# Analysis of the Block Error Probability of Concatenated Polar Code Ensembles

Giacomo Ricciutelli, *Student Member, IEEE*, Thomas Jerkovits , *Student Member, IEEE*,
Marco Baldi , *Senior Member, IEEE*, Franco Chiaraluce , *Senior Member, IEEE*,
and Gianluigi Liva , *Senior Member, IEEE*

*Abstract*—In this paper, we provide an analysis of the performance of concatenation of polar codes with outer cyclic redundancy check (CRC) codes, separated by an interleaver, in the short and moderate block length regimes. The analysis addresses maximum likelihood decoding as a proxy to the code performance under successive cancellation list decoding. The analysis is carried out by introducing the concatenated polar code (CPC) ensembles, whose distance properties can be analyzed (for sufficiently short block lengths) by means of the uniform interleaver approach. At moderate block lengths, we resort to the Monte Carlo simulations. Results show that if the inner polar code possesses a low minimum distance and the outer CRC code has a sufficiently large amount of redundancy, then the choice of the outer code generator polynomial and the interleaver may yield to a large variability in the performance of the resulting CPC.

*Index Terms*—Concatenated codes, cyclic codes, interleaving, polar codes, union bounds.

## I. INTRODUCTION

**P**OLAR codes [1], [2] provably achieve the capacity of binary-input discrete memoryless symmetric (BI-DMS) channels by means of (low complexity) successive cancellation (SC) decoding algorithm [2], in the limit of an infinite block length. On the other hand, at moderate-short block lengths, polar codes under SC decoding tend to exhibit a poor performance. In [3] it was suggested that such a behavior might be due, on one hand, to an intrinsic weakness of polar codes and, on the other hand, to the sub-optimality of SC decoding w.r.t. maximum likelihood (ML) decoding. Improved decoding algorithms were proposed in [3]–[5], while the structural properties of polar codes (e.g., their distance properties) were studied, among others, in [6]–[11]. As regards

the minimum distance properties of polar codes, they can be improved by resorting to concatenated schemes, as done in [3], where the concatenation of polar codes with an outer cyclic redundancy check (CRC) code is considered. This solution, together with the use of the list decoding algorithm, allows polar codes to become competitive in moderate-short block length regime [12]–[16].[1]

For given block length and rate, a concatenated polar coding scheme can be realized with several combinations of component codes [19], [20]. For example, after fixing the rate of the inner polar code, one may choose among various outer codes. However, as observed in [19], CRC-polar concatenated codes with list decoding achieve the best performance among several options. In [21], the optimal choice of CRC codes for the use as outer codes in polar-CRC concatenated schemes without interleaving is studied. The impact of the choice of the outer CRC code generator polynomial is demonstrated and optimal generator polynomials are investigated. The analysis of outer CRC codes is extended to the case with interleaving in [22], considering the presence of a random interleaver. The impact of the choice of the CRC code generator polynomial on the performance of the concatenated scheme also for the case with interleaving is confirmed.

Even when restricting the outer code to be a specific binary linear block code, various permutations of the outer code bits may be considered at the input of the polar encoder.[2] While the effect of different outer codes has been already studied, the impact of interleaving has still not been assessed, to the authors' best knowledge. The main role of the interleaver (i.e., of the permutation of the outer code which defines the mapping of the outer codeword bits onto the non-frozen bit set of the inner polar code) is to provide a degree of freedom in the concatenation, aiming at good distance properties. However, as we will show afterward, this cannot be taken for granted, since it depends on the interleaver choice.

The availability of the weight enumerator (i.e., distance spectrum) of a concatenated polar code (CPC) may be particularly important in order to characterize its performance under successive cancellation list (SCL) decoding. Concerning the distance spectrum of polar codes, current approaches only provide bounds [7] or rely on partial [9] or approximated

---

[1]The 3GPP standardization group has adopted short polar codes with an outer CRC for uplink and downlink control information of the upcoming 5G standard [17], [18].

[2]Strictly speaking, any permutation of the outer code coordinates results in a different, though equivalent, binary linear block code.

distance spectra [8], [23]. Unfortunately, exact closed-form results are still missing, thus hindering the weight enumerator analysis for the concatenated scheme. In order to gain insights on the role of the outer code in a concatenated polar coding scheme, we first consider short codes which allow an exhaustive distance spectrum analysis and then we investigate the performance in medium block length regime through Monte Carlo simulations.

In the short block length regime, the study is carried out by introducing *CPC ensembles* and by deriving their average weight enumerating function (AWEF) by following the classic approach in [24]. For short block lengths, we restrict our attention to high-rate polar codes for which the distance spectrum can be explicitly determined. More precisely, we consider the dual code of the selected polar code and then we find its input-output weight enumerating function (IOWEF) by exhaustive enumeration. We then obtain the IOWEF of the original polar code via the generalized MacWilliams identity [25]. As outer codes we consider cyclic codes (and CRC codes, in particular) and we compute their AWEF by following the method presented in [26]. The AWEF analysis, when feasible, permits us to estimate the average behavior of the CPCs composing the ensemble, that is, considering all possible interleavers. Additionally, we are interested in investigating the concentration of the CPCs performance around the ensemble average, as well as the impact of different generator polynomials for the outer code. Also on this point, a theoretical formulation is unfeasible, thus we resort to numerical examples whose discussion permits us to draw some empirical but significant conclusions. In particular, our analysis shows that, if the inner polar code possesses a low minimum distance and the outer CRC code has a sufficiently large amount of redundancy, then the choice of the outer code generator polynomial and of the interleaver may yield to a large variability in the performance of the resulting CPC. We remark that our target is to study the impact of interleaving and of the interplay between the interleaver and the inner/outer codes on the performance of CPCs, while finding optimal interleavers and/or optimal outer codes is out of the scope of this paper.

The paper is organized as follows. Section II introduces the notation and some basic results. CPC ensembles are presented in Section III, while their analysis in terms of AWEF is discussed in Section IV. Numerical results are shown in Section V. Conclusions follow in Section VI.

## II. PRELIMINARIES

The main symbols and preliminary concepts that will be used in the analysis are introduced below.

### A. Weight Enumerators

Let $w_H(\cdot)$ be the Hamming weight of a vector. Given an $(n, k)$ binary linear block code $\mathcal{C}$, its weight enumerating function (WEF) is defined as [25]

$$A(X) := \sum_{i=0}^{n} A_i X^i$$

where $A_i$ is the number of codewords $\boldsymbol{c}$ with $w_H(\boldsymbol{c}) = i$. Assume the encoder of $\mathcal{C}$ to be in systematic form.

Hence, without loss of generality, the first $k$ bits of $\boldsymbol{c}$ carry the information word $\boldsymbol{u}$, i.e., $\boldsymbol{c} = (\boldsymbol{u}|\boldsymbol{p})$, where $\boldsymbol{p}$ is the vector containing the parity bits. The IOWEF of $\mathcal{C}$ is then

$$A^{\mathrm{IO}}(X, Y) := \sum_{i=0}^{k} \sum_{\omega=0}^{n} A^{\mathrm{IO}}_{i,\omega} X^i Y^\omega$$

where $A^{\mathrm{IO}}_{i,\omega}$ is the multiplicity of codewords $\boldsymbol{c}$ with $w_H(\boldsymbol{u}) = i$ and $w_H(\boldsymbol{c}) = \omega$. The enumeration of the codeword weights entails a large complexity even for relatively small code dimensions. If $\mathcal{C}$ has a high rate, the MacWilliams identity [25] may be used to simplify the derivation of the IOWEF. The simplification stems from the fact that, under this assumption, the number of codewords of the dual code $\mathcal{C}^\perp$ is (much) smaller than the number of codewords of $\mathcal{C}$. Assume that the enumeration of the codeword weights is feasible for the dual code, and denote by $A^\perp(X)$ the dual code WEF. We can express the WEF of $A(X)$ as [25]

$$A(X) = \frac{(1 + X)^n}{2^{n-k}} A^\perp \left( \frac{1 - X}{1 + X} \right).$$

An analysis of the CPC based on the WEF and the MacWilliams identity has been recently developed in [27] but with reference to specific codes and then ignoring the (average) impact of different interleavers, that instead we are able to take into account through the study of the ensembles. The latter issue will be discussed in Section IV.

