A Decoding Algorithm for LDPC Codes Over Erasure Channels with Sporadic Errors

Gianluigi Liva, Enrico Paolini, Balazs Matuz, and Marco Chiani

Abstract— An efficient decoding algorithm for low-density parity-check (LDPC) codes on erasure channels with sporadic errors (i.e., binary error-and-erasure channels with error probability much smaller than the erasure probability) is proposed and its performance analyzed. A general single-error multiple-erasure (SEME) decoding algorithm is first described, which may be in principle used with any binary linear block code. The algorithm is optimum whenever the non-erased part of the received word is affected by at most one error, and is capable of performing error detection of multiple errors. An upper bound on the average block error probability under SEME decoding is derived for the linear random code ensemble. The bound is tight and easy to implement. The algorithm is then adapted to LDPC codes, resulting in a simple modification to a previously proposed efficient maximum likelihood LDPC erasure decoder which exploits the parity-check matrix sparseness. Numerical results reveal that LDPC codes under efficient SEME decoding can closely approach the average performance of random codes.

I. INTRODUCTION

The design and decoding of low-density parity-check (LDPC) codes [1] applied to erasure channels has been vastly explored in the past decade (see e.g. [2]–[7]). While originally most of the attention has been paid to the construction of LDPC codes able to approach the channel capacity under iterative (IT) decoding, more recently practical maximum-likelihood (ML) decoding algorithms for LDPC codes over erasure channels have been devised [6], [8], paving the way for the design of codes for hybrid IT/ML decoders [9], [10]. It has been shown that ML decoding of LDPC codes can largely outperform its iterative counterpart, attaining on the binary erasure channel (BEC) performances close to those of idealized maximum distance separable (MDS) codes down to moderate-low error rates [9].

In general, ML decoding of an (n, k) binary linear block code on the erasure channel turns into solving a system of $n - k$ equations (imposed by the parity-check matrix of the code) in the e unknowns corresponding to the e erased symbols of the codeword. The system is solved by means of Gauss-Jordan elimination (GJE), which is known to have a complexity scaling as $\mathcal{O}(n^3)$. For LDPC codes, the parity-check matrix sparseness can be exploited to heavily reduce the fraction of unknowns to be solved by GJE [8], [11].

Such unknowns are usually referred to as *pivots*,[1] and the algorithm to select the pivots is termed *pivoting algorithm* [12].[2] Once the pivots are solved, the remaining unknowns are recovered by the usual iterative decoding algorithm with linear complexity.

The erasure channel model is adopted in a number of applications. For example, in wireless communication systems, packets that cannot be correctly decoded are discarded (through a frame validation test involving an error detecting code), and lost packets are treated as erasures at the higher layers where a packet erasure correcting code may be used to recover the missing packets [14]. In optical communications with pulse-position modulation (PPM), erasure channel models have been adopted under the assumptions of absent background radiation and low noise power [15], [16].

Albeit accurate, the erasure channel represents only an approximation of the actual behavior of these channels. In wireless communications, the probability of undetected errors (due to error patterns that satisfy the constraints of the error detection code) is always bounded away from zero [17]. In optical communication systems, even in absence of background radiation and for low noise power, errors may take place, even if with small probabilities [16]. In both cases, the channel can be more realistically modeled by an erasure channel with *sporadic* errors, i.e. by an error-and-erasure channel with erasure probability ϵ and error probability p, where $p \ll \epsilon$. For example, when a CRC-16 is used to detect errors for an uncoded transmission over a binary symmetric channel (BSC) with error probability $q = 10^{-2}$, undetected errors may happen with probability close to 10^{-5} [17]. Hence, in this case the error probability of the equivalent packet error-and-erasure channel would be $p = 10^{-5}$. Assuming at the higher layers a packet erasure correcting code (i.e. a code only attempting to correct erasures) with block size $n = 10^3$ packets, undetected errors would compromise the recovery of a block with probability $P_e = 1 - (1 - p)^n \simeq 10^{-2}$, so that the block error probability after erasure decoding would be bounded by $P_e \geq 10^{-2}$, *regardless* the erasure probability.

Iterative belief propagation decoding of LDPC codes over the binary error-and-erasure channel (BEEC) can be naturally implemented by initializing the decoder with the appropriate log-likelihood ratios (LLRs). According to Fig. 1, assuming the channel input is $x \in \{0, 1\}$ and the channel output $y \in \{0, 1, ?\}$ (where '?' denotes an erasure), the message

G. Liva and B. Matuz are with the Institute of Communications and Navigation, German Aerospace Center (DLR), Oberpfaffenhofen, 82234 Wessling, Germany. Email: {Gianluigi.Liva,Balazs.Matuz}@dlr.de

E. Paolini and M. Chiani are with DEIS, WiLAB, University of Bologna, 47023 Cesena (FC), Italy. Email: {e.paolini,marco.chiani}@unibo.it

[1]*Reference variables* in [8].

