definition of Berman & Dual Berman Codes
II-B	Dimension and Duality
II-C	Minimum Distance
II-D	Bases for $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$
II-E	Some Useful Automorphisms of the Codes $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$
II-F	Recursive Decoding
III	**Capacity-Related Properties**
III-A	Puncturing $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$
III-B	Rate of $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$
III-C	Lack of Double Transitivity
III-D	Achieving the BEC Capacity
IV	**Constructions via Discrete Fourier Transform**
IV-A	Background
IV-B	Preliminary Results
IV-C	Construction of $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$ via DFT
IV-D	A Family of Abelian Codes that Achieve BEC Capacity
V	**Simulation Results**
VI	**Discussion**

are similar to the known decoders for RM codes [8]–[10], for correcting errors up to half the minimum distance.

Section III. We focus on the code properties that Reeves and Pfister [4] relied on to prove that RM codes achieve BMS channel capacity. We show that there are multiple ways to puncture a Berman (or a dual Berman) code to a shorter length Berman (dual Berman) code (Section III-A), and that the rate change due to this puncturing is small (Section III-B). Although these codes are not doubly transitive (Section III-C) we are able to show that they achieve BEC capacity (Section III-D) based on a condition on automorphisms identified by Kumar et al. [7].

Section IV. In this section we exclusively consider the case where $n \geq 3$ is an odd integer. We use the theory of abelian codes in semi-simple group algebras [5], [11]–[14] to construct Berman and dual Berman codes as ideals in appropriately chosen group algebras. Our primary tool in this section is Rajan and Siddiqi's characterization of abelian codes [14] based on the discrete Fourier transform (DFT). We begin this section with a review of abelian codes and DFT, and then introduce a convenient notation and present some results to work with the DFT for the group algebra $\mathbb{F}_2[G^m]$, where G is an abelian group of order n. We then construct Berman codes and their duals as abelian codes and show that this construction is equivalent to our original recursive definition of these codes when n is odd. In Appendix II we show that the special case n being an odd prime coincides with the codes studied by Berman [5] and Blackmore and Norton [6]. For all odd n, we then identify a large family of abelian codes, that includes $\{\mathcal{B}_n(r,m) : n \text{ odd}\}$ and $\{\mathcal{C}_n(r,m) : n \text{ odd}\}$, which achieves BEC capacity under bit-MAP decoding.

Section V. We present a few simulation results comparing the codes identified in this work with RM codes in the BEC. While these simulations are in no way exhaustive, we observe that in the simulation scenarios presented here the bit erasure rates (under bit-MAP decoding) of Berman code and its dual are similar to those of RM codes of comparable rate and block length, while their block erasure rates (under block-MAP decoding) are relatively worse.

We conclude this work in Section VI. The proofs of some of the technical results have been moved to

Appendix I.

Notation: For any positive integer ℓ, let $[\![\ell]\!]$ denote the set $\{0, 1, \ldots, \ell-1\}$. Let $\mathbb{Z}_\ell = [\![\ell]\!]$ be the ring where addition and multiplication are performed modulo ℓ. The binary field is $\mathbb{F}_2 = \{0, 1\}$. The empty set is $\varnothing$. For sets A, B we define $A \setminus B = \{a \in A \mid a \notin B\}$. The notation $\mathbf{0}$ denotes a zero-vector or a zero-matrix of appropriate size. We denote the identity matrix of size n by $\boldsymbol{I}_n$. For two vectors $\boldsymbol{a}, \boldsymbol{b}$, their concatenation is denoted by $(\boldsymbol{a}|\boldsymbol{b})$. The dimension of a code $\mathcal{C}$ is denoted by $\dim(\mathcal{C})$. The Hamming weight of a vector $\boldsymbol{a}$ is denoted by $w_H(\boldsymbol{a})$. The minimum distance of a code $\mathcal{C}$ is denoted by $d_{\min}(\mathcal{C})$. The binomial coefficient $\binom{n}{k}$ is assumed to be 0 if $k > n$ or if $k < 0$. We denote an n-length vector $\boldsymbol{a}$ by its components as $\boldsymbol{a} = (a_i : i \in [\![n]\!])$. All vectors are row vectors, unless otherwise stated. The notation $(.)^T$ denotes the transpose operator. 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 $a_{l,i} : i \in [\![n^{m-1}]\!]$. For any integer $m \geq 1$, the group of all permutations on $[\![m]\!]$ is denoted as $\mathcal{S}_m$.

II. Berman Codes and their Duals

A class of abelian group codes was originally studied by Berman in [5], [15] using a group algebra framework. These codes include the Reed-Muller codes as a special case. We now present a recursive construction of a large class of binary codes of length n^m (for some integers n, m), which includes the class of the Berman codes. Following this precedence, we continue to call our codes as Berman codes (and their duals). The recursive construction we present for our codes is inspired from the Plotkin $(\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v})$ construction: the Plotkin construction involves a two-fold extension, the construction we present generalizes this (in a sense) to an n-fold extension for arbitrary n. More general Plotkin-like constructions have been studied in the past in [16], [17], in which the resultant codes are called *matrix-product codes*. In the present work, our focus is on a particular Plotkin-like recursive construction that yields the Berman and dual Berman codes. We present a broad set of results for these codes, including their essential properties, automorphism groups, efficient decoding algorithms up to half the minimum distance, and their capacity achieving nature for the BEC channel.

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 $\mathcal{B}_n(r, m) \subset \mathbb{F}_2^{n^m}$ recursively as follows.

$$\mathcal{B}_n(m, m) \triangleq \{\mathbf{0} \in \mathbb{F}_2^{n^m}\}.$$

$$\mathcal{B}_n(0, m) \triangleq \{\boldsymbol{c} \in \mathbb{F}_2^{n^m} : \sum_i c_i = 0\} \quad \text{(The single parity-check code of length } n^m\text{)}.$$

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 $\mathcal{C}_n(r, m) \subset \mathbb{F}_2^{n^m}$ recursively.

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

$$\mathcal{C}_n(0,m) \triangleq \{(c,\ldots,c) \in \mathbb{F}_2^{n^m} : c \in \mathbb{F}_2\} \quad \text{(The repetition code of length } n^m\text{)}.$$

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 Section II-B, where we shall prove 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 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. Later, in Section IV, we will also show that when n is an odd prime, the code $\mathcal{B}_n(r,m)$ is identical to the code designed by Berman in [5], and $\mathcal{C}_n(r,m)$ is its dual code studied by Blackmore and Norton in [6].

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

- For $n=3, m=1, r=0$, the code $\mathcal{B}_3(0,1) = \{(v_0|v_1|v_0+v_1) : v_0, v_1 \in \mathbb{F}_2\}$ is the single parity-check code of length 3 and $\mathcal{C}_3(0,1) = \{(u|u|u) : u \in \mathbb{F}_2\}$ is its dual, the repetition code of length 3.
- 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 $n=3, m=2, r=1$,

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

- 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 $\mathcal{B}_3(1,2)$.

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

□

It is clear that the codes $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$ are linear. We shall now obtain various properties of these codes. The techniques involved in the proofs 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. In contrast, our approach is based on the recursive construction of these codes. The following lemma is key to the remaining results in this section.

Lemma II.1. *For* $1 \leq r \leq m$,

1) $\mathcal{B}_n(r,m) \subset \mathcal{B}_n(r-1,m)$.
2) $\mathcal{C}_n(r-1,m) \subset \mathcal{C}_n(r,m)$.

Proof: We prove this via induction on m.

Part 1): First, we observe that the statements are true by definition for $m=1$. We now prove the statements are true for $m \geq 2$ assuming they are true for $m-1$. Consider an arbitrary codeword of $\mathcal{B}_n(r,m)$ in its concatenation representation $\boldsymbol{v} = (\boldsymbol{v}_0|\boldsymbol{v}_1|\ldots|\boldsymbol{v}_{n-1})$, where the components of $\boldsymbol{v}_l$ are given as $v_{l,i} : i \in [\![n^{m-1}]\!]$. For each $l \in [\![n]\!]$, by definition $\boldsymbol{v}_l \in \mathcal{B}_n(r-1,m-1)$. Now consider the case $r=1$. Then

$\boldsymbol{v}_l \in \mathcal{B}_n(0, m-1)$. Thus $\sum_{i\in[\![n^{m-1}]\!]} v_{l,i} = 0, \forall l \in [\![n]\!]$. And hence, $\sum_{i\in[\![n^m]\!]} v_i = \sum_{l\in[\![n]\!]}\sum_{i\in[\![n^{m-1}]\!]} v_{l,i} = 0$, which means $\boldsymbol{v} \in \mathcal{B}_n(0, m)$, hence proving the statement for $r = 1$ for any m.

Now suppose $r \geq 2$. Then, by induction $\mathcal{B}_n(r-1, m-1) \subset \mathcal{B}_n(r-2, m-1)$, thus $\boldsymbol{v}_l \in \mathcal{B}_n(r-2, m-1)$. Further, $\sum_{l\in[\![n]\!]} \boldsymbol{v}_l \in \mathcal{B}_n(r, m-1)$ by definition, and $\mathcal{B}_n(r, m-1) \subset \mathcal{B}_n(r-1, m-1)$ by induction. Hence $\sum_{l\in[\![n]\!]} \boldsymbol{v}_l \in \mathcal{B}_n(r-1, m-1)$. Thus, the codeword $\boldsymbol{v}$ satisfies the two conditions in the definition to be a codeword of $\mathcal{B}_n(r-1, m)$ which completes the proof for Part 1.

Part 2): The statement is true for $m = 1$ by definition. We now prove for $m \geq 2$ assuming the statement is true for $m - 1$.

Suppose $r = 1$. Then, using $\boldsymbol{u}_l = \boldsymbol{0}, \forall l \in [\![n-1]\!]$ in the codewords of $\mathcal{C}_n(1, m)$ gives the codewords of $\mathcal{C}_n(0, m)$. Thus the statement is true also for $r = 1$ with any value of $m \geq 2$.

Now suppose $r \geq 2$. Consider an arbitrary codeword $\boldsymbol{u}' = (\boldsymbol{u}+\boldsymbol{u}_0|\boldsymbol{u}+\boldsymbol{u}_1|\ldots|\boldsymbol{u}+\boldsymbol{u}_{n-2}|\boldsymbol{u})$ in $\mathcal{C}_n(r-1, m)$. Then $\boldsymbol{u} \in \mathcal{C}_n(r-1, m-1)$ by definition and $\mathcal{C}_n(r-1, m-1) \subset \mathcal{C}_n(r, m-1)$ by induction, which means $\boldsymbol{u} \in \mathcal{C}_n(r, m-1)$. Similarly we can show $\boldsymbol{u}_l \in \mathcal{C}_n(r-2, m-1) \subset \mathcal{C}_n(r-1, m-1)$. Thus we have shown that $\boldsymbol{u}' \in \mathcal{C}_n(r, m)$ as it satisfies both conditions in the definition of $\mathcal{C}_n(r, m)$. This completes the proof of Part 2. ■

B. Dimension and Duality

We obtain the dimension of the two codes and show that they are duals of each other.

Lemma II.2.

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

Proof: It is straightforward to verify the statements for $m = 1$. We now prove the statements for $m \geq 2$ assuming it is true for $m-1$. We mainly use the two combinatorial identities : $n^m = \sum_{w=0}^{m}\binom{m}{w}(n-1)^w$, and $\binom{m-1}{w-1} + \binom{m-1}{w} = \binom{m}{w}, \forall w$.

Part 1). Again, the statements are easy to verify for $r = 0, m$. Hence we assume $1 \leq r \leq m-1$. We first see that an equivalent description for $\mathcal{B}_n(r, m)$ is given by

$$\mathcal{B}_n(r, m) \triangleq \left\{ (\boldsymbol{v}_0|\boldsymbol{v}_1|\ldots|\boldsymbol{v}_{n-2}|\sum_{l\in[\![n-1]\!]} \boldsymbol{v}_l + \boldsymbol{v}) \colon \boldsymbol{v}_l \in \mathcal{B}_n(r-1, m-1), \boldsymbol{v} \in \mathcal{B}_n(r, m-1) \right\}. \tag{3}$$

From the description in (3), we see that

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

which proves part 1).

Part 2): We observe that the statements are easy to verify for $m = 1$ and for any m with $r = 0, m$. Hence we consider $m \geq 2$ and $1 \leq r \leq m-1$, and proceed by induction.

$$\begin{aligned}\dim(\mathcal{C}_n(r,m)) &= (n-1)\dim(\mathcal{C}_n(r-1,m-1)) + \dim(\mathcal{C}_n(r,m-1)) \\ &= (n-1)\sum_{w=0}^{r-1}\binom{m-1}{w}(n-1)^w + \sum_{w=0}^{r}\binom{m-1}{w}(n-1)^w \\ &= \sum_{w=1}^{r}\binom{m-1}{w-1}(n-1)^w + \sum_{w=0}^{r}\binom{m-1}{w}(n-1)^w \\ &= \sum_{w=0}^{r}\binom{m}{w}(n-1)^w,\end{aligned}$$

which completes the proof of Part 2). ■

We now confirm that the codes $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$ are dual to each other.

Lemma II.3. $\mathcal{C}_n(r,m)^\perp = \mathcal{B}_n(r,m)$.

Proof: The statement holds by definition for $r = 0, m$ (for any value of m) and thus for $m = 1$ (for $r \leq 1$). Hence we now prove the statement for $m \geq 2$ and $1 \leq r \leq m-1$, assuming it is true for $m-1$.

Let $\boldsymbol{v} = (\boldsymbol{v}_0|\boldsymbol{v}_1|\ldots|\boldsymbol{v}_{n-1})$ and $\boldsymbol{u}' = (\boldsymbol{u}+\boldsymbol{u}_0|\boldsymbol{u}+\boldsymbol{u}_1|\ldots|\boldsymbol{u}+\boldsymbol{u}_{n-2}|\boldsymbol{u})$ be any two codewords in the respective codes $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$. Taking their dot product we get,

$$\boldsymbol{u}'\boldsymbol{v}^T = \sum_{l\in[\![n-1]\!]}\boldsymbol{u}_l\boldsymbol{v}_l^T + \boldsymbol{u}\left(\sum_{l\in[\![n]\!]}\boldsymbol{v}_l\right)^T.$$

Since by the definition of the codes we have $\boldsymbol{u}_l \in \mathcal{C}_n(r-1,m-1)$ and $\boldsymbol{v}_l \in \mathcal{B}_n(r-1,m-1)$, and further $\sum_{l\in[\![n]\!]}\boldsymbol{v}_l \in \mathcal{B}_n(r,m-1)$ and $\boldsymbol{u} \in \mathcal{C}_n(r,m-1)$, by the induction hypothesis we see that $\boldsymbol{u}'\boldsymbol{v}^T = 0$. Thus, we have $\mathcal{B}_n(r,m) \subset \mathcal{C}_n(r,m)^\perp$. Equality follows by observing that $\dim(\mathcal{C}_n(r,m)) = n^m - \dim(\mathcal{B}_n(r,m))$, from Lemma II.2. ■

C. Minimum Distance

We now obtain the minimum distance of the two codes.

Lemma II.4. *The minimum distance $d_{\min}$ of the two codes are as follows.*

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

Proof: The claims are straightforward for $r = 0, m$ and thus for $m = 1$. We proceed to prove the claims for $m \geq 2$ and $1 \leq r \leq m-1$ assuming they are true for $m-1$.

Part 1): Consider an arbitrary non-zero codeword of $\mathcal{B}_n(r,m)$ given by $\boldsymbol{v} = (\boldsymbol{v}_0|\boldsymbol{v}_1|\ldots|\boldsymbol{v}_{n-1})$. We consider two cases.

Case (a): *At least two of the $\boldsymbol{v}_l$'s are non-zero.* Then $w_H(\boldsymbol{v}) \geq 2d_{\min}(\mathcal{B}_n(r-1,m-1)) = 2^{r+1}$ (by induction). Further, there is a codeword $(\boldsymbol{a}|\boldsymbol{a}|\boldsymbol{0}|\ldots|\boldsymbol{0}) \in \mathcal{B}_n(r,m)$, where $\boldsymbol{a}$ is any arbitrary non-zero codeword in $\mathcal{B}_n(r-1,m-1)$ of weight 2^r, which has weight precisely 2^{r+1}.

Case (b): *Exactly one of the $\boldsymbol{v}_l$'s (say $\boldsymbol{v}_0$) is non-zero.* Then clearly $\boldsymbol{v}_0 \in \mathcal{B}_n(r,m-1)$ by definition of the code. This would mean that $r \leq m-2$, as $\mathcal{B}_n(m-1,m-1)$ contains only $\boldsymbol{0}$. Thus, $w_H(\boldsymbol{v}) = w_H(\boldsymbol{v}_0) \geq d_{\min}(\mathcal{B}_n(r,m-1)) = 2^{r+1}$ (by induction).

The two cases are exhaustive, and thus the proof of Part 1) is completed.

$$G_n(r,m) \triangleq \begin{pmatrix} G_n(r-1,m-1) & \mathbf{0} & \dots & \mathbf{0} & G_n(r-1,m-1) \\ \mathbf{0} & G_n(r-1,m-1) & \dots & \mathbf{0} & G_n(r-1,m-1) \\ \mathbf{0} & \mathbf{0} & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & G_n(r-1,m-1) & G_n(r-1,m-1) \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & G_n(r,m-1) \end{pmatrix}. \quad (4)$$

$$H_n(r,m) \triangleq \begin{pmatrix} H_n(r-1,m-1) & \mathbf{0} & \dots & \dots & \mathbf{0} \\ \mathbf{0} & H_n(r-1,m-1) & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & H_n(r-1,m-1) & \mathbf{0} \\ H_n(r,m-1) & H_n(r,m-1) & \dots & H_n(r,m-1) & H_n(r,m-1) \end{pmatrix}. \quad (5)$$

Part 2): Consider an arbitrary non-zero codeword $\boldsymbol{u}' = (\boldsymbol{u}+\boldsymbol{u}_0|\boldsymbol{u}+\boldsymbol{u}_1|\dots|\boldsymbol{u}+\boldsymbol{u}_{n-2}|\boldsymbol{u}) \in \mathcal{C}_n(r,m)$, where $\boldsymbol{u}_l \in \mathcal{C}_n(r-1,m-1)$ and $\boldsymbol{u} \in \mathcal{C}_n(r,m-1)$. Recall from Lemma II.1 that $\mathcal{C}_n(r-1,m-1) \subset \mathcal{C}_n(r,m-1)$. We consider two cases.

Case (a): *In this case,* $\boldsymbol{u} \in \mathcal{C}_n(r-1,m-1)$. In this case if $\boldsymbol{u} = \mathbf{0}$, then at least one of $\boldsymbol{u}_l \neq \mathbf{0}$. Thus at least one subvector, say $\boldsymbol{u}_0$, of $\boldsymbol{u}'$ is non-zero in $\mathcal{C}_n(r-1,m-1)$. Thus $w_H(\boldsymbol{u}') \geq w_H(\boldsymbol{u}_0) \geq d_{\min}(\mathcal{C}_n(r-1,m-1)) = n^{m-r}$ (by induction). Further the codeword $(\boldsymbol{u}_0|\mathbf{0}|\dots|\mathbf{0}) \in \mathcal{C}_n(r,m)$ where $\boldsymbol{u}_0$ is a minimum weight non-zero codeword in $\mathcal{C}_n(r-1,m-1)$ has weight precisely n^{m-r}.

Case (b): *In this case,* $\boldsymbol{u} \in \mathcal{C}_n(r,m-1) \setminus \mathcal{C}_n(r-1,m-1)$. Then each subvector $\boldsymbol{u}+\boldsymbol{u}_l \in \mathcal{C}_n(r,m-1) \setminus \mathcal{C}_n(r-1,m-1)$ as well. Then $w_H(\boldsymbol{u}') \geq n d_{\min}(\mathcal{C}_n(r,m-1)) = n^{m-r}$ (by induction).

This completes the proof of Part 2) and hence the lemma. ■

D. Bases for $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$

We identify two sets of bases, each for $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$. While the first basis follows naturally from the recursive construction of these codes and consists of minimum weight codewords, the second basis illustrates the combinatorial structure of these codes and is helpful in identifying code automorphisms.

1) Natural Minimum Weight Basis: We define recursively a generator matrix $G_n(r,m)$ for $\mathcal{B}_n(r,m)$ as follows. If $r=m$, we have nothing to define. For $r=0$, we define

$$G_n(0,m) \triangleq \left(\begin{array}{c|c} 1 & \\ 1 & \boldsymbol{I}_{n^m-1} \\ \vdots & \\ 1 & \end{array}\right).$$

For $1 \leq r \leq m-1$, we define $G_n(r,m)$ recursively as in (4). Note that, if $r=m-1$, then the last set of rows of (4) corresponding to $G_n(r,m-1)$ are absent. It is not difficult to show using (3) that the matrix $G_n(r,m)$ (for $1 \leq r \leq m-1$) defined above generates the code $\mathcal{B}_n(r,m)$.

We similarly define the generator matrix $H_n(r,m)$ for $\mathcal{C}_n(r,m)$. We define

$$H_n(0,m) \triangleq \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}, \text{(all-one vector of length } n^m)$$
$$H_n(m,m) \triangleq \boldsymbol{I}_{n^m},$$

and for $1 \leq r \leq m-1$, $H_n(r,m)$ is defined in (5). Again, using the definition of $\mathcal{C}_n(r,m)$, it is easy to verify the matrix $H_n(r,m)$ generates the code $\mathcal{C}_n(r,m)$, for $0 \leq r \leq m$.