Since code $\mathcal{C}$ is assumed to be systematic, it is convenient to derive its IOWEF from the input redundancy weight enumerating function (IRWEF) $A^{\mathrm{IR}}(x, X, y, Y)$, which is defined as

$$A^{\mathrm{IR}}(x, X, y, Y) := \sum_{i=0}^{k} \sum_{t=0}^{n-k} A^{\mathrm{IR}}_{i,t} x^{k-i} X^i y^{n-k-t} Y^t$$

where $A^{\mathrm{IR}}_{i,t}$ is the multiplicity of codewords $\boldsymbol{c}$ with $w_H(\boldsymbol{u}) = i$ and $w_H(\boldsymbol{p}) = t$. By applying the generalized MacWilliams identity [25], [28]–[30, Ch. 5, Sec. 6], the IRWEF of $\mathcal{C}$ can be derived by the one of its dual code as

$$A^{\mathrm{IR}}(x, X, y, Y)$$
$$= \frac{1}{2^{n-k}} A^{\mathrm{IR},\perp}(x + X, x - X, y + Y, y - Y).$$

Then, the IOWEF is obtained as

$$A^{\mathrm{IO}}(X, Y) = A^{\mathrm{IR}}(1, XY, 1, Y).$$

### B. Bounds on the Block Error Probability

For a given $(n, k)$ binary linear block code $\mathcal{C}$, tight upper bounds on its block error probability (BEP) $P_B$ under ML decoding can be obtained via the code weight enumerator. These bounds are not reported here for saving space but, for a thorough survey on the topic, we point the reader to [31].

On the other hand, a tight upper bound over a binary erasure channel (BEC) with erasure probability $\epsilon$ is given by [32], [33]

$$P_B(\mathcal{C}, \epsilon)$$
$$\leq \sum_{e=k+1}^{n} \binom{n}{e} \epsilon^e (1 - \epsilon)^{n-e}$$
$$+ \sum_{e=1}^{k} \binom{n}{e} \epsilon^e (1 - \epsilon)^{n-e} \min \left\{ 1, \sum_{\omega=1}^{e} \binom{e}{\omega} \frac{A_\omega}{\binom{n}{\omega}} \right\}. \quad (1)$$

A tight upper bound on the BEP over the additive white Gaussian noise (AWGN) channel is Poltyrev's tangential sphere packing bound (TSB) [34]. The latter is less explicit than (1) and is not discussed here for the sake of brevity. Both bounds will be used in Section V to estimate the BEP of CPCs by analyzing the corresponding CPC ensembles, to be discussed next.

## III. CONCATENATED POLAR CODES AND CONCATENATED POLAR CODE ENSEMBLES

We consider the serial concatenation of an $(n_\mathrm{I}, k_\mathrm{I})$ polar code $\mathcal{C}^\mathrm{I}$ with an $(n_\mathrm{o}, k_\mathrm{o})$ binary linear block code $\mathcal{C}^\mathrm{o}$, with $k_\mathrm{I} = n_\mathrm{o}$. The inner and the outer code rates are denoted by $R_\mathrm{I}$ and $R_\mathrm{o}$, respectively. As outer codes, we consider cyclic binary linear block codes (CRC codes, in particular). The generator matrix of the outer code is denoted by $\boldsymbol{G}_\mathrm{o}$, whereas the generator matrix of the inner polar code is $\boldsymbol{G}_\mathrm{I}$. The polar code generator matrix is obtained by selecting $k_\mathrm{I}$ rows of the $n_\mathrm{I} \times n_\mathrm{I}$ matrix

$$\boldsymbol{G}_\mathrm{I} := \mathbf{G}_2^{\otimes \log_2 n_\mathrm{I}}$$

with

$$\mathbf{G}_2 := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

where the selected rows are associated to the $k_\mathrm{I}$ most reliable synthesized channels [2]. The synthesized channel reliability is determined under the assumption of SC decoding via density evolution (DE) [2], [35], [36] for both the BEC and the AWGN channel, with the Gaussian approximation (GA) used in the latter case [5], [37]. The resulting $k_\mathrm{I} \times n_\mathrm{I}$ matrix is then put into systematic form following [38]. The choice of inner polar codes with generator matrix in systematic form simplifies the distance spectrum analysis of the concatenated polar coding scheme, as will be illustrated in Section IV.

The outer codeword bits may be permuted prior to encoding with the inner polar encoder. We denote the block length and dimension of the overall concatenated code as $n$ and $k$, respectively. We have that $n = n_\mathrm{I}$ and $k = k_\mathrm{o}$, whereas the rate of the concatenated code is $R = R_\mathrm{o} R_\mathrm{I}$. The generator matrix of the concatenated code is

$$\boldsymbol{G} = \boldsymbol{G}_\mathrm{o} \boldsymbol{\Pi} \boldsymbol{G}_\mathrm{I} \tag{2}$$

with $\boldsymbol{\Pi}$ being a $k_\mathrm{I} \times k_\mathrm{I}$ permutation matrix (with $\boldsymbol{\Pi}$ being an identity matrix in case of no interleaving). From now on, the terms "permutation matrix" and "interleaver" will be used as synonyms. We refer next to the code with generator matrix given by (2) as to CPC.

We are interested in the performance of the CPC under ML decoding. This is important also in view of practical implementation. In fact, it was shown in [3] that SCL decoding with a moderately large list size tightly approaches the performance of ML for concatenated polar codes of small and medium block lengths.[3] Since the performance of a code under ML is mainly driven by its distance spectrum (see Section II-B),

a weight distribution analysis of CPCs will be presented in Section IV.

As discussed in Section II-A, the enumeration of the codeword weights for a given code is feasible if either the code or its dual has a small dimension. While for a given $(n, k)$ CPC this might not be the case, for the inner and the outer codes the derivation of the weight enumerator might be still feasible. The knowledge of inner/outer code WEFs allows deriving estimates of the CPC distance spectrum by introducing the concept of concatenated code ensembles [24], [39], [40], where one of the constituent codes is here a polar code. For this reason we speak of CPC ensembles. For a given pair of inner and outer codes $(\mathcal{C}^\mathrm{I}, \mathcal{C}^\mathrm{o})$, we define the CPC ensemble $\mathscr{C}(\mathcal{C}^\mathrm{I}, \mathcal{C}^\mathrm{o})$ as the set of codes with generator matrix in the form (2), by considering all possible permutation matrices $\boldsymbol{\Pi}$.

## IV. AVERAGE WEIGHT ENUMERATORS OF CONCATENATED POLAR CODES ENSEMBLES

Given a $\mathscr{C}(\mathcal{C}^\mathrm{I}, \mathcal{C}^\mathrm{o})$ CPC ensemble, the expected multiplicity $\bar{A}_\omega$ of codewords with Hamming weight $\omega$ of a code picked uniformly at random from the ensemble has the meaning of AWEF of the concatenation. It can be obtained from the inner and outer code weight enumerators as [24]

$$\bar{A}_\omega = \sum_{i=0}^{n_\mathrm{o}} \frac{A_i^\mathrm{o} A_{i,\omega}^{\mathrm{IO},\mathrm{I}}}{\binom{n_\mathrm{o}}{i}} \tag{3}$$

where $A_i^\mathrm{o}$ is the weight enumerator of the outer code and $A_{i,\omega}^{\mathrm{IO},\mathrm{I}}$ is the input-output weight enumerator of the inner code. The upper bounds on the BEP discussed in Section II-B apply also to code ensembles by replacing a code weight enumerator with the (corresponding) ensemble average weight enumerator provided by (3). The obtained upper bound applies then to the average BEP of a code randomly picked from the ensemble.

