

Efficient Error-Correcting Codes in the Short Blocklength Regime

Mustafa Cemil Coşkun^{a,c}, Giuseppe Durisi^b, Thomas Jerkovits^a, Gianluigi Liva^a, William Ryan^d, Brian Stein^d, Fabian Steiner^c

^a*Institute of Communications and Navigation of the German Aerospace Center (DLR),
Münchner Strasse 20, 82234 Weßling, Germany. Email:*

{mustafa.coskun, thomas.jerkovits, gianluigi.liva}@dlr.de.

^b*Department of Electrical Engineering, Chalmers University of Technology, Gothenburg,
Sweden. Email: durisi@chalmers.se.*

^c*Institute of Communication Engineering of the Technical University of Munich (TUM),
Theresienstrasse 90, 80333 Munich, Germany. Email: fabian.steiner@tum.de.*

^d*Zeta Associates Inc., 10302 Eaton Place, Suite 500 Fairfax, VA 22030.*

Abstract

The design of block codes for short information blocks (e.g., a thousand or less information bits) is an open research problem that is gaining relevance thanks to emerging applications in wireless communication networks. In this paper, we review some of the most promising code constructions targeting the short block regime, and we compare them with both finite-length performance bounds and classical error-correction coding schemes. The work addresses the use of both binary and high-order modulations over the additive white Gaussian noise channel. We will illustrate how to effectively approach the theoretical bounds with various performance versus decoding complexity tradeoffs.

Keywords: Short packets, error-correcting codes, finite-length performance bounds, coded modulation.

1. Introduction

During the past sixty years, a formidable effort has been focused on the research of capacity-approaching error correcting codes [1]. Initially, the attention was directed to short and medium-length linear block codes [2] (with some notable exceptions, see, e.g., [3; 4]), mainly for complexity reasons. As

the idea of code concatenation [5] became established in the coding community [6], the design of long channel codes became a viable solution to approach the channel capacity. The effort resulted in a number of practical code constructions allowing reliable transmission at fractions of a decibel from the Shannon limit [7–16] with low-complexity (sub-optimum) decoding.

The interest in short and medium blocklength codes (i.e., codes with dimension k in the range of 50 to 1000 bits) has been rising again recently, mainly due to emerging applications that require the transmission of short data units. Examples of such applications are machine-type communications, smartmetering networks, the Internet of things, remote command links and messaging services (see, e.g., [17–20]). Due to these new emerging applications, renewed interest has been placed not only in the design of efficient short codes, but also in the development of tight bounds on the performance attainable by the best error correcting schemes, for a given blocklength and rate [21–24]. Tight bounds are now available as benchmarks not only for the unfaded additive white Gaussian noise (AWGN) case but also for fading channels [25; 26].

When the design of short iteratively-decodable codes is attempted, it turns out that some classical code construction tools that have been developed for turbo-like codes tend to fail to provide codes with acceptable performance. This is the case, for instance, for density evolution [27] and extrinsic information transfer (EXIT) charts [28], which are well-established techniques to design powerful long low-density parity-check (LDPC) and turbo codes. The reason is the asymptotic (in blocklength) nature of density evolution and EXIT analysis, which fail to model accurately the iterative decoder in the short blocklength regime. However, competitive LDPC and turbo code designs for moderate length and small blocks have been proposed, mostly based on heuristic construction techniques [29–50]. While iterative codes retain a large appeal due to their low decoding complexity, more sophisticated decoding algorithms [51–57] are feasible for short blocks leading to solutions that are competitive with (if not superior to) iterative decoding of short turbo and LDPC codes.

In this paper, we review some fundamental results on the performance achievable by codes in the short blocklength regime. This will allow us to lay the ground for a proper performance comparison among various codes and decoding algorithms. The comparison will be provided for the (unfaded) AWGN channel case with both binary modulation and high-order modulations. In the former case, the goal is to compare pure code performance,

whereas in the latter case we shall see how different coding schemes can be efficiently coupled with high-order modulations, with and without shaping. The performance comparison will be provided in terms of block error rate, also referred to as codeword error rate (CER), versus signal-to-noise ratio (SNR) with SNR given either by the E_b/N_0 ratio (here, E_b is the energy per information bit and N_0 the single-sided noise power spectral density) or by the E_s/N_0 ratio (with E_s being the energy per modulation symbol).

The remaining part of the paper is organized as follows. Section 2 reviews the fundamental limits for channel coding in the short blocklength regime. Some powerful classical short codes as well as efficient decoding algorithms are discussed in Section 3. Modern code constructions tailored to the transmission of short blocks are presented in Section 4. A comparison of various schemes is provided in Section 5. Conclusions follow in Section 6.

2. Finite-Length Performance Limits

In the following sections of the paper, with the exception of Section 5.3, we will focus on the problem of how to optimally transmit k bits of information using the discrete-time memoryless binary-input additive white Gaussian noise (bi-AWGN) channel n times

$$y_\ell = \sqrt{\rho}x_\ell + w_\ell, \quad \ell = 1, \dots, n. \quad (1)$$

Here, $\{w_\ell\}_{\ell=1}^n$, denotes a sequence of independent and identically distributed samples of the AWGN process. We shall assume that these samples are real-valued Gaussian random variables with zero mean and unit variance. Each of the input symbols $\{x_\ell\}_{\ell=1}^n$ belongs to the binary set $\{-1, 1\}$. The constant ρ models the transmit power and, hence, the SNR, since the noise has unit variance. Finally, $\{y_\ell\}_{\ell=1}^n$ is the sequence of received symbols.

To convey the k information bits, we use a (n, k) coding scheme, which consists of: i) An encoder that maps the k -bit message $J \in \{1, \dots, 2^k\}$ into one out of 2^k n -dimensional codewords with elements in $\{-1, 1\}$. We shall refer to the set of codewords together with the encoder as an (n, k) code and to n as the blocklength of the code. ii) A decoder that maps the n received symbols corresponding to the transmitted message J into an estimated k -bit message \hat{J} .

The message (codeword) error probability of a given (n, k) -coding scheme, which we denote by ϵ , is

$$\epsilon = \mathbb{P}[\hat{J} \neq J]. \quad (2)$$

We stress that different decoders may be applied to a given (n, k) code, yielding different error probabilities.

The rate R of an (n, k) code is $R = k/n$. We also let $\epsilon^*(R, n)$ be the minimum error probability for which one can find a coding scheme with blocklength n and rate R . This quantity describes the fundamental tradeoff between blocklength n , rate R , and error probability ϵ in the transmission of information. Unfortunately, determining $\epsilon^*(R, n)$ exactly is a daunting task. Indeed, computing $\epsilon^*(R, n)$ for the bi-AWGN channel (1) involves an exhaustive search over $\binom{2^n}{2^{nR}}$ codes, which is infeasible for values of R and n of practical interest.

However, the asymptotic behavior of $\epsilon^*(R, n)$ in the limit $n \rightarrow \infty$ for fixed R is well understood—a result known as Shannon’s coding theorem [1]. Specifically, $\epsilon^*(R, n)$ vanishes in the limit $n \rightarrow \infty$ for all rates R below the so-called channel capacity C [1], whereas $\epsilon^*(R, n) \rightarrow 1$ as $n \rightarrow \infty$ for all rates R above C . In other words, the sequence of functions $f_n(R) = \epsilon^*(R, n)$ converges to a step function centered at C in the limit $n \rightarrow \infty$.

For the bi-AWGN channel (1), the capacity C (measured throughout the paper in bits per channel use) is given by

$$C = \frac{1}{\sqrt{2\pi}} \int e^{-z^2/2} \left(1 - \log_2(1 + e^{-2\rho+2z\sqrt{\rho}})\right) dz. \quad (3)$$

The achievability part of Shannon’s coding theorem relies on a random coding argument and does not suggest practical capacity-approaching coding schemes. However, several advances in the coding community over the last sixty years have resulted in several low-complexity coding schemes that approach capacity (see e.g., [27; 58]).

In this paper, we are concerned with the less studied problem of how to approach $\epsilon^*(R, n)$ when the blocklength n is short. For the problem to be well posed, we need ways to estimate $\epsilon^*(R, n)$ accurately. Characterizing $\epsilon^*(R, n)$ for a fixed blocklength n is a classic problem in information theory, and many nonasymptotic upper (achievability) bounds and lower (converse) bounds are available for the bi-AWGN channel (1), such as Gallager’s random coding bound (RCB) [59], and Shannon’s sphere-packing bounds ‘59 (SPB59) [60] and ‘67 (SPB67) [61; 62]. Also, many nonasymptotic results are available on the error probability achievable using linear block codes and maximum likelihood (ML) decoding (see [23] and reference therein).

Over the last ten years, a renewed interest in the performance of communication systems operating in the short-blocklength regime, has resulted in

a significant improvement in the tightness of the best available achievability and converse bounds for many communication channels of practical interest, including the well-studied bi-AWGN channel (1).

To showcase such improvements, we will focus in this paper on two specific classes of bounds, namely converse bounds based on the so called metaconverse (MC) theorem [24, Thm. 26], and achievability bounds based on the random coding union (RCU) bound [24, Thm. 16].

The MC theorem provides a general framework that allows one to recover all previously known converse bounds on $\epsilon^*(R, n)$ (hence, its name). The theorem exploits the existence of a fundamental relation between the problem of determining the error probability of a given code under ML decoding and binary-hypothesis testing [63]. The resulting converse bound is parametric in an auxiliary output distribution (i.e., a marginal distribution on the output vector $[y_1, \dots, y_n]$), which, if chosen suitably, results in a remarkably tight bound that admits an efficient numerical implementation by using the saddlepoint approximation [64].

Similar to Gallager's RCB, the RCU bound relies on the analysis of the performance of a random coding ensemble under ML decoding. As indicated by its name, a crucial step to obtain the RCU is a judicious use of the union bound. An attractive feature of this bound, is that it generalizes naturally to mismatched decoding metrics [65; 66], which enables its use in practically relevant scenarios, such as pilot-assisted transmission over fading channels [67]. Similarly to the MC bound, the use of a saddlepoint approximation allows one to evaluate numerically the RCU bound for the bi-AWGN channel (1) in an efficient way [68].

By characterizing both MC and RCU bounds in the asymptotic limit $n \rightarrow \infty$ for a fixed R , one obtains a more precise characterization of the behavior of $\epsilon^*(R, n)$ for large n than the step-function approximation obtained via Shannon's capacity. Specifically, one can show that for the bi-AWGN channel (1),

$$\epsilon^*(R, n) = Q\left(\frac{n(C - R) + (1/2) \log_2(n) + O(1)}{\sqrt{nV}}\right) \quad (4)$$

where C is the channel capacity given in (1), V is the so-called channel dispersion

$$V = \frac{1}{\sqrt{2\pi}} \int e^{-z^2/2} \left(1 - \log_2(1 + e^{-2\rho + 2z\sqrt{\rho}}) - C\right)^2 dz \quad (5)$$

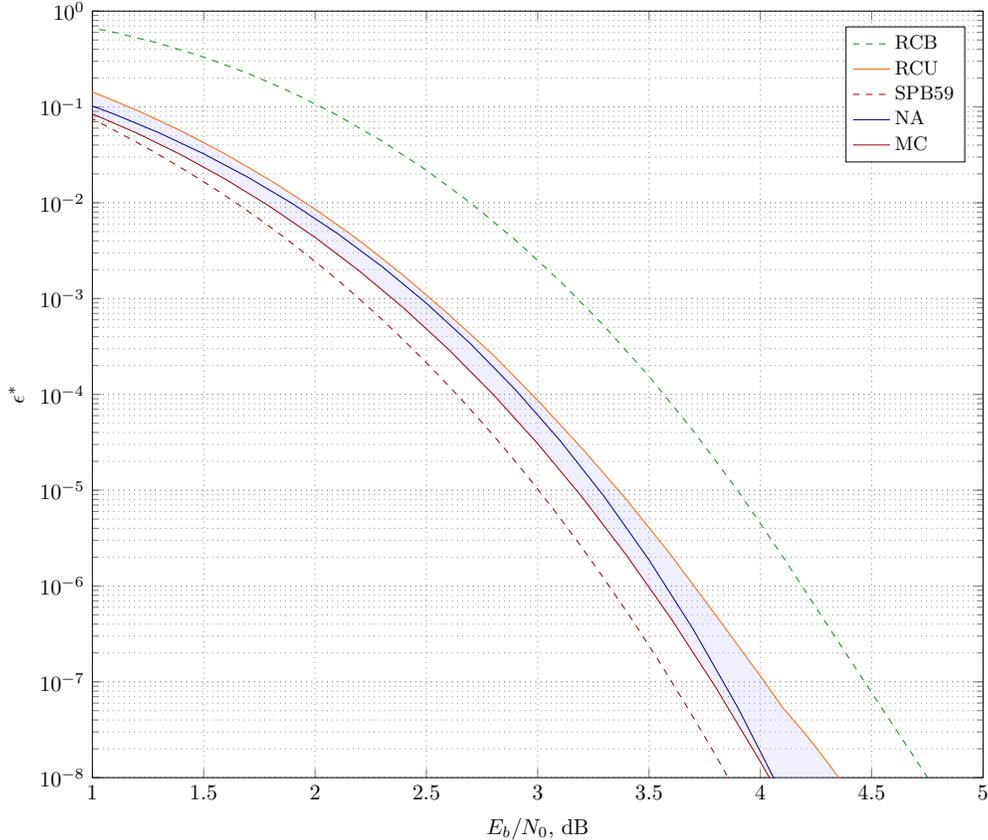


Figure 1: Bounds on the minimum codeword error probability $\epsilon^*(R, n)$ vs. E_b/N_0 for the case $n = 128$ and $k = 64$.

$Q(\cdot)$ is the Gaussian Q function and $O(1)$ comprises terms that can be upper-bounded by a constant for all sufficiently large n . The approximation on $\epsilon^*(R, n)$ obtained by neglecting the $O(1)$ term in (4) is usually referred to as normal approximation (NA).

