



**HAL**  
open science

# Dynamic Frozen-Function Design for Reed-Muller Codes With Automorphism-Based Decoding

Samet Gelincik, Charles Pillet, Pascal Giard

► **To cite this version:**

Samet Gelincik, Charles Pillet, Pascal Giard. Dynamic Frozen-Function Design for Reed-Muller Codes With Automorphism-Based Decoding. *IEEE Communications Letters*, 2023, 27 (2), pp.497-501. 10.1109/LCOMM.2022.3230202 . hal-04056274

**HAL Id: hal-04056274**

**<https://hal.science/hal-04056274v1>**

Submitted on 11 May 2023

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

# Dynamic Frozen-Function Design for Reed-Muller Codes with Automorphism-Based Decoding

Samet Gelincik, *Member, IEEE*, Charles Pillet, *Member, IEEE*, and Pascal Giard, *Senior Member, IEEE*

**Abstract**—In this paper, we propose to add dynamic frozen bits to underlying polar codes with a Reed-Muller information set with the aim of maintaining the same sub-decoding structure in Automorphism Ensemble (AE) and lowering the Maximum Likelihood (ML) bound by reducing the number of minimum weight codewords. We provide the dynamic freezing constraint matrix that remains identical after applying a permutation linear transformation. This feature also permits to drastically reduce the memory requirements of an AE decoder with polar-like codes having dynamic frozen bits. We show that, under AE decoding, the proposed dynamic freezing constraints lead to a gain of up to 0.25 dB compared to the ML bound of the  $\mathcal{R}(3, 7)$  Reed-Muller code, at the cost of small increase in memory requirements.

## I. INTRODUCTION

Polar codes [1] have been introduced as the first provably capacity-achieving linear codes for the class of symmetric binary memoryless channels under the low-complexity Successive-Cancellation (SC) decoding algorithm. However, capacity is achieved for unpractical code lengths and polar codes suffer from a poor Maximum Likelihood (ML) bound in the finite-length regime. Polar codes concatenated with a cyclic redundancy check (CRC) code, namely CRC-aided (CA) polar codes, drastically enhance the error-correction performance under SC-List (SCL) [2] decoding. Indeed, using a CRC code both enhances the distance property and approximates a genie decoder [2]–[4]. CA-polar codes have been selected among the channel coding schemes in 5G-New Radio [5].

On the other hand, recently introduced Polarization-adjusted-convolutional (PAC) codes [6] perform very close to the second-order rate approximation of the binary-input additive white Gaussian noise (BI-AWGN) in short block-length regime [7] under SCL decoding with large list sizes, i.e.,  $L \geq 128$ . In [8] and [9], the concept of single-argument dynamic frozen functions was introduced, where any dynamic frozen bit is dependent on only one previous information bit. Also, it has been shown that properly chosen dynamic frozen bits reduce the number of minimum weight codewords or increase the minimum distance. Code designs with single-argument dynamic frozen bits perform as well as PAC codes with much lower decoding complexity at short block-lengths [8]. All these modified polar codes fall into the same category, namely, *pre-transformed* polar codes [10], and can be defined by their dynamic freezing constraint matrix. With properly chosen pre-transformation matrices, pre-transformed

polar codes were proven to enhance the distance spectrum of the code without reducing the minimum distance of the underlying code [10]. Given their distance properties, Reed-Muller codes are often chosen as underlying codes of pre-transformed polar codes for short block lengths [6], [8], [9].

Automorphism Ensemble (AE) decoding [11] is a possible alternative to list decoding for codes exhibiting symmetry [12]–[14] such as Reed-Muller codes. In AE decoding,  $M$  permutations are selected in the affine automorphism group of the code to generate  $M$  instances of the noisy vector. The  $M$  permuted noisy vectors are decoded in parallel and the most likely candidate codeword is selected. AE decoding was first proposed for Reed-Muller codes [11] since the affine automorphism group is isomorphic to the general affine group [15]. AE decoding was proposed for polar codes in [16]–[18].

Recently, affine permutations outside of the affine automorphism group of a given polar code were shown to be usable in ensemble decoding [19]. Each of the permutations generates a new pre-transformed polar code. In [20], affine permutations are successfully applied to CA-polar codes decoded with AE-Belief Propagation. The error-correction performance is improved with respect to [21].

In this work, we integrate the single-argument dynamic frozen function concept into automorphism-based code design. In that sense, we propose a dynamic freezing constraint matrix for Reed-Muller codes that remains identical for a large group of permutations. The proposed dynamic freezing constraint matrix permits to lower the ML bound and achieves better error-correction performance under AE-SCL with limited list size  $L$  and automorphisms used  $M$ . Moreover, the proposed dynamic freezing constraint matrix drastically reduces the memory required by AE decoding algorithm when pre-transformed polar codes are used.