[2]Pivoting is inherently related to *guessing* in the alternative ML algorithms proposed in [6], [13].

at the input of the generic variable node would be $\Lambda(y) = \ln[\Pr(x = 0|y)/\Pr(x = 1|y)]$ resulting in $\Lambda(0) = \ln[(1 - \epsilon - p)/p]$, $\Lambda(1) = -\ln[(1 - \epsilon - p)/p]$ and $\Lambda(?) = 0$.

In this paper, we introduce an efficient decoding algorithm for LDPC codes, which extends the ML erasure decoding algorithm of [8] in the sense of correcting sporadic errors. For the sake of simplicity, we focus on the binary case and assume the BEEC as the channel model. However, the proposed algorithm may be easily extended to packet error-and-erasure channels. The proposed algorithm performs optimum decoding of errors and erasures when a received word is affected by a single error (also recovering some erasure patterns containing stopping sets of the IT decoder), and attempts to perform error detection for error patterns of larger Hamming weights. For this reason, the algorithm is named single-error multiple-erasures (SEME) decoder. The algorithm is first illustrated for the case of a generic linear block code, and a tight upper bound on its average error probability for the linear random code ensemble is developed. The algorithm is then adapted to account for parity-check matrix sparseness in the LDPC code case. It is illustrated how LDPC codes can efficiently approach the average performance of the linear random code ensemble over the BEEC with sporadic errors. We will see that the proposed algorithm largely outperforms the IT one in the region where the block error probability is limited by the channel erasures rather than by the (sporadic) channel errors.

Several previous works focused on the simultaneous correction of errors and erasures (e.g. [18]–[21]). In particular, in [21] some parity-check matrix construction techniques are developed capable to separate errors and erasures. We will see in Section III and Section V that the proposed algorithm performs a similar separation, properly and efficiently modifying the parity-check matrix of an LDPC code after receiving a word from the BEEC.

The paper is organized as follows. In Section II the notation used throughout the paper is introduced. In Section III the SEME algorithm is detailed. The average performance of the binary linear random code ensemble is analyzed in Section IV, while the efficient implementation of SEME decoding for LDPC codes is discussed in Section V. A comparison between the performance of random codes and that attainable with LDPC codes on the BEEC is given in Section VI. Conclusions follow in Section VII.

II. NOTATION AND PRELIMINARIES

The BEEC channel model is depicted in Fig. 1, where '?' denotes an erasure and where the erasure and error probabilities are denoted by ϵ and p, respectively. Moreover, we let $p^* = p/(1-\epsilon)$ be the probability that a bit transmitted over the BEEC is received in error given that the bit has not been erased. For a given linear block code $\mathcal{C}(n, k)$ over the BEEC, where n is the codeword length and k the code dimension, we denote by E and L the random variables expressing the number of erasures affecting the generic received word of length n and the number of errors affecting the non-erased bits, respectively. Similarly, we denote by
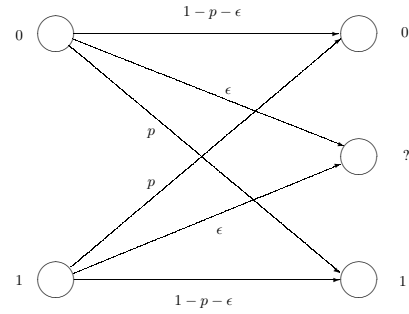

Fig. 1. BEEC channel model.

e and l realizations of E and L, respectively. In the case $n - k > e$, the number of linearly independent parity-check equations in excess with respect to the number of erasures, $n - k - e$, is defined to be the *overhead* and is denoted by δ.