We now illustrate the tightness of the MC bound, of the RCU bound, and of the NA through some numerical examples. In Fig. 1, we plot the MC computed using the exponent-achieving auxiliary output distribution given in [64, Eq. (28)], the RCU, and the NA for the case $n = 128$ and $k = 64$ (hence, $R = 1/2$). Here, and throughout the paper, the bounds on $\epsilon^*(R, n)$ given by the MC and the RCU are plotted as a function of the energy per

information bit

$$\frac{E_b}{N_0} = \frac{\rho}{2R}. \quad (6)$$

For comparison we also illustrate the SPB59 (which, for the parameters chosen in the figure, is tighter than the adaptation of the SPB67 bound given in [62]) and Gallager’s RCB. As one sees from the figure, the MC and the RCU bounds delimit tightly the $\epsilon^*(R, n)$ that is achievable for the chosen blocklength and information payload for a large range of E_b/N_0 values. For example, the two bounds predict that the minimum energy per bit to operate at a CER of 10^{-6} is between 3.5 dB and 3.7 dB. The SPB59 and the RCB are looser and give the wider range 3.3 dB and 4.2 dB. Note also that the NA provides an accurate estimate of the minimum codeword error probability, which lies between the MC and the RCU bounds. As we shall see, this is not a general phenomenon and one can find practically relevant scenarios for which the NA ceases to be as accurate.

In Figure 2, we plot the MC, the RCU, and the NA for $R = 1/2$ and $n \in \{128, 256, 512, 1024\}$. As the blocklength increases, the gap between MC and RCU diminishes. Also Figure 2 allows one to estimate the speed at which $\epsilon^*(R, n)$ converges to a step function centered at $E_b/N_0 = 0.189$ dB, which is the minimum E_b/N_0 required to communicate at a rate $C = 1/2$ in the asymptotic limit $n \rightarrow \infty$. The gap to the asymptotic limit for $n = 1024$ is about 1.4 dB at a CER of 10^{-6} . The NA is accurate in all the scenarios considered in the figure.

Finally, in Figure 3 we plot $\epsilon^*(R, n)$ as a function of the rate R for a fixed SNR $\rho = 0.189$ dB, i.e., the SNR value for which capacity is $1/2$, and for $n \in \{128, 256, 512, 1024\}$. As in the previous figure, the bounds become increasingly tight as n grows. One can also see that the NA loses accuracy when one operates at small error probability and small R —a relevant scenario for ultra-reliable low-latency communications.

3. Classical Short Codes

In this section, we will review a few approaches for efficient transmission at short blocklengths which rely on (or can be applied to) classical error-correcting code families. The first approach is based on a general decoding algorithm called ordered statistics decoding (OSD) [51] that can be applied to any (binary) linear block code. As we shall see, OSD delivers near-ML performance for short codes with manageable complexity. However, OSD

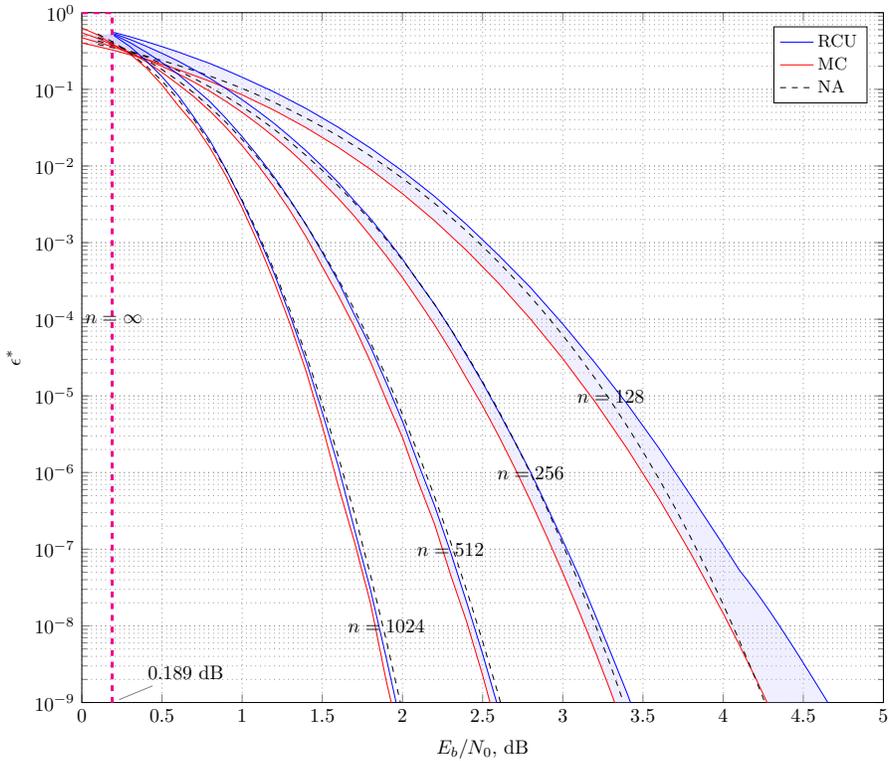


Figure 2: Bounds on the codeword error probability vs. E_b/N_0 for the case $R = 1/2$ and $n \in \{128, 256, 512, 1024\}$. Note that $E_b/N_0 = 0.189$ dB is the minimum E_b/N_0 required to transmit reliably at rate $R = 1/2$ in the limit $n \rightarrow \infty$.

becomes unfeasible when the blocklength increases. The second approach relies on tailbiting (TB) convolutional codes (CCs) and an efficient near-ML decoding algorithm based on the recursive application of Viterbi decoding to the TB trellis of the code.

3.1. Short Algebraic Codes under Ordered Statistics Decoding

Consider an (n, k) binary linear block code \mathcal{C} . Under ML decoding, the decision is given by

$$\hat{\mathbf{x}} = \arg \max_{\mathbf{x} \in \mathcal{C}} p(\mathbf{y}|\mathbf{x}) \quad (7)$$

with $p(\mathbf{y}|\mathbf{x}) = \prod_{\ell=1}^n p(y_\ell|x_\ell)$ being the channel transition probability (we assume the channel to be an arbitrary binary-input memoryless channel). The

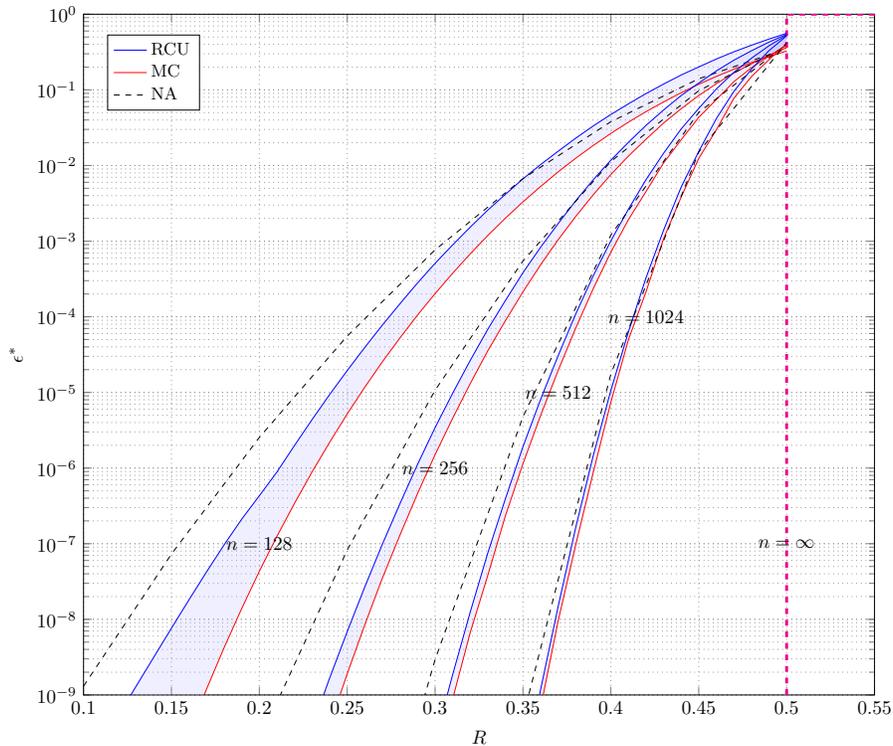


Figure 3: Bounds on the codeword error probability vs. rate for the case $\rho = 0.189$ dB and $n \in \{128, 256, 512, 1024\}$. Note that $R = 1/2$ is the channel capacity.

evaluation of (7) involves a number of computations that grow exponentially in k , unless the code exhibits some structure that enables an efficient implementation of the ML search. OSD reduces the decoding complexity by limiting the search to a subset of the codewords, i.e., to a list $\mathcal{L} \subset \mathcal{C}$. Hence, decoding reduces to

$$\hat{\mathbf{x}} = \arg \max_{\mathbf{x} \in \mathcal{L}} p(\mathbf{y}|\mathbf{x}). \quad (8)$$

The decoding complexity is directly related to the list size. OSD uses a particularly effective approach for the list construction, which is based on ranking the symbol-wise channel observations in decreasing order of reliability [51; 69]. The received vector \mathbf{y} is permuted accordingly, yielding a vector \mathbf{y}' whose first k components are the most reliable channel observations. The columns of the code generator matrix \mathbf{G} are permuted accordingly. The

permuted generator matrix \mathbf{G}' is then put in systematic form.¹ The first k observations in \mathbf{y}' are used to obtain (via bit-by-bit hard detection) a k bit vector \mathbf{u}' . All error patterns of Hamming weight up to t (where t is a parameter of the OSD algorithm) are then added to \mathbf{u}' , generating a set of vectors of cardinality $\sum_{i=0}^t \binom{k}{i}$. Each vector is then encoded via the systematic form of \mathbf{G}' , yielding the list \mathcal{L} . Typically, the OSD parameter t is kept small because the list size grows quickly with t . OSD relies on the idea that, if one takes a hard decision on the most reliable channel observations, only few errors are typically observed, whereas the majority of the errors introduced by the channel are typically associated with the least reliable channel outputs.

OSD works remarkably well with short codes, enabling near-ML decoding for small values of the parameter t . However, as the blocklength grows, t must be increased to keep the decoder performance close to optimal. For example, while for the (24,12) Golay code choosing $t = 2$ is enough to approach the ML decoding limit, for a (128,64) extended Bose-Chaudhuri-Hocquenghem (BCH) code one needs to set t as large as 4. Figure 4 shows the performance in terms of CER vs. E_b/N_0 for a (128,64) extended BCH code with $t = 3$ and $t = 4$ on the bi-AWGN channel. For the case of $t = 4$, the performance is within 0.1 dB from the NA at $\text{CER} \approx 10^{-4}$. With $t = 3$ the gap increases to ≈ 0.5 dB.

OSD does not require any specific code property (besides linearity). However, some knowledge of the code distance spectrum can be used to simplify the decoder by introducing an early stopping criterion. Consider the example of the transmission over the bi-AWGN channel. Assuming that the coded bits are mapped to symbols in the set $\{-1, +1\}$, the minimum Euclidean distance between modulated codewords is $2\sqrt{d_{\min}}$ where d_{\min} is the code minimum Hamming distance. It follows that the list construction can be halted if a codeword at a Euclidean distance less than $\delta = \sqrt{d_{\min}}$ from the channel observation is generated. This simple trick yields remarkable savings on the average list size at moderate-large SNRs [51]. Another simple approach to limit the complexity of OSD consists of applying OSD only if decoding with a lower-complexity algorithm has failed. The idea was explored, for instance, in [70; 71] in the context of iterative decoding of LDPC

¹This may require additional column permutations, which shall be applied to \mathbf{y}' too; this step is required if the k leftmost columns of \mathbf{G}' are not linearly independent. The additional permutations aim at having in the first k positions of \mathbf{y}' the most reliable information set.

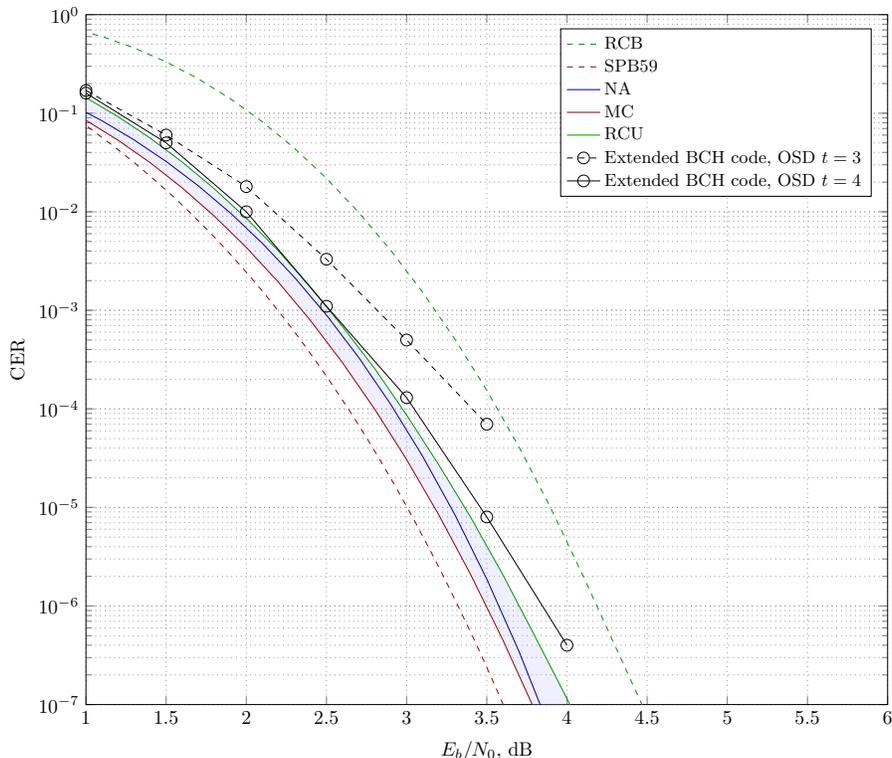


Figure 4: Codeword error rate vs. E_b/N_0 for $(128, 64)$ extended BCH code under OSD with $t = 3$ and $t = 4$, bi-AWGN channel.

codes. Here, the OSD can either intervene if the belief propagation (BP) decoder fails to converge to a valid codeword, or it can be even integrated within the iterative decoding algorithm by exploiting updated reliability estimates computed by the BP decoder. A number of additional improvements on the efficiency of OSD algorithms were further proposed during the past two decades (see, e.g., [52; 55] and the references therein).