## II. PRELIMINARIES

### A. Reed-Muller Codes, Polar Codes and Monomial Formalism

A polar code  $(N, K)$  of length  $N = 2^n$  and dimension  $K$  is a binary block code defined by the binary kernel  $\mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ , the transformation matrix  $\mathbf{G}_N = \mathbf{G}_2^{\otimes n}$ , where  $(\cdot)^{\otimes n}$  denotes the  $n^{\text{th}}$  Kronecker power, the information set  $\mathcal{I} \subseteq \{0, \dots, N-1\}$  and the frozen set  $\mathcal{F} = \mathcal{I}^c$ . Encoding is performed as  $\mathbf{x} = \mathbf{u} \cdot \mathbf{G}_N$  with the input vector  $\mathbf{u} = (u_0, \dots, u_{N-1})$  generated by assigning  $u_i = 0$  if  $i \in \mathcal{F}$  and storing information in the  $K$  bit-channels stated in  $\mathcal{I}$ . In polar coding,  $\mathcal{I}$  includes the  $K$  most reliable bit-channels resulting from channel polarization [1]. A polar-like code may use a different criteria to define  $\mathcal{I}$ , not necessarily reliability. The  $K$  rows of  $\mathbf{G}_N$  stated in  $\mathcal{I}$  form the generator matrix  $\mathbf{G}$  of the polar-like code.

Samet Gelincik was with IETR, INSA Rennes, France (email: sametgelincik@gmail.com).

Charles Pillet and Pascal Giard are with LaCIME, Department of Electrical Engineering, Ecole de technologie suprieure, Montreal, QC, Canada (email: {charles.pillet,pascal.giard}@lacime.etsmtl.ca).

The relation between polar codes and Reed-Muller codes was already pointed out in [1]. That is, the row-selection of  $\mathbf{G}_N$  to generate  $\mathbf{G}$  for a  $\mathcal{R}(r, n)$  Reed-Muller code [22], [23] is based on the Hamming weight of the rows. Hence, Reed-Muller codes are polar-like codes. The Hamming weight of row  $k$  is  $2^{i_1(\mathbf{b}_k)}$  [1], [8], where  $\mathbf{b}_k = (b_{k,0}, \dots, b_{k,n-1})$  is the binary representation of  $k$  and  $i_1(\cdot)$  returns the Hamming weight. The binary representation of indices in  $\mathcal{I}_{\mathcal{R}(r,n)}$  verifies

$$\mathcal{I}_{\mathcal{R}(r,n)} = \{k : i_1(\mathbf{b}_k) \geq n - r\}. \quad (1)$$

Note that the row  $\mathbf{g}_k$  of  $\mathbf{G}_N$  can be represented as the evaluation of a monomial in  $\mathbb{F}_2[z_0, \dots, z_{n-1}]$ , where the coordinate indexing increases from right to left:

$$\mathbf{g}_k = \left\{ \prod_{j \in \mathcal{P}_0(\mathbf{b}_k)} z_j : \mathbf{z} \in \mathbb{F}_2^n \right\}, \quad (2)$$

i.e.,

$$g_{k,m} = \prod_{j \in \mathcal{P}_0(\mathbf{b}_k)} z_j, \quad [z_0, \dots, z_{n-1}] = \mathbf{b}_{N-m-1},$$

where  $\mathcal{P}_0(\cdot)$  is the set of coordinate indices with 0 in  $\mathbf{b}_k$ .

Hence, any row  $\mathbf{g}_k$  corresponds to a monomial obtained with respect to binary representation of  $k$ :

$$\mathbf{f}_k(\mathbf{z}) = \prod_{j \in \mathcal{P}_0(\mathbf{b}_k)} z_j, \quad (3)$$

i.e., the monomial and binary representations are alternative representations of the same entity: polar matrix rows. Reed-Muller codes can thus be described through monomial formalism in such that any codeword is obtained as an evaluation of a linear combination of some monomials in the monomial set  $\mathcal{M}_{\mathcal{R}(r,n)}$  corresponding to a given information vector, where

$$\mathcal{M}_{\mathcal{R}(r,n)} = \{\mathbf{f}_k(\mathbf{z}) : i_1(\mathbf{b}_k) \geq n - r\}. \quad (4)$$

### B. Pre-transformed Polar Codes

For a given  $K$ -bit information vector  $\mathbf{v}$  and a pre-transformation matrix  $\mathbf{W} \in \mathbb{F}_2^{K \times N}$ , encoding of a pre-transformed polar code is performed as  $\mathbf{x} = \mathbf{u}\mathbf{G}_N$  with  $\mathbf{u} = \mathbf{v}\mathbf{W}$ . Pre-transformed polar codes are defined by the dynamic freezing constraint matrix  $\mathbf{V} \in \mathbb{F}_2^{(N-K) \times N}$  verifying  $\mathbf{W}\mathbf{V}^\top = \mathbf{0}$  [24], where  $(\cdot)^\top$  denotes the transpose of a matrix.  $\mathbf{V}$  transcribes the bits in  $\mathcal{F}$ , frozen at 0 (with a single 1 in the row) or data-dependent (several 1s in one row). Properly chosen pre-transformation matrices may reduce the number of low-weight codewords, enhancing the distance properties in the finite length regime [9], [10]. Reed-Muller codes are often adopted as underlying codes for pre-transformed polar codes at short block lengths [6], [8], [9].