Finally, by the recursive construction, we have the following result regarding the rows of $G_n(r,m)$ and $H_n(r,m)$.

Lemma II.5. *For $0 \le r \le m-1$, each row of the matrix $G_n(r,m)$ (respectively, $H_n(r,m)$) is a minimum weight codeword of $\mathcal{B}_n(r,m)$ (respectively, $\mathcal{C}_n(r,m)$).*

Proof: The proof follows by observing that $G_n(0,m)$ has minimum weight ($=2$) codewords of $\mathcal{B}_n(0,m)$ as its rows, and by applying the recursive construction in (4).

The argument for $H_n(r,m)$ is similar, as our recursive construction depends on $H_n(0,m)$ and $H_n(m,m)$ as the base cases, both of which have minimum weight codewords of the respective codes as their rows. ∎

2) A Patterned Basis for Berman and Dual Berman Codes: In this part of the present sub-section, we show Lemma II.6 and Lemma II.7, which give another basis for $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$ respectively. These results further reveal the strong combinatorial structure of the respective codes. Also, we shall use the basis from Lemma II.6 to obtain some automorphisms of the codes described in this work, in Section II-E. Towards stating the lemma, we 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 identified recursively 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 $(\boldsymbol{i}' \,|\, l) \in G^m$.

Observe that the concatenation representation can be used recursively, for instance the subvector $\boldsymbol{v}_l \in \mathbb{F}_2^{n^{m-1}}$ can be written as a concatenation of n subvectors from $\mathbb{F}_2^{n^{m-2}}$, and so on.

Let us denote the support of a vector $\boldsymbol{i} \in G^m$ as $\mathsf{supp}(\boldsymbol{i}) = \{k \in [\![m]\!] : i_k \neq 0\}$. The weight or the Hamming weight of $\boldsymbol{i}$ is $w_H(\boldsymbol{i}) = |\mathsf{supp}(\boldsymbol{i})|$. We now define a partial ordering among the vectors in G^m. For $\boldsymbol{i},\boldsymbol{j} \in G^m$ we will say that '$\boldsymbol{i}$ contains $\boldsymbol{j}$', or equivalently, '$\boldsymbol{j}$ is contained in $\boldsymbol{i}$' if

$$\mathsf{supp}(\boldsymbol{j}) \subset \mathsf{supp}(\boldsymbol{i}) \text{ and } \boldsymbol{j}_{\mathsf{supp}(\boldsymbol{j})} = \boldsymbol{i}_{\mathsf{supp}(j)}.$$

That is, $\boldsymbol{i}$ contains $\boldsymbol{j}$ if for each $k \in [\![m]\!]$ we have $j_k = 0$ or $j_k = i_k$. We will denote this relation as $\boldsymbol{i} \succeq \boldsymbol{j}$ or $\boldsymbol{j} \preceq \boldsymbol{i}$. Note that for any $\boldsymbol{i} \in G^m$ there are exactly $2^{w_H(\boldsymbol{i})}$ vectors contained by $\boldsymbol{i}$, and exactly $n^{m-w_H(\boldsymbol{i})}$ vectors that contain $\boldsymbol{i}$.

We also need the following definition of a patterned-vector in $\mathbb{F}_2^{n^m}$, which will be used to show a basis for $\mathcal{B}_n(r,m)$. For $m \ge 1$ and some $\boldsymbol{i}' \in G^m$, define the vector $\boldsymbol{c}_m(\boldsymbol{i}') \in \mathbb{F}_2^{n^m}$ as the binary vector with support set $\{\boldsymbol{i} \in G^m : \boldsymbol{i} \preceq \boldsymbol{i}'\}$. That is, the n^m components of $\boldsymbol{c}_m(\boldsymbol{i}')$ are

$$c_m(\boldsymbol{i}')_{\boldsymbol{i}} = \begin{cases} 1 & \text{if } \boldsymbol{i} \preceq \boldsymbol{i}', \\ 0 & \text{otherwise,} \end{cases} \qquad \forall \boldsymbol{i} \in G^m.$$

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.

$$c_3(\boldsymbol{i}')_{\boldsymbol{i}} = \begin{cases} 1 & \text{for } \boldsymbol{i} \in \{(0,0,0),(1,0,0),(0,2,0),(1,2,0)\}, \\ 0 & \text{otherwise.} \end{cases}$$

□

We are now ready to show a patterned basis for $\mathcal{B}_n(r,m)$.

Lemma II.6. *For $m \ge 1$, and $0 \le r \le m-1$, consider the collection of elements in $\mathbb{F}_2^{n^m}$ given by*

$$B_{\mathcal{B}_n}(r,m) = \{\boldsymbol{c}_m(\boldsymbol{i}') \colon \forall \boldsymbol{i}' \in G^m \text{ such that } r+1 \le w_H(\boldsymbol{i}') \le m\}. \tag{6}$$

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 $B' \subset B_{\mathcal{B}_n}(r,m)$.

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 $\mathsf{supp}(\boldsymbol{i}_d) \subset \mathsf{supp}(\boldsymbol{i}')$ 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 $\boldsymbol{i}_d^{\text{th}}$ 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 Lemma II.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 two 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.6 shows that the following collection of 20 vectors is a basis.

$$B_{\mathcal{B}_3}(1,3) = \bigcup_{a,b,c \in \{1,2\}} \Big\{ \boldsymbol{c}_3((a,b,0)), \boldsymbol{c}_3((0,a,b)), \boldsymbol{c}_3((a,0,b)), \boldsymbol{c}_3((a,b,c)) \Big\}.$$

□

We now show a basis for the dual Berman code. We need a few more notations for the rest of this sub-section. For any $\boldsymbol{i}' \in G^m$ define $\boldsymbol{d}_m(\boldsymbol{i}') \in \mathbb{F}_2^{n^m}$ as the vector with support $\{\boldsymbol{i} \in G^m : \boldsymbol{i} \succeq \boldsymbol{i}'\}$. That is, the components of $\boldsymbol{d}_m(\boldsymbol{i}')$ are

$$d_m(\boldsymbol{i}')_{\boldsymbol{i}} = \begin{cases} 1 & \text{if } \boldsymbol{i} \succeq \boldsymbol{i}' \\ 0 & \text{otherwise.} \end{cases}$$

Lemma II.7. *Consider the collection of elements in $\mathbb{F}_2^{n^m}$ given by*

$$B_{\mathcal{C}_n}(r,m) = \left\{ \boldsymbol{d}_m(\boldsymbol{i}') : \boldsymbol{i}' \in G^m \text{ and } w_H(\boldsymbol{i}') \leq r \right\}. \tag{7}$$

The collection $B_{\mathcal{C}_n}(r,m)$ is a basis for $\mathcal{C}_n(r,m)$.

Proof. We first note that $|B_{\mathcal{C}_n}(r,m)| = \sum_{w=0}^{r}\binom{m}{w}(n-1)^w = \dim(\mathcal{C}_n(r,m))$. We now show that the vectors in $B_{\mathcal{C}_n}(r,m)$ are linearly independent. To do this, we show that the sum of vectors in any non-empty subset $B' \subset B_{\mathcal{C}_n}(r,m)$ is non-zero.

Let $\boldsymbol{d}_m(\boldsymbol{i}_d) \in B'$ be such that for any $\boldsymbol{d}_m(\boldsymbol{i}') \in B'$ we have $w_H(\boldsymbol{i}_d) \le w_H(\boldsymbol{i}')$. Note that for any non-empty B' such a minimal element $\boldsymbol{i}_d$ exists. Now suppose that the $\boldsymbol{i}_d^{\text{th}}$ component of $\boldsymbol{d}_m(\boldsymbol{i}') \in B'$ is equal to 1. This implies $\boldsymbol{i}_d \succeq \boldsymbol{i}'$ and $w_H(\boldsymbol{i}_d) \ge w_H(\boldsymbol{i})$. By the minimality of $\boldsymbol{i}_d$, we have $\boldsymbol{i}' = \boldsymbol{i}_d$. Thus, the only vector in B' whose $\boldsymbol{i}_d^{\text{th}}$ component is non-zero is $\boldsymbol{d}_m(\boldsymbol{i}_d)$. Hence, the sum of the vectors in B' is non-zero. This implies that $B_{\mathcal{C}_n}(r,m)$ is linearly independent.

We now show that $B_{\mathcal{C}_n}(r,m) \subset \mathcal{C}_n(r,m)$. Firstly, it is straightforward to check that the statement holds for $r = 0, m$ for any m. Thus, the statement is also true for $m = 1$. Now we will prove the statement for $m \ge 2$ for $1 \le r \le m-1$. Let $\boldsymbol{d}_m(\boldsymbol{i}') \in B_{\mathcal{C}_n}(r,m)$. We will use the concatenation representation $\boldsymbol{d}_m(\boldsymbol{i}') = (\boldsymbol{d}_0|\cdots|\boldsymbol{d}_{n-1})$, where $\boldsymbol{d}_l \in \mathbb{F}_2^{n^{m-1}}$ for all $l \in [\![m]\!]$. We consider two cases.

Case (a): $i'_{m-1} = 0$. In this case, note that for any $\boldsymbol{j} \in G^m$ we have $\boldsymbol{j} \succeq \boldsymbol{i}'$ if and only if $\boldsymbol{j}_{[\![m-1]\!]} \succeq \boldsymbol{i'}_{[\![m-1]\!]}$. Hence,

$$d_m(\boldsymbol{i}')_{\boldsymbol{j}} = \begin{cases} 1 & \text{if } \boldsymbol{j}_{[\![m-1]\!]} \succeq \boldsymbol{i'}_{[\![m-1]\!]}, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, we observe that $\boldsymbol{d}_l = \boldsymbol{d}_{m-1}\left(\boldsymbol{i}'_{[\![m-1]\!]}\right)$ for all $l \in [\![n]\!]$. Since $i'_{m-1} = 0$, we have $w_H(\boldsymbol{i}'_{[\![m-1]\!]}) \le r$. By induction hypothesis we have $\boldsymbol{d}_0 = \cdots = \boldsymbol{d}_{n-1} \in \mathcal{C}_n(r, m-1)$. Thus, $\boldsymbol{d}_m(\boldsymbol{i}')$ satisfies the properties of a codeword of $\mathcal{C}_n(r,m)$.

Case (b): $i'_{m-1} = l' \in G \setminus \{0\}$. In this case we have

$$d_m(\boldsymbol{i}')_{\boldsymbol{j}} = \begin{cases} 1 & \text{if } \boldsymbol{j}_{[\![m-1]\!]} \succeq \boldsymbol{i'}_{[\![m-1]\!]} \text{ and } j_{m-1} = l', \\ 0 & \text{otherwise.} \end{cases}$$

This implies that $\boldsymbol{d}_l = 0$ for all $l \ne l'$, and $\boldsymbol{d}_{l'} = \boldsymbol{d}_{m-1}(\boldsymbol{i}'_{[\![m-1]\!]})$. Since $i'_{m-1} \ne 0$, we have $w_H(\boldsymbol{i}'_{[\![m-1]\!]}) \le r-1$. Hence, by induction hypothesis, $\boldsymbol{d}_{l'} = \boldsymbol{d}_{m-1}(\boldsymbol{i}'_{[\![m-1]\!]}) \in \mathcal{C}_n(r-1, m-1)$. Clearly, $\boldsymbol{d}_m(\boldsymbol{i}')$ satisfies the properties of a codeword in $\mathcal{C}_n(r,m)$. This concludes the proof. ∎

The bases presented in Lemmas II.6 and II.7 for the Berman code and its dual are related to each other, and arise as rows and columns, respectively, of a single $n^m \times n^m$ binary matrix. To see this, note that for any choice of $\boldsymbol{i}, \boldsymbol{j} \in G^m$, the $\boldsymbol{j}^{\text{th}}$ component of the vector $\boldsymbol{c}_m(\boldsymbol{i})$ has value $c_m(\boldsymbol{i})_{\boldsymbol{j}} = 1$ if and only if $\boldsymbol{j} \preceq \boldsymbol{i}$. Again, the $\boldsymbol{i}^{\text{th}}$ component of $\boldsymbol{d}_m(\boldsymbol{j})$ is equal to 1 if and only if $\boldsymbol{j} \preceq \boldsymbol{i}$. Hence, we have

$$c_m(\boldsymbol{i})_{\boldsymbol{j}} = d_m(\boldsymbol{j})_{\boldsymbol{i}} = \begin{cases} 1, & \text{if } \boldsymbol{j} \preceq \boldsymbol{i}, \\ 0, & \text{otherwise} \end{cases}, \qquad \text{for all } \boldsymbol{i}, \boldsymbol{j} \in G^m.$$

This observation leads us to define a binary $n^m \times n^m$ matrix $\boldsymbol{A}_m = [A_m(\boldsymbol{i},\boldsymbol{j})]$ whose rows and columns are indexed by tuples from G^m, with its entry in row $\boldsymbol{i}$ and column $\boldsymbol{j}$ defined as

$$A_m(\boldsymbol{i},\boldsymbol{j}) = \begin{cases} 1, & \text{if } \boldsymbol{j} \preceq \boldsymbol{i}, \\ 0, & \text{otherwise} \end{cases}.$$

We see that $\boldsymbol{c}_m(\boldsymbol{i})$ is the $\boldsymbol{i}^{\text{th}}$ row of $\boldsymbol{A}_m$ and $\boldsymbol{d}_m(\boldsymbol{j})$ is the $\boldsymbol{j}^{\text{th}}$ column of $\boldsymbol{A}_m$. We thus arrive at the following result.

Corollary II.1. *For any $m \ge 1$ and $0 \le r \le m$,*

1) *the rows of $\boldsymbol{A}_m$ indexed by $\{\boldsymbol{i} : w_H(\boldsymbol{i}) \ge r+1\}$ (or equivalently, the rows of $\boldsymbol{A}_m$ with Hamming weight at least 2^{r+1}) form a basis for $\mathcal{B}_n(r,m)$, and*

2) *the columns of* $\boldsymbol{A}_m$ *indexed by* $\{\boldsymbol{j} : w_H(\boldsymbol{j}) \le r\}$ *(equivalently, the columns of* $\boldsymbol{A}_m$ *with Hamming weight at least* n^{m-r}*) form a basis for* $\mathcal{C}_n(r,m)$.

Proof: These claims follow immediately from Lemmas II.6 and II.7 and the facts $w_H(\boldsymbol{c}_m(\boldsymbol{i})) = 2^{w_H(\boldsymbol{i})}$ and $w_H(\boldsymbol{d}_m(\boldsymbol{j})) = n^{m-w_H(\boldsymbol{j})}$. ■

The matrix $\boldsymbol{A}_m$ can be defined recursively using $\boldsymbol{A}_{m-1}$. To show this recursion, we impose the following colexicographic order on the elements of G^m. For $m = 1$, we impose the natural order $0 < 1 < \cdots < n-1$. For $m \ge 2$, and distinct $\boldsymbol{i}, \boldsymbol{i}' \in G^m$, we define

$$\boldsymbol{i} < \boldsymbol{i}' \text{ if and only if either } i_{m-1} < i'_{m-1}, \text{ or } i_{m-1} = i'_{m-1} \ \& \ \boldsymbol{i}_{[\![m-1]\!]} < \boldsymbol{i}'_{[\![m-1]\!]}.$$

We assume that the rows and columns of $\boldsymbol{A}_m$ are indexed by the elements of G^m in the ascending order (from left to right for columns, and top to bottom for rows). Now using

$$A_m(\boldsymbol{i},\boldsymbol{j}) = \begin{cases} A_{m-1}(\boldsymbol{i}_{[\![m-1]\!]}, \boldsymbol{j}_{[\![m-1]\!]}), & \text{if } i_{m-1} = j_{m-1} \text{ or } j_{m-1} = 0, \\ 0, & \text{otherwise}, \end{cases}$$

we arrive at the recursive structure of $\boldsymbol{A}_m$ given below

$$\boldsymbol{A}_m = \begin{pmatrix} \boldsymbol{A}_{m-1} & \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \boldsymbol{A}_{m-1} & \boldsymbol{A}_{m-1} & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \boldsymbol{A}_{m-1} & \boldsymbol{0} & \boldsymbol{A}_{m-1} & \cdots & \boldsymbol{0} \\ \vdots & \vdots & & \ddots & \vdots \\ \boldsymbol{A}_{m-1} & \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{A}_{m-1} \end{pmatrix}, \text{ and } \boldsymbol{A}_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathbb{F}_2^{n \times n}.$$

Note that $\boldsymbol{A}_m = \boldsymbol{A}_1^{\otimes m}$ where the exponent $\otimes m$ denotes the m-fold Kronecker product of a matrix with itself. When $n = 2$, part 2 of Corollary II.1 yields the well known characterization of RM codes in terms of the columns of $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes m}$.

E. Some Useful Automorphisms of the Codes $\mathcal{B}_n(r,m)$ *and* $\mathcal{C}_n(r,m)$

In this sub-section, we obtain some automorphisms of the code $\mathcal{B}_n(r,m)$. These will be used in a forthcoming section to show capacity achievability. Note that since the automorphism groups of a code and its dual are the same, these apply to the code $\mathcal{C}_n(r,m)$ also.

We use the scheme in Section II-D2 that identifies the coordinates of vectors in $\mathbb{F}_2^{n^m}$ with G^m (for any set G with n elements) for specifying the automorphisms of the code $\mathcal{B}_n(r,m)$.

Lemma II.8. *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* $\mathcal{B}_n(r,m)$.

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

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 $v'_{\boldsymbol{i}} = v_{\pi_{m-1,\sigma}(\boldsymbol{i})}$, lies in $\mathcal{B}_n(r,m)$.

To see this, observe that if we write $\boldsymbol{v}'$ as $(\boldsymbol{v}'_0 | \ldots | \boldsymbol{v}'_{n-1})$, then by the notation developed in Section II-D2, 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.9. *For any* $t \in [\![m-1]\!]$, *the permutation* β_t *on* G^m *defined below is an automorphism of* $\mathcal{B}_n(r,m)$ *and* $\mathcal{C}_n(r,m)$.

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

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 (6), 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 $B_{\mathcal{B}_n}(r,m)$.

$$c'_{\boldsymbol{i}} = c_m(\boldsymbol{i}')_{\beta_t(\boldsymbol{i})}, \ \forall \boldsymbol{i} \in G^m. \tag{8}$$

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-to-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.

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

Now, using the above equivalence and (8), we have,

$$c'_{\boldsymbol{i}} = \begin{cases} 1 & \text{if } \boldsymbol{i} \preceq \beta_t(\boldsymbol{i}') \\ 0 & \text{otherwise,} \end{cases} \tag{9}$$

for all $\boldsymbol{i} \in G^m$. Clearly, by (9), 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.1. *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 $\mathcal{C}_n(r,m)$.*

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

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.8 and Lemma II.9 respectively. Thus, the permutation

$$(i_0, \ldots, i_{m-1}) \to (\sigma_0(i_0), \ldots, \sigma_{m-1}(i_{m-1})), \tag{10}$$

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.8 and II.9, we have that (10) is an automorphism of $\mathcal{B}_n(r,m)$.

Part 2): It is known (see for example, [18]) 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.9 is precisely the transposition that interchanges t with $m-1$. Further, a transposition in $\mathcal{S}_m$ 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.9 and because the automorphisms of $\mathcal{B}_n(r,m)$ form a group. ■

F. Recursive Decoding

The structure of the code families $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$ allow us to perform efficient bounded distance decoding up to half the minimum distance. The decoders proposed in this sub-section are similar to the recursive decoding technique known for RM codes [8], [9]. We will assume that $\boldsymbol{v} \in \mathbb{F}_2^{n^m}$ is a codeword transmitted through a noisy binary-input binary-output channel and $\boldsymbol{y} \in \mathbb{F}_2^{n^m}$ is the channel output. The number of errors introduced by the channel is the Hamming distance between $\boldsymbol{v}$ and $\boldsymbol{y}$, which is

$$d(\boldsymbol{v},\boldsymbol{y}) = |\{i \in [\![n^m]\!] \ : \ v_i \neq y_i\}| \,.$$

We consider the scenario where $d(\boldsymbol{v},\boldsymbol{y})$ is less than half the minimum distance of the code, and provide algorithms to decode $\boldsymbol{y}$ to the transmitted codeword $\boldsymbol{v}$.

1) Recursive Decoding for $\mathcal{C}_n(r,m)$: For $r=0$ and $r=m$, we perform minimum distance decoding of the channel output to the codebook $\mathcal{C}_n(r,m)$. When $1 \leq r \leq m-1$, our decoder $\texttt{Dec}_{\mathcal{C}_{n,r,m}}$ for $\mathcal{C}_n(r,m)$ will use $\texttt{Dec}_{\mathcal{C}_{n,r,m-1}}$ and $\texttt{Dec}_{\mathcal{C}_{n,r-1,m-1}}$ as subroutines. In this case, we will assume that the transmitted codeword is

$$\boldsymbol{v} = (\boldsymbol{u}|\cdots|\boldsymbol{u}|\boldsymbol{u}) + (\boldsymbol{u}_0|\cdots|\boldsymbol{u}_{n-2}|\boldsymbol{u}_{n-1})$$

where $\boldsymbol{u} \in \mathcal{C}_n(r,m-1)$, $\boldsymbol{u}_0,\ldots,\boldsymbol{u}_{n-2} \in \mathcal{C}_n(r-1,m-1)$ and $\boldsymbol{u}_{n-1} = \mathbf{0}$. Our decoder will first decode $\boldsymbol{u}_0,\ldots,\boldsymbol{u}_{n-2}$, remove their effect in the channel output $\boldsymbol{y}$, and then decode $\boldsymbol{u}$. We prove the correctness of the decoder (by induction on the parameter m) when the number of errors introduced in the channel is less than $n^{m-r}/2$.