3.2. Tailbiting Convolutional Codes

Short codes based on (compact) TB trellises have been the subject of thorough studies from both a theoretical and a practical viewpoint [72–76]. In particular, in [74; 75] TB CCs with excellent distance properties were proposed for various encoder memories, code rates, and blocklengths. The TB

structure of the trellis hinders the adoption of the standard Viterbi decoder. In fact, ML decoding of a TB CC may be naively achieved by starting M Viterbi decoders in parallel, where M is the number of states in a trellis section. Each Viterbi decoder will have a different assumption on the starting state (that shall coincide with the final state due to the TB constraint). The paths selected by the M Viterbi decoders can be then used to form a list, within which lies the codeword that maximizes the likelihood $p(\mathbf{y}|\mathbf{x})$. This solution may become expensive from a computation viewpoint already for moderate-size encoder memories. A simple alternative to this approach is given by the wrap-around Viterbi algorithm (WAVA) [77]. The WAVA is based on the recursive application of the Viterbi algorithm. In particular, one round of the Viterbi algorithm is applied to the TB trellis at each iteration, using the final state probabilities computed in the past iteration as initial state probabilities, with the first round assuming the initial states to be equally likely. At the end of each iteration, the decoder checks if the selected path starts and ends in the same state (hence, fulfilling the TB constraint). If the check is satisfied, then the decoder is stopped and the selected path is declared as final decision. Otherwise, another iteration of the Viterbi algorithm is performed. The process can be iterated for some preset maximum number of times. It turns out that, for many TB CCs, four iterations are sufficient to attain near-ML performance.

Figure 5 shows the performance in terms of CER vs. E_b/N_0 of (128, 64) binary TBCCs with different memory m and polynomials as specified in Table 1. For the case of $m = 14$ the performance is within 0.07 dB from the NA at CER $\approx 10^{-4}$. This results show that TBCCs work very well for short blocks. Unfortunately, as we will see in Section 5, the memory must be increased as the blocklength grows in order to approach the finite-length bounds, rendering the scheme less practical.²

3.3. CRC/TBCC Concatenation

An alternative is the concatenation of CRC error-detection code with a punctured tailbiting convolutional code. Because the addition of the CRC

²For large memory, sequential decoding algorithms may be considered to reduce the decoding complexity. We refer the reader to [76] for a thorough presentation of sequential decoders, including the advanced a bidirectional efficient algorithm for searching trees (BEAST) algorithm of [78].

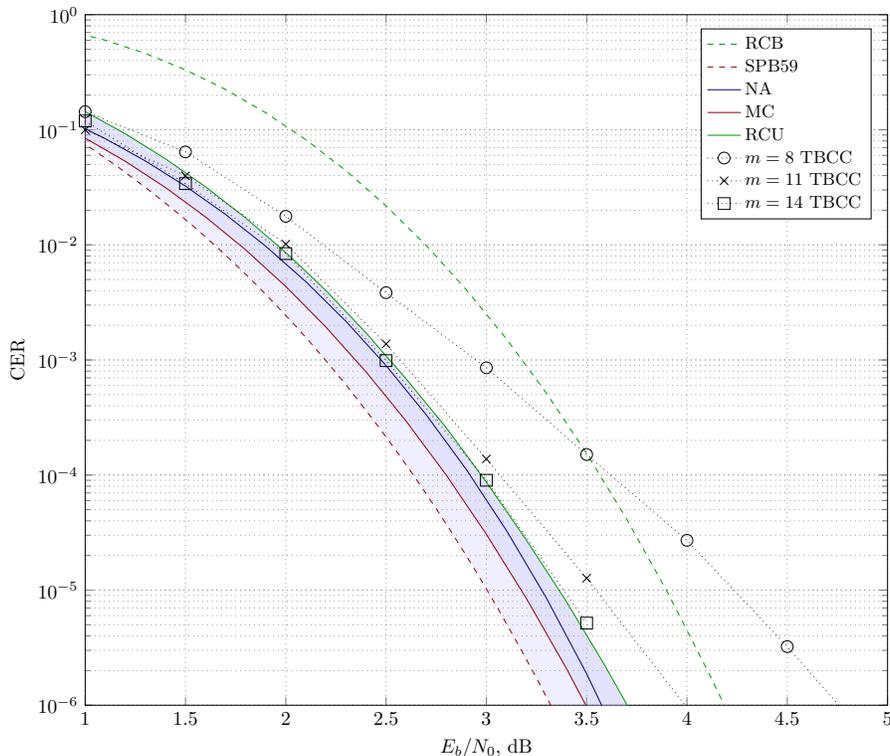


Figure 5: Codeword error rate vs. E_b/N_0 for (128, 64) binary TBCCs with different memory m , bi-AWGN channel.

code substantially increases coding overhead for short blocklengths, puncturing of the TBCC can be used to reduce the overhead back to the original level. Further, it is possible to jointly decode the CRC and TBCC codes so that the concatenated code error-correction performance and error-detection performance are both superior to that of the TBCC operating on its own.

One algorithm for decoding the cyclic redundancy check (CRC)/TB CC concatenation is the list Viterbi algorithm (LVA) [79]. The LVA would keep a list of the best paths to the termination node and choose the one that passed the CRC check. Of course, since the CC is a TB code, the algorithm would have to be a list version of the WAVA algorithm.

One may consider the concatenation of a CRC code with generator $g(x)$ and a CC with generators $[g_1(x) \ g_2(x)]$ to be a catastrophic CC (or encoder)

with generators $[g(x)g_1(x) \ g(x)g_2(x)]$. In principle then, because the encoding will be terminated, one may decode the CRC/TB CC combination with a WAVA. Of course, there will be a large number of states, making the decoder very complex. Even if the application allowed such a large complexity, this approach gives up the ability to reliably detect errors at the decoder output.

An algorithm that nicely trades off the error-correction and error-detection capabilities of the CRC/TB CC will now be presented.³ To simplify the presentation, we start with the assumption that there is a soft-input soft-output (SISO) trellis decoder for the TB CC that has full knowledge of the starting and ending state of the TB CC encoder. We provide Algorithm 1 with the necessary definitions given below:

- weak position \triangleq unreliable position, bit position whose log-likelihood ratio (LLR) has small magnitude
- $w \triangleq$ current number of weak positions under test; hypothesized extrinsic information will be placed in these positions
- $p \triangleq$ current w -bit pattern being tested in w weak positions
- $MaxWeak \triangleq$ maximum value of w (Typically, $3 \leq MaxWeak \leq 10$.)
- $\text{int mask}[MaxWeak + 1] \triangleq \{1, 2^1 - 1, 2^2 - 1, 2^3 - 1, \dots, 2^{MaxWeak} - 1\}$
- strong 1 \triangleq large positive value (e.g., 100.0) used for extrinsic information
- strong 0 \triangleq large negative value (e.g., -100.0) used for extrinsic information
- $\text{weakposn}[w][p] \triangleq$ weakest position found after decoding with candidate (or hypothesized) w -bit pattern p as strong 0's and 1's placed in the w weak positions via extrinsic information
- $p_0(b_0) \triangleq$ value of bit b_0 in binary representation of integer p_0 (least significant bit is bit 0)
- $\text{strong } p_0(b_0) \triangleq$ strong 1 if $p_0(b_0) = 1$, strong 0 if $p_0(b_0) = 0$

³To our knowledge, this algorithm has not been previously presented in the literature.

Algorithm 1 High-level description of the decoding algorithm

```
1: for  $w = 0, \dots, MaxWeak$  do
2:   for  $p = 0, \dots, 2^w - 1$  do
3:     if  $w > 0$  then
4:       Set extrinsic information (see Algorithm 3)
5:     end if
6:     SISO decode (see Algorithm 2)
7:     if CRC fails (i.e., syndrome  $\neq 0$ ) then
8:       weakposn[ $w$ ][ $p$ ] = weakest LLR position
9:     else
10:      break
11:    end if
12:  end for
13:  if syndrome == 0 then
14:    break
15:  end if
16: end for
```

Algorithm 2 SISO Decode Step

```
1: Apply the SISO decoder, utilizing any extrinsic information provided, to
   the channel output word to provide LLRs for the TB CC encoder's input
2: if the decoder output passes the CRC check then
3:   Decoding is complete
4: else
5:   Note CRC failure
6: end if
```

Algorithm 3 Set Extrinsic Information Step (for w -bit pattern p in w weak positions)

```
1: for  $b_0 = 0, \dots, w - 1$  do
2:    $p_0 = p \& \text{mask}[b_0]$ 
3:   extrinsic[weakposn[ $n_0$ ][ $p_0$ ]] = strong  $p_0(n_0)$ 
4: end for
```

Note that the decoder uses no extrinsic information the first time through the outer for loop, after which the weakest LLR position is found (if CRC fails). The second time through the outer loop, strong 0 and then strong 1 extrinsic values are tested in the weakest position. The strong 1 is attempted only if the CRC fails when strong 0 is tested. New weakest positions are found after each strong value is attempted. The third time through the loop, two-bit patterns of strong 0's and strong 1's are attempted, each time checking the CRC and finding the newest weakest position if the CRC fails. The algorithm continues until there is a passed CRC event or the outer loop completes.

It should be clear from the algorithm that the larger the value of $MaxWeak$, the better the error-correction performance and the worse the error-detection performance. Note also, at low SNR values, there can be up to $2^{MaxWeak+1}$ SISO decodings—quite a large number. However, most applications with short blocklengths do not require decoding at high speeds. Also, as we shall see, the error-correction performance of this algorithm can be very good and it can be easily traded off with error-detection performance by decreasing $MaxWeak$.

The CRC code we consider has generator polynomial $g(x) = x^{16} + x^{12} + x^5 + 1$. The TB CC we consider has generator polynomials $[g_1 \ g_2] = [5537, 6131]_{oct}$. With 64 input bits, the natural parameters for this CRC/TB CC are $(n, k) = (160, 64)$. Consequently, to attain a $(128, 64)$ code, we puncture every fifth bit of the encoder output, starting with the third bit.

The SISO decoder employs the Bahl-Cocke-Jelinek-Raviv (BCJR) algorithm. We consider two situations: (1) the TB CC encoder's starting and ending state is unknown to the SISO decoder and (2) the starting and ending state is known to the SISO decoder. For the first case, we use a WAVA-like approach in the BCJR decoder. We justify the second case by arguing that, in many applications, a packet number or an identification number is expected. Such a number can be moved to the end of the TB CC encoder input word so that the encoder starting and ending state is known.

Figure 6 plots the performance of the CRC/TB CC under consideration on the bi-AWGN channel for the unknown-state and known-state cases. Decoder parameter $MaxWeak$ was set to 10. As seen in the figure, the unknown-state case is superior to the turbo and LDPC codes in Figure 5. Although it is unfair to compare the known-state case to the bounds, we see that the known-state CER curve is about 0.1 dB to the right of the SPB59 curve.

As for error-detection performance, we first define $P_{ud|e}$ to be the probability that an error at the decoder output is undetected by the decoder. For the simulation curves in the figure for which $MaxWeak = 10$, we measured $P_{ud|e}$ to be just under 0.1 for both cases. With $MaxWeak = 4$, we measured $P_{ud|e}$ to be less than 0.001 for both cases. For $MaxWeak = 4$, the known-state CER curve moves rightward about 0.4 dB and the unknown-state CER curve moves rightward about 0.7 dB.

We point out that the CRC and TB CC polynomials we chose were “off the shelf” and it might be possible to design an improved CRC code for a specific TB CC using the techniques in [80].

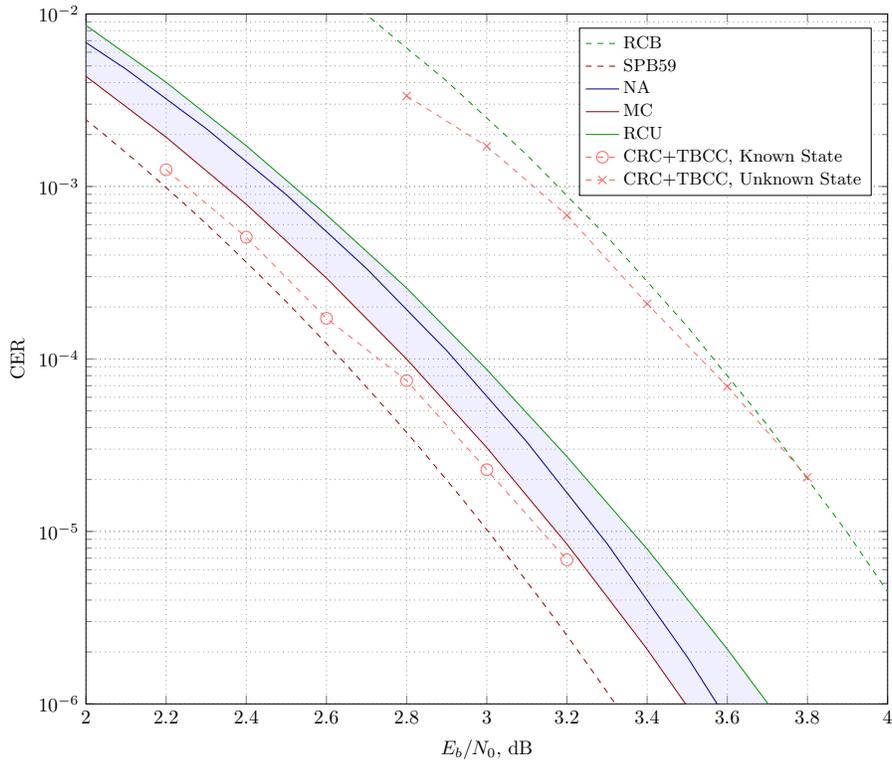


Figure 6: Codeword error rate vs. E_b/N_0 for (128, 64) CRC/TB CC concatenation over the bi-AWGN channel.

4. Modern Short Codes

In the following subsections, we briefly review some of the best constructions of modern channel codes for short blocklengths. The review includes both binary and non-binary turbo and LDPC codes, as well as polar codes.

4.1. Binary Turbo and LDPC Codes

For short blocklengths, turbo and LDPC codes are typically outperformed by the code classes discussed in the previous section. Their performance becomes competitive in the moderate blocklength regime thanks to their linear (in blocklength) decoding complexity for a fixed number of iterations. While this holds true for both binary and non-binary turbo/LDPC codes, binary turbo and LDPC codes retain a larger appeal from the perspective of decoder complexity.