### C. Automorphism Group of Reed-Muller Codes

An automorphism  $\pi$  of a code  $\mathcal{C}$  is a permutation on  $\{0, \dots, N-1\}$ , mapping every codeword  $\mathbf{x} \in \mathcal{C}$  into another codeword  $\pi(\mathbf{x}) \in \mathcal{C}$ . The automorphism group  $\text{Aut}(\mathcal{C})$  of a code  $\mathcal{C}$  is the set containing all automorphisms of the code.

The general affine group of order  $n$ ,  $\text{GA}(n)$ , is defined as the set of all transformations of  $n$  variables described by

$$\mathbf{z} \mapsto \mathbf{z}' = \mathbf{A}\mathbf{z} + \mathbf{b} \text{ mod } 2, \quad (5)$$

with  $\mathbf{z}, \mathbf{z}' \in \mathbb{F}_2^n$ ,  $\mathbf{A} \in \mathbb{F}_2^{n \times n}$  an invertible matrix and  $\mathbf{b} \in \mathbb{F}_2^{n \times 1}$ . The affine automorphism group  $\mathcal{A}(\mathcal{C}) \subseteq \text{Aut}(\mathcal{C})$  of any Reed-Muller code is known to be general affine group  $\text{GA}(n)$  [15]. The affine automorphism group of polar codes contains the lower-triangular-affine group (LTA) of order  $n$ .

The two aforementioned groups can be described by the block-lower-triangular affine (BLTA) group [11], namely the group of affine transformations having a block-lower-triangular transformation matrix. A BLTA group is recovered by the sizes of the blocks alongside the diagonal, defining the block structure  $\mathbf{S} = (s_1, \dots, s_l)$ ,  $s_1 + \dots + s_l = n$ . LTA and  $\text{GA}(n)$  correspond to  $\text{BLTA}(1, \dots, 1)$  and  $\text{BLTA}(n)$ , respectively.

The permutation linear transformation PL corresponds to the group in which  $\mathbf{A}$  is a permutation matrix and  $\mathbf{b} = \mathbf{0}$ . Note that any PL automorphism (except identity) maps each monomial  $\mathbf{f}_k(\mathbf{z})$  in  $\mathcal{M}_{\mathcal{R}(r,n)}$  to a different  $\mathbf{f}_{k'}(\mathbf{z})$  in  $\mathcal{M}_{\mathcal{R}(r,n)}$  with the same degree. This leads to the following corollary.

**Proposition 1.** Let  $\pi \in \text{PL}$  be an automorphism with  $\mathbf{A}$  as the corresponding permutation matrix. Then,  $\mathbf{f}_k(\mathbf{A}\mathbf{z}) = \mathbf{f}_{k'}(\mathbf{z})$  such that

$$\mathbf{b}_{k'} = \mathbf{A}\mathbf{b}_k. \quad (6)$$

*Proof.* Application of  $\pi$  to row  $\mathbf{g}_k$  is given as

$$\begin{aligned} \pi(\mathbf{g}_k) &\stackrel{(a)}{=} \pi(\{\mathbf{f}_k(\mathbf{z}), \mathbf{z} \in \mathbb{F}_2^n\}), \\ &= \{\mathbf{f}_k(\mathbf{A}\mathbf{z}), \mathbf{z} \in \mathbb{F}_2^n\}, \\ &\stackrel{(b)}{=} \left\{ \prod_{j \in \mathcal{P}_0(\mathbf{b}_k)} z'_j, \mathbf{z} \in \mathbb{F}_2^n \right\}, \\ &\stackrel{(c)}{=} \left\{ \prod_{j \in \mathcal{P}_0(\mathbf{A}\mathbf{b}_k)} z_j, \mathbf{z} \in \mathbb{F}_2^n \right\}, \\ &= \left\{ \prod_{j \in \mathcal{P}_0(\mathbf{b}_{k'})} z_j, \mathbf{z} \in \mathbb{F}_2^n \right\}, \\ &= \{\mathbf{f}_{k'}(\mathbf{z}), \mathbf{z} \in \mathbb{F}_2^n\}, \end{aligned}$$

where  $z'_j$  is obtained from vector multiplication of the  $j^{\text{th}}$  row of  $\mathbf{A}$  with  $[z_0, \dots, z_{n-1}]^\top$ , (a) comes from (2) and (3) while (b) and (c) are induced by the permutation matrix  $\mathbf{A}$ .  $\square$

### D. Automorphism Ensemble Decoder of Reed-Muller Codes

Given a decoder  $\text{dec}$  for a code  $\mathcal{C}$ , the corresponding automorphism decoder  $\text{adec}$  is given by

$$\text{adec}(\mathbf{y}, \pi) = \pi^{-1}(\text{dec}(\pi(\mathbf{y}))), \quad (7)$$

where  $\mathbf{y}$  is the received signal and  $\pi \in \mathcal{A}(\mathcal{C})$ . An automorphism ensemble (AE) decoder [11] consists of  $M$   $\text{adec}$  instances running in parallel with  $\pi \in \mathcal{A}(\mathcal{C})$ . Each of the  $M$   $\text{adec}$  returns a codeword candidate and the least-squares metric is used to select the most likely candidate.