Note that a $\mathscr{C}(\mathcal{C}^\mathrm{I}, \mathcal{C}^\mathrm{o})$ ensemble contains the codes generated by all possible permutation matrices. Thus, also bad codes (i.e., codes characterized by a low minimum distance) may belong to the ensemble. It is clear that the bad codes adversely affect the average weight enumerator obtained through (3) causing raise of the average BEP. A tighter estimate of the BEP for the best codes in the ensemble can be obtained by expurgating the ensemble from the bad codes. Following [39], we observe that the cumulative distribution of the minimum distance for the codes in $\mathscr{C}(\mathcal{C}^\mathrm{I}, \mathcal{C}^\mathrm{o})$ satisfies

$$\Pr\{d_{\min}(\mathcal{C}) \leq d\} \leq \sum_{\omega=0}^{d} \bar{A}_\omega - 1 =: f(d).$$

For an arbitrary $\theta \in (0, 1)$, define

$$d^\star := \max_{d \in \mathbb{N}_0} \{d | f(d) \leq \theta\}$$

with $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$. Then

$$\Pr\{d_{\min}(\mathcal{C}) \leq d^\star\} \leq \sum_{\omega=0}^{d^\star} \bar{A}_\omega - 1 \leq \theta$$

---

[3]Because of its low complexity, SCL is commonly used for polar codes decoding.

i.e., the probability of picking a code with minimum distance lower than or equal to $d^\star$ is upper bounded by $\theta$. It follows that a fraction of at least $(1 - \theta)$ codes belonging to the ensemble has $d_{\min} > d^\star$. We refer to the subset of codes with $d_{\min} > d^\star$ as the expurgated ensemble. The average weight enumerator of the expurgated ensemble can be upper bounded as [39, Sec. 2.2]

$$\bar{A}_\omega^{\exp} \leq \frac{1}{1-\theta} \bar{A}_\omega$$

for $\omega > d^\star$, whereas $\bar{A}_\omega^{\exp} = 0$ for $1 \leq \omega \leq d^\star$.

## V. ANALYSIS OF THE BLOCK ERROR PROBABILITY

The object of this section is to apply the analysis methods described in the previous sections to some practical cases, and to discuss the impact on the error rate performance of the outer code as well as of the interleaver between the inner and the outer code. In particular, we analyze the BEP of (expurgated, where applicable) CPC ensembles over the binary input AWGN channel and the BEC.

For the AWGN channel case, we will provide estimates of the BEP as a function of the channel signal-to-noise ratio (SNR) expressed as $E_b/N_0$, where $E_b$ is the energy per information bit and $N_0$ is the single-sided noise power spectral density. When providing the design SNR for the inner polar code, by using the DE algorithm, we will refer instead to the ratio $E_s/N_0$, where $E_s = RE_b$ is the energy per codeword symbol. This choice allows avoiding confusion about the rate used in the conversion (rate of the overall scheme vs. rate of the inner code only). Different values of $E_s/N_0$ are considered in the design. This is because of the "non-universality" of polar codes, that holds if the standard construction is used and according to which different polar codes are generated depending on the specified value of the SNR. Consequently, in this way we are able to investigate the impact of the design SNR whose optimization is not easy [41]. When the results over the BEC are of interest, following a classic approach, we design the inner polar code by fixing $\epsilon$.

In the short block length regime, we estimate the expected BEP by means of the upper bounds discussed in Section II-B. When complexity allows, we make use of the (generalized) MacWilliams identity. In particular, for the codes with rate larger than $1/2$ and $n - k$ small enough, we resort to the analysis of the dual code, as this reduces the computational burden (a further reduction of complexity in the derivation of the ensemble average weight enumerator is presented in the Appendix). The analysis of the expected BEP is complemented by Monte Carlo simulations aiming at analyzing the concentration of the BEP to the average. In the moderate block length regime, only Monte Carlo simulations are employed due to the increase in complexity for the weight enumeration.

### A. Performance of Short Codes

A first implication of the non-universality of polar codes is that polar codes designed at different $E_s/N_0$ may have different values of $d_{\min}$. As an example, we have designed two $(64, 40)$ polar codes over the AWGN channel, the first at
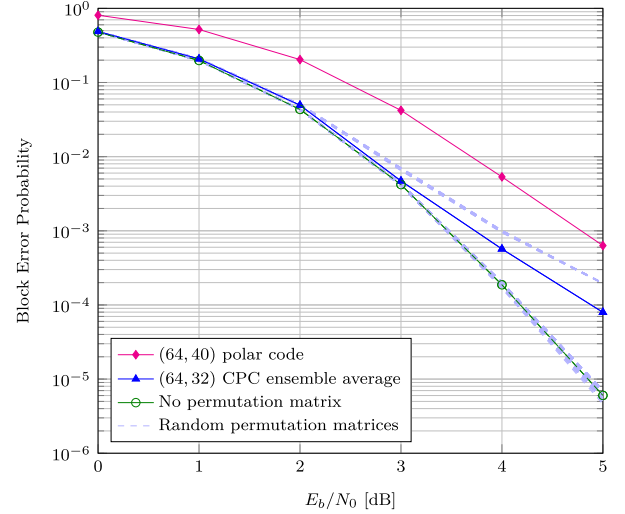


Fig. 1. TSBs on the ML performance of CPC (ensembles) with and without random interleavers composed by a $(64, 40)$ polar code with CRC-$8_1$ over the AWGN channel. TSB on the $(64, 40)$ polar code alone is also reported. The polar code is designed at $E_s/N_0 = 0$ dB.
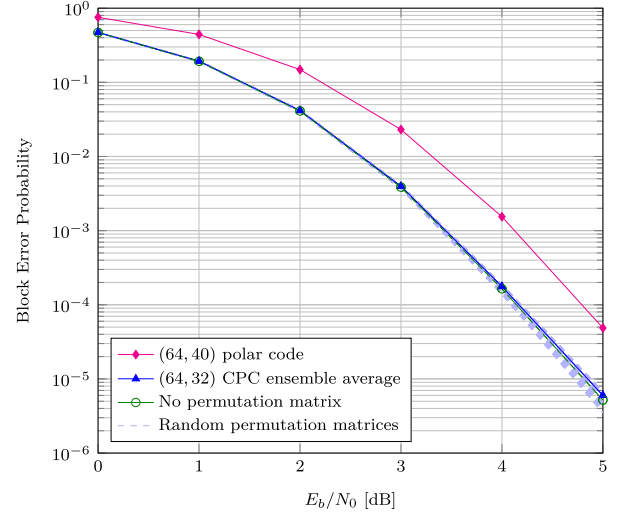


Fig. 2. TSBs on the ML performance of CPC (ensembles) and without random interleavers composed by a $(64, 40)$ polar code with CRC-$8_1$ over the AWGN channel. TSB on the $(64, 40)$ polar code alone is also reported. The polar code is designed at $E_s/N_0 = 3$ dB.

$E_s/N_0 = 0$ dB and the second at $E_s/N_0 = 3$ dB; for the first code we have $d_{\min} = 4$, while for the second code $d_{\min} = 8$. In both cases, the polar code has been concatenated with the CRC$-8_1$ code whose generator polynomial is reported in Table I, yielding a $(64, 32)$ CPC, that is, with rate $1/2$. Their ML BEP performance estimates obtained by applying the TSB to the code distance spectrum is shown in Fig. 1 (design for $E_s/N_0 = 0$ dB) and Fig. 2 (design for $E_s/N_0 = 3$ dB). By comparing the two plots, we see that (as expected) the performance of the polar code with smaller minimum distance is worse than that of the code with greater minimum distance at large SNRs.

The impact of the concatenation is evident in the figures, which report the results obtained with 1000 random interleavers, including the case without permutation. In both cases,

TABLE I

CRC CODES CONSIDERED IN THE ANALYSIS

| Code | Generator polynomial, $g(x)$ |
|------|------------------------------|
| CRC-$8_1$ | $x^8 + x^2 + x + 1$ |
| CRC-$8_2$ | $x^8 + x^7 + x^6 + x^4 + x^2 + 1$ |
| CRC-$8_3$ | $x^8 + x^4 + x^3 + x^2 + 1$ |
| CRC-$16_1$ | $x^{16} + x^{12} + x^5 + 1$ |
| CRC-$16_2$ | $x^{16} + x^{15} + x^{11} + x^9 + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ |
| CRC-$16_3$ | $x^{16} + x^{10} + x^8 + x^7 + x^3 + 1$ |

the concatenation introduces significant improvements[4] and, most important for our analysis, the scheme using the polar code with $d_{\min} = 4$ can reach the same performance as the scheme using the polar code with $d_{\min} = 8$, when certain interleavers are used. On the other hand, as reported in Table II, 32 out of 1000 randomly-generated interleavers do not yield an improved minimum distance, limiting the gain attained over the inner polar code at large SNRs.