Binary turbo codes [7] have been successfully included as a channel coding scheme in the 3G/4G cellular standards. Turbo codes are known to provide excellent coding gains in the moderate blocklength regime and (if carefully designed) at short blocklengths as well. If low error rates are required ($\text{CER} < 10^{-4}$), a convenient design choice is to adopt 16-state component codes, i.e., to use memory-4 convolutional codes in the parallel concatenation, together with TB termination for the component codes [81]. The small size of the information word permits an efficient interleaver optimization. Code-matched [82] and protograph-based [83] interleavers in particular turn out to be very effective in lowering error floors. The performance of two (128, 64) turbo codes with memory-3 and memory-4 component codes is provided in Figure 7. The first code is from the long term evolution (LTE) standard, whereas the second code has been designed with the interleaver construction of [37] and exploits TB component codes. The second code performs fairly close to the RCB, and nearly 1 dB away from the NA at $\text{CER} = 10^{-4}$. The LTE turbo code loses almost 0.4 dB at the same target CER. Remarkably, the simple 16-state construction provides a performance that is among the best achievable by binary iteratively-decodable codes, at least down to moderate error rates.

LDPC codes [4] are particularly attractive thanks to their excellent performance and to the possibility of developing high-throughput iterative decoders based on the codes' Tanner graph [84] with a large degree of parallelism. LDPC codes can be subdivided into two broad categories: unstructured and structured LDPC codes [27; 58]. For an unstructured LDPC

code, the code parity-check matrix is designed according to a computer-based pseudo-random algorithm that places the non-zero entries (aiming, for instance, at maximizing the girth of the corresponding Tanner graph [85]). Unstructured LDPC codes are rarely implemented in practice [86]. Among structured LDPC codes, protograph-based codes [86; 87] are particularly interesting from a decoder implementation viewpoint. A protograph is a relatively small graph from which a larger Tanner graph can be obtained by a copy-and-permute procedure: the protograph is copied Q times, and then the edges of the individual replicas are permuted among the replicas (under some restrictions described in [86]) to obtain a single, large graph. The parameter Q is often referred to as a *lifting factor*.

When cyclic edge permutations are used, the code associated with the Tanner graph is quasi-cyclic, facilitating the implementation of efficient encoders and decoders [58; 88]. Powerful protograph LDPC codes have been designed during the past decade [89]. A class of protograph LDPC codes that performs remarkably well down to short blocklengths is that of the accumulate-repeat-accumulate (ARA) codes [90]. The performance of an (128, 64) ARA code is provided in Figure 7. The code performs close to the LTE turbo code. An error floor appears at a CER below 10^{-5} . The performance of an (128, 64) LDPC code based on a slightly modified protograph, dubbed accumulate-repeat-jagged-accumulate (ARJA) [89], is provided too. The ARJA code trades a negligible loss in the waterfall region for a superior performance at large SNRs, i.e., it has a lower error floor.

Another class of protograph LDPC codes with excellent performance is the one proposed in [91], which relies on the concatenation of an outer high-rate LDPC code with an inner LDPC code. The inner LDPC code construction resembles an LT code [92], resulting in an overall LDPC code structure that closely mimics that of a Raptor code [93] (the main difference is that here the bits at the input of the inner LT encoder are, with the exception of the punctured ones, sent over the channel). This design paradigm has been adopted in the 5G standard [94].

In particular, the upcoming 5G New Radio (NR) standard foresees the use of two protograph-based codes for its enhanced Mobile Broadband (eMBB) use case. Their design reflects the requirements for 5G NR, which includes the support of a wide range of blocklengths and code rates and a naive integration of hybrid automatic repeat request (H-ARQ). Additionally, the nested structure of the codes and the quasi-cyclic lifting allow a hardware-friendly implementation with minimal description complexity as well as var-

ious possibilities for parallelization. Base graph⁴ 1 (BG 1) targets larger blocklengths and higher rates ($500 \leq k \leq 8448$, $1/3 \leq R \leq 8/9$), whereas base graph 2 (BG 2) is optimized for smaller blocklengths and lower rates ($40 \leq k \leq 2560$, $1/5 \leq R \leq 2/3$). Both base graphs make use of punctured variable nodes. This construction is known to significantly improve the decoding threshold [89]. We observe in Figure 7 that the (128, 64) 5G NR LDPC code based on BG 2 even slightly outperforms the ARA code with the same code parameters. In contrast, the performance of an LDPC code constructed from BG 1 (which is optimized for larger blocklengths and higher code rates) is severely degraded due to its poor minimum distance.

As described in Section 3.1, a conceptually simple improvement to the BP decoder performance can be obtained by applying OSD whenever the BP decoding fails to converge to a valid codeword. In Figure 7, we provide the performance of (3, 6) regular LDPC code under the BP decoder followed by an additional OSD (with order $t = 4$) step applied whenever the BP decoder fails after a maximum number of 50 iterations. The performance gain over iterative decoding is around 1 dB at $\text{CER} \approx 10^{-4}$. However, the gap reduces to 0.5 dB at $\text{CER} \approx 10^{-5}$. Besides OSD, another list decoding algorithm that can improve remarkably the performance of short (binary) LDPC codes is the bit flipping (BF) algorithm proposed in [95, Algorithm 8.6]. In Figure 7, we depict the performance of this algorithm when applied to the (3, 6) regular LDPC code, for the case of a maximum number of 200 bit flips. The gain over iterative decoding exceeds 0.5 dB at $\text{CER} \approx 10^{-5}$.

4.2. Non-Binary Turbo and LDPC Codes

Turbo codes constructed over non-binary finite fields were originally investigated in [39]. In [48], a design based on memory-1 (in terms field elements) time-varying recursive TB encoders was proposed, which yields among the best known performance for iteratively-decodable short codes down to very low error rates. The construction is particularly effective for relatively large finite fields (e.g., \mathbb{F}_{64} and \mathbb{F}_{128}). The component-code BCJR decoder can be efficiently implemented by means of the fast Fourier transform (FFT) [40; 48], yielding remarkable savings in complexity (although the decoding complexity remains considerably larger than that of a binary turbo code). Further efficient decoder implementations have been recently investigated

⁴In the 5G NR jargon, base graph is synonymous with protograph.

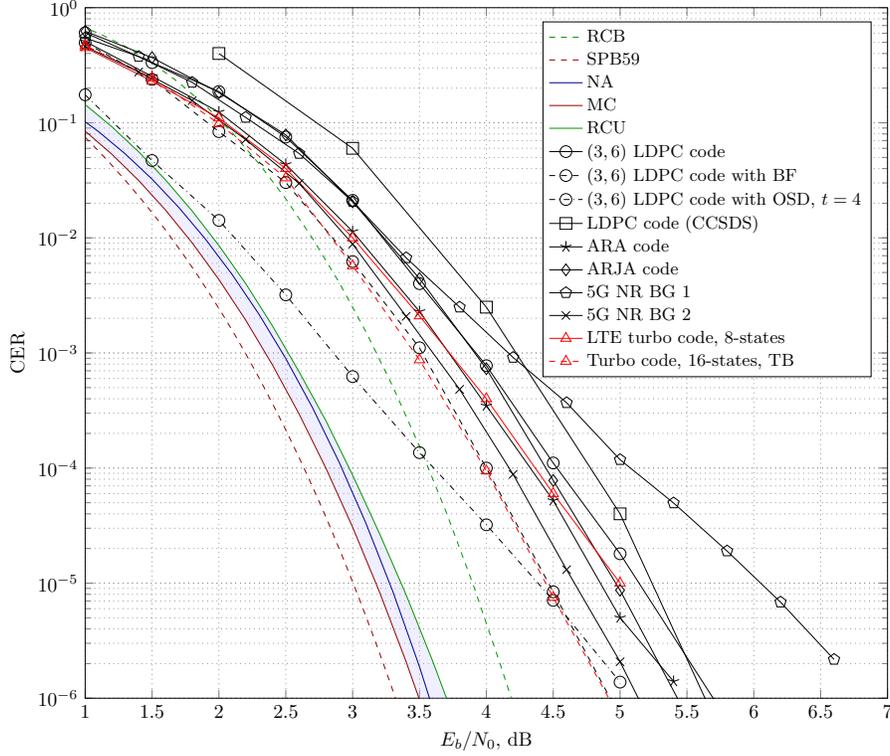


Figure 7: Codeword error rate vs. E_b/N_0 for $(128, 64)$ binary LDPC and turbo codes, bi-AWGN channel.

in [96] showing how most of the coding gains can be preserved even when dramatically reducing the decoding complexity.

Non-binary LDPC codes [38] based on ultra-sparse parity-check matrices [41] match tightly the performance of non-binary turbo codes, down to very low error rates, when constructed on finite fields of order larger than or equal to 64 [47; 97]. In fact, it was shown in [48] that non-binary turbo codes based on memory-1 time-varying recursive TB encoders admit a simple protograph LDPC representation, and correspond to a special class of non-binary ultra-sparse LDPC codes. While the decoding of non-binary LDPC codes can be largely simplified by employing the FFT at the check nodes (with probability-domain decoding), efficient implementations in the log-domain are still an area of active research [98].

Figure 8 shows the performance of non-binary turbo/LDPC codes with block length 128 and dimension 64 on the bi-AWGN channel. Both codes are constructed on \mathbb{F}_{256} . The LDPC code has been considered for standardization within Consultative Committee for Space Data Systems (CCSDS) (as error-correcting code for satellite telecommand) [97; 99; 100] and it has been designed according to the method proposed in [41]. The turbo code has been designed according to the method proposed in [48]. Both codes perform almost identically down to very low error rates, almost matching the RCB.

Also for the non-binary case, a further decoding step based on OSD decoding can be applied to any iteratively-decodable code whenever the BP decoder fails. As an example, Figure 8 reports the performance of a (128, 64) non-binary LDPC code constructed on \mathbb{F}_{256} on the bi-AWGN channel. After iterative decoding, when the decoder output does not fulfill the code parity-check equations, an additional OSD step is applied with t set to 4. Specifically, OSD is applied to the binary image of the non-binary LDPC code. The performance is very close to the one attained by the (128, 64) extended BCH code, first presented in Figure 4, gaining 0.5 dB over the code performance under BP decoding. Considering as reference an SNR of 3 dB, the BP decoder for the non-binary LDPC code fails with a probability close to 2×10^{-3} . Hence, the OSD is effectively activated only for a very small fraction of the transmissions.

4.3. Polar Codes

Polar codes [101; 102] are the first class of provably capacity-achieving codes with low encoding/decoding complexity over any symmetric binary-input memoryless channels (B-MC) under successive cancellation (SC) decoding [102]. The underlying idea behind polar codes, called channel polarization, is to take the independent copies of a symmetric B-MC and convert them into noiseless and useless synthetic channels by applying a transform to input bits and by imposing a decoding order so that coding becomes trivial: Transmit information bits over the noiseless synthetic channels while inputs to the useless ones are set (frozen) to a predetermined value, e.g., to 0, and the decoder knows these bits before transmission. Those input bits are called frozen bits. As the number of polarization steps grows, the fraction of noiseless synthetic channels tends to the channel capacity, while the fraction of useless channels tends to its complement to one.

For a given SNR, constructing an (n, k) polar code requires one to find the least reliable $n - k$ synthetic channels, or equivalently, bit positions. The

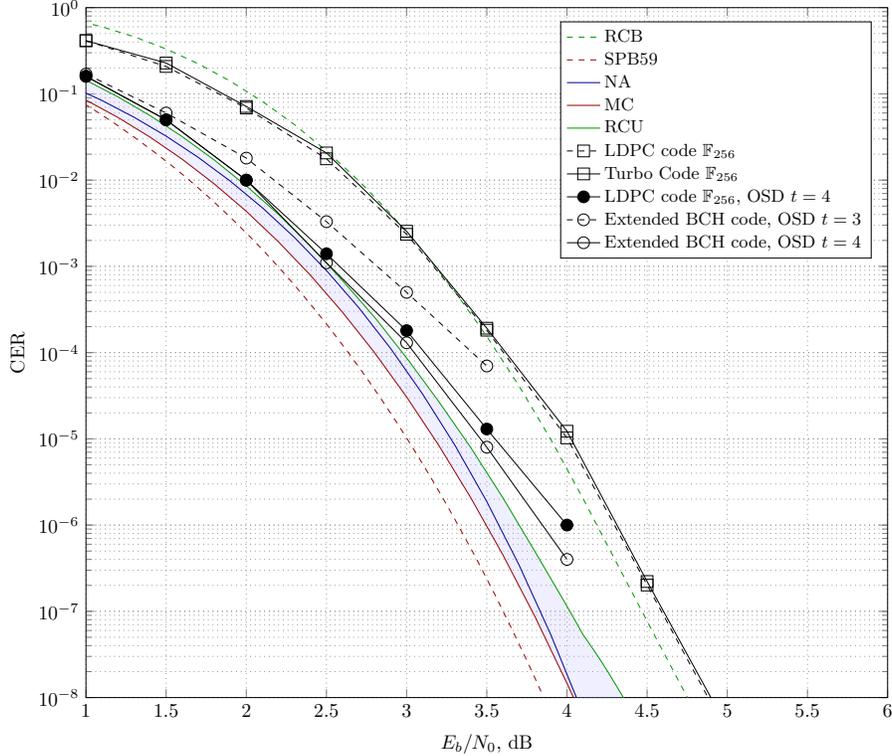


Figure 8: Codeword error rate vs. E_b/N_0 for (128, 64) LDPC and turbo codes over \mathbb{F}_{256} , bi-AWGN channel.

design is not universal, i.e., the polar code design differs depending on the channel quality. Monte Carlo-based designs were proposed in [101; 102], while a density evolution-based construction is introduced in [103]. An efficient implementation for density evolution is provided in [104] together with an analysis providing lower and upper bounds for the reliabilities of the bit positions. The Gaussian approximation (GA) for design was proposed in [105]. Other methods based on a partial order among the positions were proposed in [106; 107]. These methods allow one to design frozen bit sequences that show a good behavior for a wide range of channel parameters and rates. This has been of particular importance during 5G standardization [108] with its strong emphasis on lowering the description complexity.