The key property used in our induction argument will be the fact that the output of the decoder is a valid codeword for any channel output (irrespective of the number of errors introduced in the channel). For the boundary cases $r=0$ (the repetition code) and $r=m$ (the universe code), $\texttt{Dec}_{\mathcal{C}_{n,r,m}}$ is the minimum distance decoder. It is clear that for $m=1$, and any $r \in [\![2]\!]$, the output of $\texttt{Dec}_{\mathcal{C}_{n,r,m}}$ is a valid codeword for any channel output, and the decoder outputs the correct codeword if the number of channel errors is less than half the minimum distance.

Let us now assume that $m \geq 2$, and $1 \leq r \leq m-1$. We will denote the channel output by $\boldsymbol{y} = (\boldsymbol{y}_0|\cdots|\boldsymbol{y}_{n-1})$. Now consider the first stage of the decoder where we decode $\boldsymbol{u}_0,\ldots,\boldsymbol{u}_{n-2}$. For each $l \in [\![n-1]\!]$, note that $\boldsymbol{u}_l$ is a codeword of $\mathcal{C}_n(r-1,m-1)$ which has minimum distance n^{m-r}. To decode $\boldsymbol{u}_l$ we will use $\texttt{Dec}_{\mathcal{C}_{n,r-1,m-1}}(\tilde{\boldsymbol{y}}_l)$ where

$$\tilde{\boldsymbol{y}}_l \triangleq \boldsymbol{y}_l + \boldsymbol{y}_{n-1}$$

is a noisy version of $\boldsymbol{u}_l$. If the number of channel errors in $\boldsymbol{y}$ is less than $n^{m-r}/2$, then the effective number of channel errors in $\tilde{\boldsymbol{y}}_l$ is also less than $n^{m-r}/2$, which is half the minimum distance of $\mathcal{C}_n(r-1,m-1)$. By induction, if $\boldsymbol{y}$ contains less than $n^{m-r}/2$ errors then the output of $\texttt{Dec}_{\mathcal{C}_{n,r-1,m-1}}(\tilde{\boldsymbol{y}}_l)$ is correct (that is, equal to $\boldsymbol{u}_l$), otherwise $\texttt{Dec}_{\mathcal{C}_{n,r-1,m-1}}(\tilde{\boldsymbol{y}}_l)$ will be some codeword of $\mathcal{C}_n(r-1,m-1)$.

In the next stage, we decode $\boldsymbol{u}$ by using $\texttt{Dec}_{\mathcal{C}_{n,r,m-1}}(\boldsymbol{y}_l+\boldsymbol{u}_l)$ for $l \in [\![n]\!]$, where $\boldsymbol{u}_{n-1} = \mathbf{0}$. Now consider the scenario where the number of channel errors in $\boldsymbol{y}$ less than $n^{m-r}/2$. We know that the receiver has correctly decoded $\boldsymbol{u}_0,\ldots,\boldsymbol{u}_{n-2}$. Hence, $\boldsymbol{y}_l + \boldsymbol{u}_l$ is a noisy version of $\boldsymbol{u}$, and the total number of channel errors in $\boldsymbol{y}$ is

$$\sum_{l \in [\![n]\!]} d(\boldsymbol{y}_l + \boldsymbol{u}_l, \boldsymbol{u}) < \frac{n^{m-r}}{2}.$$

Hence, there will be at least once choice of l such that $d(\boldsymbol{y}_l + \boldsymbol{u}_l, \boldsymbol{u}) < n^{m-r-1}/2$, and by induction, $\texttt{Dec}_{\mathcal{C}_{n,r,m-1}}(\boldsymbol{y}_l + \boldsymbol{u}_l) = \boldsymbol{u}$ for this l. Our decoder will look for an l such that

$$\sum_{k \in [\![n]\!]} d(\texttt{Dec}_{\mathcal{C}_{n,r,m-1}}(\boldsymbol{y}_l + \boldsymbol{u}_l), \boldsymbol{y}_k + \boldsymbol{u}_k) < \frac{n^{m-r}}{2}$$

and use $\texttt{Dec}_{\mathcal{C}_{n,r,m-1}}(\boldsymbol{y}_l + \boldsymbol{u}_l)$ as the decoded value of $\boldsymbol{u}$ if such an l exists. If more than one such l exists, each of these choices of l will yield the correct value of $\boldsymbol{u}$ (this follows from the fact that

$\texttt{Dec}_{\mathcal{C}_{n,r,m-1}}(\boldsymbol{y}_l+\boldsymbol{u}_l) \in \mathcal{C}_n(r,m-1)$, and the minimum distance of the concatenation of $\mathcal{C}_n(r,m-1)$ and the n-length repetition code is n^{m-r}). If no such l exists (this could happen when the number of errors in $\boldsymbol{y}$ is at least $n^{m-r}/2$), the decoder uses $\texttt{Dec}_{\mathcal{C}_{n,r,m-1}}(\boldsymbol{y}_{n-1})$ (which, even if incorrect, will still belong to $\mathcal{C}_n(r,m-1)$) as the decoded value of $\boldsymbol{u}$. Finally, the decoder will output $(\boldsymbol{u}|\boldsymbol{u}|\cdots|\boldsymbol{u})+(\boldsymbol{u}_0|\cdots|\boldsymbol{u}_{n-2}|\mathbf{0})$, which belongs to $\mathcal{C}_n(r,m)$ irrespective of the number of errors in the channel output $\boldsymbol{y}$.

Algorithm 1 $\texttt{Dec}_{\mathcal{C}_{n,r,m}}$ algorithm for decoding $\mathcal{C}_n(r,m)$

Input: Channel output $\boldsymbol{y} \in \mathbb{F}_2^{n^m}$
Output: A codeword $\boldsymbol{v} \in \mathcal{C}_n(r,m)$
1: **if** $r=0$ **then**
2: $\quad \boldsymbol{v} \leftarrow \mathbf{0}$
3: $\quad$ **if** $w_H(\boldsymbol{y}) > n^m/2$ **then**
4: $\quad\quad \boldsymbol{v} \leftarrow (1\ 1\ \cdots\ 1)$
5: $\quad$ **end if**
$\quad$ **return** $\boldsymbol{v}$
6: **end if**
7: **if** $r=m$ **then**
8: $\quad \boldsymbol{v} \leftarrow \boldsymbol{y}$
$\quad$ **return** $\boldsymbol{v}$
9: **end if**
10: **if** $1 \leq r \leq m-1$ **then**
11: $\quad$ **for** each $l \in [\![n-1]\!]$ **do**
12: $\quad\quad \tilde{\boldsymbol{y}}_l \leftarrow \boldsymbol{y}_l + \boldsymbol{y}_{n-1}$
13: $\quad\quad \boldsymbol{u}_l \leftarrow \texttt{Dec}_{\mathcal{C}_{n,r-1,m-1}}(\tilde{\boldsymbol{y}}_l)$
14: $\quad\quad \boldsymbol{y'}_l \leftarrow \boldsymbol{y}_l + \boldsymbol{u}_l$
15: $\quad$ **end for**
16: $\quad \boldsymbol{u}_{n-1} \leftarrow \mathbf{0}$
17: $\quad \boldsymbol{y'}_{n-1} \leftarrow \boldsymbol{y}_{n-1}$
18: $\quad$ **for** each $l \in [\![n]\!]$ **do**
19: $\quad\quad \boldsymbol{u} \leftarrow \texttt{Dec}_{\mathcal{C}_{n,r,m-1}}(\boldsymbol{y'}_l)$
20: $\quad\quad$ **if** $\sum_{k \in [\![n]\!]} d(\boldsymbol{u}, \boldsymbol{y'}_k) < n^{m-r}/2$ **then**
21: $\quad\quad\quad$ **break**
22: $\quad\quad$ **end if**
23: $\quad$ **end for**
24: $\quad \boldsymbol{v} \leftarrow (\boldsymbol{u}|\boldsymbol{u}|\cdots|\boldsymbol{u}) + (\boldsymbol{u}_0|\boldsymbol{u}_1|\cdots|\boldsymbol{u}_{n-1})$
$\quad$ **return** $\boldsymbol{v}$
25: **end if**

The decoder $\texttt{Dec}_{\mathcal{C}_{n,r,m}}$ is summarized in Algorithm 1. We now derive an upper bound on the complexity of this decoder. We will denote the complexity of this algorithm by $g(r,m)$ and derive an upper bound of the form $b_m n^m$ on $g(r,m)$, where b_m, $m \geq 1$, is a constant. Clearly, $g(0,m), g(m,m) \leq n^m$, and $b_1 = 1$ is a valid choice for upper bounding $g(0,1)$ and $g(1,1)$. Now consider an arbitrary $m \geq 2$ and $1 \leq r \leq m-1$. The complexity of steps 11–15 is at the most $n(2n^{m-1} + g(r-1,m-1))$. Steps 18–23 incur at the most $n(g(r,m-1)+n^m)$ computations. Finally, step 24 uses less than n^m XORs. Hence, we have

$$\begin{aligned} g(r,m) &\leq 3n^m + n^{m+1} + n(g(r-1,m-1)+g(r,m-1)) \\ &\leq (3+n+2b_{m-1})n^m. \end{aligned}$$

Hence, we choose $b_1 = 1$ and $b_m = (3 + n + 2b_{m-1})$ to arrive at the bound $g(r, m) \le b_m n^m$ for all r and m. The solution to this linear recursion is $b_m = 2^{m-1}(n+4) - (n+3)$. Thus, we have the bound

$$g(r, m) \le b_m n^m \le 2^m \frac{(n+4)}{2} n^m,$$

which is $O(N^{1+\log_n 2})$, where N is the code length.

2) Recursive Decoding for $\mathcal{B}_n(r, m)$*:* Our decoder for $\mathcal{B}_n(r, m)$ is defined recursively using the decoders of $\mathcal{B}_n(r, m-1)$ and $\mathcal{B}_n(r-1, m-1)$. We will denote the decoding function for $\mathcal{B}_n(r, m)$ as $\mathtt{Dec}_{\mathcal{B}_{n,r,m}}$. Similar to the decoder for $\mathcal{C}_n(r, m)$, the key property of $\mathtt{Dec}_{\mathcal{B}_{n,r,m}}$ is that its output is always a codeword of $\mathcal{B}_n(r, m)$ and this output is the transmitted codeword if the number of channel errors is less than 2^r.

For the boundary cases $r = 0$ (the single parity-check code) and $r = m$ (the all-zero code), we perform minimum distance decoding. We will now assume $1 \le r \le m-1$. While decoding the channel output $\boldsymbol{y}$ to $\mathcal{B}_n(r, m)$, we are searching for the transmitted codeword $\boldsymbol{v} = (\boldsymbol{v}_0 | \cdots | \boldsymbol{v}_{n-1})$ with each $\boldsymbol{v}_l \in \mathcal{B}_n(r-1, m-1)$ and $\boldsymbol{v}_{\text{sum}} \triangleq \sum_l \boldsymbol{v}_l \in \mathcal{B}_n(r, m-1)$. Let us denote the channel output as $\boldsymbol{y} = (\boldsymbol{y}_0 | \cdots | \boldsymbol{y}_{n-1})$. We have assumed that the number of channel errors is less than 2^r. Hence, we observe that the distance between $\boldsymbol{y}_{\text{sum}} \triangleq \sum_l \boldsymbol{y}_l$ and $\boldsymbol{v}_{\text{sum}}$ is less than 2^r. When $r \le m-2$, since the minimum distance of $\mathcal{B}_n(r, m-1)$ is 2^{r+1}, we observe that (by using an induction argument on the parameter m) we can use $\mathtt{Dec}_{\mathcal{B}_{n,r,m-1}}(\boldsymbol{y}_{\text{sum}})$ to decode $\boldsymbol{v}_{\text{sum}}$. When $r = m-1$, we know that $\mathcal{B}_n(m-1, m-1) = \{\mathbf{0}\}$, and hence, $\boldsymbol{v}_{\text{sum}} = \mathbf{0}$.

We now assume that the receiver knows $\boldsymbol{v}_{\text{sum}}$. Observe that for each $l \in [\![n-1]\!]$, we now have two noisy versions of $\boldsymbol{v}_l$, which are

$$\boldsymbol{y}_l \text{ and } \tilde{\boldsymbol{y}}_l \triangleq \boldsymbol{v}_{\text{sum}} + \sum_{k \neq l} \boldsymbol{y}_k.$$

Since the total number of channel errors in $\boldsymbol{y}$ is less than 2^r, at least one of $\boldsymbol{y}_l$ and $\tilde{\boldsymbol{y}}_l$ is within a distance of $2^{r-1} - 1$ to $\boldsymbol{v}_l$. By induction, we then see that at least one of

$$\hat{\boldsymbol{v}}_l(0) \triangleq \mathtt{Dec}_{\mathcal{B}_{n,r-1,m-1}}(\boldsymbol{y}_l),\ \hat{\boldsymbol{v}}_l(1) \triangleq \mathtt{Dec}_{\mathcal{B}_{n,r-1,m-1}}(\tilde{\boldsymbol{y}}_l),$$

is equal to $\boldsymbol{v}_l$ and the other belongs to $\mathcal{B}_n(r-1, m-1)$. We thus see that $\boldsymbol{v}$ belongs to the below collection of 2^{n-1} vectors if the number of channel errors in $\boldsymbol{y}$ is less than 2^r,

$$\mathcal{L} \triangleq \left\{ \left(\hat{\boldsymbol{v}}_0(a_0) \Big| \cdots \Big| \hat{\boldsymbol{v}}_{n-2}(a_{n-2}) \Big| \boldsymbol{v}_{\text{sum}} + \sum_{l \in [\![n-1]\!]} \hat{\boldsymbol{v}}_l(a_l) \right) \,:\, (a_0, \ldots, a_{n-2}) \in \{0,1\}^{n-1} \right\}.$$

Note that every vector in $\mathcal{L}$ is a codeword from $\mathcal{B}_n(r, m)$ irrespective of the number of channel errors in $\boldsymbol{y}$. This is because, by induction, we have that $\boldsymbol{v}_{\text{sum}} \in \mathcal{B}_n(r, m-1)$, each $\hat{\boldsymbol{v}}_l(a_l) \in \mathcal{B}_n(r-1, m-1)$ and the structure of the vectors in $\mathcal{L}$ follows the definition of $\mathcal{B}_n(r, m)$. Thus, we deduce that performing a minimum distance decoding among the vectors in $\mathcal{L}$ will return the correct codeword if the number of errors is less than 2^r, and this will return some codeword of $\mathcal{B}_n(r, m)$ otherwise. This recursive decoding technique for $\mathcal{B}_n(r, m)$ is summarized in Algorithm 2.

We now derive an upper bound on the complexity of this algorithm. Let $f(r, m)$ denote the number of computations incurred by $\mathtt{Dec}_{\mathcal{B}_{n,r,m}}$. We see that $f(0, m) \le n^m$ and $f(m, m) = 0$. We will derive a loose upper bound of the form

$$f(r, m) \le c_m n^m, \text{ for all } r \in [\![m+1]\!], \tag{11}$$

where the constants c_m, $m \ge 1$, are appropriately chosen. Clearly, $f(r, 1) \le n$ for all $r \in [\![2]\!]$, and hence, we choose $c_1 = 1$.

We now derive a recursive upper bound on $f(r, m)$ when $1 \le r \le m-1$. We see that step 11 incurs n^m computations, step 12 uses $f(r, m-1)$ computations, steps 13-17 have complexity at the most $n(2n^{m-1} +$

Algorithm 2 $\texttt{Dec}_{\mathcal{B}_n,r,m}$ algorithm for decoding $\mathcal{B}_n(r,m)$

Input: Channel output $\boldsymbol{y} \in \mathbb{F}_2^{n^m}$
Output: A codeword $\boldsymbol{v} \in \mathcal{B}_n(r,m)$
1: **if** $r = m$ **then**
2: $\quad \boldsymbol{v} \leftarrow \mathbf{0}$
$\quad$ **return** $\boldsymbol{v}$
3: **end if**
4: **if** $r = 0$ **then**
5: $\quad \boldsymbol{v} \leftarrow \boldsymbol{y}$
6: $\quad$ **if** $w_H(\boldsymbol{v})$ is odd **then**
7: $\quad\quad$ Flip the first bit of $\boldsymbol{v}$
8: $\quad$ **end if**
$\quad$ **return** $\boldsymbol{v}$
9: **end if**
10: **if** $1 \le r \le m-1$ **then**
11: $\quad \boldsymbol{y}_{\text{sum}} \leftarrow \sum_{l \in [\![n]\!]} \boldsymbol{y}_l$
12: $\quad \boldsymbol{v}_{\text{sum}} \leftarrow \texttt{Dec}_{\mathcal{B}_n,r,m-1}(\boldsymbol{y}_{\text{sum}})$
13: $\quad$ **for** each $l \in [\![n-1]\!]$ **do**
14: $\quad\quad \tilde{\boldsymbol{y}}_l \leftarrow \boldsymbol{v}_{\text{sum}} + \boldsymbol{y}_{\text{sum}} + \boldsymbol{y}_l$
15: $\quad\quad \hat{\boldsymbol{v}}_l(0) \leftarrow \texttt{Dec}_{\mathcal{B}_n,r-1,m-1}(\boldsymbol{y}_l)$
16: $\quad\quad \hat{\boldsymbol{v}}_l(1) \leftarrow \texttt{Dec}_{\mathcal{B}_n,r-1,m-1}(\tilde{\boldsymbol{y}}_l)$
17: $\quad$ **end for**
18: $\quad \boldsymbol{v} \leftarrow$ Minimum distance decode $\boldsymbol{y}$ to $\mathcal{L}$
$\quad$ **return** $\boldsymbol{v}$
19: **end if**

$2f(r-1,m-1))$, and step 18 uses $2^{n-1}n^m$ computations. Computing all the vectors in $\mathcal{L}$ takes at the most $2^{n-1}n^m$ further computations. Combining these terms we arrive at the following upper bound

$$\begin{aligned} f(r,m) &\le n^m + f(r,m-1) \; + n\left(2f(r-1,m-1) + 2n^{m-1}\right) + 2^{n-1}n^m + 2^{n-1}n^m \\ &\le (3+2^n)n^m + c_{m-1}n^{m-1} + 2c_{m-1}n^m \\ &\le \left(3 + 2^n + c_{m-1}\left(2 + \frac{1}{n}\right)\right) n^m. \end{aligned}$$

Thus, we choose $c_m = 3 + 2^n + c_{m-1}(2+\frac{1}{n})$ to satisfy (11), with $c_1 = 1$. This is a linear recurrence with constant coefficients, and its solution c_m grows with m as $O\left(\left(2+\frac{1}{n}\right)^m\right)$. Thus, the complexity of $\texttt{Dec}_{\mathcal{B}_n,r,m}$ is at the most $c_m n^m$, which is $O\left(N^{1+\log_n\left(2+\frac{1}{n}\right)}\right)$ since $N = n^m$.

III. Capacity-Related Properties

Reeves and Pfister [4] recently showed that Reed-Muller (RM) codes achieve the capacity of binary-input memoryless symmetric (BMS) channels. They rely on the following properties of the RM codes in their work.

1) For every $R^* \in (0,1)$ there exists a sequence of RM codes of increasing block lengths with rates converging to R^*.
2) RM codes are transitive (that is, for any chosen pair of coordinates, there is an automorphism that maps the first coordinate to the second), and more importantly, RM codes are doubly transitive (that is, for any three distinct coordinates i, j, k, there is a code automorphism that fixes i and sends j to k).

3) For $1 \leq k \leq m$ and $r \leq m-k$, we can puncture $\mathrm{RM}(r, m+k)$ to obtain $\mathrm{RM}(r, m)$. Further, there are multiple ways to do this puncturing. In particular, suppose we use the elements of $\mathbb{F}_2^{m+k}$ to represent the coordinates of the codewords in $\mathrm{RM}(r, m+k)$. For any $H \subset \mathbb{F}_2^{m+k}$ and any vector $\boldsymbol{v} = (v_{\boldsymbol{i}} : \boldsymbol{i} \in \mathbb{F}_2^{m+k}) \in \mathbb{F}_2^{2^{m+k}}$, define the puncturing operation $\mathcal{P}_H$ as $\mathcal{P}_H(\boldsymbol{v}) = (v_{\boldsymbol{i}} : \boldsymbol{i} \in H)$. Let $H_1 = \mathbb{F}_2^m \times \{0\}^k$ and $H_2 = \mathbb{F}_2^{m-k} \times \{0\}^k \times \mathbb{F}_2^k$. Then,
$$\begin{aligned} \mathcal{P}_{H_1}\left(\mathrm{RM}(r, m+k)\right) &= \mathrm{RM}(r, m), \\ \mathcal{P}_{H_2}\left(\mathrm{RM}(r, m+k)\right) &= \mathrm{RM}(r, m), \text{ and} \\ \mathcal{P}_{H_1 \cap H_2}\left(\mathrm{RM}(r, m+k)\right) &= \mathrm{RM}(r, m-k), \end{aligned}$$
see Lemma 8 of [4].
4) For long RM codes the rate change due to puncturing is small. Let us denote the rate of $\mathrm{RM}(r, m)$ as $R_{\mathrm{RM}}(r, m)$. For any $r \leq m$ and $k \geq 1$, we have
$$0 \leq R_{\mathrm{RM}}(r, m) - R_{\mathrm{RM}}(r, m+k) \leq \frac{3k+4}{5\sqrt{m}}.$$
Reeves and Pfister derive this bound and exploit the fact that this rate change is $O(k/\sqrt{m})$.