The figures also include the BEP over the CPC ensemble obtained by applying the TSB to the AWEF. Figure 2 shows that, for the case where the polar code has been designed for high SNR (yielding a $d_{\min} = 8$), the performance of the codes sampled in the ensemble is concentrated on the ensemble average. The situation is different in Fig. 1. Here, the codes sampled from the ensemble can be clustered in two groups: A first group with *good* codes clearly outperforming the ensemble average, and a second group of *bad* codes which exhibit a high error probability. The set of sampled bad codes consists of the 32 codes with $d_{\min} = 4$ (see Table II). Despite being a small fraction of the overall sample population, their performance dominates the ensemble average at high SNR.

Following [22], an investigation of the impact of the choice of the outer code has been carried out. In particular, we have considered two additional outer codes, noted as CRC-$8_2$ and CRC-$8_3$, whose generator polynomials are also reported in Table I. The codes have been concatenated with the inner polar code with $d_{\min} = 8$. The average ensemble performances (upper bounded via the TSB) are shown in Fig. 3. The ensemble averages turn to be insensitive, in this particular case, on the choice of the outer CRC-8 code. This behavior, however, does not hold in general. As a counter-example we can study a scheme using a $(64, 48)$ polar code designed for $E_s/N_0 = 3.25$ dB. By applying a CRC-16 code as outer code, we obtain a rate-$1/2$ CPC. As before, three different CRC codes have been considered, with generator polynomials reported in Table I. The average ensemble performances (upper bounded via the TSB) are shown in Fig. 4. In this case the choice of the CRC code has a relevant impact. In fact, the performance of the scheme using CRC-$16_1$ is significantly worse than those obtained with the other outer codes. The average expurgated ensemble performances (upper bounded via the TSB) are also provided. We observe that expurgation

[4]Clearly, the comparison between the performance of the polar code and those of the corresponding CPCs is not fair due to the difference in rate.
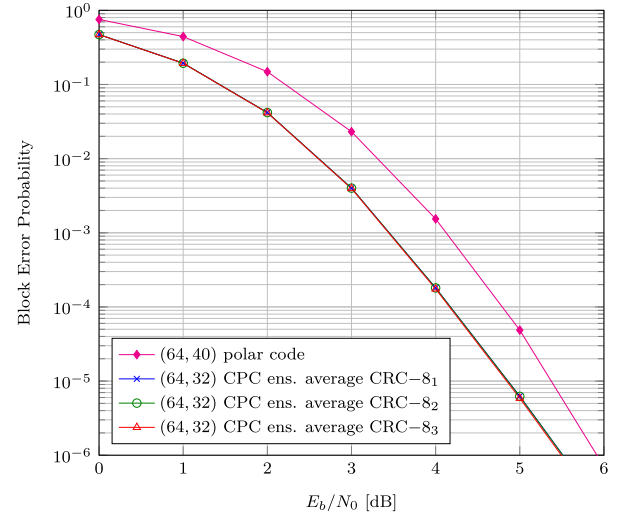


Fig. 3. TSBs on the ML performance of CPC (ensembles) composed by a $(64, 40)$ inner polar code with different CRC$-8$ outer codes over the AWGN channel. TSB on the performance of the $(64, 40)$ polar code alone is also reported. The polar code is designed at $E_s/N_0 = 3$ dB.
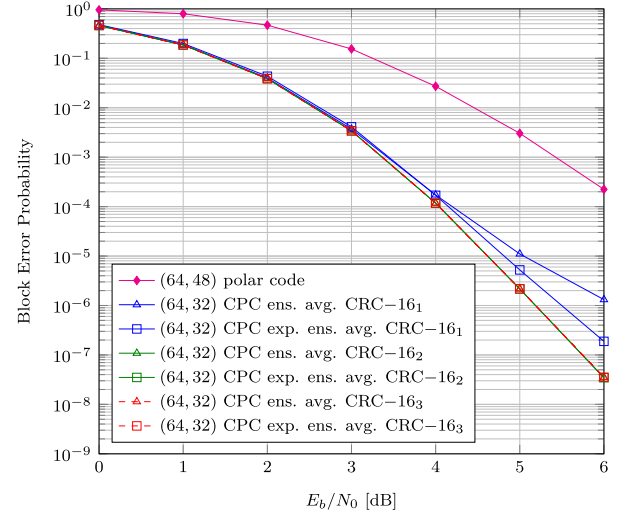


Fig. 4. TSBs on the ML performance of CPC (ensembles) composed by a $(64, 48)$ polar code with different CRC$-16$ outer codes over the AWGN channel. TSB on the $(64, 48)$ polar code alone is also reported. The polar code is designed at $E_s/N_0 = 3.25$ dB.

has no effect on the error probability of the schemes with the CRC-$16_2$ code and the CRC-$16_3$ code, while for the case of the CRC-$16_1$ code the effect is visible. Still, the average performance of the expurgated CPC ensemble based on the CRC-$16_1$ outer code is inferior to the other two ensembles' average performance.

As for the shorter CPC ensemble of Fig. 1, the poor average performance of the CPC ensemble employing the CRC-$16_1$ code can be attributed to the presence, in the ensemble, of a fraction of bad codes, i.e., of codes characterized by a small minimum distance. As documented in Table II, 2 codes out of the 1000 composing the sample population have $d_{\min} = 4$ and 45 codes have $d_{\min} = 6$ (for the case of the CRC-$16_2$ and the CRC-$16_3$ codes we observed instead a strong concentration around $d_{\min} = 8$).

TABLE II
NUMBER OF CPCs SAMPLED WITHIN EACH ENSEMBLE, FOR A GIVEN MINIMUM DISTANCE

| $(n_i,k_i)$ polar code | Design channel | CRC | $d_{\min} = 4$ | $d_{\min} = 6$ | $d_{\min} = 8$ | $d_{\min} = 10$ |
|---|---|---|---|---|---|---|
| $(64, 40)$ | AWGN $E_s/N_0 = 0$ dB | CRC-$8_1$ | 32 | - | 968 | - |
| $(64, 40)$ | AWGN $E_s/N_0 = 3$ dB | CRC-$8_1$ | - | - | 1000 | - |
| $(64, 40)$ | BEC $\epsilon = 0.3$ | CRC-$8_1$ | 48 | - | 952 | - |
| $(64, 48)$ | AWGN $E_s/N_0 = 3.25$ dB | CRC-$16_1$ | 2 | 45 | 902 | 51 |
| $(64, 48)$ | BEC $\epsilon = 0.3$ | CRC-$16_1$ | 939 | 6882 | 12177 | 2 |
| $(128, 112)$ | AWGN $E_s/N_0 = 3.72$ dB | CRC-$16_1$ | 167 | 833 | - | - |
| $(128, 112)$ | BEC $\epsilon = 0.3$ | CRC-$16_1$ | 266 | 734 | - | - |

Based on the above examples, we can draw the following conclusion. The choice of the outer code and of a proper permutation is particularly critical when (i) the inner polar code has a small minimum distance and (ii) the outer code introduces enough redundancy to *prune* the inner code from low-weight codewords. Conversely, when the inner polar code has a large minimum distance and the outer code adds too little redundancy, the performance of the codes in the CPC ensemble concentrates around the ensemble average.

The considerations above find empirical confirmations on the BEC, too. An example is reported in Fig. 5, by assuming codes with the same parameters in the example of Fig. 1. Here, the polar code has been designed for a BEC with erasure probability $\epsilon = 0.3$. The union bound (UB) (1) has been used to estimate the BEP under ML decoding. As for the case of Fig. 1, the codes sampled from the CPC ensemble can be clustered in two sub-ensembles: a first group of (few) bad codes, and a larger group of good codes. The few bad codes dominate the error probability at low erasure probabilities. The bad codes are characterized by $d_{\min} = 4$, while the good codes have $d_{\min} = 8$ (see Table II). The average performance (upper bounded via (1)) of the expurgated CPC ensemble is provided, too: as expected, the expurgated ensemble performance well captures the performance of the good codes in the ensemble.

As one may expect, the omission of an interleaving block (which, in fact, just represents a specific instance of how the outer code constrains are applied to the input of the polar code encoder) does not yield a consisted behavior in the CPC performance.