Although being capacity-achieving under SC decoding, the effectiveness

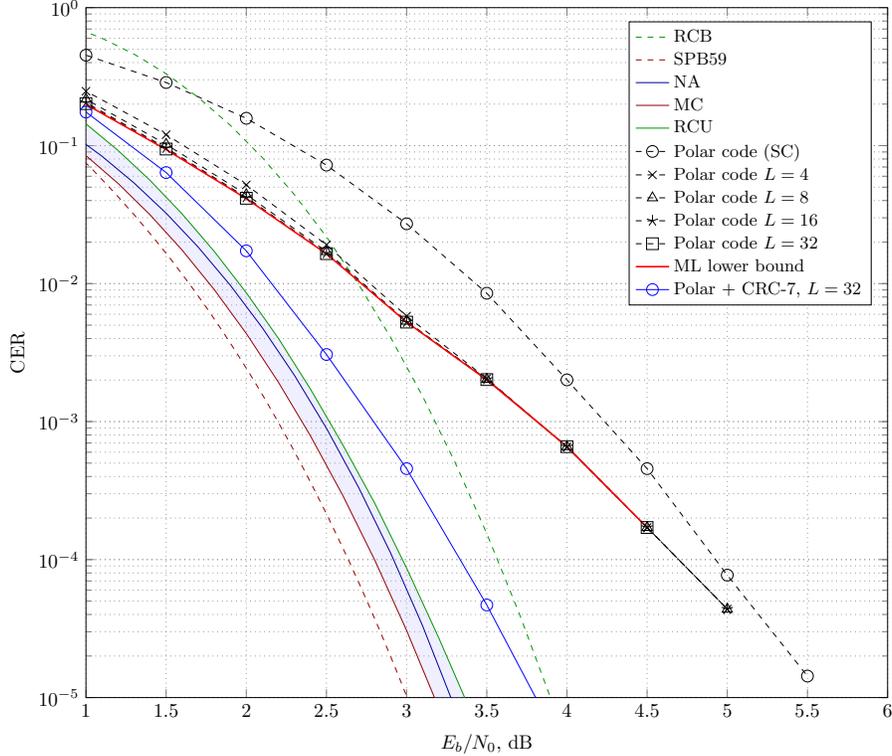


Figure 9: Codeword error rate vs. E_b/N_0 for a (128, 64) polar code, bi-AWGN channel.

of polar codes for short blocklengths comes only after modifying both the decoder and the code, i.e., by employing the SC list (SCL) decoder of [57] aided by the addition of an outer high-rate code (typically, a CRC code). In fact, in the short and moderate-blocklength regimes the performance of SC decoding of polar codes falls short of the performance under ML decoding. In the SCL decoding algorithm, a set of SC decoders work in parallel producing a list of different codeword candidates for the same observed channel output. The complexity of the algorithm is linear in the list size. The outer high-rate code, which improves the distance properties of the resulting code, is used to test the list of codewords produced by the SCL decoder. Among the survivors, the one with the largest likelihood is picked as the decoder output. The design of the concatenated code for SCL decoding becomes more sophisticated due to the increased search space, i.e., unmanageable

number of possible interleavers and outer codes [109–112].

The performance of a (128, 64) polar code designed by using the GA of density evolution (DE) for the bi-AWGN channel with $E_b/N_0 = 4.5$ dB under SC and SCL decoding is shown in Figure 9. By increasing the list size, close-to-ML performance is achieved. In fact, a lower bound on the ML error probability can be obtained by artificially introducing the correct codeword in the final list, prior to the final selection. One can see from the figure that the lower bound on the ML error probability is approached quickly as the list size L grows. Already for $L = 8$, the gap from the the ML lower bound is nearly invisible for the setup considered in the figure. The performance of the concatenation of a (128, 71) polar code with a CRC-7 code as an outer code is shown as well. The inner polar code was designed for $E_b/N_0 = 5$ dB. The outer CRC code has generator polynomial $g(x) = x^7 + x^3 + 1$, leading to a code with dimension 64. A list size of 32 has been used in the simulation. The code performs remarkably close to the RCU bound down to low error rates.

5. Code Comparison: Examples

5.1. Very Short Codes

In this section, we summarize the results reported in the previous sections about the performance of very short codes over the bi-AWGN channel. We focus on codes with blocklength $n = 128$ and code dimension $k = 64$ bits. The performance of the codes is compared in Figure 10. As reference, the performance of the (128, 64) binary protograph-based [33] LDPC code from the CCSDS telecommand standard [99] is provided too. The CCSDS LDPC code performs somehow poorly in terms of coding gain and is outperformed by the ARA LDPC code.⁵ At low error rates (e.g. CER $\approx 10^{-6}$) the CCSDS LDPC code is likely to attain lower error rates than the ARA code thanks to its remarkable distance properties [33]. Among the LDPC codes adopted for the 5G NR standard, the codes based on BG 2 are seen to be competitive, outperforming the ARA code.

⁵All LDPC codes considered in this section have been designed by means of a girth optimization based on the progressive edge growth (PEG) algorithm [85]. A maximum of 200 belief propagation iterations have been used in the simulations (although the average iteration count is much lower, especially at high SNRs, thanks to early decoding stopping rules).

The performance of a turbo code introduced in [113] based on 16-state component recursive convolutional codes is also provided. The turbo code shows superior performance with respect to binary LDPC codes, down to low error rates. The code attains a CER $\approx 10^{-4}$ at almost 0.4 dB from the RCB. The code performance diverges remarkably from the RCB at lower error rates, due to the relatively low code minimum distance. Results for a non-binary LDPC code are included in Figure 10. The code has been constructed over \mathbb{F}_{256} , and it attains visible gains with respect to its binary counterparts, performing on top of the RCB (and 0.7 dB away from the NA) down to low error rates (no floors down to CER $\approx 10^{-9}$ were observed in [97]). The error probability of the polar-code concatenation using a CRC-7 as an outer code is shown. The polar code has parameters (128, 71). A list size of 32 has been used in the simulation. The code outperforms all the competitors that rely on iterative decoding algorithms. Finally, the CER of three TB CCs is included [114; 115]. The three codes have memory 8, 11 and 14, respectively. Their generators (in octal notation) and their distance properties are summarized in Table 1. The WAVA algorithm has been used for decoding [77]. The memory-11 convolutional code reaches the performance of the BCH and LDPC codes under OSD. The memory-8 code loses 1 dB at CER $\approx 10^{-5}$, but still outperforms binary LDPC and turbo codes over the whole simulation range. The third code (memory-14) outperforms all other codes in Figure 10 (at the expense of a high decoding complexity due to the large number of states in the code trellis).

Table 1: Summary of the TB CCs used in the comparisons.

Generators	m	(n, k)	Weight enumerating function $A(\mathbf{x})$
[515, 677]	8		$1 + 576\mathbf{x}^{12} + 1152\mathbf{x}^{13} + 1856\mathbf{x}^{14} + \dots$
[5537, 6131]	11	(128, 64)	$1 + 64\mathbf{x}^{14} + 960\mathbf{x}^{15} + 1356\mathbf{x}^{16} + \dots$
[75063, 56711]	14		$1 + 8\mathbf{x}^{16} + 1856\mathbf{x}^{18} + 19392\mathbf{x}^{20} + \dots$
[515, 677]	8		$1 + 2304\mathbf{x}^{12} + 4608\mathbf{x}^{13} + 7424\mathbf{x}^{14} + \dots$
[5537, 6131]	11	(512, 256)	$1 + 256\mathbf{x}^{14} + 3840\mathbf{x}^{15} + 5376\mathbf{x}^{16} + \dots$
[75063, 56711]	14		$1 + 6656\mathbf{x}^{18} + 42240\mathbf{x}^{20} + 216320\mathbf{x}^{22} + \dots$

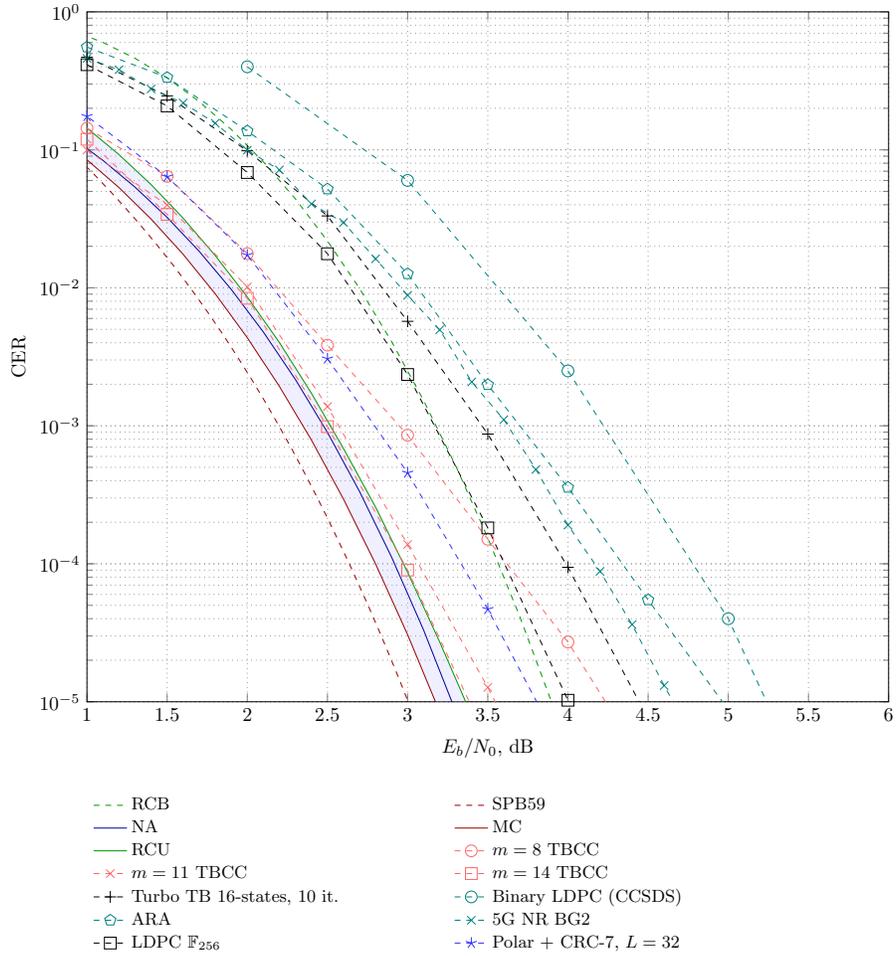


Figure 10: Codeword error rate vs. E_b/N_0 for several (128, 64) codes over the bi-AWGN channel.

5.2. Moderate-length Codes

In this section, we address a second case study, where an intermediate blocklength of $n = 512$ bits is considered. The code dimension is fixed to $k = 256$ bits yielding a rate $R = 1/2$. The performance of the codes is compared in Figure 11 for transmission over the bi-AWGN channel. Also here, the performance of the (512, 256) binary protograph-based [33] LDPC code from the CCSDS telecommand standard [99] is provided as a reference. Most of the considerations that are valid in the very short blocklength regime are still valid here, with a few notable exceptions. First, we observe that the performance of the polar code (concatenated with an outer 16 bits CRC code) is still competitive, but it performs only marginally better than binary LDPC and turbo codes when the list size is limited to 32. To close the gap to the finite length bounds, a larger list size (e.g., 1024) has to be used. A second major discrepancy with respect to the very short block regime deals with the performance of TB CCs. For the code parameters considered in Figure 11, TB CCs are far from the finite length bounds even for the memory-14 case. This is an instance of a well known limitation of (TB) CCs, i.e., the saturation, for large enough n , of the TB CC minimum distance to the free distance of the underlying (unterminated) convolutional code (in addition, the minimum weight multiplicity grows with n). This phenomenon is illustrated in Figure 12, where the SNR required to achieve a target CER = 10^{-4} is provided as a function of the code dimension k , for various code families.

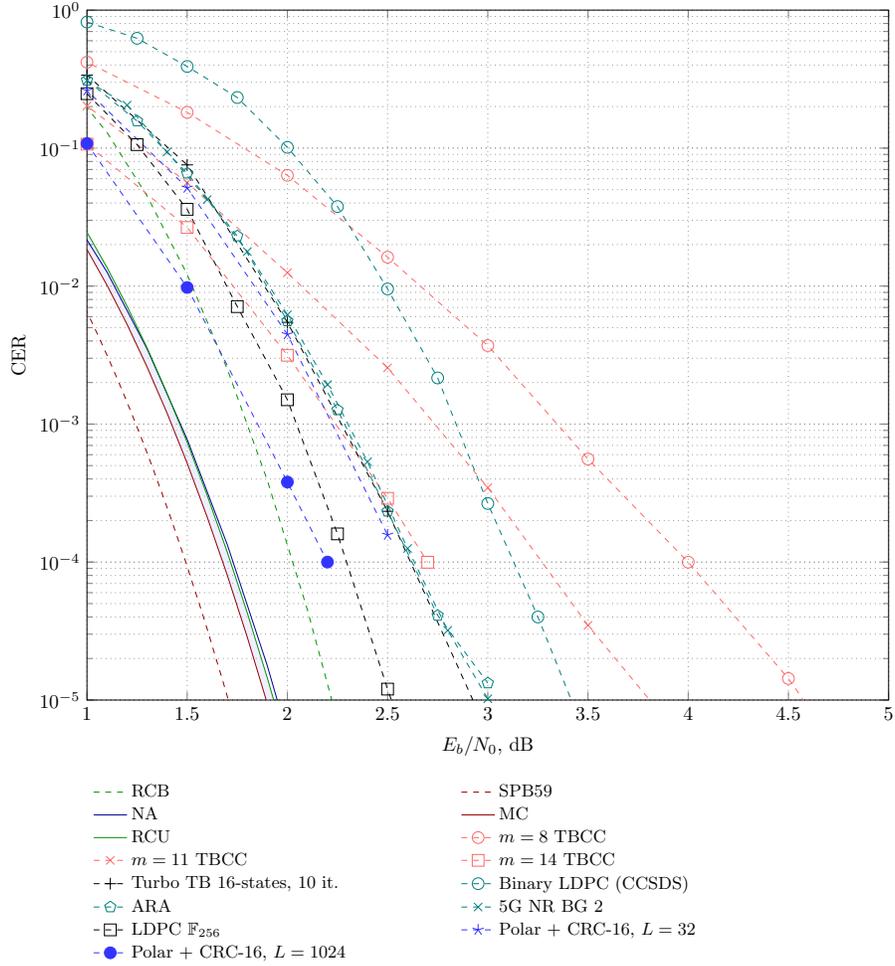


Figure 11: Codeword error rate vs. E_b/N_0 for several (512, 256) codes over the bi-AWGN channel.