In [19], permutations outside of  $\mathcal{A}(\mathcal{C})$  are used and proved to result in a pre-transformed polar code. For a pre-transformed polar code defined by  $\mathbf{V}$ , applying a permutation  $\pi \in \text{GA}(n)$  results in a pre-transformed polar code defined by the transformed dynamic freezing constraint matrix [20]

$$\mathbf{V}_T = \mathbf{V} (\mathbf{G}_N \mathbf{T}^{-1} \mathbf{G}_N)^\top, \quad (8)$$

with  $\mathbf{T}^{-1} \in \mathbb{F}_2^{N \times N}$ , the post-transformation matrix of  $\pi$ , defined as the permutation matrix related to  $\pi$ .

According to (8), the transformed dynamic freezing constraint matrix  $\mathbf{V}_T$  is permutation dependent. Hence, if pre-transformed polar codes are used in AE decoder, every adeg decoder needs to store its related transformed dynamic freezing constraint matrix leading to large memory requirements.

### III. STABLE DYNAMIC FREEZING CONSTRAINT MATRIX

In this section, given that  $\mathbf{T}^{-1}$  is a post-transformation matrix of a permutation in  $\text{BLTA}(n-1, 1) \cap \text{PL}$ , a dynamic freezing constraint matrix  $\mathbf{V}$  is proposed such that  $\mathbf{V}_T$  returns an equivalent dynamic freezing constraint. Next,  $\mathcal{R}(r, n)$  Reed-Muller codes are used having  $\mathcal{A}(\mathcal{R}(r, n)) = \text{BLTA}(n)$ .

#### A. Structure of $\mathbf{V}$

First, the definition of two equivalent dynamic freezing constraint matrices is given.

**Definition 1** (Equivalent dynamic freezing constraint matrices). Given a pre-transformation matrix  $\mathbf{W}$ , two dynamic freezing constraint matrices  $\mathbf{V}_1$  and  $\mathbf{V}_2$  are equivalent if  $\mathbf{W}\mathbf{V}_1^\top = \mathbf{W}\mathbf{V}_2^\top = \mathbf{0}$ .

After row reduction of  $\mathbf{V}_1$  and  $\mathbf{V}_2$ , the same dynamic freezing constraints are obtained. It follows that a given pre-transformed polar code can be defined in various ways. Next, the stability of  $\mathbf{V}$  under a set of permutations is defined.

**Definition 2** (Stability of  $\mathbf{V}$ ). A dynamic freezing constraint matrix  $\mathbf{V}$  is said to be *stable* under the set of permutations  $\mathcal{B}$  if and only if for any  $\pi \in \mathcal{B}$ , the transformed dynamic freezing constraint matrix  $\mathbf{V}_T$  is equivalent to  $\mathbf{V}$ .

First, the input vector  $\mathbf{u}$  stores the information in the  $K$  positions stated in  $\mathcal{I}$ . The proposed freezing constraint is:

$$\forall i \in \mathcal{F} \begin{cases} u_i = 0, & \text{if } b_{i,n-1} = 0 \iff i < N/2, \\ u_i = u_j, & \text{if } b_{i,n-1} = 1 \text{ with } \mathbf{b}_j = \bar{\mathbf{b}}_i, \end{cases} \quad (9)$$

where  $(\bar{\cdot})$  denotes the complement operation, i.e., for any  $0 \leq \ell < n$ ,  $b_{j,\ell} = 1 + b_{i,\ell} \pmod{2}$ .

The second line in (9) can be sub-divided as either  $j \in \mathcal{F}$  or  $j \in \mathcal{I}$ . In the former case, we have  $u_i = u_j = 0$ , in the latter case, the bit  $i$  is a dynamic frozen bit with  $u_i = u_j \in \{0, 1\}$ . Hence, in most cases, the matrix  $\mathbf{V}$ , that transcribes the bits in  $\mathcal{F}$  as induced by the constraint (9), can be row reduced. The maximum number of dynamic frozen bits  $D$  is given by

$$D = \min(|\{i \in \mathcal{F} | b_{i,n-1} = 1\}|, |\{j \in \mathcal{I} | b_{j,n-1} = 0\}|). \quad (10)$$

Next, we prove that the dynamic freezing constraint matrix  $\mathbf{V}$  induced by (9), compliant with the concept of single-argument dynamic frozen functions [8], is stable after applying any permutation  $\pi \in \text{BLTA}(n-1, 1) \cap \text{PL}$ .

**Theorem 1** (Stability over  $\text{BLTA}(n-1, 1) \cap \text{PL}$ ). *The dynamic freezing constraint matrix  $\mathbf{V}$  induced by (9) is stable under any permutation  $\pi \in \text{BLTA}(n-1, 1) \cap \text{PL}$ .*

*Proof.* The permutation  $\pi$  is generated with the permutation matrix  $\mathbf{A} \in \mathbb{F}_2^{n \times n}$ . Let us denote by  $f$ , the vector such that  $\mathbf{A}_{k,f(k)} = 1$  for  $1 \leq k \leq n$ , we have  $f(n) = n$ .

By Proposition 1, application of PL automorphisms to monomials can also be represented by matrix multiplication of  $\mathbf{A}$  with binary representation of the corresponding indices. Hence, in the following, the proof is given in terms of binary representations of row indices.