In the examples of Figs. 1, 2 and 5 the CPC without interleaver provides an excellent performance. This is however not true in general, and in [42], [43] examples are given where the interleaver optimization allows achieving significant gains. One of these examples is shown in Fig. 6. These codes have the same parameters of the scheme of Fig. 4 and the polar code has been designed again fixing $\epsilon = 0.3$. In this case, the scheme without interleaver does not achieve the best performance. A similar behavior can occur even when practical decoders are considered instead of ML decoding. An example is shown in Fig. 7, where the block error rate (BLER) estimated through Monte Carlo simulations of transmission over the AWGN channel with SCL decoding is assumed as a performance metric. The considered code is the CPC obtained
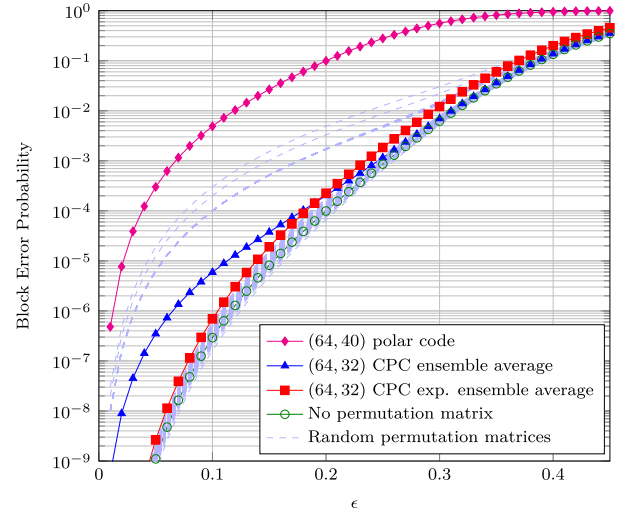


Fig. 5. Upper bounds (1) on the ML performance of CPC (ensembles) with and without random interleavers composed by a $(64, 40)$ polar code and the CRC-$8_1$ code over the BEC. The upper bound (1) on the ML performance of the $(64, 40)$ polar code alone is also reported.

by concatenating a $(64, 48)$ polar code with the CRC-$16_1$ code. The list length used for SCL decoding is $L = 4096$. We observe that the "no permutation matrix" curve is not the best one in this case, as in Fig. 6. Generally, there are cases in which the scheme without interleaver provides good (or even the best) error rate performance and others in which this is not true and the choice of a proper outer code coordinates permutation can provide significant gains.

In the latter cases, one may ask which is the interleaver providing optimal performance. Unfortunately, designing optimal interleavers for CPCs is generally a very hard task, and it is out of the scope of this paper. We refer the interested reader to [43], where a procedure has been introduced that allows accelerating the search of an optimal interleaver for CPCs. Following such a procedure, two interleavers able to achieve $d_{\min} = 10$ were found (out of 20000 randomly generated interleavers[5] for the code parameters considered in Fig. 6), as shown in Table II. Although such an approach accelerates the search of optimal interleavers with respect to a naïve search, it is feasible only for rather short codes.

---

[5]For the sake of readability, in Fig. 6 only 1000 of them have been plotted, including the best and the worst found.
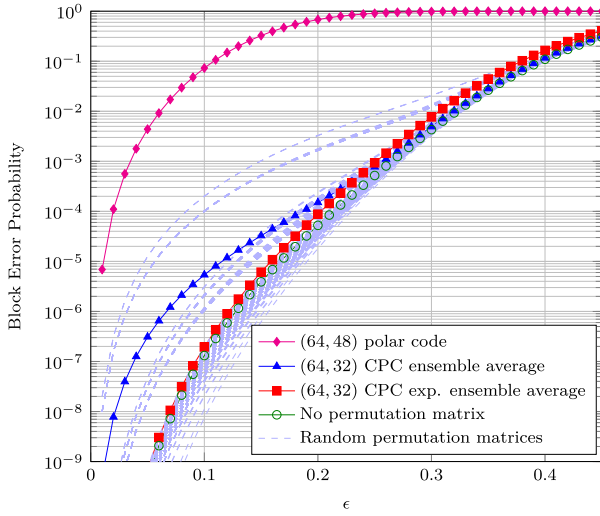
Fig. 6. Upper bounds (1) on the ML performance of CPC (ensembles) with and without random interleavers composed by a $(64, 48)$ polar code and the CRC-$16_1$ code over the BEC. The upper bound (1) on the ML performance of the $(64, 48)$ polar code alone is also reported.



Fig. 8. TSBs on the ML performance of CPC (ensembles) with and without random interleavers composed by a $(128, 112)$ polar code with the CRC-$16_1$ outer code over the AWGN channel. TSB on the performance of the $(128, 112)$ polar code alone is also reported. The polar code is designed at $E_s/N_0 = 3.72$ dB.
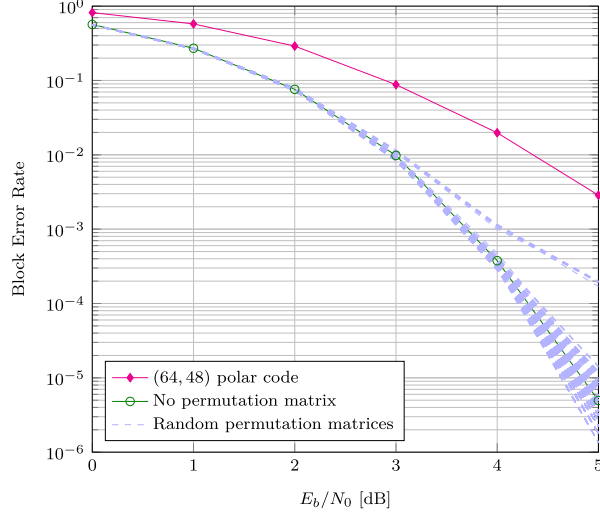


Fig. 7. BLER performance of CPC codes with random interleavers. CPCs obtained by concatenating a $(64, 48)$ polar code with the CRC-$16_1$ code. SCL decoding with list size $L = 4096$. The performance of the $(64, 48)$ polar code alone is also reported. The polar code is designed at $\frac{E_s}{N_0} = 3.25$ dB.



Fig. 9. Upper bounds (1) on the ML performance of CPC (ensembles) with and without random interleavers composed by a $(128, 112)$ polar code and the CRC-$16_1$ code over the BEC. The upper bound (1) on the ML performance of the $(128, 112)$ polar code alone is also reported.

## B. Moderate Block Length Regime

The AWEF analysis of the CPC ensembles becomes quickly intractable when, for a given rate, the CPC block length increases. Hence, in order to study the performance of longer CPCs, we have designed codes with rates $R > 1/2$. The analysis of higher rate codes is simplified by the use of the MacWilliams identity, jointly with an optimized search process presented in the Appendix. Two examples are shown in Figs. 8 and 9, relative to the AWGN channel and the BEC, respectively. Two inner $(128, 112)$ polar codes have been designed by assuming $E_s/N_0 = 3.72$ dB over the AWGN channel and $\epsilon = 0.3$ over the BEC. The outer code is the CRC$-16_1$ code yielding a CPC rate $R = 3/4$. The behavior follows the ones already discussed for shorter CPCs (ensembles). So, similar comments hold and are not repeated, for the sake of brevity. The $d_{\min}$ distributions for these codes,
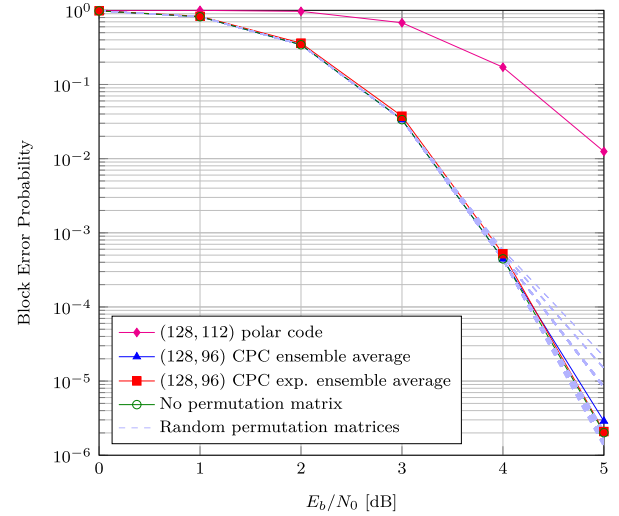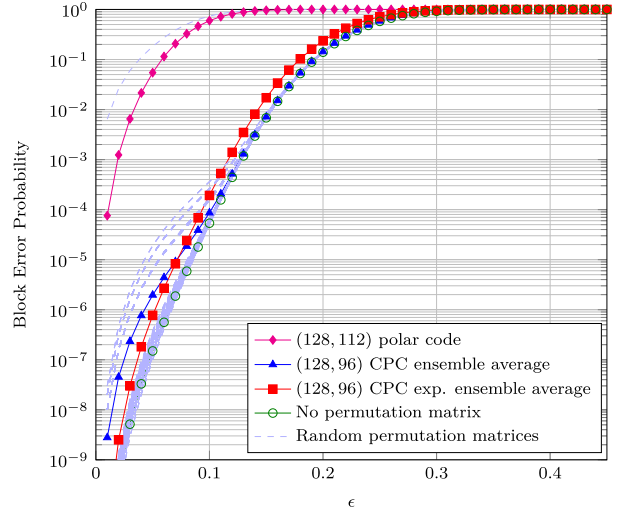
computed over 1000 randomly generated interleavers, are reported in Table II.