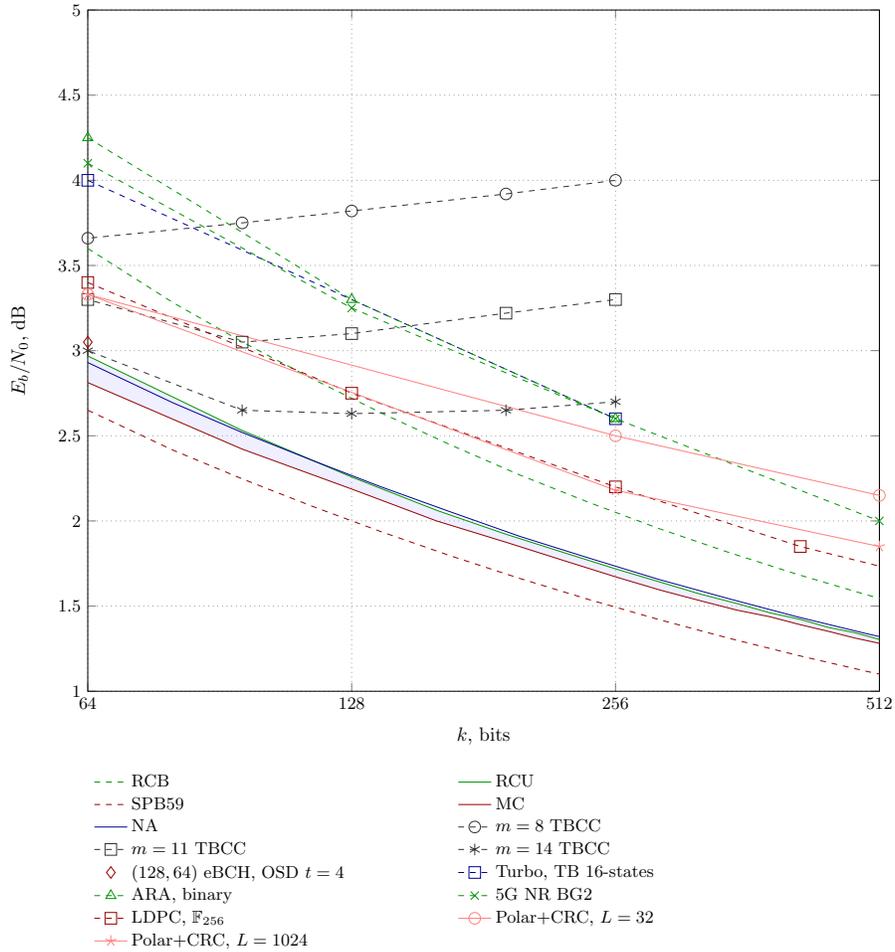


Figure 12: E_b/N_0 required to achieve a codeword error rate of 10^{-4} for several code families over the bi-AWGN channel. Here $R = 1/2$.

5.3. Short Codes in Coded Modulation Schemes

Higher-order modulation increases the spectral efficiency (SE) of a communication system by using constellations with more than two signal points (e.g., M -amplitude shift keying (ASK) or M -quadrature amplitude modulation (QAM)) and transmitting more than one bit per channel use [116]. As this requires an interplay of both modulation and coding techniques, the

term “coded modulation” (CM) has been established. The most straightforward CM approach combines an M -ary constellation with a non-binary channel code over a field of order M .⁶ In this case, symbol-metric decoding (SMD) can be employed at the receiver. This is the common approach for non-binary LDPC and Turbo codes.

Practical receivers resort to “pragmatic” CM schemes with binary channel codes. In such pragmatic schemes, an m -bit binary labeling is assigned to each of the $M = 2^m$ constellation points (e.g., a binary reflected gray code (BRGC) code [117]) and a bit-wise decoding (BMD) metric is used at the decoder. The BMD metric is obtained by marginalizing over all bit levels except the one of interest, which causes a performance loss compared to SMD. This loss is particularly pronounced at low code rates. The best known example of pragmatic CM scheme is bit-interleaved coded modulation (BICM) [118; 119]. Binary LDPC and turbo codes are commonly combined with higher-order modulations using BICM. Polar codes achieve superior performance with multi-level coding and multistage decoding [120–122] due to the improved polarization process.

The use of ASK/QAM constellations with uniformly distributed constellation points incurs a performance degradation for the AWGN channel, which is known as *shaping loss*. Recently, many research efforts have focused on geometric and probabilistic shaping (GS/PS) approaches to overcome this deficit [123; 124] and close the gap to the Shannon limit. Simulation results [125] show that PS signaling generally performs better than GS for the same constellation size. Additionally, PS allows a fine granularity in SE as it can be tuned by means of a distribution matcher (DM) [126] and does not require different modulation and code rate combinations. To implement PS with coding, probabilistic amplitude shaping (PAS) was proposed [124], which circumvents the drawbacks of previous approaches (e.g., error propagation and the need for iterative demapping as a result of a one-to-many mapping). PAS uses a shaping encoder before the encoder (reverse concatenation), and a systematic generator matrix for encoding to maintain the desired distribution. Furthermore, it exploits the symmetry of the capacity achieving distribution of the Gaussian channel.

All coding schemes discussed in the previous sections can be used in a

⁶It is also possible to map sequences of constellation points to one Galois field symbol of appropriate field order.

CM scenario with higher-order modulation formats. In Fig. 13 and 14 we compare CM approaches for a target SE of 3 bits per channel use for the case of 64-QAM and a blocklength of 192 bits, i.e., we have a number of $192/6 = 32$ channel uses. In Fig. 13, we illustrate a performance comparison for the case of uniform signaling.

- The binary LDPC code is from the 5G standard [94] and derived from BG 2 (cf. Section 4.1). We use a random bit-mapper, i.e., the BMD bit channels are assigned randomly to the variable nodes.
- The NB-LDPC code is an ultra-sparse code of rate $1/2$ and it is constructed over \mathbb{F}_{64} . It exhibits a gap of about 0.4 dB to the RCB at $\text{CER} = 10^{-4}$.
- The polar code was designed according to [122] for $E_s/N_0 = 13.45$ dB. The list size is $L = 32$ and a 8-bit CRC is used in the concatenation.
- OSD uses a (255, 99) BCH code that is punctured in 60 parity positions and shortened in 3 information bit positions to obtain a (192, 96) code. The OSD parameter is $t = 4$.

In Fig. 14, we use PAS to reduce the shaping loss incurred by uniform signaling and improve the power efficiency. We target a SE of 3.0 bits per channel use, which is achieved by adjusting the DM rate. We show results for two DM approaches, namely constant composition distribution matching (CCDM) and shell mapping distribution matching (SMDM). CCDM was proposed first in [126] and shown to be the optimal fixed-to-fixed blocklength distribution matcher (DM) for the normalized informational divergence metric and long output blocklengths. Instead, SMDM has favorable performance for short blocklengths and is the informational divergence optimal DM for finite blocklength. It uses the shell mapping algorithm [127] internally to perform the mapping to power-efficient channel input sequences.

- The binary LDPC code is from the 5G standard [94], has rate $3/4$ and is derived from BG 1 (cf. Sec. 4.1). We use a random bit-mapper for the amplitude bit levels, the uniform sign bits are assigned to the last variable nodes in the graph. At a CER of 10^{-3} we see that SMDM is 0.4 dB more power efficient than CCDM.

- The NB-LDPC code is an ultra sparse cycle code of rate $2/3$, constructed over \mathbb{F}_{256} . It is operated with PAS as discussed in [128]. The gain of SMDM compared to CCDM is about 0.6 dB.
- The polar code was designed according to [122; 129] for $E_s/N_0 = 12.95$ dB. The list size is $L = 32$ and a 4-bit CRC is used in the concatenation. Additionally, it makes use of a type check during the list decoding to compensate for the finite length losses of CCDM [129, Sec. IV].

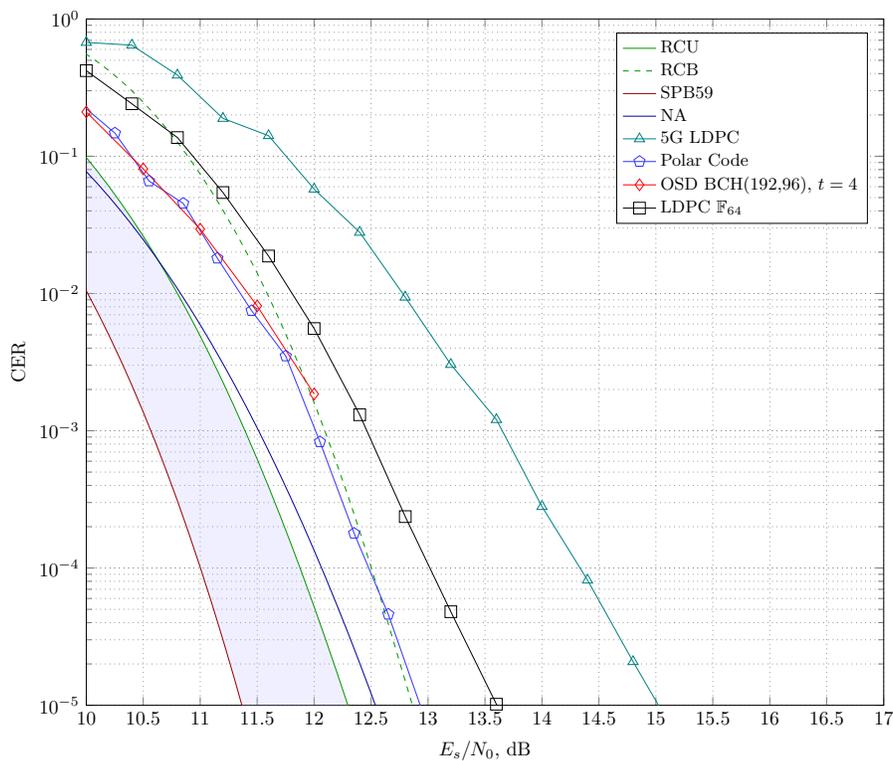


Figure 13: Codeword error rate vs. E_s/N_0 for 64-QAM, uniform signaling and an SE of 3.0 bpcu for several codes over the AWGN channel. The number of channel uses is 32.

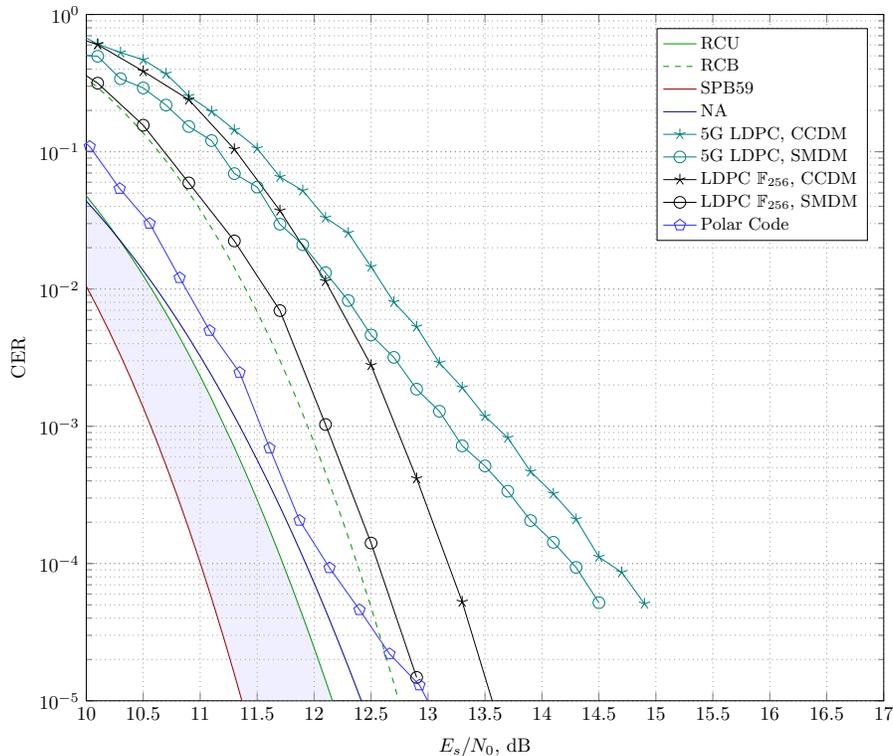


Figure 14: Codeword error rate vs. E_s/N_0 for 64-QAM, shaped signaling and an SE of 3.0 bpcu for several codes over the AWGN channel. The number of channel uses is 32.

6. Conclusions

In this paper, we reviewed several code constructions tailored to the transmission of short information blocks. The performance of the codes has been compared with tight information theoretic bounds on the error probability achievable by the best codes. Our review illustrates that there is a wide spectrum of solutions for efficient transmission in the short-blocklength regime. To conclude, we provide a brief list of interesting open directions, which were not addressed in this manuscript:

- Some of the decoding algorithms described in the previous sections are complete, i.e., the output of the decoder is always a codeword. Incomplete algorithms, such as belief propagation for LDPC codes, may output an *erasure*, i.e., the iterative decoder may converge to a decision

that is not a (valid) codeword but the error is detected. Hence, while for complete decoders all error events are *undetected*, incomplete decoders provide the additional capability of notifying the receiver when decoding does not succeed. In some applications, it is of paramount importance to deliver very low undetected error rates. This is the case, for instance, for telecommand systems, where wrong command sequences may be harmful. The CCSDS LDPC code of Figure 10 has been designed with this objective in mind, trading part of the coding gain for a strong error detection capability [130]. Complete decoders, such as those based on OSD and Viterbi decoding, may be used in such critical applications by adding an error detection mechanism. One possibility is to include an outer error detection code. In the short blocklength regime, the overhead incurred by such solution may be unacceptable. In this context, a more appealing solution is provided by a post-decoding threshold test as proposed in [131]. Examples of the application of this approach are given in, e.g., [132–134].