For any  $i \in \mathcal{F}$  with  $b_{i,n-1} = 1$ , the bit value is data dependent on index  $j \in \mathcal{I}$  with  $\mathbf{b}_j = \bar{\mathbf{b}}_i$ . The indices  $\mathbf{b}_i$  and  $\mathbf{b}_j$  are mapped to  $\mathbf{b}_{i'} = \mathbf{A} * \mathbf{b}_i$  and  $\mathbf{b}_{j'} = \mathbf{A} * \mathbf{b}_j$  with

$$\mathbf{b}_{i'} = \begin{bmatrix} b_{i,f(1)} \\ b_{i,f(2)} \\ \vdots \\ b_{i,f(n)=n} \end{bmatrix}, \quad \mathbf{b}_{j'} = \begin{bmatrix} b_{j,f(1)} \\ b_{j,f(2)} \\ \vdots \\ b_{j,f(n)=n} \end{bmatrix} = \bar{\mathbf{b}}_{i'}. \quad (11)$$

Note that, since  $\pi \in \text{PL} \subset \mathcal{A}(\mathcal{R}(r, n))$ , the information set  $\mathcal{I}$  is preserved, i.e.,  $\pi(\mathcal{I}) = \mathcal{I}$ , and for any  $(i, j)$  pair there is a corresponding  $(i', j')$  pair such that  $i_1(\mathbf{b}_i) = i_1(\mathbf{b}'_i)$  and  $i_1(\mathbf{b}_j) = i_1(\mathbf{b}'_j)$ . Hence, by construction of dynamic frozen set and functions, by (9), the dynamic frozen set and corresponding functions are preserved as well.  $\square$

The equivalence between  $\mathbf{V}$  and  $\mathbf{V}_T$  for a single permutation  $\pi$  can also be verified with (8). As an example, the  $\mathcal{R}(1, 3)$  code, having frozen set  $\mathcal{F} = \{0, 1, 2, 4\}$ , is constrained according to (9). The matrices  $\mathbf{V}$  and  $\mathbf{W}$  are:

$$\mathbf{V} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}, \quad \mathbf{W} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (12)$$

The code is permuted with  $\pi_1 = (0, 2, 1, 3, 4, 6, 5, 7)$  retrieved as  $\pi_1(i) = \text{bi2int} \left( \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} * \mathbf{b}_i \right)$ , with  $0 \leq i < 8$  and  $\text{bi2int}(\mathbf{b}_x) = \sum_{t=0}^2 2^t * b_{x,t}$ , a function that converts a binary number to an integer. Its transformed dynamic freezing constraint matrix  $\mathbf{V}_{T_1}$  is shown in (13).  $\mathbf{V}_{T_1}$  and  $\mathbf{V}$  are equivalent, as expected since  $\pi_1 \in \text{BLTA}(2, 1) \cap \text{PL}$ .

Some transformed dynamic freezing constraint matrices  $\mathbf{V}_T$  generated after applying permutation  $\pi \notin \text{BLTA}(2, 1) \cap \text{PL}$  are equivalent to  $\mathbf{V}$  such as  $\pi_2 = (7, 2, 5, 0, 3, 6, 1, 4) \in \text{LTA}$ .  $\pi_2$  is retrieved as  $\pi_2(i) = \text{bi2int} \left( \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} * \mathbf{b}_i + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right)$ . The transformed dynamic freezing constraint matrix  $\mathbf{V}_{T_2}$  is:

$$\mathbf{V}_{T_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}, \quad \mathbf{V}_{T_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}. \quad (13)$$

After row reduction on  $\mathbf{V}_{T_2}$ ,  $\mathbf{V}$  and  $\mathbf{V}_{T_2}$  have the same dynamic freezing constraint, i.e.,  $\mathbf{V}$  and  $\mathbf{V}_{T_2}$  are equivalent. We also note that

$$\mathbf{W}\mathbf{V}^\top = \mathbf{W}\mathbf{V}_{T_1}^\top = \mathbf{W}\mathbf{V}_{T_2}^\top = \mathbf{0}, \quad (14)$$

satisfying Definition 1. However, we conjecture that the transformed dynamic freezing constraint is not equivalent with respect to  $\mathbf{V}$  for longer codes and  $\pi \notin \text{BLTA}(n-1, 1) \cap \text{PL}$ .

Next, we study dynamic freezing constraint matrices that are variants of  $\mathbf{V}$  as described in (9). Let  $\mathcal{F}_{d_i} = \{k \in \mathcal{F} :$

TABLE I: Memory required by AE under three scenarios

$\mathbf{V}_T$ generated	Decoder knowledge	$\mathcal{R}(r, n)$			
		(3,7)	(3,8)	(4,8)	(5,8)
Stable	Irrelevant	22	29	29	8
Not stable	Known $\pi$	1889	5724	4199	1140
	Unknown $\pi$	65536	333824	190464	75776
Additional memory required (in bits)					

$b_{k,n-1} = 1, i_1(\mathbf{b}_k) = i\}$  and  $\mathcal{I}_{d_i} = \{k \in \mathcal{I} : b_{k,n-1} = 0, i_1(\mathbf{b}_k) = i\}$ . By (9),  $\mathbf{V}$  is obtained by setting  $\mathbf{u}_{\mathcal{F}_{d_i}} = \mathbf{u}_{\mathcal{I}_{d_{n-i}}}$ , where applicable. Then, any variant of  $\mathbf{V}$  is obtained by setting  $\mathbf{u}_{\mathcal{F}_{d_i}} = \mathbf{0}$  for some  $i \in \{1, \dots, n\}$ .