For longer block lengths and intermediate rates (i.e., rates that do not allow deriving the inner polar code IOWEFs by either direct enumeration or by enumeration in the dual code domain) we resort to Monte Carlo simulations with SCL decoding.

In Fig. 10 and Fig. 11 we show the BLER performance for $(256, 128)$ CPCs obtained by using as outer codes the CRC-$8_1$ and the CRC-$16_1$ codes, respectively, over the AWGN channel. For each of the 1000 generated interleavers, at least 25 block errors are collected. In both cases, we have restricted the list size of the SCL decoder to $L = 1024$. In the case of the CRC-$8_1$ code, the inner $(256, 136)$ polar code was designed for $E_s/N_0 = 3.25$ dB while in the case of the CRC-$16_1$ the inner $(256, 144)$ polar code was designed for $E_s/N_0 = 5.25$ dB.
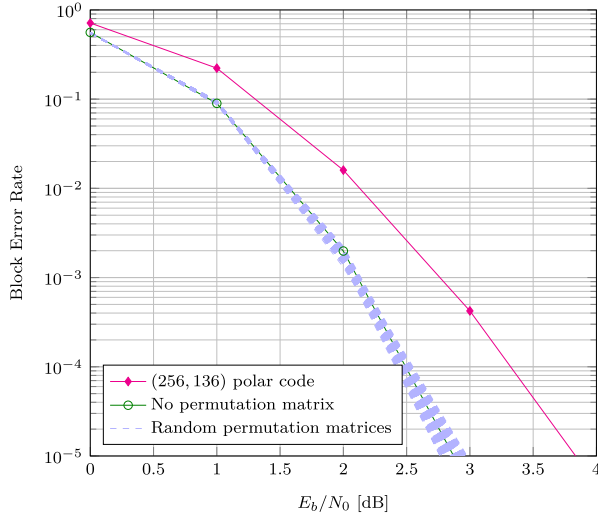
Fig. 10.　BLER performance of CPC codes with random interleavers. CPCs obtained by concatenating a $(256, 136)$ polar code with the CRC-$8_1$ code. SCL decoding with list size $L = 1024$. The performance of the $(256, 136)$ polar code alone is also reported. The polar code is designed at $\frac{E_s}{N_0} = 3.25$ dB.
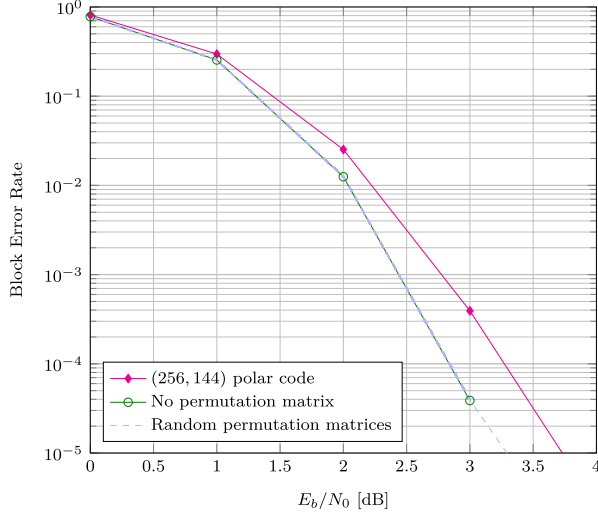


Fig. 11.　BLER performance of CPC codes with random interleavers. CPCs obtained by concatenating a $(256, 144)$ polar code with the CRC-$16_1$ code. SCL decoding with list size $L = 1024$. The performance of the $(256, 144)$ polar code alone is also reported. The polar code is designed at $\frac{E_s}{N_0} = 5.25$ dB.

In both cases, the dispersion of the code performance for the sampled codes within the ensembles is rather limited. This is in accordance with the empirical observation that being the minimum distance of the polar codes rather large ($d_{\min} = 16$ in both cases) the choice of the outer code (interleaver) plays a limited role.

## VI. CONCLUSION

We have provided an analysis of the performance of concatenation of polar codes with outer CRC codes (separated by an interleaver) in the short and moderate block length regimes. The analysis, performed by introducing CPC ensembles, shows that if the inner polar code has a low minimum distance and the outer CRC code has a sufficiently large amount of redundancy,

then the choice of the outer code generator polynomial and of the interleaver may yield to a large variability in the performance of the resulting CPC, pointing to the need of a judicious selection of the outer code and interleaver. The developed analysis provides useful information in view of optimizing the performance of the concatenated scheme. In this respect, another interesting issue, left for future work, concerns the evaluation of the gain achievable against other approaches that do not exploit concatenation, like those based on the selection of parity check frozen symbols.

## APPENDIX

In this appendix, we present a method for reducing the complexity of the exhaustive search of codewords for short CPCs with $R > 1/2$, and demonstrate that it can yield a significant speedup in the computation, thus extending the range of block lengths that can be analyzed through the AWEF approach. We first decompose the polars code generator matrix $\boldsymbol{G}_{\mathsf{I}}$ in (2) in two matrices, $\mathbf{L}$ and $\mathbf{R}$, having dimensions $k_{\mathsf{I}} \times k_{\mathsf{I}}$ and $k_{\mathsf{I}} \times r_{\mathsf{I}}$, respectively, such that $\boldsymbol{G}_{\mathsf{I}} = [\mathbf{L}|\mathbf{R}]$ and $\mathbf{L}$ is non-singular.[6] Then, the polar code generator matrix can be rewritten as

$$\boldsymbol{G}_{\mathsf{I}} = \mathbf{L} \left[ \mathbf{I}_{k_{\mathsf{I}} \times k_{\mathsf{I}}} | \mathbf{L}^{-1}\mathbf{R} \right],$$

where $\mathbf{I}_{k_{\mathsf{I}} \times k_{\mathsf{I}}}$ is the $k_{\mathsf{I}} \times k_{\mathsf{I}}$ identity matrix. The generator matrix of the CPC in (2) can therefore be written as

$$\boldsymbol{G} = \boldsymbol{G}_{\mathsf{o}} \boldsymbol{\Pi} \mathbf{L} \left[ \mathbf{I}_{k_{\mathsf{I}} \times k_{\mathsf{I}}} | \mathbf{L}^{-1}\mathbf{R} \right] = \boldsymbol{G}' \boldsymbol{G}''$$

with

$$\boldsymbol{G}' = \boldsymbol{G}_{\mathsf{o}} \boldsymbol{\Pi} \mathbf{L}$$

and

$$\boldsymbol{G}'' = \left[ \mathbf{I}_{k_{\mathsf{I}} \times k_{\mathsf{I}}} | \mathbf{L}^{-1}\mathbf{R} \right].$$

Let $\mathbf{H}'$ and $\mathbf{H}''$ be two parity-check matrices for the two codes, that is:

i. $\mathbf{H}'$ with size $r_{\mathsf{o}} \times n_{\mathsf{o}}$ such that $\mathbf{H}'\boldsymbol{G}'^T = \mathbf{0}$, where $^T$ denotes matrix transposition and $r_{\mathsf{o}} = n_{\mathsf{o}} - k_{\mathsf{o}}$ is the number of parity-check equations of the outer code.

ii. $\mathbf{H}''$ with size $r_{\mathsf{I}} \times n_{\mathsf{I}}$ such that $\mathbf{H}''\boldsymbol{G}''^T = \mathbf{0}$, where $r_{\mathsf{I}} = n_{\mathsf{I}} - k_{\mathsf{I}}$ is the number of parity-check equations of the inner code.