In this section we show that $\mathcal{B}_n(r, m)$ and $\mathcal{C}_n(r, m)$ satisfy all these properties except double transitivity when $n \geq 3$. The proof that these codes are not doubly transitive is based on the observation in [19] that the product of the minimum distances of a code and its dual is much smaller than the block length.

Since $\mathcal{B}_n(r, m)$ and $\mathcal{C}_n(r, m)$ are not doubly transitive, we can not use [3, Theorem 20] for capacity-achievability in the BEC. Fortunately, these codes do satisfy the weaker sufficient conditions put forth in [7, Theorem 19] for a code sequence to achieve the BEC capacity. (In fact, for all odd n, we are able to show that a broader class of abelian codes are capacity-achieving in the BEC under bit-MAP decoding, see Section IV).

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

We intend to show that there are multiple ways to puncture $\mathcal{C}_n(r, m+k)$ to obtain $\mathcal{C}_n(r, m-k)$, and similarly, puncture $\mathcal{B}_n(r+k, m+k)$ to $\mathcal{B}_n(r-k, m-k)$. The key observation will be the fact that $\mathcal{C}_n(r, m)$ can be punctured to get $\mathcal{C}_n(r, m-1)$ (similarly, puncturing $\mathcal{B}_n(r, m)$ yields $\mathcal{B}_n(r-1, m-1)$).

We first set up some terminology to work with puncturing operation. Recall the notation from Section II-D2 for representing the coordinates of codewords using tuples $\boldsymbol{i} = (i_0, \ldots, i_{m-1}) \in G^m$ where $G = [\![n]\!]$. For any set $\mathcal{K} \subset [\![m]\!]$ and any $\boldsymbol{b} \in G^{|\mathcal{K}|}$, we say that '$H \subset G^m$ is the *direct-product subset* of G^m corresponding to $\mathcal{K}$ and $\boldsymbol{b}$' if
$$H = \{\boldsymbol{i} \in G^m : \boldsymbol{i}_{\mathcal{K}} = \boldsymbol{b}\},$$
where $\boldsymbol{i}_{\mathcal{K}} = (i_l : l \in \mathcal{K})$ is a sub-vector of $\boldsymbol{i}$. For any such H, we define the puncturing operation $\mathcal{P}_H$ as follows
$$\mathcal{P}_H(\boldsymbol{v}) = \mathcal{P}_H\left(\,(v_{\boldsymbol{i}} : \boldsymbol{i} \in G^m)\,\right) = (v_{\boldsymbol{i}} : \boldsymbol{i} \in H).$$
That is, $\mathcal{P}_H$ discards all the coordinates not in H. The size of H and the length of the vector $\mathcal{P}_H(\boldsymbol{v})$ are both equal to $n^{m-|\mathcal{K}|}$. For instance, with our usual concatenated representation $\boldsymbol{v} = (\boldsymbol{v}_0|\cdots|\boldsymbol{v}_{n-1})$, we see that $\boldsymbol{v}_l = (v_{\boldsymbol{i}} : i_{m-1} = l)$. Hence, if H is the direct-product subset corresponding $\mathcal{K} = \{m-1\}$ and $b = l$, then $\mathcal{P}_H(\boldsymbol{v}) = \boldsymbol{v}_l$.

Lemma III.1. *Let* $\mathcal{K} = \{m-1\}$*,* $l \in G$*, and* $H = G^{m-1} \times \{l\}$ *be the corresponding direct-product subset of* G^m*. Then,*
1) $\mathcal{P}_H\left(\mathcal{C}_n(r, m)\right) = \mathcal{C}_n(r, m-1)$ *if* $r \leq m-1$*,*
2) $\mathcal{P}_H\left(\mathcal{B}_n(r, m)\right) = \mathcal{B}_n(r-1, m-1)$ *if* $r \geq 1$*.*

Proof. We will use the code definitions to prove this result. We know that $\mathcal{P}_H\left((\boldsymbol{v}_0|\cdots|\boldsymbol{v}_{n-1})\right) = \boldsymbol{v}_l$. From the definition of $\mathcal{C}_n(r,m)$ and the fact $\mathcal{C}_n(r-1,m-1) \subset \mathcal{C}_n(r,m-1)$, we see that $\mathcal{P}_H(\mathcal{C}_n(r,m)) = \mathcal{C}_n(r,m-1)$, irrespective of the value of l. The proof for $\mathcal{B}_n(r,m)$ is similar. $\square$

We can easily generalize the results of Lemma III.1 to include arbitrary direct-product subsets of G^m.

Theorem III.1. *Let $\mathcal{K} \subset [\![m]\!]$, $\boldsymbol{b} \in G^{|\mathcal{K}|}$ and H be the corresponding direct-product subset of G^m. Then*

1) $\mathcal{P}_H\left(\mathcal{C}_n(r,m)\right) = \mathcal{C}_n(r,m-|\mathcal{K}|)$ *if* $r \leq m-|\mathcal{K}|$,
2) $\mathcal{P}_H\left(\mathcal{B}_n(r,m)\right) = \mathcal{B}_n(r-|\mathcal{K}|,m-|\mathcal{K}|)$ *if* $r \geq |\mathcal{K}|$.

Proof. We will prove only Part 1, the proof of Part 2 uses the same ideas.

Let us first consider the case $|\mathcal{K}| = 1$. Suppose $\mathcal{K} = \{k\}$ and $b = l$. Let $\gamma \in \mathcal{S}_m$ be such that $\gamma(k) = m-1$, $\gamma(m-1) = k$ and γ fixes all other points in $[\![m]\!]$. We note that the map $\mathcal{P}_H$ is equal to the composite of the permutation γ applied on the coordinates G^m followed by the puncturing operation $\mathcal{P}_{G^{m-1}\times\{l\}}$. Since γ is an automorphism of $\mathcal{C}_n(r,m)$ (see Theorem II.1) we have

$$\begin{aligned}\mathcal{P}_H(\mathcal{C}_n(r,m)) &= \mathcal{P}_{G^{m-1}\times\{l\}}\Big(\gamma(\mathcal{C}_n(r,m))\Big)\\ &= \mathcal{P}_{G^{m-1}\times\{l\}}(\mathcal{C}_n(r,m))\\ &= \mathcal{C}_n(r,m-1),\end{aligned}$$

where the last step follows from Lemma III.1.

The case $|\mathcal{K}| \geq 2$ now simply follows by induction. To see this consider $\mathcal{K} = \{k_1,k_2\}$ with $k_1 > k_2$ and $\boldsymbol{b} \in G^2$ consisting of elements l_1 and l_2. Let H_1 be the direct-product subset of G^m corresponding to $\{k_1\}$ and l_1, and H_2 be the direct-product subset of G^{m-1} corresponding to $\{k_2\}$ and l_2. We notice that $\mathcal{P}_H$ is the composite of the functions $\mathcal{P}_{H_1}$ and $\mathcal{P}_{H_2}$. Hence,

$$\begin{aligned}\mathcal{P}_H(\mathcal{C}_n(r,m)) &= \mathcal{P}_{H_2}\left(\mathcal{P}_{H_1}(\mathcal{C}_n(r,m))\right)\\ &= \mathcal{P}_{H_2}(\mathcal{C}_n(r,m-1))\\ &= \mathcal{C}_n(r,m-2).\end{aligned}$$

The proof for other values of $|\mathcal{K}|$ is similar. $\square$

We can puncture $\mathcal{C}_n(r,m+k)$, $1 \leq k \leq m$, in multiple ways to obtain $\mathcal{C}_n(r,m-k)$. Let H_1 and H_2 be direct-product subsets of G^{m+k} such that

$$|H_1| = |H_2| = n^m \text{ and } |H_1 \cap H_2| = n^{m-k}.$$

Note that $H_1 \cap H_2$ is also a direct-product subset of G^{m+k}. For instance, we could have $H_1 = G^m \times \{0\}^k$ and $H_2 = G^{m-k} \times \{0\}^k \times G^k$. In this case, $H_1 \cap H_2 = G^{m-k} \times \{0\}^{2k}$. Applying Theorem III.1, we have

$$\begin{aligned}\mathcal{P}_{H_1}\left(\mathcal{C}_n(r,m+k)\right) &= \mathcal{C}_n(r,m),\\ \mathcal{P}_{H_2}\left(\mathcal{C}_n(r,m+k)\right) &= \mathcal{C}_n(r,m), \text{ and}\\ \mathcal{P}_{H_1\cap H_2}\left(\mathcal{C}_n(r,m+k)\right) &= \mathcal{C}_n(r,m-k).\end{aligned}$$

A similar property holds for $\mathcal{B}_n(r,m)$ also. Let $1 \leq k \leq r$, and let H_1 and H_2 be as defined above, then

$$\begin{aligned}\mathcal{P}_{H_1}\left(\mathcal{B}_n(r+k,m+k)\right) &= \mathcal{B}_n(r,m),\\ \mathcal{P}_{H_2}\left(\mathcal{B}_n(r+k,m+k)\right) &= \mathcal{B}_n(r,m), \text{ and}\\ \mathcal{P}_{H_1\cap H_2}\left(\mathcal{B}_n(r+k,m+k)\right) &= \mathcal{B}_n(r-k,m-k).\end{aligned}$$

B. *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. Let $X_0,\dots,X_{m-1}$ be independent and identically distributed Bernoulli random variables with $\Pr(X_k=1)=(n-1)/n$ for all $k\in[\![m]\!]$. The mean and variance of X_k are

$$\mu=\frac{n-1}{n} \text{ and } \sigma^2=\frac{n-1}{n^2},$$

respectively. Define $Y_m = X_0+\cdots+X_{m-1}$, which follows binomial distribution. We observe that

$$\begin{aligned}
R_n(r,m) &= \sum_{w=0}^{r}\binom{m}{w}\left(\frac{n-1}{n}\right)^w\left(\frac{1}{n}\right)^{m-w}\\
&= \Pr\left(Y_m\le r\right)\\
&= \Pr\left(\frac{\sum_{k\in[\![m]\!]}\left(X_k-\mu\right)}{\sqrt{m\sigma^2}}\le\frac{r-m\mu}{\sqrt{m\sigma^2}}\right).
\end{aligned}$$

Note that $(X_k-\mu)/\sigma$ has zero mean and unit variance, and the distribution of $(X_k-\mu)/\sigma$ is completely determined by the value of n. The ***Berry-Esseen inequality*** [20] can be used to approximate the distribution function of $\sum_k(X_k-\mu)/(\sqrt{m\sigma^2})$ 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

$$\left|R_n(r,m)-\left(1-Q\left(\frac{r-m\mu}{\sqrt{m\sigma^2}}\right)\right)\right|\le\frac{\kappa}{\sqrt{m}}. \tag{12}$$

Let $R^*\in(0,1)$ and let $\{\mathcal{C}_n(r_l,m_l)\}$ be a sequence of codes with $m_l\to\infty$ and rates converging to R^*. From (12), we have

$$r_l = m_l\mu + Q^{-1}\left(1-R^*-o(1)\right)\sqrt{m_l\sigma^2}.$$

Observe that

$$\frac{r_l}{m_l}\to\mu,\ \text{ as } l\to\infty. \tag{13}$$

We also note that $1-R_n(r,m)$ is the rate of $\mathcal{B}_n(r,m)$. Hence, from (12), we deduce that, for a fixed n, the rate of $\mathcal{B}_n(r,m)$ is

$$Q\left(\frac{r-m\mu}{\sqrt{m\sigma^2}}\right)+O\left(\frac{1}{\sqrt{m}}\right).$$

1) Rate Change from Puncturing: We now compare the rates of $\mathcal{C}_n(r,m)$ and $\mathcal{C}_n(r,m+k)$ where $k\ge1$. We recognize that $\mathcal{C}_n(r,m)$ can be obtained from $\mathcal{C}_n(r,m+k)$ via puncturing where a fraction $1-\frac{1}{n^k}$ of the code symbols are removed. Hence $R_n(r,m)-R_n(r,m+k)$ is the increase in the rate due to this puncturing operation. We first observe that $R_n(r,m)-R_n(r,m+k)$ equals

$$\Pr(X_0+\cdots+X_{m-1}\le r)-\Pr(X_0+\cdots+X_{m+k-1}\le r).$$

This implies $R_n(r,m)-R_n(r,m+k)\ge0$. Using (12) it is easy to show that this rate change is $O(k/\sqrt{m})$.

Lemma III.2. *For any $k\ge1$ and $0\le r\le m$,*

$$0\le R_n(r,m)-R_n(r,m+k)\le\frac{2\kappa}{\sqrt{m}}+\frac{k}{\sqrt{m}}\left(\frac{1+\mu}{\sqrt{8\pi\sigma^2}}\right).$$

Proof. Using (12) we observe that $R_n(r,m) - R_n(r,m+k)$ is upper bounded by

$$\begin{aligned}
&\frac{\kappa}{\sqrt{m}} + \frac{\kappa}{\sqrt{m+k}} + Q\left(\frac{r-(m+k)\mu}{\sigma\sqrt{m+k}}\right) - Q\left(\frac{r-m\mu}{\sigma\sqrt{m}}\right) \\
&\leq \frac{2\kappa}{\sqrt{m}} + \int\limits_{\frac{r}{\sigma\sqrt{m+k}}-\frac{\mu\sqrt{m+k}}{\sigma}}^{\frac{r}{\sigma\sqrt{m}}-\frac{\mu\sqrt{m}}{\sigma}} \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{t^2}{2}\right)\mathrm{d}t \\
&\leq \frac{2\kappa}{\sqrt{m}} + \frac{1}{\sqrt{2\pi}}\left(\frac{r}{\sigma\sqrt{m}} - \frac{r}{\sigma\sqrt{m+k}} + \frac{\mu\sqrt{m+k}}{\sigma} - \frac{\mu\sqrt{m}}{\sigma}\right).
\end{aligned}$$

We now use the AM-GM inequality $\sqrt{m(m+k)} \leq m + \frac{k}{2}$, i.e., $\sqrt{m+k} - \sqrt{m} \leq \frac{k}{2\sqrt{m}}$, to further loosen the above upper bound to

$$\begin{aligned}
&\frac{2\kappa}{\sqrt{m}} + \frac{r}{\sigma\sqrt{2\pi m(m+k)}}\frac{k}{2\sqrt{m}} + \frac{\mu}{\sigma\sqrt{2\pi}}\frac{k}{2\sqrt{m}} \\
&\leq \frac{2\kappa}{\sqrt{m}} + \frac{k}{\sqrt{m}}\left(\frac{1+\mu}{\sqrt{8\pi\sigma^2}}\right),
\end{aligned}$$

where we have used the fact $r \leq m \leq \sqrt{m(m+k)}$. □

The following similar result holds for the family of codes $\{\mathcal{B}_n(r,m)\}$.

Lemma III.3. *For any $k \geq 1$, the rate of $\mathcal{B}_n(r,m)$ is greater than or equal to the rate of $\mathcal{B}_n(r+k,m+k)$, and the difference in these rates is upper bounded by*

$$\frac{2\kappa}{\sqrt{m}} + \frac{k}{\sqrt{m}}\frac{(\mu+2)}{\sqrt{8\pi\sigma^2}}.$$

Proof. Proof is similar to the proof of Lemma III.2 and is available in Appendix I. □

C. Lack of Double Transitivity

It is well known that RM codes (the case $n = 2$) are doubly transitive. In the rest of this sub-section we will assume that $n \geq 3$.

We now show that for long block lengths, $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$ are not doubly transitive. We will rely on the following property of doubly transitive codes [19, Theorem E.9], viz., for any doubly transitive code

$$(d_{\min}-1)(d_{\min}^{\perp}-1) \geq N-1,$$

where N is the block length of the code, $d_{\min}$ is the minimum distance of the code and $d_{\min}^{\perp}$ is the minimum distance of its dual code.

Let $R^* \in (0,1)$ and let $\{\mathcal{C}_n(r_l,m_l)\}$ be a sequence of codes with $m_l \to \infty$ and rates converging to R^*. From (13) we have $r_l = m_l\,(\mu + o(1))$. Now consider the product $(d_{\min}-1)(d_{\min}^{\perp}-1)$ for the code $\mathcal{C}_n(r_l,m_l)$ (or equivalently for the code $\mathcal{B}_n(r_l,m_l)$). We have

$$\begin{aligned}
(d_{\min}-1)(d_{\min}^{\perp}-1) &\leq n^{m_l-r_l} \times 2^{r_l+1} \\
&= n^{m_l} \times 2 \times \left(\frac{2}{n}\right)^{r_l} \\
&= n^{m_l} \times 2 \times \left(\frac{2}{n}\right)^{m_l(\mu+o(1))}.
\end{aligned}$$

Since $n \geq 3$, we deduce that

$$(d_{\min} - 1)(d_{\min}^{\perp} - 1) < n^{m_l} - 1$$

for all sufficiently large l. Hence, we have proved

Lemma III.4. *Let $n \geq 3$, $R^* \in (0,1)$ and $\{\mathcal{C}_n(r_l, m_l)\}$ be a sequence of codes with increasing block lengths and rates converging to R^*. For every sufficiently large l, the code $\mathcal{C}_n(r_l, m_l)$ does not have a doubly transitive automorphism group.*

D. 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 in the sequence, the orbits 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 (12) 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 block lengths and rates converging to R^*.

2) Transitivity: We now use Theorem II.1 to observe that for any choice of parameters n, r, m, the code $\mathcal{C}_n(r, m)$ is transitive. We will use the notation introduced in Section II-D2 for the coordinates of a codeword. 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.1 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.1, 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 $\boldsymbol{i} \neq \mathbf{0}$, $\mathcal{O}_{r,m}(\boldsymbol{i}) \supset \{\boldsymbol{j} \in G^m : w_H(\boldsymbol{j}) = w_H(\boldsymbol{i})\}$. 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 $\epsilon < (1 - R^*)$. Since a similar result holds for $\{\mathcal{B}_n(r,m)\}$, we have thus proved the following.

Theorem III.2. *Consider any BEC with capacity $C \in (0,1)$. For any $n \geq 3$ and any $R \in [0, C)$, there exists a sequence of codes from the family $\{\mathcal{C}_n(r,m)\}$ with strictly increasing blocklengths with rates converging to R and the bit erasure probability under bit-MAP decoding converging to zero. The same statement holds for the family $\{\mathcal{B}_n(r,m)\}$ as well.*

It is well known that the above result is true for $n = 2$, i.e., for RM codes. In particular, we know that RM codes achieve BEC capacity under both bit-MAP and block-MAP decoding [3].

IV. Constructions via Discrete Fourier Transform

A number of good binary error correcting codes are abelian codes, that is, they are ideals in commutative group algebras. Examples include BCH codes, quadratic residue codes, and RM codes [5], [11]–[13], [15], [21], [22]. When the order of the abelian group is odd (the order of the group is relatively prime with the characteristic of $\mathbb{F}_2$), the corresponding group algebra is semi-simple. It is well known that abelian codes constructed from semi-simple group algebras can be characterized using discrete Fourier transform (DFT) over finite fields [11], [14], [23].

Unless specified otherwise, throughout this section we will assume that $n \geq 3$ is an odd integer. We will use the transform domain characterization of abelian codes of Rajan and Siddiqi [14] to identify $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$ as ideals in appropriate group algebras. Further, with the help of the DFT tool, we will identify a large class of abelian codes (containing $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$) that achieve the capacity of the BEC under bit-MAP decoding. During this process, we will also show that when n is an odd prime, $\mathcal{B}_n(r,m)$ is identical to the code designed by Berman in [5], and $\mathcal{C}_n(r,m)$ is its dual code studied by Blackmore and Norton in [6].

In this section we first review the necessary background on abelian codes and DFT, we then derive some preliminary results related to DFT, and provide a construction of $\mathcal{C}_n(r,m)$ and $\mathcal{B}_n(r,m)$ for odd n using the transform domain approach. Finally, we identify a large family of abelian codes that achieve BEC capacity.

A. Background

Throughout this section we will assume that $(G, \oplus)$ is any finite abelian group of odd order, with $|G| \geq 3$. Please be aware that $|G|$ will replace the role played by the parameter n in the previous sections. We denote the identity element of G by 0. Since G is finite abelian, it is a direct product of cyclic groups [24]. Let the number of cyclic groups in this decomposition be s and let their orders be $m_0, \dots, m_{s-1}$, i.e., $G = \mathbb{Z}_{m_0} \times \cdots \times \mathbb{Z}_{m_{s-1}}$. Since $|G|$ is odd, so are $m_0, \dots, m_{s-1}$. We will treat each element $i \in G$ as an s-tuple

$$i = \big(i[0], \quad i[1], \quad \cdots, \quad i[s-1]\big) \in \mathbb{Z}_{m_0} \times \cdots \times \mathbb{Z}_{m_{s-1}}.$$

The sum of two elements $i, j \in G$ is performed component-wise, that is, $(i \oplus j)[\ell] = (i[\ell] + j[\ell]) \mod m_\ell$ for each $\ell \in [\![s]\!]$. We denote the sum of i and the additive inverse of j as $i \ominus j$, i.e., $(i \ominus j)[\ell] = (i[\ell] - j[\ell])$ $\mod m_\ell$.