**Proposition 2.** The alternative dynamic freezing constraint is also stable under  $\text{BLTA}(n-1, 1) \cap \text{PL}$ .

*Proof.* The proof of Theorem 1 corresponds to the case having  $D$  dynamic frozen bits. Freezing to 0 all the indices whose binary representations share the same Hamming weight does not violate the validity of Theorem 1 since the permutation matrix  $\mathbf{A}$  maps any binary number to another one with the same Hamming weight.  $\square$

Consider the  $\mathcal{R}(3, 7)$  Reed-Muller code. By (9), each dynamic frozen bit of the sets  $\mathcal{F}_{d_1}, \mathcal{F}_{d_2}$  and  $\mathcal{F}_{d_3}$  is associated with an information bit of the sets  $\mathcal{I}_{d_6}, \mathcal{I}_{d_5}$  and  $\mathcal{I}_{d_4}$ , respectively. Then, designing a pre-transformation matrix with respect to any combination of dynamic frozen constraints  $\mathcal{F}_{d_1}, \mathcal{F}_{d_2}$  and  $\mathcal{F}_{d_3}$  satisfies the PL automorphism imposed by Theorem 1.

Proposition 3 gives the total number of stable dynamic freezing constraint matrices under  $\text{BLTA}(n-1, 1) \cap \text{PL}$ .

**Proposition 3.** The  $\mathcal{R}(r, n)$  Reed-Muller code has  $\min(2^{n-r-1}, 2^r)$  stable dynamic freezing constraint matrices under  $\text{BLTA}(n-1, 1) \cap \text{PL}$ .

*Proof.* The number of stable dynamic freezing constraint matrices corresponds to the number of existing combinations of dynamic freezing constraints  $\mathcal{F}_{d_i}$  with  $\mathcal{I}_{d_{n-i}}$ . The size of sets  $\mathcal{F}_{d_i}$  and  $\mathcal{I}_{d_{n-i}}$  is  $r$ -dependent. For a  $\mathcal{R}(r, n)$  Reed-Muller code, the number of non-empty sets  $\mathcal{F}_{d_i}$  and  $\mathcal{I}_{d_i}$  is respectively  $n-r-1$  and  $r$ . Hence, the number of stable dynamic freezing constraint matrices corresponds to the number of  $k$ -combinations for all  $0 \leq k \leq \min(n-r-1, r)$ , i.e.,  $\min(2^{n-r-1}, 2^r)$ . The dynamic freezing constraint matrix having zero dynamic frozen bit is included in the formula.  $\square$

For the  $\mathcal{R}(3, 7)$  Reed-Muller code, there are  $\min(2^3, 2^3) = 8$  stable dynamic freezing constraint matrices. Each combination returns a different number of low-weight codewords affecting the ML bound of the resulting pre-transformed code. However, the best combination is not in the scope of this paper.

### B. Memory Requirements

In the following, the additional memory requirements to perform AE decoding with pre-transformed polar codes are evaluated. The freezing constraint evaluated is that of (9) with  $M = 8$  permutations. Any of the proposed stable dynamic freezing constraint matrix can be synthesized with a maximum of  $D$  bits (see (10)). For any code rate,  $D$  has  $\frac{N}{2}$  as the

TABLE II: Number of codewords with weight  $w$  for  $\mathcal{R}(3, 7)$ -based codes and various dynamic freezing constraint matrices

	$w$				
	16	18	20	22	24
$\mathbf{V}_0$	94488	0	0	0	74078592
$\mathbf{V}_d$	20760	0	203420	$> 0$	$> 0$
$\mathbf{V}_D$	28632	13504	172800	$> 0$	$> 0$

upper bound. In the following, the dynamic and fixed decoder scenarios are studied. In the dynamic case, the permutations are unknown. Each adec needs to store their corresponding transformed dynamic freezing constraint matrix  $\mathbf{V}_T$  since  $\mathbf{V}_T$  is permutation dependent (8). In the fixed scenario, the  $M$  permutations are known *a priori* and a row reduction of each  $\mathbf{V}_T$  is performed, reducing the amount of memory required.

Table I shows the memory required, in bits, to store the dynamic freezing constraint  $\mathbf{V}$  for AE with  $M = 8$  permutations for the aforementioned cases. If permutations in  $\text{BLTA}(n-1, 1) \cap \text{PL}$  are used, regardless of the scenario,  $\mathbf{V}$  is stable and shared among the  $M = 8$  adec instances. As a result, at the cost of a reduction in permutation diversity, storing  $\mathbf{V}$  requires less memory, i.e.,  $D \ll N(N-K)$  bits. Table I shows that  $D \leq 29$  for Reed-Muller codes of length  $N \leq 256$ .