In particular, we choose

$$\mathbf{H}'' = \left[ \left(\mathbf{L}^{-1}\mathbf{R}\right)^T | \mathbf{I}_{r_{\mathsf{I}} \times r_{\mathsf{I}}} \right].$$

Then a valid parity-check matrix for the CPC is

$$\mathbf{H} = \begin{bmatrix} \mathbf{A} \\ \mathbf{H}'' \end{bmatrix},$$

with $\mathbf{A} = [\mathbf{H}'|\mathbf{0}_{r_{\mathsf{o}} \times r_{\mathsf{I}}}]$ where $\mathbf{0}_{r_{\mathsf{o}} \times r_{\mathsf{I}}}$ denotes the all-zero $r_{\mathsf{o}} \times r_{\mathsf{I}}$ matrix.

The dual code of the CPC has generator matrix $\mathbf{H}$. If we aim at enumerating all its codewords, we can take into account that only $\mathbf{H}'$ is affected by the choice of the permutation matrix $\boldsymbol{\Pi}$.

[6] A permutation of the polar code coordinates may be needed in order to find a non-singular matrix $\mathbf{L}$.

Therefore, in order to reduce the computational burden, we could enumerate codewords by using the following procedure, that needs to be repeated only partially every time that $\mathbf{\Pi}$ is changed:

1) Enumerate the weights of all codewords resulting from linear combinations of the rows of $\mathbf{A}$. The linear space spanned by the rows of $\mathbf{A}$ is denoted by $\mathcal{A}$.
2) Enumerate the weights of all codewords resulting from linear combinations of the rows of $\mathbf{H}''$. The linear space spanned by the rows of $\mathbf{H}''$ is denoted by $\mathcal{B}$.
3) For all $\mathbf{c}_a \in \mathcal{A}/\mathbf{0}$ and for all $\mathbf{c}_b \in \mathcal{B}/\mathbf{0}$, enumerate the weights of all vectors resulting from $\mathbf{c}_a + \mathbf{c}_b$.

When $\mathbf{\Pi}$ is modified, the set $\mathcal{A}$ changes accordingly, while the set $\mathcal{B}$ is unchanged. Therefore, any time $\mathbf{\Pi}$ is changed, step 1) needs to be repeated, while step 2) does not. Step 3) also needs to be repeated, although the set of codewords $\mathbf{c}_b \in \mathcal{B}/\mathbf{0}$ can be reused. Then, by exploiting the MacWilliams identity, the weights spectrum of the original code is derived.

Next, we report an estimate of the complexity reduction introduced by the procedure described above, with respect to a standard exhaustive enumeration of the codeword weights in the dual code.

The generation of the codewords of the dual code has complexity

$$\mathsf{C}_{\text{std}} = 2^{n_{\mathsf{I}}-k_{\mathsf{O}}}(n_{\mathsf{I}} - k_{\mathsf{O}})n_{\mathsf{I}} = 2^r r n_{\mathsf{I}} \qquad (4)$$

having set $r = n_{\mathsf{I}} - k_{\mathsf{O}}$. The complexity of the proposed approach can be divided into the following contributions:

1) *Generation of $\mathcal{A}$.* The generation of all codewords in $\mathcal{A}$ has complexity

$$\mathsf{C}_{\mathsf{O}} = 2^{n_{\mathsf{O}}-k_{\mathsf{O}}}(n_{\mathsf{O}} - k_{\mathsf{O}})n_{\mathsf{O}} = 2^{r_{\mathsf{O}}} r_{\mathsf{O}} n_{\mathsf{O}}$$

2) *Generation of $\mathcal{B}$.* The generation of all codewords in $\mathcal{B}$ has complexity

$$\mathsf{C}_{\mathsf{I}} = 2^{n_{\mathsf{I}}-k_{\mathsf{I}}}(n_{\mathsf{I}} - k_{\mathsf{I}})n_{\mathsf{I}} = 2^{r_{\mathsf{I}}} r_{\mathsf{I}} n_{\mathsf{I}}$$

3) *Linear combinations.* The sum between $\mathbf{c}_a$ and $\mathbf{c}_b$ for all possible pairs has the following cost in terms of complexity

$$\mathsf{C}_{\mathsf{S}} = 2^{n_{\mathsf{I}}-k_{\mathsf{O}}} n_{\mathsf{I}} = 2^r n_{\mathsf{I}}.$$

Note that, for the sake of simplicity, we neglect that the zero vector in $\mathcal{A}$ and $\mathcal{B}$ should not be considered, as this approximation has a negligible impact on the computation.

The complexity of both methods is also affected by the computation of the weight of each codeword. However this term has the same cost in both solutions, thus it can be omitted from the comparison. For the considered codes, the dominant term is due to $\mathsf{C}_{\mathsf{S}}$. Hence, keeping apart the weight computation and neglecting the other two terms, if we compare $\mathsf{C}_{\mathsf{S}}$ with (4), we can conclude that the speedup introduced by the proposed method is in the order of $r$.

## REFERENCES

[1] N. Stolte, "Rekursive codes mit der Plotkin-konstruktion und ihre decodierung," Ph.D. dissertation, TU Darmstadt, Darmstadt, Germany, 2002.

[2] 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, Jul. 2009.

[3] I. Tal and A. Vardy, "List decoding of polar codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2213–2226, May 2015.

[4] E. Arikan, H. Kim, G. Markarian, Ü. Özgür, and E. Poyraz, "Performance of short polar codes under ML decoding," in *Proc. ICT-Mobile Summit Conf.*, Santander, Spain, 2009, pp. 1–6.

[5] P. Trifonov, "Efficient design and decoding of polar codes," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3221–3227, Nov. 2012.

[6] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, 2009.

[7] J. Guo, A. G. I. Fàbregas, and J. Sayir, "Fixed-threshold polar codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Istanbul, Turkey, Jul. 2013, pp. 947–951.

[8] M. Valipour and S. Yousefi, "On probabilistic weight distribution of polar codes," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2120–2123, Nov. 2013.

[9] Z. Liu, K. Chen, K. Niu, and Z. He, "Distance spectrum analysis of polar codes," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, Apr. 2014, pp. 490–495.

[10] B. Li, H. Shen, and D. Tse, "A RM-polar codes," Jul. 2014, *arXiv:1407.5483*. [Online]. Available: https://arxiv.org/abs/1407.5483

[11] M. Bardet, V. Dragoi, A. Otmani, and J.-P. Tillich, "Algebraic properties of polar codes from a new polynomial formalism," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 230–234.

[12] B. Li, H. Shen, and D. Tse, "An adaptive successive cancellation list decoder for polar codes with cyclic redundancy check," *IEEE Commun. Lett.*, vol. 16, no. 12, pp. 2044–2047, Dec. 2012.

[13] K. Niu and K. Chen, "CRC-aided decoding of polar codes," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1668–1671, Oct. 2012.

[14] A. Bhatia *et al.*, "Polar codes for magnetic recording channels," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Jerusalem, Israel, Apr. 2015, pp. 1–5.

[15] D. Wu, Y. Li, X. Guo, and Y. Sun, "Ordered statistic decoding for short polar codes," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1064–1067, Jun. 2016.

[16] G. Liva, L. Gaudio, T. Ninacs, and T. Jerkovits, "Code design for short blocks: A survey," Oct. 2016, *arXiv:1610.00873*. [Online]. Available: https://arxiv.org/abs/1610.00873

[17] *Evaluation of TBCC and Polar Codes for Small Block Lengths*, document 3GPP TSG RAN WG1 N.85, Huawei, 2016.