1) Group Algebra & Abelian Codes: The group algebra $\mathbb{F}_2[G]$ is $\left\{\sum_{i\in G} a_i X^i \ : \ a_i \in \mathbb{F}_2\right\}$, where each element a of the group algebra is a formal sum $\sum_{i\in G} a_i X^i$. The sum of two elements a and b is

$$a + b = \sum_{i\in G} a_i X^i + \sum_{i\in G} b_i X^i = \sum_{i\in G} (a_i + b_i) X^i,$$

where the addition $a_i + b_i$ is over $\mathbb{F}_2$. The product ab of two elements $a, b \in \mathbb{F}_2[G]$ is

$$\begin{aligned}\left(\sum_{i\in G} a_i X^i\right) \cdot \left(\sum_{j\in G} b_j X^j\right) &= \sum_{i\in G}\sum_{j\in G} a_i b_j X^{i\oplus j} \\ &= \sum_{i\in G} (\sum_{k\in G} a_k b_{i\ominus k}) X^i.\end{aligned}$$

The multiplication operation in $\mathbb{F}_2[G]$ is a convolution of the length-$|G|$ binary vectors $(a_i : i \in G)$ and $(b_i : i \in G)$. Since G is abelian, this multiplication operation is commutative, and $\mathbb{F}_2[G]$ is a commutative ring.

An abelian code $\mathcal{C}$ is an ideal in the group algebra $\mathbb{F}_2[G]$, that is, $(\mathcal{C}, +)$ is an additive subgroup of $\mathbb{F}_2[G]$ and for any $a \in \mathcal{C}$ and $b \in \mathbb{F}_2[G]$ we have $ab \in \mathcal{C}$. Observe that $\mathcal{C}$ yields a length-$|G|$ binary linear code

$$\{(a_i : i \in G) \ : \ a \in \mathcal{C}\} \subset \mathbb{F}_2^{|G|}.$$

We will make no distinction between an ideal $\mathcal{C}$ and the binary linear code associated with this ideal. We make the following simple observation here.

Lemma IV.1. *Abelian codes are transitive.*

Proof. Let $\mathcal{C}$ be an ideal in $\mathbb{F}_2[G]$, and $j, k \in G$. We want to show that there exists an automorphism of $\mathcal{C}$ that maps the coordinate k to j. For any $a \in \mathcal{C}$, consider $c = X^{j\ominus k} a = \sum_{i\in G} a_i X^{i\oplus j\ominus k}$. Note that $c_{i\oplus j\ominus k} = a_i$. Hence, c is obtained by permuting the coordinates of a, and this permutation sends k to j, i.e., $c_j = a_k$. Since $\mathcal{C}$ is an ideal $c = X^{j\ominus k} a \in \mathcal{C}$. Hence, the map $a \to X^{j\ominus k} a$ is a code automorphism that maps k to j. $\square$

2) Discrete Fourier Transform: We now review the approach of [14] in studying abelian codes in semi-simple group algebras. This approach uses the DFT to explicitly characterize all the ideals in $\mathbb{F}_2[G]$. This will be the primary tool used in this section. We will first recall the notion of *conjugacy classes* and then review the DFT.

Conjugacy Classes: For any integer $\ell \geq 0$ and any $i \in G$, we use ℓi to denote the ℓ-fold sum $(i \oplus i \oplus \cdots \oplus i)$. The *conjugacy class* of G containing the element $i \in G$ is the set

$$\Gamma_i = \{i, 2i, 2^2 i, \ldots, 2^{\ell-1} i\}$$

where $\ell = |\Gamma_i|$ is the smallest integer such that $2^\ell i = i$. Such an integer ℓ exists since 2 is not a divisor of $|G|$. For any $i, j \in G$, either $\Gamma_i = \Gamma_j$ or $\Gamma_i \cap \Gamma_j = \varnothing$. Thus, the distinct conjugacy classes of G partition G. We note that $\Gamma_i = \Gamma_j$ if and only if $i \in \Gamma_j$ (or equivalently, $j \in \Gamma_i$). The conjugacy class of the identity element Γ_0 is $\{0\}$, and this is the only conjugacy class with size equal to 1.

Lemma IV.2. *If* $i \in G \setminus \{0\}$ *then* $|\Gamma_i| \geq 2$.

Proof. Since $i \neq 0$, $2i = i \oplus i \neq i$, and hence, $|\Gamma_i| \geq 2$. $\square$

We will denote the set of all distinct conjugacy classes of G by Λ. Note that $\sum_{\Gamma\in\Lambda} |\Gamma| = |G|$ since the distinct conjugacy classes partition G.

Example IV.1. We will use $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ to illustrate the definitions introduced in this sub-section. Each element $i \in G$ is a 2-tuple $(i[0] \ \ i[1])$. The distinct conjugacy classes of G are

$$\{(0\ 0)\}, \ \{(0\ 1), (0\ 2)\}, \ \{(1\ 0), (2\ 0)\}, \ \{(1\ 1), (2\ 2)\}, \ \{(1\ 2), (2\ 1)\}.$$

In this case Λ contains 5 classes, and all classes except $\Gamma_0 = \{(0\ 0)\}$ have size 2. $\square$

We will be interested in subsets of G that are unions of conjugacy classes. Note that $Z \subset G$ is a union of conjugacy classes if and only if there exists a $\Lambda' \subset \Lambda$ such that $Z = \cup_{\Gamma \in \Lambda'} \Gamma$. Alternatively, Z is a union of conjugacy classes if and only if for each $j \in Z$ we have $2j \in Z$.

Discrete Fourier Transform: The DFT for $\mathbb{F}_2[G]$ is based on the decomposition $\mathbb{Z}_{m_0} \times \cdots \times \mathbb{Z}_{m_{s-1}}$ of G. Let $\mathbb{F}_q$ be a finite extension of $\mathbb{F}_2$ that contains the primitive m_ℓ^{th} root of unity for every $\ell \in [\![s]\!]$. Let $\alpha_0, \ldots, \alpha_{s-1}$ be elements of $\mathbb{F}_q^*$ with multiplicative orders $m_0, \ldots, m_{s-1}$, respectively.

The DFT is an $\mathbb{F}_2$-linear injective map $\Phi : \mathbb{F}_2[G] \to \mathbb{F}_q[G]$. We will denote the DFT of $a = \sum_{i \in G} a_i X^i \in \mathbb{F}_2[G]$ by

$$\Phi(a) = A = \sum_{j \in G} A_j X^j \in \mathbb{F}_q[G].$$

The DFT is defined as follows

$$A_j = \sum_{i \in G} \alpha_0^{i[0]\cdot j[0]}\, \alpha_1^{i[1]\cdot j[1]} \cdots \alpha_{s-1}^{i[s-1]\cdot j[s-1]}\, a_i,$$

where $i[\ell] \cdot j[\ell]$ is the product of two elements in the ring $\mathbb{Z}_{m_\ell}$. If $A \in \Phi(\mathbb{F}_2[G])$ we can obtain $a = \Phi^{-1}(A)$ through the inverse DFT

$$a_i = \sum_{j \in G} \alpha_0^{-i[0]\cdot j[0]}\, \alpha_1^{-i[1]\cdot j[1]} \cdots \alpha_{s-1}^{-i[s-1]\cdot j[s-1]}\, A_j.$$

We will often refer to the elements a and A as sequences existing in the ‘time-domain’ and the ‘transform-domain’, respectively. We now recall some key properties of the DFT.

The Convolution Property. Let $a, b \in \mathbb{F}_2[G]$ and $c = ab$. If A, B, C are the images of a, b, c, respectively, under the DFT then $C_j = A_j B_j$ for all $j \in G$. Hence convolution in time-domain is equivalent to component-wise product in the transform-domain.

The Modulation Property. Component-wise product in time-domain is equivalent to convolution in the transform-domain. The proof of this property is similar to that of the convolution property above. Since [14] does not include a proof of this fact, we provide a proof in Appendix I for completeness.

The Reversal Property. Let $a, b \in \mathbb{F}_2[G]$ be such that $a_i = b_{0 \ominus i}$ for all $i \in G$. That is, a is obtained via a ‘reversal’ permutation on the coordinates of b. Then A and B satisfy $A_j = B_{0 \ominus j}$ for all $j \in G$, i.e., reversals in time-domain and transform-domain are equivalent.

The Conjugate Symmetry Property. The image of $\mathbb{F}_2[G]$ under the DFT is a proper subset of $\mathbb{F}_q[G]$. An element $A \in \mathbb{F}_q[G]$ belongs to $\Phi(\mathbb{F}_2[G])$ if and only if

$$A_j^2 = A_{2j} \text{ for all } j \in G.$$

If $A \in \Phi(\mathbb{F}_2[G])$ then the value of A_j completely determines the value of A_k for all $k \in \Gamma_j$. In particular, if $k = 2^l j$ then $A_k = A_j^{2^l}$.

3) Characterization of Abelian Codes: There are two direct consequences of the conjugate symmetry property. Assume that $a \in \mathbb{F}_2[G]$ and $A = \Phi(a)$. The first consequence is that, since $j = 2^{|\Gamma_j|} j$, we have $A_j = A_j^{2^{|\Gamma_j|}}$. Hence, for each $j \in G$, A_j belongs to a subfield of $\mathbb{F}_q$ of size $2^{|\Gamma_j|}$. Second, $A_j = 0$ if and only if $A_k = 0$ for all $k \in \Gamma_j$. Hence, the set of coordinates j for which $A_j = 0$ is always a union of conjugacy classes.

Let $Z \subset G$ be a union of conjugacy classes. Define

$$\mathcal{C}(Z) \triangleq \{a \in \mathbb{F}_2[G] \mid A_j = 0 \text{ for all } j \in Z\}.$$

Using the convolution property of DFT it is easy to show that $\mathcal{C}(Z)$ is an ideal in $\mathbb{F}_2[G]$. We will say that Z is the *zero-set* of the abelian code $\mathcal{C}(Z)$. A key structural property of semi-simple abelian group algebras is that every ideal is of the form $\mathcal{C}(Z)$ for some choice of Z.

Theorem IV.1. *(DFT Characterization of Abelian Codes [14].) Let G be an abelian group of odd order and $\mathcal{C}$ be any ideal in $\mathbb{F}_2[G]$. There exists a $Z \subset G$, which is a union of conjugacy classes, such that $\mathcal{C} = \mathcal{C}(Z)$.*

The *non-zeros* of $\mathcal{C}(Z)$ is $\bar{Z} = G \setminus Z$. If $j \in \bar{Z}$ then there exists an $a \in \mathcal{C}(Z)$ such that $A_j \neq 0$. The dimension of $\mathcal{C}(Z)$ over $\mathbb{F}_2$ is $|\bar{Z}| = |G| - |Z|$, see [14].

An ideal of $\mathbb{F}_2[G]$ is *minimal* if it is non-trivial and if it contains no non-trivial ideal as a proper subset. Any abelian code is a direct sum of a collection of *irreducible codes*, which are minimal ideals of $\mathbb{F}_2[G]$ [5], [12], [14]. There is a one-to-one correspondence between the conjugacy classes of G and the minimal ideals of $\mathbb{F}_2[G]$. Let Γ be a conjugacy class of G. The minimal ideal corresponding to the class Γ is the abelian code whose non-zeros are precisely Γ, that is $\mathcal{C}(G \setminus \Gamma)$. In general, if Z is a union of conjugacy classes of G, then

$$\mathcal{C}(Z) = \sum_{\substack{\Gamma \subset G \setminus Z \\ \Gamma \text{ is a conjugacy class}}} \mathcal{C}(G \setminus \Gamma).$$

The dimension of the minimal ideal corresponding to Γ is $|\Gamma|$.

B. Preliminary Results

Let $G^m = G \times \cdots \times G$ be the m-fold product of a group G with itself. We will define two families of codes $\mathcal{B}_G(r,m)$ and $\mathcal{C}_G(r,m)$ as ideals in the group algebra $\mathbb{F}_2[G^m]$. Later in this section we will show that these codes are indeed identical to $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$, where $n = |G|$. In this sub-section, we will introduce some notation to work with the group algebra $\mathbb{F}_2[G^m]$ and its DFT and present some preliminary results related to abelian codes from $\mathbb{F}_2[G^m]$.

As in Section IV-A, let $G = \mathbb{Z}_{m_0} \times \cdots \times \mathbb{Z}_{m_{s-1}}$. We will represent the elements of G^m as vectors and denote them using bold font. If $\boldsymbol{i} \in G^m$, then $\boldsymbol{i} = (i_0, \ldots, i_{m-1})$ where $i_k \in G$ for each $k \in [\![m]\!]$. Recall that since $i_k \in G$, we treat i_k itself as an s-tuple $(i_k[0], \ \cdots \ , i_k[s-1]) \in \mathbb{Z}_{m_0} \times \cdots \times \mathbb{Z}_{m_{s-1}}$. The identity element of G^m is $\mathbf{0} = (0, \ldots, 0)$ where 0 is the identity element of G. The sum of two elements $\boldsymbol{i}, \boldsymbol{j} \in G^m$ is $\boldsymbol{i} \oplus \boldsymbol{j} = (i_0 \oplus j_0, \ldots, i_{m-1} \oplus j_{m-1})$.

The group algebra $\mathbb{F}_2[G^m]$ is $\left\{\sum_{\boldsymbol{i} \in G^m} a_{\boldsymbol{i}} X^{\boldsymbol{i}} \ : \ a_{\boldsymbol{i}} \in \mathbb{F}_2\right\}$. Let $\mathbb{F}_q$, $\alpha_0, \ldots, \alpha_{s-1}$ be as defined in Section IV-A. Applying the definition of DFT from Section IV-A to the group G^m (instead of G) we observe that the DFT Φ is map from $\mathbb{F}_2[G^m]$ into $\mathbb{F}_q[G^m]$. If $\Phi(a) = A = \sum_{\boldsymbol{j} \in G^m} A_{\boldsymbol{j}} X^{\boldsymbol{j}}$ then we have

$$\begin{aligned} A_{\boldsymbol{j}} &= \sum_{\boldsymbol{i} \in G^m} \prod_{k \in [\![m]\!]} \alpha_0^{i_k[0] \cdot j_k[0]} \, \alpha_1^{i_k[1] \cdot j_k[1]} \cdots \alpha_{s-1}^{i_k[s-1] \cdot j_k[s-1]} \, a_{\boldsymbol{i}} \\ &= \sum_{\boldsymbol{i} \in G^m} \left(\prod_{k \in [\![m]\!]} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{i_k[\ell] \cdot j_k[\ell]} \right) a_{\boldsymbol{i}}. \end{aligned}$$

The inverse DFT is given by

$$a_{\boldsymbol{i}} = \sum_{\boldsymbol{j} \in G^m} \left(\prod_{k \in [\![m]\!]} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{-i_k[\ell] \cdot j_k[\ell]} \right) A_{\boldsymbol{j}}. \tag{14}$$

We will need the following result about the conjugacy classes of G^m. Define the Hamming weight, or simply the weight, $w_H(\boldsymbol{i})$ of $\boldsymbol{i} \in G^m$ as the number of non-zero components in the vector $\boldsymbol{i}$, i.e., $w_H(\boldsymbol{i}) = |\{k \mid i_k \neq 0\}|$.

Lemma IV.3. *Let Γ be a conjugacy class of G^m. The weights of all the vectors in Γ are equal.*

Proof. Observe that for every $\boldsymbol{i} \in \Gamma$ there exists a $\boldsymbol{j} \in \Gamma$ such that $\boldsymbol{i} = 2\boldsymbol{j} = \boldsymbol{j} \oplus \boldsymbol{j}$. Hence, it is enough to show that $w_H(\boldsymbol{j}) = w_H(2\boldsymbol{j})$ for all $\boldsymbol{j} \in G^m$. Note that $2\boldsymbol{j} = (j_0 \oplus j_0, \ldots, j_{m-1} \oplus j_{m-1})$. If $j_k \neq 0$ and

$j_k \oplus j_k = 0$, then j_k has order 2 in G. Since $|G|$ is odd this is impossible. Thus, $j_k \oplus j_k = 0$ if and only if $j_k = 0$. This completes the proof. $\square$

We say that $W \subset G^m$ is a *weight class of weight* w if W is the set of all vectors in G^m of weight w. We now consider ideals $\mathcal{C}(Z)$ where Z is a union of weight classes from G^m. Using Lemma IV.3 we observe that such a Z is a union of conjugacy classes and hence $\mathcal{C}(Z)$ is indeed an ideal.

Lemma IV.4. *Let $Z \subset G^m$ be a union of weight classes. The code $\mathcal{C}(Z)$ is closed under time-reversal permutation, that is, if $a \in \mathcal{C}(Z)$ and if $c \in \mathbb{F}_2[G^m]$ is such that $c_{\boldsymbol{i}} = a_{\mathbf{0}\ominus\boldsymbol{i}}$ for all $\boldsymbol{i}$, then $c \in \mathcal{C}(Z)$.*

Proof. From the reversal property of DFT we know that $C_{\boldsymbol{j}} = A_{\mathbf{0}\ominus\boldsymbol{j}}$ for all $\boldsymbol{j}$. Since Z is a union of weight classes and $w_H(\mathbf{0} \ominus \boldsymbol{j}) = w_H(\boldsymbol{j})$ we observe that $\boldsymbol{j} \in Z$ if and only if $\mathbf{0} \ominus \boldsymbol{j} \in Z$. We conclude that $C_{\boldsymbol{j}} = 0$ for all $\boldsymbol{j} \in Z$. This completes the proof. $\square$

We are now ready to identify $\mathcal{C}(Z)^\perp$ when Z is a union of weight classes.

Lemma IV.5. *Let $Z \subset G^m$ be a union of weight classes. The ideal with zero-set $G^m \setminus Z$, i.e., $\mathcal{C}(G^m \setminus Z)$, is the dual code of $\mathcal{C}(Z)$.*

Proof. Let $\bar{Z} = G^m \setminus Z$. Note that $\bar{Z}$ is a union of weight classes. The dimension of $\mathcal{C}(\bar{Z})$ is $|G^m| - |\bar{Z}| = |Z|$, which is equal to the dimension of $\mathcal{C}(Z)^\perp$. Hence, to complete the proof, it is sufficient to show that every codeword in $\mathcal{C}(\bar{Z})$ is orthogonal to every codeword in $\mathcal{C}(Z)$.

We first observe that $cb = 0$ in $\mathbb{F}_2[G^m]$ if $c \in \mathcal{C}(Z)$ and $b \in \mathcal{C}(\bar{Z})$. This follows from applying the convolution property of DFT and observing that for any $\boldsymbol{j} \in G^m$ either $C_{\boldsymbol{j}} = 0$ or $B_{\boldsymbol{j}} = 0$. Since $cb = 0$, the $\mathbf{0}^{\text{th}}$ component of the product cb is $\sum_{\boldsymbol{i} \in G^m} c_{\mathbf{0}\ominus\boldsymbol{i}}\, b_{\boldsymbol{i}} = 0$ for any $c \in \mathcal{C}(Z)$ and $b \in \mathcal{C}(\bar{Z})$.

We are now ready to complete the proof. Let $a \in \mathcal{C}(Z)$ and $b \in \mathcal{C}(\bar{Z})$. Let c be the time-reversal of a. From Lemma IV.4, we know that $c \in \mathcal{C}(Z)$, and hence, $cb = 0$. This implies $\sum_{\boldsymbol{i}} c_{\mathbf{0}\ominus\boldsymbol{i}} b_{\boldsymbol{i}} = 0$. Since $c_{\mathbf{0}\ominus\boldsymbol{i}} = a_{\boldsymbol{i}}$, we have $\sum_{\boldsymbol{i}} a_{\boldsymbol{i}} b_{\boldsymbol{i}} = 0$. $\square$

C. Construction of $\mathcal{B}_n(r,m)$ and $\mathcal{C}_n(r,m)$ via DFT

We will now define two codes $\mathcal{B}_G(r,m)$ and $\mathcal{C}_G(r,m)$ as ideals in $\mathbb{F}_2[G^m]$. Let

$$\mathcal{Z}(r,m) = \{\boldsymbol{j} \in G^m \mid w_H(\boldsymbol{j}) \geq r+1\}$$

be the set of all elements in G^m with weight greater than r. The complement of $\mathcal{Z}(r,m)$ is

$$\bar{\mathcal{Z}}(r,m) = G^m \setminus \mathcal{Z}(r,m) = \{\boldsymbol{j} \in G^m \mid w_H(j) \leq r\}\,.$$

Note that both $\mathcal{Z}(r,m)$ and $\bar{\mathcal{Z}}(r,m)$ are unions of weight classes.

Definition IV.1. The code $\mathcal{C}_G(r,m)$ is the ideal in $\mathbb{F}_2[G^m]$ with zero-set $\mathcal{Z}(r,m)$, and $\mathcal{B}_G(r,m)$ is the dual code of $\mathcal{C}_G(r,m)$.

Clearly, $\mathcal{C}_G(r,m)$ has block length $|G|^m$ and dimension

$$|G^m| - |\mathcal{Z}(r,m)| = |\bar{\mathcal{Z}}(r,m)| = \sum_{w=0}^{r} \binom{m}{w} (|G|-1)^w\,.$$

Since $|G^m| = \sum_{w=0}^{m} \binom{m}{w}(|G|-1)^w$, we deduce that the dimension of $\mathcal{B}_G(r,m)$ is

$$\sum_{w=r+1}^{m} \binom{m}{w} (|G|-1)^w,$$

which is equal to $|\mathcal{Z}(r,m)|$.

The following properties are direct consequences of the above definition.