The last two rows of Table I show the memory required by the fixed and dynamic scenarios, respectively, for permutations in  $\text{LTA} \not\subset \text{BLTA}(n-1, 1) \cap \text{PL}$ . The matrix  $\mathbf{V}$  is thus not stable and cannot be shared among the  $M = 8$  adec instances. The dynamic scenario requires to store the  $M$  transformed dynamic constraints;  $MN(N-K)$  bits are required in total. With regard to memory requirements, the dynamic scenario is an upper bound of the fixed scenario (highlighted in gray in Table I). For the fixed scenario, the permutations are known in advance as well as the 8 transformed matrices  $\mathbf{V}_T$ . The  $\mathbf{V}_T$  matrices can thus be row-reduced before storage, reducing the memory requirements for the fixed case by over 97%, as can be seen by comparing the last two rows of Table I.

For example, the proposed constraint reduces the memory requirements by 98.8% for the  $\mathcal{R}(3, 7)$  Reed-Muller code with respect to the fixed scenario having permutations in LTA.

## IV. SIMULATION RESULTS

In this section, simulation results with  $\mathcal{R}(3, 7)$  as the underlying code are performed over the AWGN channel with BPSK modulation. Three different stable dynamic freezing constraint matrices are compared:  $\mathbf{V}_0$  having no dynamic frozen bits,  $\mathbf{V}_D$  with all  $D = 22$  dynamic frozen bits, and  $\mathbf{V}_d$  with  $0 < d = 15 < D$  dynamic frozen bits. The  $d$  dynamic frozen bits correspond to all indices  $k \in \mathcal{F}$  with  $i_1(\mathbf{b}_k) = 3$ .

The codes are decoded under AE decoding with  $M = 8$  automorphisms in  $\text{BLTA}(n-1, 1) \cap \text{PL}$  and having SCL with  $L = 16$  as sub-decoders. This decoder is denoted as AE-8-SCL-16 in the following. The code defined by  $\mathbf{V}_0$  is the  $\mathcal{R}(3, 7)$  Reed-Muller code and AE decoding was shown to perform close to the ML bound [11], [25]. By lowering the ML bound with the proposed freezing constraint, a gain is expected at the cost of a small memory overhead.

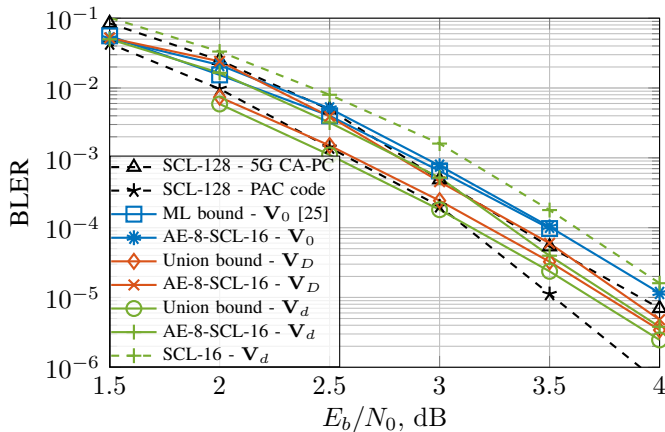


Fig. 1: Decoding performance of  $\mathcal{R}(3,7)$ -based codes under AE-8-SCL-16 and SCL-16 against other codes and bounds.

Figure 1 shows the error-correction performance of the three codes of interest under AE-8-SCL-16 decoding and their ML bound approximated with the truncated union bound (computed from the number of low-weight codewords). For reference, Figure 1 also shows 2 other pre-transformed polar codes: a PAC code [6] and a 5G CA-polar code [5]. Both are decoded with SCL-128, thus having similar complexity but higher latency with respect to AE-8-SCL-16.

Table II shows the number of low-weight codewords computed as in [26] for codes defined by  $\mathbf{V}_D$ ,  $\mathbf{V}_d$  and  $\mathbf{V}_0$ . It can be seen that the  $\mathcal{R}(3,7)$  Reed-Muller code has a large number of minimum weight ( $w = 16$ ) codewords with respect to the two other pre-transformed polar codes investigated. The pre-transformed polar code defined by  $\mathbf{V}_D$  has 28632 codewords of weight  $w = 16$ , a reduction of 70% with respect to  $\mathcal{R}(3,7)$ , but has generated 13504 codewords of weight  $w = 18$ . From Table II, the results for  $\mathbf{V}_d$  show that freezing some of the dynamic frozen bits of  $\mathbf{V}_D$  to 0 allows to reduce the amount of codewords of weight  $w = 16$  by approximately 27%, i.e., from 28632 down to 20760 (78% with respect to  $\mathcal{R}(3,7)$ ) while having 0 codeword of weight  $w = 18$ . Comparing the union-bound curve for  $\mathbf{V}_d$  against either of the other two bound curves in Figure 1, it can be seen that a reduction in the number of low-weight codewords lowers the ML bound.

Figure 1 also shows that AE-8-SCL-16 decoding reaches the ML bound of  $\mathcal{R}(3,7)$  while AE decoding with the proposed dynamic freezing constraints, i.e.,  $\mathbf{V}_D$  and  $\mathbf{V}_d$ , gains up to 0.25 dB with respect to this bound. At the cost of a higher latency than AE-8-SCL-16, the 5G CA-polar code manages a similar error-correction performance under SCL-128. Also under SCL-128, PAC codes exhibit the best performance, however the convolution inherent to PAC codes incurs more computations than our proposed constraint (9) that only requires to read former decision values. The use of 8 automorphisms improves the error-correction performance of SCL-16 by 0.3 dB for the code defined by  $\mathbf{V}_d$ .

and that are stable under permutation linear transformations.