[18] V. Bioglio, C. Condo, and I. Land, "Design of polar codes in 5G new radio," Apr. 2018, *arXiv:1804.04389*. [Online]. Available: https://arxiv.org/abs/1804.04389

[19] Y. Wang, K. R. Narayanan, and Y.-C. Huang, "Interleaved concatenations of polar codes with BCH and convolutional codes," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 2, pp. 267–277, Feb. 2016.

[20] Y. Wang, W. Zhang, Y. Liu, L. Wang, and Y. Liang, "An improved concatenation scheme of polar codes with Reed–Solomon codes," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 468–471, Mar. 2017.

[21] Q. Zhang, A. Liu, X. Pan, and K. Pan, "CRC code design for list decoding of polar codes," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1229–1232, Jun. 2017.

[22] T. Murata and H. Ochiai, "Performance analysis of CRC codes for systematic and nonsystematic polar codes with list decoding," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 7286909:1–7286909:8, May 2018.

[23] Q. Zhang, A. Liu, and X. Pan, "An enhanced probabilistic computation method for the weight distribution of polar codes," *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 2562–2565, Dec. 2017.

[24] S. Benedetto and G. Montorsi, "Unveiling turbo codes: Some results on parallel concatenated coding schemes," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 409–428, Mar. 1996.

[25] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[26] J. K. Wolf and R. D. Blakeney, "An exact evaluation of the probability of undetected error for certain shortened binary CRC codes," in *Proc. IEEE 21st Mil. Commun. Conf.*, San Diego, CA, USA, vol. 1, Oct. 1988, pp. 287–292.

[27] M. Xu, P. Chen, B. Bai, and S. Tong, "Distance spectrum and optimized design of concatenated polar codes," in *Proc. 9th Int. Conf. Wireless Commun. Signal (WCSP)*, Nanjing, China, Oct. 2017, pp. 1–6.

[28] G. Battail, M. Decouvelaere, and P. Godlewski, "Replication decoding," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 3, pp. 332–345, May 1979.

[29] C. Weiss, C. Bettstetter, and S. Riedel, "Code construction and decoding of parallel concatenated tail-biting codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 366–386, Jan. 2001.

[30] F. Chiaraluce and R. Garello, "Extended Hamming product codes analytical performance evaluation for low error rate applications," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 2353–2361, Nov. 2004.

[31] I. Sason and S. Shamai (Shitz), "Performance analysis of linear codes under maximum-likelihood decoding: A tutorial," *Found. Trends Commun. Inf. Theory*, vol. 3, pp. 1–222, Jul. 2006.

[32] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, Jun. 2002.

[33] G. Liva, E. Paolini, and M. Chiani, "Bounds on the error probability of block codes over the $q$-ary erasure channel," *IEEE Trans. Commun.*, vol. 61, no. 6, pp. 2156–2165, Jun. 2013.

[34] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1284–1292, Jul. 1994.

[35] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.

[36] R. Mori and T. Tanaka, "Performance of polar codes with the construction using density evolution," *IEEE Commun. Lett.*, vol. 13, no. 7, pp. 519–521, Jul. 2009.

[37] S.-Y. Chung, T. J. Richardson, and R. L. Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 657–670, Feb. 2001.

[38] E. Arıkan, "Systematic polar coding," *IEEE Commun. Lett.*, vol. 15, no. 8, pp. 860–862, Aug. 2011.

[39] R. G. Gallager, "Low-density parity-check codes," Ph.D. dissertation, Dept. Elect. Eng., MIT, Cambridge, MA, USA, Jul. 1963.

[40] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for 'turbo-like,' codes," in *Proc. 36th Annu. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, Sep. 1998, pp. 201–210.

[41] H. Vangala, E. Viterbo, and Y. Hong, "A comparative study of polar code constructions for the AWGN channel," Jan. 2015, *arXiv:1501.02473*. [Online]. Available: https://arxiv.org/abs/1501.02473

[42] G. Ricciutelli, M. Baldi, F. Chiaraluce, and G. Liva, "On the error probability of short concatenated polar and cyclic codes with interleaving," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 1858–1862.

[43] G. Ricciutelli, M. Baldi, and F. Chiaraluce, "Interleaver design for short concatenated codes," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1762–1765, Sep. 2018.

**Marco Baldi** received the Laurea degree (Hons.) in electronic engineering and the Ph.D. degree in electronic, computer science and telecommunications engineering from the Polytechnic University of Marche, Ancona, Italy, in 2003 and 2006, respectively. Since 2016, he has been a tenure-track Assistant Professor with the Polytechnic University of Marche. He has co-authored over 150 scientific papers, one book, and three patents. His research is focused on coding and cryptography for information security and reliability. He received the Italian National Scientific Habilitation (ASN) as an Associate Professor of telecommunications engineering in 2017. He was a co-organizer of the 13th International Workshop on Security and High Performance Computing Systems (SHPCS 2018), the First and Second Workshop on Communication Security (WCS 2014 and 2017), and the Seventh Code-Based Cryptography Workshop (CBC 2019). He currently serves as an Associate Editor for IEEE COMMUNICATIONS LETTERS, *EURASIP Journal on Wireless Communications and Networking*, and *Information* (MDPI).



**Franco Chiaraluce** was born in Ancona, Italy, in 1960. He received the Laurea degree *(summa cum laude)* in electronic engineering from the University of Ancona in 1985. Since 1987, he has been with the Department of Electronics and Automatics, University of Ancona. He is currently an Associate Professor with the Polytechnic University of Marche. He is a co-author of about 300 scientific papers and 2 books. His main research interests involve various aspects of communication systems theory and design, with special emphasis on error correcting codes, cryptography, and physical layer security. On these topics, he collaborates with national and international companies. He is also a member of the IEICE.



**Giacomo Ricciutelli** received the Ph.D. degree in electronic engineering from the Università Politecnica delle Marche, Ancona, Italy, in 2018. Until 2018, he was a Research Fellow with the Department of Information Engineering, Università Politecnica delle Marche. During his Ph.D. work, his research topics were focused on error correcting codes for reliability and security purposes. He is currently a Project Leader with Gitronica S.P.A., Montelupone, Italy, where his research topics concern the Internet-of-Things applications and communications among low-power devices.



**Thomas Jerkovits** received the B.Sc. degree in electrical engineering from Ulm University (UUlm), Ulm, Germany, in 2013, and the M.Sc. degree in electrical engineering from the Technical University of Munich (TUM), Munich, Germany, in 2015, where he is currently pursuing the Ph.D. degree with the Institute for Communications Engineering. He is also a member of the Information Transmission Group, German Aerospace Center (DLR).



**Gianluigi Liva** was born in Spilimbergo, Italy, in 1977. He received the M.S. and Ph.D. degrees in electrical engineering from the University of Bologna, Italy, in 2002 and 2006, respectively. Since 2003, he has been investigating channel codes for high-data rate with the Consultative Committee for Space Data Systems (CCSDS) missions. From 2004 to 2005, he was involved in research at the University of Arizona, Tucson, where he was involved in designing low-complexity error correcting codes for space communications. Since 2006, he has been with the Institute of Communications and Navigation, German Aerospace Center (DLR), where he currently leads the Information Transmission Group. In 2010, he was appointed as a Lecturer of channel coding with the Institute for Communications Engineering (LNT), Technical University of Munich (TUM). From 2012 to 2013, he was a Lecturer of channel coding with the Nanjing University of Science and Technology, China. Since 2014, he has been a Lecturer of channel codes with iterative decoding with LNT, TUM. His main research interests include satellite communications, random access techniques, and error control coding. He has been active in the DVB-SH, DVB-RCS, and DVB-S2 standardization groups and in the standardization of error correcting codes for deep-space communications within CCSDS. He received the Italian National Scientific Habilitation (ASN) as a Full Professor of telecommunication engineering in 2017. He received the 2007 IST Mobile and Wireless Communication Summit Best Paper Award. He was the Co-Chair of the First DLR Workshop on Random Access and Coding in 2013, the 2014 Sino-German Workshop on Bridging Theory and Practice in Wireless Communications and Networking, Shenzhen, China, the IEEE ICC 2014 Workshop on Massive Uncoordinated Access Protocols, Sydney, Australia, the 2015 Munich Workshop on Coding and Modulation, and the 2018 IEEE European School on Information Theory.