Lemma IV.6. *Let $0 \leq r_1 \leq r_2 \leq m$.*

1) $\mathcal{C}_G(r_1, m) \subset \mathcal{C}_G(r_2, m)$.
2) $\mathcal{C}_G(0, m)$ *is the repetition code of length* $|G|^m$.
3) $\mathcal{C}_G(m, m) = \mathbb{F}_2[G^m]$.

Proof. Part 1. Let $a \in \mathcal{C}_G(r_1, m)$. Then $A_{\boldsymbol{j}} = 0$ if $w_H(\boldsymbol{j}) \geq r_1 + 1$. This implies $A_{\boldsymbol{j}} = 0$ for all $\boldsymbol{j}$ with $w_H(\boldsymbol{j}) \geq r_2 + 1$. Hence, $a \in \mathcal{C}_G(r_2, m)$.

Part 2. Note that $\bar{\mathcal{Z}}(0, m) = \{\mathbf{0}\}$. Hence, $a \in \mathcal{C}_G(0, m)$ if and only if $A_{\boldsymbol{j}} = 0$ for all $\boldsymbol{j} \neq \mathbf{0}$ and $A_{\mathbf{0}}$ satisfies the conjugate symmetry property. That is, $A_{\mathbf{0}}^2 = A_{2 \cdot \mathbf{0}} = A_{\mathbf{0}}$, or equivalently, $A_{\mathbf{0}} \in \mathbb{F}_2$. Using the inverse DFT, we deduce that $a_{\boldsymbol{i}} = A_{\mathbf{0}}$ for all $\boldsymbol{i} \in G^m$. This proves that $\mathcal{C}_G(0, m)$ is the repetition code.

Part 3. Since the zero-set $\mathcal{Z}(m, m) = \varnothing$, we have $\mathcal{C}_G(m, m) = \mathbb{F}_2[G^m]$. □

The following results on $\mathcal{B}_G(r, m)$ are consequences of Lemmas IV.4 and IV.5.

Corollary IV.1. *For any* $0 \leq r \leq m$*, we have*
1) $\mathcal{B}_G(r, m) = \mathcal{C}(\bar{\mathcal{Z}}(r, m))$.
2) Both $\mathcal{C}_G(r, m)$ *and* $\mathcal{B}_G(r, m)$ *are closed under time-reversal permutation.*
3) $\mathcal{C}_G(r, m)$ *and* $\mathcal{B}_G(r, m)$ *are complementary duals.*

Proof. The proofs of parts 1 and 2 follow directly from Lemmas IV.5 and IV.4, respectively.

Part 3. Let $a \in \mathcal{C}_G(r, m) \cap \mathcal{B}_G(r, m)$. Consider $A = \Phi(a)$. If $w_H(\boldsymbol{j}) \leq r$ then $A_{\boldsymbol{j}} = 0$ since $a \in \mathcal{B}_G(r, m)$. If $w_H(\boldsymbol{j}) \geq r + 1$ then $A_{\boldsymbol{j}} = 0$ since $a \in \mathcal{C}_G(r, m)$. Hence, $A = 0$ and $a = 0$. Thus, $\mathcal{C}_G(r, m) \cap \mathcal{B}_G(r, m) = \{0\}$. □

We note that codes with complementary duals are known to be useful in cryptography [25].

1) Relation to the Classical Berman Codes: The subclass of codes corresponding to $G = \mathbb{Z}_p$ with p being an odd prime was introduced and studied by Berman [5], and Blackmore and Norton [6]. Both [5] and [6] provide a time-domain description of $\mathcal{B}_{\mathbb{Z}_p}(r, m)$ and $\mathcal{C}_{\mathbb{Z}_p}(r, m)$. In Appendix II we recall the original description of these codes from [6] and show that this is identical to our transform-domain description for the case $G = \mathbb{Z}_p$.

2) Relation to $\mathcal{B}_n(r, m)$ *and* $\mathcal{C}_n(r, m)$*:* We will use a technique from [6] to identify a recursive structure for $\mathcal{C}_G(r, m)$, and use this structure to show that $\mathcal{C}_G(r, m)$ and $\mathcal{B}_G(r, m)$ are in fact the same as $\mathcal{C}_n(r, m)$ and $\mathcal{B}_n(r, m)$ for any choice of G with $|G| = n$. This technique was used in [6] to show that the minimum distance of $\mathcal{C}_{\mathbb{Z}_p}(r, m)$ is p^{m-r} for any odd prime p. The key difference between our work and [6] is that we rely on the DFT tool for our analysis, and our results hold for any odd-ordered abelian group G.

Towards obtaining the recursive structure we will assume an ordering on the index set G^m of the coordinates of any $a \in \mathbb{F}_2[G^m]$. Suppose the elements of G are $\{g_0, \ldots, g_{|G|-1}\}$ with $g_0 = 0$. We represent a as

$$a = \left(a_0 \mid a_1 \mid \cdots \mid a_{|G|-1}\right)$$

where $a_\ell \in \mathbb{F}_2[G^{m-1}]$ for each $\ell \in [\![\, |G| \,]\!]$. We will use the standard notation

$$a_\ell = \sum_{\boldsymbol{i'} \in G^{m-1}} a_{\ell, \boldsymbol{i'}} X^{\boldsymbol{i'}}, \text{ where } a_{\ell, \boldsymbol{i'}} \in \mathbb{F}_2,$$

and relate $a_0, \ldots, a_{|G|-1}$ to a as follows

$$a = \sum_{\ell \in [\![\, |G| \,]\!]} \sum_{\boldsymbol{i'} \in G^{m-1}} a_{\ell, \boldsymbol{i'}} \, X^{(\boldsymbol{i'} | g_\ell)}.$$

Equivalently, if $a = \sum_{\boldsymbol{i} \in G^m} a_{\boldsymbol{i}} X^{\boldsymbol{i}}$, and if for a given $\boldsymbol{i} \in G^m$ we have $\boldsymbol{i} = (i_0, \ldots, i_{m-2}, g_\ell)$ for some choice of ℓ, then $a_{\ell, (i_0, \ldots, i_{m-2})} = a_{\boldsymbol{i}}$.

Lemma IV.7. *(Recursive structure of* $\mathcal{C}_G(r, m)$*.) For any odd ordered abelian group* G *and any* $1 \leq r \leq m - 1$*, we have*

$$\mathcal{C}_G(r, m) = \left\{ (u + u_0 | u + u_1 | \cdots | u + u_{|G|-2} | u) \ : \ u_l \in \mathcal{C}_G(r - 1, m - 1), u \in \mathcal{C}_G(r, m - 1) \right\}.$$

Proof. The full proof is available in Appendix I. The proof uses two fundamental properties of the DFT, viz., *(i)* the DFT of the indicator function of the subgroup $G^{m-1} \times \{0\}$ is the indicator function of $\{0\}^{m-1} \times G$; and *(ii)* the characterization of the DFT of the periodic sequence $a = (b \mid \cdots \mid b)$ in terms of the DFT of its fundamental copy b. Both these results are also included as part of the proof of this lemma.

An intermediate step in the proof is to identify two subcodes $\mathcal{C}_1$ and $\mathcal{C}_2$ of $\mathcal{C}_G(r,m)$, and show that $\mathcal{C}_G(r,m)$ is a direct sum of $\mathcal{C}_1$ and $\mathcal{C}_2$. A similar idea was used in [6] to derive the minimum distance of $\mathcal{C}_{\mathbb{Z}_p}(r,m)$. Please see Appendix I for the complete proof. $\square$

The recursive construction of $\mathcal{C}_G(r,m)$ in Lemma IV.7 ultimately uses codes of the form $\mathcal{C}_G(0,m')$ and $\mathcal{C}_G(m',m')$, for some choices of m', as its building blocks. Note that $\mathcal{C}_G(0,m')$ and $\mathcal{C}_G(m',m')$ are the repetition code and the universe code of length $|G|^{m'}$, and hence, both these codes depend on G only via $|G|$. By using an induction argument, we conclude that the construction shown in Lemma IV.7 depends on the choice of G only through its order $|G|$. Furthermore, we observe that this recursion is identical to the definition of $\mathcal{C}_n(r,m)$ if $n = |G|$. Using this observation together with the facts $\mathcal{C}_G(r,m)^\perp = \mathcal{B}_G(r,m)$ and $\mathcal{C}_n(r,m)^\perp = \mathcal{B}_n(r,m)$ immediately leads us to the following main result of this sub-section.

Corollary IV.2. *Let $n \geq 3$ be an odd integer and let G be any abelian group of order n. Then for all $0 \leq r \leq m$,*

$$\mathcal{C}_G(r,m) = \mathcal{C}_n(r,m) \text{ and } \mathcal{B}_G(r,m) = \mathcal{B}_n(r,m).$$

D. A Family of Abelian Codes that Achieve BEC Capacity

We will now study a family of abelian codes that includes $\mathcal{C}_G(r,m)$ and $\mathcal{B}_G(r,m)$. The family of codes that we are interested in are ideals $\mathcal{C}(Z)$ in $\mathbb{F}_2[G^m]$ with the property that the zero-set Z is closed under certain permutations of G^m. We detail these permutations next.

1) Two Classes of Permutations on G^m: We will first need the result that the map $i \to 2i$ is a permutation on G. If there exist $i, i' \in G$ such that $2i = 2i'$ then we have $2(i - i') = 0$. Since there is no element in G of order 2 (because $|G|$ is odd), we conclude that $i = i'$. Hence, $i \to 2i$ is a permutation on G. We observe that for each $j \in G$ there exists a unique element in G, which we will denote as $2^{-1}j$, such that $j = 2\,(2^{-1}j)$, i.e., $j = 2^{-1}j \oplus 2^{-1}j$.

For each $k \in [\![m]\!]$, let π_k be the permutation

$$(i_0, \ldots, i_{m-1}) \to (i_0, \ldots, i_{k-1}, 2i_k, i_{k+1}, \ldots, i_{m-1}).$$

The inverse permutation π_k^{-1} is

$$(j_0, \ldots, j_{m-1}) \to (j_0, \ldots, j_{k-1}, 2^{-1}j_k, j_{k+1}, \ldots, j_{m-1}). \tag{15}$$

Note that the permutation $i_k \to 2i_k$ on G fixes 0, hence, we see that $i_k \neq 0$ if and only if $2i_k \neq 0$. Thus, both π_k and π_k^{-1} are weight preserving permutations on G^m, that is $w_H(\pi_k(\boldsymbol{i})) = w_H(\boldsymbol{i})$ for all $\boldsymbol{i} \in G^m$.

Note that each $\gamma \in \mathcal{S}_m$ is a permutation on $[\![m]\!]$. We let $\gamma \in \mathcal{S}_m$ act on G^m as follows

$$(j_0, \ldots, j_{m-1}) \to \left(j_{\gamma(0)}, \ldots, j_{\gamma(m-1)}\right).$$

With this group action we view $\gamma \in \mathcal{S}_m$ as a permutation on G^m. The inverse permutation is γ^{-1}, which is the inverse of γ in $\mathcal{S}_m$. Similar to π_k, we see that γ is also a weight preserving permutation.

The following two lemmas show the interplay between the permutations γ and π_k and the DFT.

Lemma IV.8. *Let $k \in [\![m]\!]$ and $a \in \mathbb{F}_2[G^m]$, and let $b \in \mathbb{F}_2[G^m]$ be the sequence obtained by applying π_k on the coordinates of a, i.e., $b_{\pi_k(\boldsymbol{i})} = a_{\boldsymbol{i}}$ for all $\boldsymbol{i} \in G^m$. Then*

$$B_{\boldsymbol{j}} = A_{\pi_k^{-1}(\boldsymbol{j})} \text{ for all } \boldsymbol{j} \in G^m.$$

Proof. Viewing $j_k \in G = \mathbb{Z}_{m_0} \times \cdots \mathbb{Z}_{m_{s-1}}$ as an s-tuple we have

$$2^{-1} j_k = (2^{-1} j_k[0],\, \ldots,\, 2^{-1} j_k[s-1]),$$

where $2^{-1} j_k[\ell]$ is the product of $j_k[\ell]$ with the multiplicative inverse of 2 in the ring $\mathbb{Z}_{m_\ell}$ (since m_ℓ is odd, 2 is a unit in $\mathbb{Z}_{m_\ell}$). For any $i_k[\ell], j_k[\ell] \in \mathbb{Z}_{m_\ell}$, we observe that

$$2 i_k[\ell] \cdot 2^{-1} j_k[\ell] = i_k[\ell] \cdot j_k[\ell]. \tag{16}$$

Since $b_{\pi_k(\boldsymbol{i})} = a_{\boldsymbol{i}}$, the DFT of b at $\boldsymbol{j}$ is

$$B_{\boldsymbol{j}} = \sum_{\boldsymbol{i} \in G^m} \left(\prod_{\substack{k' \in [\![m]\!] \\ k' \neq k}} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{i_{k'}[\ell] \cdot j_{k'}[\ell]} \cdot \prod_{\ell \in [\![s]\!]} \alpha_\ell^{2 i_k[\ell] \cdot j_k[\ell]} \right) a_{\boldsymbol{i}}.$$

Using the inverse permutation (15) and the property (16), we immediately deduce that $B_{\pi_k^{-1}(\boldsymbol{j})} = A_{\boldsymbol{j}}$ for all $\boldsymbol{j} \in G^m$. □

Lemma IV.9. *Let $\gamma \in \mathcal{S}_m$, and $a, b \in \mathbb{F}_2[G^m]$ be such that $b_{\gamma(\boldsymbol{i})} = a_{\boldsymbol{i}}$ for all $\boldsymbol{i} \in G^m$. Then $B_{\boldsymbol{j}} = A_{\gamma^{-1}(\boldsymbol{j})}$ for all $\boldsymbol{j} \in G^m$.*

Proof. We note that

$$B_{\boldsymbol{j}} = \sum_{\boldsymbol{i} \in G^m} \left(\prod_{k \in [\![m]\!]} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{i_{\gamma(k)}[\ell] \cdot j_k[\ell]} \right) a_{\boldsymbol{i}}.$$

Clearly,

$$B_{\boldsymbol{j}} = \sum_{\boldsymbol{i} \in G^m} \left(\prod_{k \in [\![m]\!]} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{i_k[\ell] \cdot j_{\gamma^{-1}(k)}[\ell]} \right) a_{\boldsymbol{i}} = A_{\gamma^{-1}(\boldsymbol{j})}.$$

This completes the proof. □

2) A Family of Abelian Codes from $\mathbb{F}_2[G^m]$: The codes studied in this sub-section are precisely the ideals $\mathcal{C}(Z) \subset \mathbb{F}_2[G^m]$ whose zero-set Z is closed under all the below permutations

$$\pi_k, k \in [\![m]\!] \text{ and all } \gamma \in \mathcal{S}_m.$$

Example IV.2. Consider the group $G = \mathbb{Z}_{15}$ and use $m = 2$. In the additive group $\mathbb{Z}_{15} = \{0, 1, \ldots, 14\}$, the set $\{5, 10\}$ forms a conjugacy class, i.e., this set is closed under multiplication by 2 in the ring $\mathbb{Z}_{15}$. Now consider

$$Z_1 = \{(0,5), (0,10), (5,0), (10,0)\} \subset \mathbb{Z}_{15}^2.$$

This is a union of two conjugacy classes $\{(0,5), (0,10)\}$ and $\{(5,0), (10,0)\}$. Further, Z_1 is closed under the permutation $(j_0\ j_1) \to (j_1\ j_0)$. Clearly, Z_1 is a zero-set of an ideal in $\mathbb{F}_2[\mathbb{Z}_{15}^2]$ and is closed under π_0, π_1 and all $\gamma \in \mathcal{S}_2$.

Another such choice of zero-set is

$$Z_2 = \{(5,5), (5,10), (10,5), (10,10)\} \subset \mathbb{Z}_{15}^2.$$

We observe that neither Z_1 nor Z_2 is the zero-set of $\mathcal{C}_{\mathbb{Z}_{15}}(r, 2)$ or $\mathcal{B}_{\mathbb{Z}_{15}}(r, 2)$ for any choice of r. □

Remark IV.1. We remark that if W is a weight class in G^m, then it is closed under $\pi_0, \ldots, \pi_{m-1}$ and $\gamma \in \mathcal{S}_m$. To see this, note that π_k and γ are weight preserving maps and W is the set of all tuples in G^m of a given weight. This immediately implies that any zero-set that is a union of weight classes is also closed under the permutations $\{\pi_0, \ldots, \pi_{m-1}\}$ and $\mathcal{S}_m$. Therefore, the zero-sets of $\mathcal{B}_G(r, m)$ and $\mathcal{C}_G(r, m)$ belong to this class of zero-sets. $\square$

We will now analyse some automorphisms of this family of abelian codes. Unless otherwise specified, we will assume that Z is a zero-set closed under the actions of $\{\pi_k : k \in [\![m]\!]\} \cup \mathcal{S}_m$. Since $\mathcal{C}(Z)$ is an ideal in a group algebra, it is transitive, see Lemma IV.1. From the proof of Lemma IV.1 we recognize that for each choice of $\boldsymbol{k} \in G^m$ the following permutation of the set of coordinates G^m is an automorphism of $\mathcal{C}(Z)$

$$\boldsymbol{i} \to \boldsymbol{i} \oplus \boldsymbol{k},$$

which corresponds to multiplication of a codeword $a \in \mathcal{C}(Z)$ by the element $X^{\boldsymbol{k}} \in \mathbb{F}_2[G^m]$. We now identify two more classes of automorphisms of $\mathcal{C}(Z)$.

Theorem IV.2. *Let $Z \subset G^m$ be a zero-set that is closed under the actions of $\pi_0, \ldots, \pi_{m-1}$ and all $\gamma \in \mathcal{S}_m$. For each $k \in [\![m]\!]$, and for each $\gamma \in \mathcal{S}_m$, the permutations π_k and γ applied on the coordinates $\boldsymbol{i} \in G^m$ of a codeword $a = \sum_{\boldsymbol{i} \in G^m} a_{\boldsymbol{i}} X^{\boldsymbol{i}} \in \mathbb{F}_2[G^m]$ are automorphisms of $\mathcal{C}(Z)$.*

Proof. Let $a \in \mathcal{C}(Z)$ and b be the sequence obtained by applying π_k on the coordinates of a. We know that $A_{\boldsymbol{j}} = 0$ for all $\boldsymbol{j} \in Z$. We want to show that $B_{\boldsymbol{j}} = 0$ for all $\boldsymbol{j} \in Z$. Towards this, observe that $\pi_k(Z) = Z$, and hence, $\pi_k^{-1}(\boldsymbol{j}) \in Z$. Now using Lemma IV.8, we have $B_{\boldsymbol{j}} = A_{\pi_k^{-1}(\boldsymbol{j})} = 0$ for all $\boldsymbol{j} \in Z$. Hence, $b \in \mathcal{C}(Z)$.

The proof for $\gamma \in \mathcal{S}_m$ is similar and uses Lemma IV.9. $\square$

Remark IV.2. The proof of the π_k part of Theorem IV.2 mainly relies on the fact that the integer 2 is a unit in all the rings $\mathbb{Z}_{m_0}, \ldots, \mathbb{Z}_{m_{s-1}}$. These results in Lemma IV.8 and Theorem IV.2 will hold if the role played by 2 is taken by any integer that is a common unit of $\mathbb{Z}_{m_0}, \ldots, \mathbb{Z}_{m_{s-1}}$. $\square$

3) Achieving the Capacity of BEC: Our proof for capacity achievability relies on the sufficient condition identified by Kumar et al. [7].

Let $\mathcal{G}$ be the automorphism group of $\mathcal{C}(Z)$. Let $\mathcal{G}_0$ be the subgroup of automorphisms for which $\mathbf{0}$ is a fixed point. Of main interest to us are the orbits of the non-zero points of G^m under the action of $\mathcal{G}_0$. We will now derive a lower bound on the sizes of these orbits. For each $\boldsymbol{i} \in G^m \setminus \{\mathbf{0}\}$ define

$$\mathcal{O}(\boldsymbol{i}) = \{\pi(\boldsymbol{i}) \ : \ \pi \in \mathcal{G}_0\},$$

to be the orbit of $\boldsymbol{i}$ under the action of $\mathcal{G}_0$. From Theorem IV.2 we know that π_k, $k \in [\![m]\!]$, and $\gamma \in \mathcal{S}_m$ are code automorphisms that are weight preserving. In particular, these automorphisms have $\mathbf{0}$ as a fixed point, and hence, they belong to $\mathcal{G}_0$. We observe that the automorphisms $\pi_k, \pi_k^2, \ldots$ acting on $\boldsymbol{i} \in G^m$ generate the set of vectors

$$\{\, (i_0, \ldots, i_{k-1}, j, i_{k+1}, \ldots, i_{m-1}) \quad : \quad j \in \Gamma_{i_k} \,\},$$

where Γ_{i_k} is the conjugacy class of i_k in the group G. Considering the actions of all possible powers and products of π_k, $k \in [\![m]\!]$, and $\gamma \in \mathcal{S}_m$, we conclude that $\mathcal{O}(\boldsymbol{i})$ includes

$$\bigcup_{\gamma \in \mathcal{S}_m} \{\, (j_0, \ldots, j_{m-1}) \in G^m \ : \ j_{\gamma(k)} \in \Gamma_{i_k} \text{ for all } k \in [\![m]\!] \,\}. \tag{17}$$

Using the fact $|\Gamma_{i_k}| \geq 2$ if $i_k \in G \setminus \{0\}$ (see Lemma IV.2), we observe that the size of (17), and hence $|\mathcal{O}(\boldsymbol{i})|$ is lower bounded by

$$\binom{m}{w_H(\boldsymbol{i})} 2^{w_H(\boldsymbol{i})}.$$

We note that

$$\min_{\boldsymbol{i} \in G^m \setminus \{\mathbf{0}\}} |\mathcal{O}(\boldsymbol{i})| \geq \min_{w \in \{1, \ldots, m\}} \binom{m}{w} 2^w = 2m. \tag{18}$$

Theorem IV.3. *Let G be any odd-ordered abelian group with $|G| \geq 3$ and $\{m_l\}$ be a sequence of positive integers with $m_l \to \infty$. If for each l, $Z_l \subset G^{m_l}$ is a union of conjugacy classes satisfying the following conditions*

1) *Z_l is closed under the actions of $\pi_0, \ldots, \pi_{m_l-1}$ and $\mathcal{S}_{m_l}$, and*
2) *the rates of the sequence of abelian codes $\{\mathcal{C}(Z_l)\}$ converges to $R^* \in (0,1)$,*

then the bit erasure probability of the sequence of codes $\{\mathcal{C}(Z_l)\}$ converges to zero under bit-MAP decoding on any BEC with channel erasure probability $\epsilon \in [0, 1-R^*)$. Further, for any $R^* \in (0,1)$ there exists a sequence of abelian codes satisfying the above conditions.