## V. CONCLUSIONS

In this letter, we proposed several dynamic freezing constraint matrices for Reed-Muller codes that lower the ML bound

The stability of the dynamic freezing constraints reduces the memory requirements by 99% with respect to a dynamic AE decoder. The decoding performance under AE-8-SCL-16 was shown to be 0.3 dB better than under SCL-16 while the ML bound of the  $\mathcal{R}(3,7)$  Reed-Muller code is beaten by 0.25 dB.

## REFERENCES

- [1] E. Arıkan, "Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.
- [2] I. Tal and A. Vardy, "List decoding of polar codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2213–2226, Mar. 2015.
- [3] Q. Zhang et al., "CRC code design for list decoding of polar codes," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1229–1232, Feb. 2017.
- [4] J. Piao et al., "Approaching the normal approximation of the finite blocklength capacity within 0.025 dB by short polar codes," *IEEE Wireless Commun. Lett.*, vol. 9, no. 7, pp. 1089–1092, Mar. 2020.
- [5] V. Bioglio et al., "Design of polar codes in 5G new radio," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 29–40, Jan. 2021.
- [6] E. Arıkan, "From sequential decoding to channel polarization and back again," in *arXiv preprint arXiv:1908.09594*, Aug. 2019.
- [7] Y. Polyanskiy, V. H. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, Apr. 2010.
- [8] S. Gelincik et al., "Achieving PAC code performance with SCL decoding without extra computational complexity," in *IEEE Int. Conf. Commun. (ICC)*, Apr. 2022, pp. 104–109.
- [9] S. Gelincik et al., "Preserving the minimum distance of polar-like codes while increasing the information length," in *IEEE Int. Symp. Inf. Theory (ISIT)*, June 2022, pp. 2130–2135.
- [10] B. Li, H. Zhang, and J. Gu, "On pre-transformed polar codes," *arXiv preprint arXiv:1912.06359*, Dec. 2019.
- [11] M. Geiselhart et al., "Automorphism ensemble decoding of Reed-Muller codes," *IEEE Trans. Commun.*, vol. 69, no. 10, pp. 6424–6438, 2021.
- [12] M. Kamenev et al., "A new permutation decoding method for Reed-Muller codes," in *IEEE Int. Symp. Inf. Theory (ISIT)*, July 2019, pp. 26–30.
- [13] K. Ivanov and R. Urbanke, "On the efficiency of polar-like decoding for symmetric codes," *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 163–170, Jan. 2022.
- [14] C. Pillet and V. Bioglio, "On the distribution of partially symmetric codes for automorphism ensemble decoding," *arXiv preprint arXiv:2205.04338*, May 2022.
- [15] MacWilliams F.J. and Sloane N.J.A., *The theory of error correcting codes*, North-Holland Publishing Company, 1977.
- [16] M. Geiselhart et al., "On the automorphism group of polar codes," in *IEEE Int. Symp. Inf. Theory (ISIT)*, July 2021, pp. 1230–1235.
- [17] C. Pillet et al., "Polar codes for automorphism ensemble decoding," in *IEEE Inf. Theory Workshop (ITW)*, Oct. 2021, pp. 1–6.
- [18] C. Pillet et al., "Classification of automorphisms for the decoding of polar codes," in *IEEE Int. Conf. Commun. (ICC)*, May 2022, pp. 110–115.
- [19] M. Kamenev, "Improved permutation-based successive cancellation decoding of polar codes," in *IEEE Int. Conf. Young Prof. Electron Devices and Materials (EDM)*, Aug. 2021, pp. 110–115.
- [20] M. Geiselhart et al., "A polar subcode approach to belief propagation list decoding," in *IEEE Inf. Theory Workshop (ITW)*, Nov. 2022, pp. 243–248.
- [21] M. Geiselhart et al., "CRC-aided belief propagation list decoding of polar codes," in *IEEE Int. Symp. Inf. Theory (ISIT)*, Aug. 2020, pp. 395–400.
- [22] I. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *Trans. IRE Prof. Group Inf. Theory*, vol. 4, no. 4, pp. 38–49, Sept. 1954.
- [23] D. E. Muller, "Application of boolean algebra to switching circuit design and to error detection," *Trans. IRE Prof. Group Inf. Theory*, no. 3, pp. 6–12, Sept. 1954.
- [24] P. Trifonov and V. Miloslavskaya, "Polar subcodes," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 2, pp. 254–266, Nov. 2016.
- [25] M. Helmling et al., "Database of channel codes and ML simulation results," [www.uni-kl.de/channel-codes](http://www.uni-kl.de/channel-codes), 2019.
- [26] Bin Li et al., "An adaptive successive cancellation list decoder for polar codes with cyclic redundancy check," *IEEE Commun. Lett.*, vol. 16, no. 12, pp. 2044–2047, Nov. 2012.