- The development of codes and decoding algorithms that address channels with unknown state such as fading channels with no *a priori* channel-state information available at the encoder and decoder (see, e.g., [67]) is still an open problem. Here, the decoding task is made complicated by the need of accounting for the uncertainty on the channel coefficients. A naive approach is to introduce sufficiently large pilot fields to allow for an accurate channel estimation step. However, when short blocks are transmitted, the use of large pilot fields leads to considerable overheads, i.e., rate losses. This suggests that in this setting channel decoding and channel estimations should be performed jointly (see, e.g., [135]).
- Throughout the paper, we focused exclusively on the analysis of fixed-length coding schemes. In some applications where communication is bidirectional and a feedback link is hence present, it is more natural to consider variable-length coding schemes with decision (ACK/NACK) feedback. Finite-blocklength bounds for this scenarios are available [136; 137], but are not as tight as the corresponding bound for the fixed-blocklength case. Also, a more accurate modeling of the ACK/NACK message compared to what is available in the literature may unveil interesting tradeoffs between coding rate and reliability of the feedback

information. Indeed, for a fixed frame size, the more channel uses are used for the ACK/NACK message, the less channel uses are available for the coded bits. Code design for this setup have been recently proposed [138–140]. However, the overall code design space is largely unexplored.

References

- [1] C. Shannon, A mathematical theory of communication, *Bell System Tech. J.* 27 (1948) 379–423, 623–656.
- [2] E. R. Berlekamp, *Key papers in the development of coding theory*, IEEE Press, 1974.
- [3] P. Elias, Error-free coding, *IRE Trans. Inform. Theory* 4 (4) (1954) 29–37.
- [4] R. G. Gallager, *Low-density parity-check codes*, M.I.T. Press, Cambridge, MA, USA, 1963.
- [5] G. D. Forney, Jr., *Concatenated codes*, M.I.T. Press, Cambridge, MA, USA, 1966.
- [6] D. J. Costello, Jr., G. D. Forney, Jr., Channel coding: The road to channel capacity, *Proc. IEEE* 95 (6) (2007) 1150–1177.
- [7] C. Berrou, A. Glavieux, P. Thitimajshima, Near Shannon limit error-correcting coding and decoding: Turbo-codes, in: *Proc. IEEE Int. Conf. Commun. (ICC)*, Geneva, Switzerland, 1993, pp. 1064–1070.
- [8] D. J. C. MacKay, Good error-correcting codes based on very sparse matrices, *IEEE Trans. Inf. Theory* 45 (2) (1999) 399–431.
- [9] T. Richardson, M. Shokrollahi, R. Urbanke, Design of capacity-approaching irregular low-density parity-check codes, *IEEE Trans. Inf. Theory* 47 (2) (2001) 619–637.
- [10] T. Richardson, R. Urbanke, The capacity of low-density parity-check codes under message-passing decoding, *IEEE Trans. Inf. Theory* 47 (2) (2001) 599–618.

- [11] M. Luby, M. Mitzenmacher, M. A. Shokrollahi, D. A. Spielman, Improved low-density parity-check codes using irregular graphs, *IEEE Trans. Inf. Theory* 47 (2) (2001) 585–598.
- [12] H. D. Pfister, I. Sason, R. Urbanke, Capacity-achieving ensembles for the binary erasure channel with bounded complexity, *IEEE Trans. Inf. Theory* 51 (7) (2005) 2352–2379.
- [13] H. D. Pfister, I. Sason, Accumulate-repeat-accumulate codes: Capacity-achieving ensembles of systematic codes for the erasure channel with bounded complexity, *IEEE Trans. Inf. Theory* 53 (6) (2007) 2088–2115.
- [14] E. Arıkan, Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels, *IEEE Trans. Inf. Theory* 55 (7) (2009) 3051–3073.
- [15] M. Lentmaier, A. Sridharan, D. Costello, Jr., K. Zigangirov, Iterative decoding threshold analysis for LDPC convolutional codes, *IEEE Trans. Inf. Theory* 56 (10) (2010) 5274–5289.
- [16] S. Kudekar, T. Richardson, R. Urbanke, Threshold saturation via spatial coupling: Why convolutional LDPC ensembles perform so well over the BEC, *IEEE Trans. Inf. Theory* 57 (2) (2011) 803–834.
- [17] T. de Cola, E. Paolini, G. Liva, G. Calzolari, Reliability options for data communications in the future deep-space missions, *Proc. IEEE* 99 (11) (2011) 2056–2074.
- [18] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, P. Popovski, Five disruptive technology directions for 5G, *IEEE Commun. Mag.* 52 (2) (2014) 74–80.
- [19] E. Paolini, C. Stefanovic, G. Liva, P. Popovski, Coded random access: applying codes on graphs to design random access protocols, *IEEE Commun. Mag.* 53 (6) (2015) 144–150.
- [20] G. Durisi, T. Koch, P. Popovski, Toward massive, ultrareliable, and low-latency wireless communication with short packets, *Proc. IEEE* 104 (9) (2016) 1711–1726.

- [21] S. Dolinar, D. Divsalar, F. Pollara, Code performance as a function of block size, TMO progress report 42-133, JPL, Pasadena, CA, USA (May 1998).
- [22] T. M. Duman, M. Salehi, New performance bounds for turbo codes, *IEEE Trans. Commun.* 46 (6) (1998) 717–723.
- [23] I. Sason, S. Shamai, Performance analysis of linear codes under maximum-likelihood decoding: A tutorial, *Found. and Trends in Commun. and Inf. Theory* 3 (1–2) (2006) 1–222.
- [24] Y. Polyanskiy, V. Poor, S. Verdù, Channel coding rate in the finite blocklength regime, *IEEE Trans. Inf. Theory* 56 (5) (2010) 2307–235.
- [25] W. Yang, G. Durisi, T. Koch, Y. Polyanskiy, Quasi-static multiple-antenna fading channels at finite blocklength, *IEEE Trans. Inf. Theory* 60 (7) (2014) 4232–4265.
- [26] G. Durisi, T. Koch, J. Östman, Y. Polyanskiy, W. Yang, Short-packet communications over multiple-antenna rayleigh-fading channels, *IEEE Trans. Commun.* 64 (2) (2016) 618–629.
- [27] T. Richardson, R. Urbanke, *Modern coding theory*, Cambridge University Press, 2008.
- [28] S. Ten Brink, Convergence behavior of iteratively decoded parallel concatenated codes, *IEEE Trans. Commun.* 49 (10) (2001) 1727–1737.
- [29] H. R. Sadjadpour, M. Salehi, N. J. A. Sloane, G. Nebe, Interleaver design for short block length turbo codes, in: *Proc. IEEE Int. Conf. on Commun. (ICC)*, Vol. 2, 2000, pp. 628–632.
- [30] C. Radebaugh, C. Powell, R. Koetter, Wheel codes: Turbo-like codes on graphs of small order, in: *Proc. IEEE Inf. Theory Workshop (ITW)*, Paris, France, 2003, pp. 78–81.
- [31] M. Yang, W. E. Ryan, Y. Li, Design of efficiently encodable moderate-length high-rate irregular LDPC codes, *IEEE Trans. on Commun.* 52 (4) (2004) 564–571.
- [32] G. Liva, W. Ryan, Short low-error-floor Tanner codes with Hamming nodes, in: *Proc. IEEE Milcom*, Atlantic City, US, 2005, pp. 208–213.

- [33] D. Divsalar, S. Dolinar, C. Jones, Short protograph-based LDPC codes, in: Proc. IEEE Milcom, Orlando, FL, USA, 2007, pp. 1–6.
- [34] G. Liva, W. E. Ryan, M. Chiani, Quasi-cyclic generalized LDPC codes with low error floors, *IEEE Trans. Commun.* 56 (1) (2008) 49–57.
- [35] I. E. Bocharova, B. D. Kudryashov, R. V. Satyukov, S. Stiglmayry, Short quasi-cyclic LDPC codes from convolutional codes, in: *IEEE Int. Symp. Inf. Theory (ISIT)*, 2009, pp. 551–555.
- [36] T.-Y. Chen, K. Vakulinia, D. Divsalar, R. D. Wesel, Protograph-based raptor-like LDPC codes, *IEEE Trans. Commun.* 63 (5) (2015) 1522–1532.
- [37] T. Jerkovits, B. Matuz, Turbo code design for short blocks, in: Proc. 7th Adv. Sat. Mobile Sys. Conf. (ASMS), Majorca (Spain), 2016, pp. 1–6.
- [38] M. C. Davey, D. MacKay, Low density parity-check codes over $GF(q)$, *IEEE Commun. Lett.* 2 (6) (1998) 165–167.
- [39] J. Berkmann, Iterative Decoding of Nonbinary Codes, Ph.D. dissertation, Tech. Univ. München, Munich, Germany, 2000.
- [40] J. Berkmann, C. Weiss, On dualizing trellis-based APP decoding algorithms, *IEEE Trans. Commun.* 50 (11) (2002) 1743–1757.
- [41] C. Poulliat, M. Fossorier, D. Declercq, Design of regular $(2, d_c)$ -LDPC codes over $GF(q)$ using their binary images, *IEEE Trans. Commun.* 56 (10) (2008) 1626–1635.
- [42] A. Venkiah, D. Declercq, C. Poulliat, Design of cages with a randomized progressive edge-growth algorithm, *IEEE Commun. Lett.* 12 (4) (2008) 301–303.
- [43] W. Chen, C. Poulliat, D. Declercq, Structured high-girth non-binary cycle codes, in: *Asia-Pacific Conf. Commun. (APCC)*, Shanghai, China, 2009, pp. 462–466.

- [44] L. Costantini, B. Matuz, G. Liva, E. Paolini, M. Chiani, On the performance of moderate-length non-binary LDPC codes for space communications, in: Proc. 5th Adv. Sat. Mobile Sys. Conf. (ASMS), Cagliari, Italy, 2010.
- [45] K. Kasai, D. Declercq, C. Poulliat, K. Sakaniwa, Multiplicatively repeated nonbinary LDPC codes, *IEEE Trans. Inf. Theory* 57 (10) (2011) 6788–6795.
- [46] G. Liva, B. Matuz, E. Paolini, M. Chiani, Short non-binary IRA codes on large-girth Hamiltonian graphs, in: Proc. IEEE Int. Conf. on Commun. (ICC), Ottawa, Canada, 2012.
- [47] B. Y. Chang, D. Divsalar, L. Dolecek, Non-binary protograph-based LDPC codes for short block-lengths, in: Proc. IEEE Inf. Theory Workshop (ITW), Lausanne, Switzerland, 2012.
- [48] G. Liva, E. Paolini, B. Matuz, S. Scalise, M. Chiani, Short turbo codes over high order fields, *IEEE Trans. Commun.* 61 (6) (2013) 2201–2211.
- [49] B. Matuz, G. Liva, E. Paolini, M. Chiani, G. Bauch, Low-rate non-binary LDPC codes for coherent and blockwise non-coherent AWGN channels, *IEEE Trans. Commun.* 61 (10) (2013) 4096–4107.
- [50] L. Dolecek, D. Divsalar, Y. Sun, B. Amiri, Non-binary protograph-based LDPC codes: Enumerators, analysis, and designs, *IEEE Trans. Inf. Theory* 60 (7) (2014) 3913–3941.
- [51] M. Fossorier, S. Lin, Soft-decision decoding of linear block codes based on ordered statistics, *IEEE Trans. Inf. Theory* 41 (5) (1995) 1379–1396.
- [52] A. Valembois, M. Fossorier, Box and match techniques applied to soft-decision decoding, *IEEE Trans. Inf. Theory* 50 (5) (2004) 796–810.
- [53] T. Hehn, J. B. Huber, S. Laendner, O. Milenkovic, Multiple-bases belief-propagation for decoding of short block codes, in: Proc. IEEE Int. Symp. Inf. Theory (ISIT), 2007, pp. 311–315.
- [54] T. Hehn, J. B. Huber, O. Milenkovic, S. Laendner, Multiple-bases belief-propagation decoding of high-density cyclic codes, *IEEE Trans. Commun.* 58 (1) (2010) 1–8.

- [55] Y. Wu, C. Hadjicostis, Soft-decision decoding using ordered recodings on the most reliable basis, *IEEE Trans. Inf. Theory* 53 (2) (2007) 829–836.
- [56] G. Liva, E. Paolini, M. Chiani, On optimum decoding of certain product codes, *IEEE Commun. Lett.* 18 (6) (2014) 905–908.
- [57] I. Tal, A. Vardy, List decoding of polar codes, *IEEE Trans. Inf. Theory* 61 (5) (2015) 2213–2226.
- [58] W. E. Ryan, S. Lin, *Channel Codes – Classical and Modern*, Cambridge University Press, 2009.
- [59] R. Gallager, A simple derivation of the coding theorem and some applications, *IEEE Trans. Inf. Theory* 11 (1) (1965) 3–18.
- [60] C. Shannon, Probability of error for optimal codes in a Gaussian channel, *Bell System Tech. J.* 38 (1959) 611–656.
- [61] C. E. Shannon, R. G. Gallager, E. R. Berlekamp, Lower bounds to error probability for coding on discrete memoryless channels—Part I, *Inf. Contr.* 10 (1967) 65–103.
- [62] A. Valembois, M. Fossorier, Sphere-packing bounds revisited for moderate block lengths, *IEEE Trans. Inf. Theory* 50 (12) (2004) 2998 – 3014.
- [63] G. Vazquez-Vilar, A. T. Campo, A. Guillén i Fàbregas, A. Martinez, Bayesian M-ary hypothesis testing: The meta-converse and Verdú-Han bounds are tight, *IEEE Trans. Inf. Theory* 62 (5) (2016) 2324 – 2333.
- [64] G. Vazquez-Vilar, A. Guillén i Fàbregas, T. Koch, A. Lancho, Saddlepoint approximation of the error probability of binary hypothesis testing, in: *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Veil, CO, USA, 2018, pp. 2306–2310.
- [65] A. Martinez, A. Guillén i Fàbregas, Saddlepoint approximation of random-coding bounds, in: *Proc. Inf. Theory Applicat. Workshop (ITA)*, San Diego, CA, U.S.A., 2011, pp. 1–6.