Proof. We observe that each code $\mathcal{C}(Z_l)$ is an ideal, and hence, transitive (see Lemma IV.1). From Theorem IV.2 and (18), we have

$$\min_{\boldsymbol{i} \in G^{m_l} \setminus \{\boldsymbol{0}\}} |\mathcal{O}_l(\boldsymbol{i})| \geq 2m_l$$

where $\mathcal{O}_l(\boldsymbol{i})$ is the orbit of $\boldsymbol{i}$ under the action of the subgroup $\mathcal{G}_0$ of automorphisms of the code $\mathcal{C}(Z_l)$. Clearly,

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

Now using [7, Theorem 19], we conclude that in any BEC with channel erasure probability less than $1-R^*$, the bit erasure probabilities of the sequence of codes $\{\mathcal{C}(Z_l)\}$ under bit-MAP decoding converges to 0.

From Theorem III.2 we know that for any choice of $R^* \in (0,1)$ there exists a sequence of dual Berman codes $\{\mathcal{C}_n(r_l, m_l)\}$ with rates converging to R^*. Choosing $n = |G|$, and using Corollary IV.2, we observe that $\mathcal{C}_n(r_l, m_l)$ is an abelian code in $\mathbb{F}_2[G^{m_l}]$, and its zero-set $Z_l \subset G^{m_l}$ is a union of weight classes. From the discussion in Remark IV.1, we observe that this zero-set Z_l is closed under the actions of $\pi_0, \ldots, \pi_{m-1}$ and $\mathcal{S}_{m_l}$. This completes the proof of the second part of this theorem. ☐

V. Simulation Results

We present a few simulation results to get a glimpse of the performance of the codes identified in this work in comparison with the RM codes in the BEC. For a given code $\mathcal{C} \subset \mathbb{F}_2^{n^m}$, we assume that the transmitted codeword $c = (c_i : i \in [\![n^m]\!])$ is picked uniformly at random from the codebook. The code symbols $c_i \in \{0,1\}$ are transmitted sequentially through the BEC with erasure probability ϵ. The channel output corresponding to the input c_i is y_i, i.e., $\Pr(y_i = c_i) = 1-\epsilon$ and $\Pr(y_i = ?) = \epsilon$. We use $y = (y_i \ : \ i \in [\![n^m]\!])$ to denote the channel output sequence, and $y_{\sim i}$ to denote the collection of all channel outputs except y_i. Please note that c_i and y_i are random variables.

The EXIT function for the i^{th} transmitted bit is $h_i(\epsilon) = \mathcal{H}(c_i | y_{\sim i})$, where $\mathcal{H}(\cdot|\cdot)$ is the conditional entropy. The average EXIT function is

$$h(\epsilon) = \frac{1}{n^m} \sum_{i \in [\![n^m]\!]} h_i(\epsilon).$$

All the codes considered in this section are transitive. For transitive codes we have $h(\epsilon) = h_i(\epsilon)$ for all i [3]. The average bit erasure probability under bit-MAP decoding satisfies $P_b = \epsilon h(\epsilon)$ [3]. For transitive codes $P_b = \epsilon h_i(\epsilon)$ for every $i \in [\![n^m]\!]$. We perform bit-MAP decoding for exactly one of the transmitted bits, viz., c_0, and numerically estimate the value of $h_0(\epsilon)$. We then obtain the bit erasure probability as $P_b = \epsilon h_0(\epsilon)$.

We have tried to compare 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. 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).

The codes considered in our simulations use $n = 3$, or equivalently the abelian group $G = \mathbb{Z}_3$. This abelian group belongs to the family of cyclic groups $(\mathbb{Z}_p, +)$ of odd prime order p, with 2 being a primitive

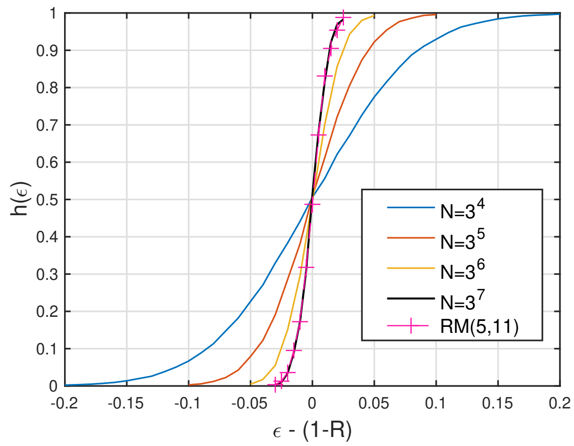

Fig. 2. EXIT functions of abelian codes from $\mathbb{F}_2[\mathbb{Z}_3^m]$, with $m = 4, 5, 6, 7$, whose zero-set is the collection of all vectors of odd weight from $\mathbb{Z}_3^m$. The EXIT function of rate $1/2$ RM code of length 2^{11} is also shown.

TABLE II
BASIC PARAMETERS OF THE CODES COMPARED IN FIG. 2.

Code	Length	Dimension	Rate
Ideal in $\mathbb{F}_2[\mathbb{Z}_3^4]$	81	41	0.5062
Ideal in $\mathbb{F}_2[\mathbb{Z}_3^5]$	243	121	0.4979
Ideal in $\mathbb{F}_2[\mathbb{Z}_3^6]$	729	365	0.5007
Ideal in $\mathbb{F}_2[\mathbb{Z}_3^7]$	2187	1093	0.4998
$\mathrm{RM}(5, 11)$	2048	1024	0.5

TABLE III
PARAMETERS OF THE CODES COMPARED IN FIG. 3 AND 4.

Code	Length	Dimension	Rate	Minimum Distance
$\mathcal{B}_3(5, 7)$	2187	576	0.2634	64
$\mathrm{RM}(4, 11)$	2048	562	0.2744	128
$\mathcal{C}_3(5, 7)$	2187	1611	0.7366	9
$\mathrm{RM}(6, 11)$	2048	1486	0.7256	32

root modulo p. For such values of p, we explicitly identify the generator matrices of all abelian codes obtained from $\mathbb{F}_2[\mathbb{Z}_p^m]$ in Appendix III.

We illustrate the sharp 0-to-1 transition of the EXIT function (for increasing block length N) in Fig. 2 using a sequence of four codes with rates close to $1/2$. These codes are ideals in $\mathbb{F}_2[\mathbb{Z}_3^m]$, with $m = 4, 5, 6, 7$, respectively. We choose the zero-set of the code of length 3^m as the collection of all odd-weight vectors in $\mathbb{Z}_3^m$. Clearly, this zero-set is a union of weight classes, and satisfies the conditions required by Theorem IV.3. The basic parameters of these four codes are summarized in Table II. Fig. 2 also shows the EXIT function of the RM code of rate 0.5 and length 2048. The rate and dimension of this RM code are similar to those of the abelian code with $m = 7$.

We compare the block erasure rate P_B (under block-MAP decoding) and bit erasure rate P_b (under bit-MAP decoding) of $\mathcal{B}_3(5, 7)$ and $\mathcal{C}_3(5, 7)$ with RM codes in Fig. 3 and 4. The basic parameters of these codes are summarized in Table III. The code $\mathcal{B}_3(5, 7) = \mathcal{B}_{\mathbb{Z}_3}(5, 7)$ belongs to a class of codes identified by Berman [5], and $\mathcal{C}_3(5, 7) = \mathcal{C}_{\mathbb{Z}_3}(5, 7)$ is the dual of this Berman code. In the simulation scenarios presented in Fig. 3 and 4, the bit erasure rates P_b of $\mathcal{B}_3(5, 7)$ and $\mathcal{C}_3(5, 7)$ are similar to those of RM

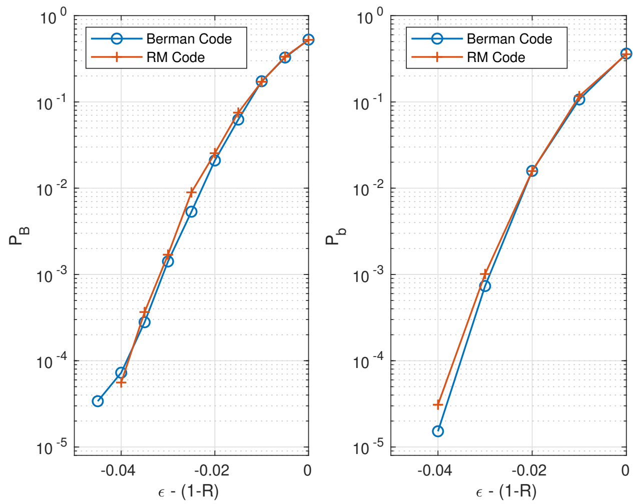

Fig. 3. The block erasure rate P_B and bit erasure rate P_b of $\mathcal{B}_3(5,7)$ and $\mathrm{RM}(4,11)$ in the BEC.

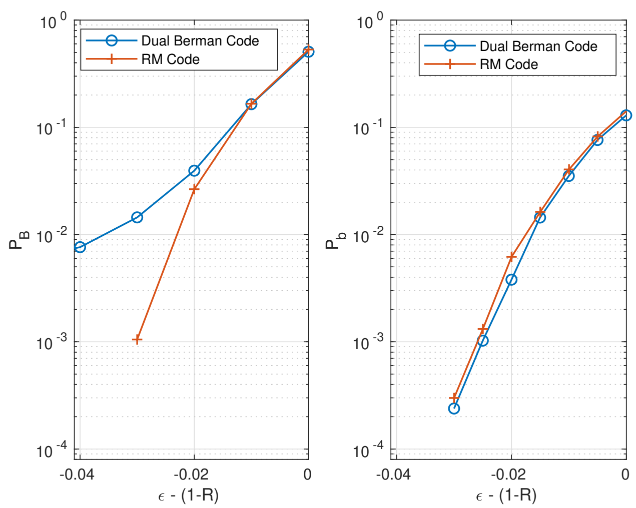

Fig. 4. The block erasure rate P_B and bit erasure rate P_b of $\mathcal{C}_3(5,7)$ and $\mathrm{RM}(6,11)$ in the BEC.

codes of similar rate and block length. However, note the small minimum distance and the high floor in the block erasure rate of $\mathcal{C}_3(5,7)$ in Fig. 4.

VI. Discussion

We identified a family of codes, that includes the RM codes [1], [2] ($n = 2$) and the Berman codes [5], [6] (n an odd prime) and whose properties are similar to RM codes. When n is odd, we used the semi-simple structure of $\mathbb{F}_2[G^m]$ and its associated DFT to identify a larger class of codes that achieve the BEC capacity. 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. Note that this family contains codes corresponding to a richer set of block lengths and dimensions than RM codes. The code properties identified in Section III and the simulation results presented in Section V support the idea that these codes might enjoy a good performance in BMS channels when the block lengths are large.

The current work exposes some questions that seem to deserve investigation.

1) 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.
2) 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 [26].

APPENDIX I
PROOFS

A. *Proof of The Modulation Property of DFT*

Let $a, b, c \in \mathbb{F}_2[G]$ be such that $c_i = a_i b_i$ for all $i \in G$. Then taking the DFT of c we have

$$\begin{aligned}
C_j &= \sum_{i\in G}\prod_{\ell\in[\![s]\!]} \alpha_\ell^{i[\ell]\cdot j[\ell]} a_i b_i \\
&= \sum_{i\in G}\prod_{\ell\in[\![s]\!]} \alpha_\ell^{i[\ell]\cdot j[\ell]} \left(\sum_{k\in G}\prod_{\ell'\in[\![s]\!]} \alpha_\ell^{-i[\ell']\cdot k[\ell']} A_k\right) b_i \\
&= \sum_{k\in G} A_k \sum_{i\in G}\prod_{\ell\in[\![s]\!]} \alpha_\ell^{-i[\ell]\cdot(j[\ell]-k[\ell])} b_i \\
&= \sum_{k\in G} A_k B_{j\ominus k}.
\end{aligned}$$

Hence, $C = AB$ in $\mathbb{F}_q[G]$.

B. *Proof of Lemma III.3*

We first observe that $1 - R_n(r,m) \geq 1 - R_n(r+k, m+k)$. To see this we use the fact that $R_n(r+k, m+k) - R_n(r,m)$ equals

$$\Pr(X_0 + \cdots + X_{m+k-1} \leq r+k) - \Pr(X_0 + \cdots + X_{m-1} \leq r).$$

Using similar ideas as in the proof of Lemma III.2 we can show that the difference in the rates of $\mathcal{B}_n(r,m)$ and $\mathcal{B}_n(r+k, m+k)$ is at the most

$$\frac{2\kappa}{\sqrt{m}} + \frac{1}{\sqrt{2\pi}}\left|\frac{r+k-(m+k)\mu}{\sigma\sqrt{m+k}} - \frac{r-m\mu}{\sigma\sqrt{m}}\right|.$$

Using triangle inequality, we see that the second term in the above sum is at the most

$$\frac{1}{\sigma\sqrt{2\pi m(m+k)}}\Big(\ |(r+k)\sqrt{m} - r\sqrt{m+k}| + \mu\sqrt{m(m+k)}\ |\sqrt{m+k} - \sqrt{m}|\ \Big).$$

Now using $\sqrt{m+k} - \sqrt{m} \leq \frac{k}{2\sqrt{m}}$ we can show that $(r+k)\sqrt{m} - r\sqrt{m+k} \geq 0$. Making use of the fact $k \geq 0$, we then have

$$0 \leq (r+k)\sqrt{m} - r\sqrt{m+k} \leq k\sqrt{m}.$$

Straightforward algebraic manipulations then lead us to the following upper bound on the rate difference

$$\frac{2\kappa}{\sqrt{m}} + \frac{k}{\sqrt{m}}\frac{(\mu+2)}{\sqrt{8\pi\sigma^2}}.$$

C. Proof of Lemma IV.7

We first need the following basic results about the DFT.

Lemma I.1. *(DFT of the indicator function of a direct-product subgroup.) If a is the indicator function of $G^{m-1} \times \{0\}$ then its DFT A is the indicator function of $\{0\}^{m-1} \times G$.*

Proof. We need to show that if $A \in \mathbb{F}_q[G^m]$ is such that $A_{\boldsymbol{j}} = 1$ if $(j_0, \ldots, j_{m-2}) = \mathbf{0}$ and $A_{\boldsymbol{j}} = 0$ otherwise, then its inverse DFT is such that $a_{\boldsymbol{i}} = 1$ if $i_{m-1} = 0$ and $a_{\boldsymbol{i}} = 0$ otherwise. Taking the inverse DFT of A we have

$$\begin{aligned} a_{\boldsymbol{i}} &= \sum_{\substack{\boldsymbol{j} \in G^m \\ j_0, \ldots, j_{m-2} = 0}} \left(\prod_{k \in [\![m]\!]} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{-i_k[\ell] \cdot j_k[\ell]} \right) \cdot 1 \\ &= \sum_{j_{m-1} \in G} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{-i_{m-1}[\ell] \cdot j_{m-1}[\ell]} \\ &= \sum_{n_0 \in \mathbb{Z}_{m_0}} \cdots \sum_{n_{s-1} \in \mathbb{Z}_{m_{s-1}}} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{-i_{m-1}[\ell] \cdot n_\ell} \\ &= \prod_{\ell \in [\![s]\!]} \left(\sum_{n_\ell \in \mathbb{Z}_{m_\ell}} \alpha_\ell^{-i_{m-1}[\ell] \cdot n_\ell} \right). \end{aligned}$$

Since α_ℓ is a primitive m_ℓ^{th} root of unity we know that

$$\sum_{n_\ell \in \mathbb{Z}_{m_\ell}} \alpha_\ell^{-i_{m-1}[\ell] \cdot n_\ell} = 1 + \alpha_\ell^{-i_{m-1}[\ell]} + \cdots + \alpha_\ell^{-i_{m-1}[\ell](m_\ell - 1)}$$

is equal to 0 if $i_{m-1}[\ell] \neq 0$ and is equal to $m_\ell \mod 2 = 1$ if $i_{m-1}[\ell] = 0$. Thus we conclude that $a_{\boldsymbol{i}} = 1$ if $i_{m-1} = 0$ and $a_{\boldsymbol{i}} = 0$ otherwise. $\square$

Lemma I.2. *(DFT of a periodic sequence.) Let $b \in \mathbb{F}_2[G^{m-1}]$, and let $a = (b \mid b \mid \cdots \mid b) \in \mathbb{F}_2[G^m]$. The DFT of a is related to that of b as follows: $A_{\boldsymbol{j}} = 0$ if $j_{m-1} \neq 0$ and $A_{\boldsymbol{j}} = B_{(j_0, \ldots, j_{m-2})}$ otherwise.*

Proof. Let us assume that b is given and a is defined via its DFT as: $A_{\boldsymbol{j}} = 0$ if $j_{m-1} \neq 0$ and $A_{\boldsymbol{j}} = B_{(j_0, \ldots, j_{m-2})}$ otherwise. We now show that a is the m-fold repetition of b.

Let $\boldsymbol{i} \in G^m$ and $\boldsymbol{i'} = (i_0, \ldots, i_{m-2})$. From the inverse DFT, we have

$$\begin{aligned} a_{\boldsymbol{i}} &= \sum_{\substack{\boldsymbol{j} \in G^m \\ j_{m-1} = 0}} \left(\prod_{k \in [\![m]\!]} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{-i_k[\ell] \cdot j_k[\ell]} \right) A_{\boldsymbol{j}} \\ &= \sum_{\substack{\boldsymbol{j} \in G^m \\ j_{m-1} = 0}} \left(\prod_{k \in [\![m-1]\!]} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{-i_k[\ell] \cdot j_k[\ell]} \right) A_{\boldsymbol{j}} \\ &= \sum_{\boldsymbol{j'} \in G^{m-1}} \left(\prod_{k \in [\![m-1]\!]} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{-i_k[\ell] \cdot j'_k[\ell]} \right) A_{(\boldsymbol{j'} \mid 0)} \\ &= \sum_{\boldsymbol{j'} \in G^{m-1}} \left(\prod_{k \in [\![m-1]\!]} \prod_{\ell \in [\![s]\!]} \alpha_\ell^{-i'_k[\ell] \cdot j'_k[\ell]} \right) B_{\boldsymbol{j'}} \\ &= b_{\boldsymbol{i'}}, \end{aligned}$$

where the second equality uses the fact $j_{m-1} = 0$, and the third equality uses the change of variables $\boldsymbol{j} = (\boldsymbol{j'}|0)$. Hence we have

$$a = \sum_{\boldsymbol{i'} \in G^{m-1}} \sum_{\ell \in [\![\, |G| \,]\!]} b_{\boldsymbol{i'}} \, X^{(\boldsymbol{i'}|g_\ell)}.$$

This shows that $a = (b \mid \cdots \mid b)$. □

We are now ready to prove Lemma IV.7. Let $\Gamma_{r,m-1}$ be the set of all vectors of weight r in G^{m-1}. Using Lemma IV.3, we observe that $\Gamma_{r,m-1}$ is a union of conjugacy classes. We define $\mathcal{C}(G^{m-1} \setminus \Gamma_{r,m-1})$ to be the ideal in $\mathbb{F}_2[G^{m-1}]$ whose non-zeros are $\Gamma_{r,m-1}$. Note that the dimension of $\mathcal{C}(G^{m-1} \setminus \Gamma_{r,m-1})$ is $|\Gamma_{r,m-1}| = \binom{m-1}{r}(|G|-1)^r$.

In the first stage of the proof, we will show that $\mathcal{C}_G(r,m)$ is the direct sum of

$$\begin{aligned} \mathcal{C}_1 &= \left\{ \, (b_0 \mid \cdots \mid b_{|G|-1}) \ : \ b_\ell \in \mathcal{C}_G(r-1, m-1) \, \right\}, \text{ and} \\ \mathcal{C}_2 &= \left\{ \, (b \mid b \mid \cdots \mid b) \ : \ b \in \mathcal{C}(G^{m-1} \setminus \Gamma_{r,m-1}) \, \right\}. \end{aligned}$$

We will complete the proof of this first stage by showing

1) $\mathcal{C}_1$ is a subcode of $\mathcal{C}_G(r,m)$,
2) $\mathcal{C}_2$ is a subcode of $\mathcal{C}_G(r,m)$,
3) $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0\}$, and
4) $\dim(\mathcal{C}_1) + \dim(\mathcal{C}_2) = \dim(\mathcal{C}_G(r,m))$.