- [66] J. Scarlett, A. Martinez, A. Guillén i Fàbregas, Mismatched decoding: Error exponents, second-order rates and saddlepoint approximations, *IEEE Trans. Inf. Theory* 60 (5) (2014) 2647–2666.
- [67] J. Östman, G. Durisi, E. Ström, M. C. Coşkun, G. Liva, Short Packets Over Block-Memoryless Fading Channels: Pilot-Assisted or Noncoherent Transmission?, *IEEE Trans. Commun.* To appear.
- [68] J. Font-Segura, G. Vazquez-Vilar, A. Martinez, A. Guillén i Fàbregas, A. Lancho, Saddlepoint approximations of lower and upper bounds to the error probability in channel coding, in: *Proc. Conf. Inf. Sci. Sys. (CISS)*, Princeton, NJ, 2018.
- [69] S. Lin, D. Costello, Jr., *Error control coding*, Prentice Hall, Englewood Cliffs, NJ, USA, 2004, second edition.
- [70] M. P. C. Fossorier, Iterative reliability-based decoding of low-density parity check codes, *IEEE J. Sel. Areas Commun.* 19 (5) (2001) 908–917.
- [71] M. Baldi, F. Chiaraluce, N. Maturo, G. Liva, E. Paolini, A hybrid decoding scheme for short non-binary LDPC codes, *IEEE Commun. Lett.* 18 (12) (2014) 2093–2096.
- [72] S. Lin, T. Kasami, T. Fujiwara, M. Fossorier, *Trellises and trellis-based decoding algorithms for linear block codes*, Springer Science & Business Media, 1998.
- [73] A. R. Calderbank, G. D. Forney, A. Vardy, Minimal tail-biting trellises: The Golay code and more, *IEEE Trans. Inf. Theory* 45 (5) (1999) 1435–1455.
- [74] P. Stahl, J. B. Anderson, R. Johannesson, Optimal and near-optimal encoders for short and moderate-length tail-biting trellises, *IEEE Trans. Inf. Theory* 45 (7) (1999) 2562–2571.
- [75] I. E. Bocharova, R. Johannesson, B. D. Kudryashov, P. Stahl, Tailbiting codes: Bounds and search results, *IEEE Trans. Inf. Theory* 48 (1) (2002) 137–148.
- [76] R. Johannesson, K. S. Zigangirov, *Fundamentals of Convolutional Coding (Second Edition)*, John Wiley & Sons, 2015.

- [77] R. Y. Shao, S. Lin, M. P. C. Fossorier, Two decoding algorithms for tailbiting codes, *IEEE Trans. Commun.* 51 (10) (2003) 1658–1665.
- [78] I. E. Bocharova, M. Handlery, R. Johannesson, B. D. Kudryashov, A BEAST for prowling in trees, *IEEE Trans. Inf. Theory* 50 (6) (2004) 1295–1302.
- [79] N. Seshadri, C. E. W. Sundberg, List viterbi decoding algorithms with applications, *IEEE Trans. Commun.* 42 (234) (1994) 313–323.
- [80] C. Lou, B. Daneshrad, R. D. Wesel, Convolutional-code-specific crc code design, *IEEE Trans. Commun.* 63 (10) (2015) 3459–3470.
- [81] S. Crozier, P. Guinand, High-performance low-memory interleaver banks for turbo-codes, in: *IEEE VTC*, Vol. 4, 2001, pp. 2394–2398 vol.4.
- [82] W. Feng, J. Yuan, B. S. Vucetic, A code-matched interleaver design for turbo codes, *IEEE Trans. Commun.* 50 (6) (2002) 926–937.
- [83] R. Garzón-Bohórquez, C. A. Nour, C. Douillard, Protograph-based interleavers for punctured turbo codes, *IEEE Trans. Commun.* 66 (5) (2018) 1833–1844.
- [84] R. Tanner, A recursive approach to low complexity codes, *IEEE Trans. Inf. Theory* 27 (1981) 533–547.
- [85] X. Hu, E. Eleftheriou, D. Arnold, Regular and irregular progressive edge-growth tanner graphs, *IEEE Trans. Inf. Theory* 51 (1) (2005) 386–398.
- [86] J. Thorpe, Low-density parity-check (LDPC) codes constructed from protographs, IPN progress report 42-154, JPL (Aug. 2003).
- [87] T. J. Richardson, R. L. Urbanke, Multi-edge type LDPC codes, Workshop Honoring Prof. Bob McEliece on His 60th Birthday (2002).
- [88] M. M. Mansour, N. R. Shanbhag, High-throughput LDPC decoders, *IEEE Trans. VLSI Syst.* 11 (6) (2003) 976–996.

- [89] D. Divsalar, S. Dolinar, C. R. Jones, K. Andrews, Capacity-approaching protograph codes, *IEEE J. Sel. Areas Commun.* 27 (6) (2009) 876–888.
- [90] A. Abbasfar, D. Divsalar, K. Yao, Accumulate-repeat-accumulate codes, *IEEE Trans. Commun.* 55 (4) (2007) 692–702.
- [91] T. Y. Chen, K. Vakilinia, D. Divsalar, R. D. Wesel, Protograph-Based Raptor-Like LDPC Codes, *IEEE Trans. Commun.* 63 (5) (2015) 1522–1532.
- [92] M. Luby, LT codes, in: *Proc. of the 43rd IEEE Symp. Foundations of Computer Science*, Vancouver, Canada, 2002, pp. 271–282.
- [93] M. Shokrollahi, Raptor codes, *IEEE Trans. Inf. Theory* 52 (6) (2006) 2551–2567.
- [94] T. Richardson, S. Kudekar, Design of low-density parity check codes for 5G new radio, *IEEE Commun. Mag.* 56 (3) (2018) 28–34.
- [95] M. Ostojic, Multitree Search Decoding of Linear Codes, Ph.D. dissertation, ETH, Zurich, Switzerland, 2010.
- [96] R. Klaimi, C. A. Nour, C. Douillard, J. Farah, Low-complexity decoders for non-binary turbo codes, in: *10th International Symposium on Turbo Codes & Iterative Information Processing (ISTC 2018)*, Hong Kong, 2018.
- [97] G. Liva, E. Paolini, T. D. Cola, M. Chiani, Codes on high-order fields for the CCSDS next generation uplink, in: *Proc. 6th Adv. Sat. Mobile Sys. Conf. (ASMS) and 12th Signal Process. for Space Commun. Workshop (SPSC)*, 2012, pp. 44–48.
- [98] D. Declercq, M. Fossorier, Decoding algorithms for nonbinary LDPC codes over $\text{GF}(q)$, *IEEE Trans. Commun.* 55 (4) (2007) 633–643.
- [99] Next Generation Uplink, Tech. Rep. 230.2-G-1, Consultative Committee for Space Data Systems (CCSDS), Washington, DC, USA (Jul. 2014).

- [100] Short block length LDPC codes for TC synchronization and channel coding, Tech. Rep. 231.1-O-1, Consultative Committee for Space Data Systems (CCSDS), Washington, DC, USA (Apr. 2015).
- [101] N. Stolte, Rekursive Codes mit der Plotkin-Konstruktion und ihre Decodierung, Ph.D. dissertation, TU Darmstadt, Darmstadt, Germany, 2002.
- [102] E. Arıkan, Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels, *IEEE Trans. Inf. Theory* 55 (7) (2009) 3051–3073.
- [103] R. Mori, T. Tanaka, Performance and construction of polar codes on symmetric binary-input memoryless channels, in: *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2009, pp. 1496–1500.
- [104] I. Tal, A. Vardy, How to construct polar codes, *IEEE Trans. Inf. Theory* 59 (10) (2013) 6562–6582.
- [105] P. Trifonov, Efficient design and decoding of polar codes, *IEEE Trans. Commun.* 60 (11) (2012) 3221–3227.
- [106] M. Mondelli, S. H. Hassani, R. Urbanke, Construction of polar codes with sublinear complexity, in: *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2017, pp. 1853–1857.
- [107] G. He, J. Belfiore, I. Land, G. Yang, X. Liu, Y. Chen, R. Li, J. Wang, Y. Ge, R. Zhang, W. Tong, Beta-expansion: A theoretical framework for fast and recursive construction of polar codes, in: *Proc. IEEE Global Telecommun. Conf.*, 2017, pp. 1–6.
- [108] V. Bioglio, C. Condo, I. Land, Design of polar codes in 5G new radio, [arXiv:1804.04389](https://arxiv.org/abs/1804.04389).
- [109] B. Li, H. Shen, D. Tse, A RM-polar codes, [arXiv:1407.5483](https://arxiv.org/abs/1407.5483).
- [110] G. Ricciutelli, M. Baldi, F. Chiaraluce, G. Liva, On the error probability of short concatenated polar and cyclic codes with interleaving, in: *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2017, pp. 1858–1862.
- [111] G. Ricciutelli, M. Baldi, F. Chiaraluce, Interleaver design for short concatenated codes, *IEEE Commun. Lett.* 22 (9) (2018) 1762–1765.

- [112] P. Yuan, T. Prinz, G. Böcherer, O. İřcan, R. Böhnke, W. Xu, Polar code construction for list decoding, in: Proc. ITG Int. Conf. Syst., Commun. and Coding (SCC), Rostock, Germany, 2019.
- [113] M. Baldi, M. Bianchi, F. Chiaraluce, R. Garello, I. Sanchez, S. Cioni, Advanced channel coding for space mission telecommand links, in: IEEE VTC Fall, Las Vegas, NV, USA, 2013, pp. 1–5.
- [114] P. Stahl, J. B. Anderson, R. Johannesson, Optimal and near-optimal encoders for short and moderate-length tail-biting trellises, *IEEE Trans. Inf. Theory* 45 (7) (1999) 2562–2571.
- [115] L. Gaudio, T. Ninacs, T. Jerkovits, G. Liva, On the performance of short tail-biting convolutional codes for ultra-reliable communications, in: Proc. 11th Int. ITG Conf. Systems, Commun. and Coding (SCC), Hamburg, Germany, 2017.
- [116] G. Ungerboeck, Channel coding with multilevel/phase signals, *IEEE Trans. Inf. Theory* 28 (1) (1982) 55–67.
- [117] F. Gray, Pulse code communication, Tech. Rep. 2632058, U.S. Patent (1953).
- [118] E. Zehavi, 8-PSK trellis codes for a Rayleigh channel, *IEEE Trans. Commun.* 40 (5) (1992) 873–884.
- [119] A. Guillén i Fàbregas, A. Martinez, G. Caire, Bit-Interleaved Coded Modulation, *Foundations and Trends® in Communications and Information Theory* 5 (1–2) (2008) 1–153.
- [120] H. Imai, S. Hirakawa, A new multilevel coding method using error-correcting codes, *IEEE Trans. Inf. Theory* 23 (3) (1977) 371–377.
- [121] M. Seidl, A. Schenk, C. Stierstorfer, J. B. Huber, Polar-Coded Modulation, *IEEE Trans. Commun.* 61 (10) (2013) 4108–4119.
- [122] G. Böcherer, T. Prinz, P. Yuan, F. Steiner, Efficient polar code construction for higher-order modulation, in: Proc. IEEE Wireless Commun. and Netw. Conf. (WCNC), San Francisco, USA, 2017.

- [123] F.-W. Sun, H. C. A. van Tilborg, Approaching capacity by equiprobable signaling on the Gaussian channel, *IEEE Trans. Inf. Theory* 39 (5) (1993) 1714–1716.
- [124] G. Böcherer, F. Steiner, P. Schulte, Bandwidth efficient and rate-matched low-density parity-check coded modulation, *IEEE Trans. Commun.* 63 (12) (2015) 4651–4665.
- [125] F. Steiner, G. Böcherer, Comparison of geometric and probabilistic shaping with application to ATSC 3.0, in: *Proc. ITG Int. Conf. Syst., Commun. and Coding (SCC)*, Hamburg, Germany, 2017.
- [126] P. Schulte, G. Böcherer, Constant composition distribution matching, *IEEE Trans. Inf. Theory* 62 (1) (2016) 430–434.
- [127] R. Laroia, N. Farvardin, S. A. Tretter, On optimal shaping of multidimensional constellations, *IEEE Trans. Inf. Theory* 40 (4) (1994) 1044–1056.
- [128] F. Steiner, G. Liva, G. Böcherer, Ultra-sparse non-binary LDPC codes for probabilistic amplitude shaping, in: *Proc. IEEE Global Telecommun. Conf.*, 2017, pp. 1–5.
- [129] T. Prinz, P. Yuan, G. Böcherer, F. Steiner, O. Iscan, R. Böhnke, W. Xu, Polar coded probabilistic amplitude shaping for short packets, in: *Proc. IEEE Int. Workshop on Signal Process. Adv. in Wireless Commun. (SPAWC)*, 2017.
- [130] S. Dolinar, K. Andrews, F. Pollara, D. Divsalar, Bounded angle iterative decoding of LDPC codes, in: *Proc. 2008 IEEE Milcom*, 2008, pp. 1–6.
- [131] G. D. Forney, Jr., Exponential error bounds for erasure, list, and decision feedback schemes, *IEEE Trans. Inf. Theory* 14 (2) (1968) 206–220.
- [132] E. Hof, I. Sason, S. Shamai, On optimal erasure and list decoding schemes of convolutional codes, in: *Proc. Tenth Int. Symp. Commun. Theory and Applications (ISCTA)*, 2009, pp. 6–10.
- [133] E. Hof, I. Sason, S. Shamai, Performance bounds for erasure, list, and decision feedback schemes with linear block codes, *IEEE Trans. Inf. Theory* 56 (8) (2010) 3754–3778.

- [134] A. R. Williamson, M. J. Marshall, R. D. Wesel, Reliability-output decoding of tail-biting convolutional codes, *IEEE Trans. Commun.* 62 (6) (2014) 1768–1778.
- [135] M. C. Coşkun, G. Liva, J. Östman, G. Durisi, Low-complexity joint channel estimation and list decoding of short codes, in: *Proc. 12th ITG Int. Conf. Syst., Commun. and Coding (SCC)*, Rostock, Germany, 2019.
- [136] Y. Polyanskiy, H. V. Poor, S. Verdú, Feedback in the non-asymptotic regime, *IEEE Trans. Inf. Theory* 57 (8) (2011) 4903–4925.
- [137] J. Östman, G. C. Ferrante, R. Devassy, G. Durisi, Low-latency short-packet transmissions: Fixed length or HARQ?, in: *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Abu Dhabi, UAE, 2018.
- [138] A. R. Williamson, T.-Y. Chen, R. D. Wesel, Variable-length convolutional coding for short blocklengths with decision feedback, *IEEE Trans. Commun.* 63 (7) (2015) 2389–2403.
- [139] H. Wang, N. Wong, A. M. Baldauf, C. K. Bachelor, S. V. S. Ranganathan, D. Divsalar, R. D. Wesel, An information density approach to analyzing and optimizing incremental redundancy with feedback, in: *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, 2017.
- [140] H. Yang, E. Liang, R. D. Wesel, Joint design of convolutional code and CRC under serial list viterbi decoding, *arXiv:1811.11932*.