We now provide the proofs of these results.

1) $\mathcal{C}_1$ is a subcode of $\mathcal{C}_G(r,m)$: Observe that it is sufficient to show that

$$\{ \ (b \mid 0 \mid 0 \mid \cdots \mid 0) \quad : \quad b \in \mathcal{C}_G(r-1, m-1) \ \}$$

is a subcode of $\mathcal{C}_G(r,m)$. The transitive property of $\mathcal{C}_G(r,m)$ (this follows from Lemma IV.1) can then be leveraged to show that elements of the form $(0 \mid b \mid 0 \mid \cdots \mid 0)$ etc. also belong to $\mathcal{C}_G(r,m)$.

Now suppose $b \in \mathcal{C}_G(r-1, m-1)$. Let us define $a \in \mathbb{F}_2[G^m]$ as $(b \mid \cdots \mid b)$. Using the fact $B_{\boldsymbol{j}} = 0$ if $w_H(\boldsymbol{j}) \geq r$ and using Lemma I.2 we deduce that $A_{\boldsymbol{j}} = 0$ if $w_H(\boldsymbol{j}) \geq r$. Hence, $a \in \mathcal{C}_G(r-1, m)$.

Let $c \in \mathbb{F}_2[G^m]$ be the indicator function of $G^{m-1} \times \{0\}$, and $d \in \mathbb{F}_2[G^m]$ be defined as $d_{\boldsymbol{i}} = c_{\boldsymbol{i}} a_{\boldsymbol{i}}$ for all $\boldsymbol{i}$. That is, $d = (b \mid 0 \mid \cdots \mid 0)$. From the modulation property of DFT we deduce that the DFT of d is the convolution of C and A. Hence,

$$D = \sum_{\boldsymbol{j} \in G^m} \sum_{\boldsymbol{k} \in G^m} C_{\boldsymbol{j}} A_{\boldsymbol{k}} X^{\boldsymbol{j} \oplus \boldsymbol{k}}.$$

Now using Lemma I.1 with respect to C we obtain

$$\begin{aligned} D &= \sum_{\substack{\boldsymbol{j} \in G^m \\ j_0, \ldots, j_{m-2} = 0}} \sum_{\boldsymbol{k} \in G^m} A_{\boldsymbol{k}} X^{\boldsymbol{j} \oplus \boldsymbol{k}} \\ &= \sum_{\substack{\boldsymbol{j} \in G^m \\ j_0, \ldots, j_{m-2} = 0}} \sum_{\substack{\boldsymbol{k} \in G^m \\ w_H(\boldsymbol{k}) \leq r-1}} A_{\boldsymbol{k}} X^{\boldsymbol{j} \oplus \boldsymbol{k}}, \end{aligned}$$

where in the last step we have used the fact $a \in \mathcal{C}_G(r-1, m)$. If $j_0, \ldots, j_{m-2} = 0$ and $w_H(\boldsymbol{k}) \leq r-1$, we have $w_H(\boldsymbol{j} \oplus \boldsymbol{k}) \leq w_H(\boldsymbol{k}) + 1 \leq r$. Hence $d \in \mathcal{C}_G(r,m)$.

2) $\mathcal{C}_2$ is a subcode of $\mathcal{C}_G(r,m)$: Let $b \in \mathcal{C}(G^{m-1} \setminus \Gamma_{r,m-1})$, and a be the m-fold repetition of b. Using the fact $B_{\boldsymbol{j'}} = 0$ if $w_H(\boldsymbol{j'}) \neq r$, and using Lemma I.2, we deduce that $A_{\boldsymbol{j}} = 0$ if $w_H(\boldsymbol{j}) \geq r+1$. Hence, $a \in \mathcal{C}_G(r,m)$.

3) $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0\}$: Let $(b \mid b \mid \cdots \mid b) \in \mathcal{C}_1 \cap \mathcal{C}_2$. Then

$$b \in \mathcal{C}_G(r-1, m-1) \cap \mathcal{C}(G^{m-1} \setminus \Gamma_{r,m-1}).$$

The non-zeros of $\mathcal{C}_G(r-1, m-1)$ are the vectors in G^{m-1} of weight at the most $r-1$, and the non-zeros of $\mathcal{C}(G^{m-1} \setminus \Gamma_{r,m-1})$ are the vectors of weight r. Hence, $B_{\boldsymbol{j'}} = 0$ for all $\boldsymbol{j'} \in G^{m-1}$. We deduce that $b = 0$, and therefore, $\mathcal{C}_1 \cap \mathcal{C}_2 = \{0\}$.

4) Comparing the dimensions: The dimension of $\mathcal{C}_1$ is $|G| \dim(\mathcal{C}_G(r-1, m-1))$ and the dimension of $\mathcal{C}_2$ is equal to $\dim(\mathcal{C}(G^m \setminus \Gamma_{r,m-1}))$. We have

$$\begin{aligned}
\dim(\mathcal{C}_1 + \mathcal{C}_2) &= \dim(\mathcal{C}_1) + \dim(\mathcal{C}_2) \\
&= |G| \sum_{w=0}^{r-1} \binom{m-1}{w} (|G|-1)^w + |\Gamma_{r,m-1}| \\
&= |G| \sum_{w=0}^{r-1} \binom{m-1}{w} (|G|-1)^w + \binom{m-1}{r} (|G|-1)^r.
\end{aligned}$$

Using $|G| = 1 + (|G|-1)$, we have

$$\begin{aligned}
\dim(\mathcal{C}_1 + \mathcal{C}_2) &= \sum_{w=0}^{r} \binom{m-1}{w} (|G|-1)^w + \sum_{w=0}^{r-1} \binom{m-1}{w} (|G|-1)^{w+1} \\
&= \binom{m-1}{0} + \sum_{w=1}^{r} \left(\binom{m-1}{w} + \binom{m-1}{w-1} \right) (|G|-1)^w \\
&= \sum_{w=0}^{r} \binom{m}{w} (|G|-1)^w \\
&= \dim(\mathcal{C}_G(r,m)).
\end{aligned}$$

This is the end of the first stage of the proof of Lemma IV.7.

To complete the proof we now apply a change of variables in the direct sum decomposition of $\mathcal{C}_G(r,m)$ into $\mathcal{C}_1$ and $\mathcal{C}_2$. We define $u, u_0, \ldots, u_{|G|-2}$ in terms of $b, b_0, \ldots, b_{|G|-1}$ as follows

$$u = b_{|G|-1} + b, \text{ and } u_l = b_l + b_{|G|-1} \text{ for all } l \in [\![|G|-1]\!].$$

Hence, every element of $\mathcal{C}_G(r,m)$ is of the form $(u+u_0|\cdots|u+u_{|G|-2}|u)$. Since $b \in \mathcal{C}(G^{m-1} \setminus \Gamma_{r,m-1})$ and $b_l \in \mathcal{C}_G(r-1, m-1)$, and since $\mathcal{C}_G(r, m-1)$ is the direct sum of $\mathcal{C}(G^{m-1} \setminus \Gamma_{r,m-1})$ and $\mathcal{C}_G(r-1, m-1)$, we deduce that

$$u \in \mathcal{C}_G(r, m-1) \text{ and } u_0, \ldots, u_{|G|-2} \in \mathcal{C}_G(r-1, m-1).$$

The last piece of argument required to show that $\mathcal{C}_G(r,m)$ is equal to

$$\left\{ (u+u_0|u+u_1|\cdots|u+u_{|G|-2}|u) \ : \ u_l \in \mathcal{C}_G(r-1, m-1), u \in \mathcal{C}_G(r, m-1) \right\} \tag{19}$$

is based on the dimension of these two codes. Clearly, the dimension of the code in (19) is

$$\begin{aligned}
&= \dim(\mathcal{C}_G(r, m-1)) + (|G|-1) \dim(\mathcal{C}_G(r-1, m-1)) \\
&= \sum_{w=0}^{r} \binom{m-1}{w} (|G|-1)^w \ + \ \sum_{w=0}^{r-1} \binom{m-1}{w} (|G|-1)^{w+1} \\
&= \sum_{w=0}^{r} \binom{m}{w} (|G|-1)^w \\
&= \dim(\mathcal{C}_G(r,m)).
\end{aligned}$$

Thus, we conclude that the code (19) is indeed $\mathcal{C}_G(r,m)$.

APPENDIX II
RELATION TO THE CLASSICAL CODES OF BERMAN AND BLACKMORE-NORTON

Let p be any odd prime, $G = \mathbb{Z}_p$, and let $\mathbb{F}_q$ be a finite algebraic extension of $\mathbb{F}_2$ that contains a primitive p^{th} root of unity α. Since p is prime each of $\alpha, \alpha^2, \ldots, \alpha^{p-1}$ is a primitive p^{th} root of unity. For any $\ell \in \{1, \ldots, p-1\}$, we have

$$1 + \alpha^{\ell} + \alpha^{2\ell} + \cdots + \alpha^{(p-1)\ell} = 0.$$

The DFT and inverse DFT in $\mathbb{F}_2[\mathbb{Z}_p^m]$ are

$$A_{\boldsymbol{j}} = \sum_{\boldsymbol{i} \in \mathbb{Z}_p^m} \alpha^{\boldsymbol{i}\cdot\boldsymbol{j}} a_{\boldsymbol{i}} \quad \text{and} \quad a_{\boldsymbol{i}} = \sum_{\boldsymbol{j} \in \mathbb{Z}_p^m} \alpha^{-\boldsymbol{i}\cdot\boldsymbol{j}} A_{\boldsymbol{j}},$$

where $\boldsymbol{i} \cdot \boldsymbol{j} = \sum_{k \in [\![m]\!]} i_k j_k$ is the dot product in $\mathbb{Z}_p^m$.

We will use the definition used by Blackmore and Norton [6] as our point of reference. We will recall this definition using the notation followed in Section IV.

For $k \in [\![m]\!]$, let $\boldsymbol{e}_k \in \mathbb{Z}_p^m$ be the vector with a 1 in the k^{th} position and 0 elsewhere. Define

$$a^{(k)} = X^{\boldsymbol{0}} + X^{\boldsymbol{e}_k} + X^{2\boldsymbol{e}_k} + \cdots + X^{(p-1)\boldsymbol{e}_k} = \sum_{\beta \in \mathbb{Z}_p} X^{\beta \boldsymbol{e}_k}.$$

Note that $a^{(k)}$ is denoted as $e_p(X_k)$ in [6]. Let $A^{(k)}$ be the DFT of $a^{(k)}$. Then

$$A_{\boldsymbol{j}}^{(k)} = \sum_{\beta \in \mathbb{Z}_p} \alpha^{\beta \boldsymbol{e}_k \cdot \boldsymbol{j}} = \sum_{\beta \in \mathbb{Z}_p} \alpha^{\beta j_k}.$$

Thus, $A_{\boldsymbol{j}}^{(k)} = 1$ if $j_k = 0$ and $A_{\boldsymbol{j}}^{(k)} = 0$ if $j_k \neq 0$.

Now consider $b^{(k)} = 1 + a^{(k)}$, where $1 = X^{\boldsymbol{0}}$ is the multiplicative identity of $\mathbb{F}_2[\mathbb{Z}_p^m]$. Since the DFT of $X^{\boldsymbol{0}}$ is $\sum_{\boldsymbol{j} \in \mathbb{Z}_p^m} X^{\boldsymbol{j}}$, we see that the DFT of $b^{(k)}$ is given by $B_{\boldsymbol{j}}^{(k)} = 1 + A_{\boldsymbol{j}}^{(k)}$ which equals 0 if $j_k = 0$ and equals 1 if $j_k \neq 0$.

Blackmore and Norton define $E_p(r, m) \subset \mathbb{F}_2[\mathbb{Z}_p^m]$ to be the set of all products of the form

$$b^{(k_0)} \cdots b^{(k_{s-1})} \cdot a^{(k_s)} \cdots a^{(k_{m-1})}, \tag{20}$$

where $\{k_0, \ldots, k_{m-1}\} = [\![m]\!]$ and $0 \leq s \leq r$. The DFT of (20) at $\boldsymbol{j} \in \mathbb{Z}_p^m$ is equal to 1 if $j_{k_0}, \ldots, j_{k_{s-1}} \neq 0$ and $j_{k_s}, \ldots, j_{k_{m-1}} = 0$, and the DFT at $\boldsymbol{j}$ is equal to 0 otherwise. That is, the DFT of (20) at $\boldsymbol{j}$ is equal to $\mathbb{1}\left(\mathsf{supp}(\boldsymbol{j}) = \{k_0, \ldots, k_{s-1}\}\right)$ where $\mathbb{1}$ denotes the indicator function and supp is the support set of a vector.

Let $\langle E_p(r, m) \rangle$ be the ideal generated by the elements of $E_p(r, m)$ in $\mathbb{F}_2[\mathbb{Z}_p^m]$. Using the convolution property of the DFT we observe that $a \in \langle E_p(r, m) \rangle$ if and only if $A_{\boldsymbol{j}} = 0$ for all $\boldsymbol{j}$ with $w_H(\boldsymbol{j}) \geq r + 1$. That is, $\langle E_p(r, m) \rangle = \mathcal{C}_{\mathbb{Z}_p}(r, m)$.

Blackmore and Norton show that the family of codes $\langle E_p(r, m) \rangle = \mathcal{C}_{\mathbb{Z}_p}(r, m)$ are the duals of the codes designed by Berman. The code $\mathcal{C}_{\mathbb{Z}_p}(r, m)$ is denoted as $\mathcal{B}_p(r, m)^{\perp}$ in [6].

APPENDIX III
GENERATOR MATRICES OF ABELIAN CODES FROM $\mathbb{F}_2[\mathbb{Z}_p^m]$, WITH 2 A PRIMITIVE ROOT MODULO p

We utilize the fact that every abelian code in $\mathbb{F}_2[\mathbb{Z}_p^m]$ is a direct sum of its irreducible subcodes [5], [12]. A generator matrix of an abelian code can therefore be obtained by juxtaposing the generator matrices of its irreducible subcodes. Hence, we will now consider only the irreducible codes of $\mathbb{F}_2[\mathbb{Z}_p^m]$.

The inverse DFT for $\mathbb{F}_2[\mathbb{Z}_p^m]$ is given by $a_{\boldsymbol{i}} = \sum_{\boldsymbol{j} \in \mathbb{Z}_p^m} \alpha^{-\boldsymbol{i}\cdot\boldsymbol{j}} A_{\boldsymbol{j}}$, where α is a primitive p^{th} root of unity. Note that $\alpha, \alpha^2, \ldots, \alpha^{p-1}$ are the roots of $x^{p-1} + x^{p-2} + \cdots + 1$. Since 2 is primitive in $\mathbb{Z}_p$, $x^{p-1} + x^{p-2} + \cdots + 1$

is irreducible. The field extension $\mathbb{F}_q = \mathbb{F}_2[\alpha]$ is of degree $(p-1)$ over $\mathbb{F}_2$, and $\{\alpha, \alpha^2, \ldots, \alpha^{p-1}\}$ is an $\mathbb{F}_2$-basis of $\mathbb{F}_q$.

Let $\Gamma \subset \mathbb{Z}_p^m$ be any conjugacy class and let $\boldsymbol{j} \in \Gamma$. If $\boldsymbol{j} = \boldsymbol{0}$ then $\Gamma = \{\boldsymbol{0}\}$ and the irreducible code corresponding to Γ is the repetition code.

If $\boldsymbol{j} \neq \boldsymbol{0}$, then

$$\Gamma = \{\boldsymbol{j}, 2\boldsymbol{j}, 2^2\boldsymbol{j}, \ldots\} = \{\beta \boldsymbol{j} \ : \ \beta \in \{1, 2, \ldots, p-1\}\},$$

where we have used the fact that 2 is a primitive root in the finite field $\mathbb{Z}_p$. Thus, $|\Gamma| = p - 1$ and the irreducible code corresponding to Γ has dimension $p-1$. This code consists of all $a \in \mathbb{F}_2[\mathbb{Z}_p^m]$ such that

$$a_{\boldsymbol{i}} = \sum_{t=0}^{p-2} \alpha^{-\boldsymbol{i}\cdot 2^t \boldsymbol{j}} A_{2^t \boldsymbol{j}},$$

where $A_{\boldsymbol{j}} \in \mathbb{F}_q$ and $A_{2^t\boldsymbol{j}} = A_{\boldsymbol{j}}^{2^t}$. Hence,

$$a_{\boldsymbol{i}} = \sum_{t=0}^{p-2} \left(\alpha^{-\boldsymbol{i}\cdot\boldsymbol{j}} A_{\boldsymbol{j}}\right)^{2^t} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\alpha^{-\boldsymbol{i}\cdot\boldsymbol{j}} A_{\boldsymbol{j}}\right),$$

where $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}$ is the trace function. We represent $A_{\boldsymbol{j}}$ in the $\mathbb{F}_2$-basis $\{\alpha, \alpha^2, \ldots, \alpha^{p-1}\}$ as $A_{\boldsymbol{j}} = \sum_{k=1}^{p-1} m_k \alpha^k$, where $m_1, \ldots, m_k \in \mathbb{F}_2$. Since the trace function is $\mathbb{F}_2$-linear we have

$$a_{\boldsymbol{i}} = \sum_{k=1}^{p-1} m_k \,\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\alpha^{k-\boldsymbol{i}\cdot\boldsymbol{j}}\right).$$

Let us denote $k - \boldsymbol{i}\cdot\boldsymbol{j} \in \mathbb{Z}_p$ by l. If $l = 0$, then $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha^l) = 0$. For $l \neq 0$, we have

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha^l) &= \alpha^l + \alpha^{2l} + \alpha^{2^2 l} + \cdots + \alpha^{2^{p-2} l} \\
&= \alpha^l + \alpha^{2l} + \alpha^{3l} + \cdots + \alpha^{(p-1)l} \\
&= 1,
\end{aligned}$$

since α^l is a root of $x^{p-1} + x^{p-2} + \cdots + x + 1$. Hence,

$$a_{\boldsymbol{i}} = \sum_{k=1}^{p-1} m_k \,\mathbb{1}(\boldsymbol{i}\cdot\boldsymbol{j} \neq k),$$

where $\mathbb{1}$ is the indicator function.

We thus arrive at the following generator matrix $\boldsymbol{G}$ for the irreducible code corresponding to the conjugacy class $\Gamma = \{\boldsymbol{j}, 2\boldsymbol{j}, \ldots\}$. Let $\boldsymbol{G}$ be a $(p-1) \times p^m$ binary matrix whose rows are indexed by $k \in \{1, \ldots, p-1\}$ and columns by $\boldsymbol{i} \in \mathbb{Z}_p^m$. The entry of $\boldsymbol{G}$ in row k and column $\boldsymbol{i}$ is $\mathbb{1}(\boldsymbol{i}\cdot\boldsymbol{j} \neq k)$.

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] G. Schnabl and M. Bossert, "Soft-decision decoding of Reed-Muller codes as generalized multiple concatenated codes," *IEEE Transactions on Information Theory*, vol. 41, no. 1, pp. 304–308, 1995.
[9] I. Dumer and K. Shabunov, "Recursive decoding of Reed-Muller codes," in *2000 IEEE International Symposium on Information Theory (Cat. No.00CH37060)*, 2000, pp. 63–.
[10] E. Abbe, A. Shpilka, and M. Ye, "Reed–Muller codes: Theory and algorithms," *IEEE Transactions on Information Theory*, vol. 67, no. 6, pp. 3251–3277, 2021.
[11] P. Camion, "Abelian codes," *Math. Res. Ctr., Univ. Wisconsin, Madison, Tech. Rep. 1059*, 1971.
[12] F. J. M. Williams, "Binary codes which are ideals in the group algebra of an abelian group," *The Bell System Technical Journal*, vol. 49, no. 6, pp. 987–1011, 1970.
[13] A. Kelarev and P. Solé, "Error-correcting codes as ideals in group rings," *Contemporary Mathematics*, vol. 273, pp. 11–18, 2001.
[14] B. S. Rajan and M. U. Siddiqi, "Transform domain characterization of abelian codes," *IEEE Transactions on Information Theory*, vol. 38, no. 6, pp. 1817–1821, 1992.
[15] S. Berman, "On the theory of group codes," *Cybernetics*, vol. 3, no. 1, pp. 25–31, 1967.
[16] T. Blackmore and G. Norton, "Matrix-product codes over $\mathbb{F}_q$," *Applicable Algebra in Engineering, Communication and Computing*, vol. 12, no. 6, pp. 477–500, 2001.
[17] F. Hernando, K. Lally, and D. Ruano, "Construction and decoding of matrix-product codes from nested codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 20, no. 5, 2009.
[18] 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
[19] P. O. Vontobel, *Algebraic coding for iterative decoding*. PhD dissertation, ETH Zurich, 2003.
[20] 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.
[21] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*. Elsevier, 1977, vol. 16.
[22] E. Assmus, "On Berman's characterization of the Reed-Muller codes," *Journal of Statistical Planning and Inference*, vol. 56, no. 1, pp. 17–21, 1996, orthogonal Arrays and Affine Designs, Part I.
[23] R. E. Blahut, *Algebraic Codes for Data Transmission*. Cambridge University Press, 2003.
[24] N. Jacobson, *Basic Algebra I*. Dover Publications, Incorporated, 2009.
[25] C. Carlet and S. Guilley, "Complementary dual codes for counter-measures to side-channel attacks," in *Coding Theory and Applications*. Cham: Springer International Publishing, 2015, pp. 97–105.
[26] 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.