Assume now a codeword $\mathbf{x}'$ is transmitted over the BEEC, resulting in a received word $\mathbf{y}'$ with e erasures and l non-erased bits in error. We let $\mathbf{H}$ be a permuted version of a full-rank $((n-k) \times n)$ parity-check matrix of the code $\mathcal{C}(n, k)$, in which the columns of the parity-check matrix corresponding to the erased bits occupy the e left-most positions and the columns corresponding to the non-erased bits (l of which are in error) the $n-e$ right-most positions. In this way, $\mathbf{H}$ may be split as $\mathbf{H} = [\mathbf{H}_{\bar{K}}|\mathbf{H}_K]$, where $\mathbf{H}_{\bar{K}}$ is an $((n-k) \times e)$ matrix and $\mathbf{H}_K$ is an $((n - k) \times (n - e))$ matrix. Similarly, we let $\mathbf{x}$ and $\mathbf{y}$ be permuted versions of the transmitted codeword and of the received word, respectively, according to the same permutation leading to $\mathbf{H}$. The vectors $\mathbf{x}$ and $\mathbf{y}$ may be split as $\mathbf{x} = [\mathbf{x}_{\bar{K}}|\mathbf{x}_K]$ and $\mathbf{y} = [\mathbf{y}_{\bar{K}}|\mathbf{y}_K]$, where $\mathbf{x}_{\bar{K}}$ and $\mathbf{y}_{\bar{K}}$ are vectors of length e associated with the erased bits, while $\mathbf{x}_K$ and $\mathbf{y}_K$ are vectors of length $n - e$ associated with the non-erased bits (so that the Hamming distance between $\mathbf{x}_K$ and $\mathbf{y}_K$ is equal to l). The vector $\mathbf{x}$ must satisfy the relation $\mathbf{x}\,\mathbf{H}^T = \mathbf{0}$, where $\mathbf{H}^T$ is the transpose of $\mathbf{H}$, which may be written as $\mathbf{x}_{\bar{K}}\mathbf{H}_{\bar{K}}^T = \mathbf{x}_K\mathbf{H}_K^T$. Accordingly, the starting point of the proposed algorithm will consist of imposing and analyzing the equality

$$\mathbf{y}_{\bar{K}}\mathbf{H}_{\bar{K}}^T = \mathbf{y}_K\mathbf{H}_K^T. \tag{1}$$

The product $\mathbf{y}_K\mathbf{H}_K^T$ in the right-hand side of (1) is a vector of length $n - k$ that we denote by $\mathbf{s}$ and, for reasons that will be clear in Section III, refer to as the *syndrome*. In the case where $\mathbf{y}_K$ is affected by one error ($l = 1$), we denote by $\mathbf{h}^{\mathrm{err}}$ the column of $\mathbf{H}_K$ associated with the bit in error.

Throughout the paper, we often exploit the following result.

Proposition 1: Let $\mathbf{A}$ be an $((n - k) \times e)$ random matrix with $e \leq n - k$ and whose entries are independent and identically distributed (i.i.d.) Bernoulli random variables with parameter $1/2$. Then

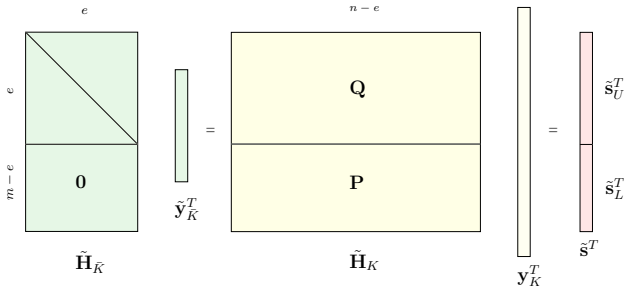$$\Pr(\mathrm{rank}(\mathbf{A}) < e) = 1 - \prod_{i=1}^{e} \left(1 - \frac{2^{i-1}}{2^{n-k}}\right). \tag{2}$$

Fig. 2. Pictorial representation of the equivalent linear system $\tilde{\mathbf{y}}_{\bar{K}}\tilde{\mathbf{H}}_{\bar{K}}^T = \mathbf{y}_K\tilde{\mathbf{H}}_K^T$. In the figure $m = n - k$.

Moreover, we have

$$2^{-(n-k-e)-1} \leq \Pr(\mathrm{rank}(\mathbf{A}) < e) < 2^{-(n-k-e)}. \quad (3)$$

Equality (2) is a classical result [22]. The lower bound in (3) is proved in [23], while a proof of the upper bound is available [24] where the tightness of both bounds is also illustrated.

III. SEME Decoding of Linear Block Codes

A. Maximum Likelihood Decoding of Linear Block Codes over the BEC

Let us assume that the communication channel is a standard BEC introducing erasures but not errors ($p = 0$). In this case, $\mathbf{x}_K = \mathbf{y}_K$ and (1) represents a linear system of $n - k$ (or more than $n - k$, if $\mathbf{H}$ is redundant) equations in e unknowns which may be simply written as $\mathbf{x}_{\bar{K}}\mathbf{H}_{\bar{K}}^T = \mathbf{x}_K\mathbf{H}_K^T$. Here, the unknowns are the elements of $\mathbf{x}_{\bar{K}}$ and $\mathbf{s} = \mathbf{x}_K\mathbf{H}_K^T$ is not affected by any error. Moreover, in this case we always have $\mathrm{rank}(\mathbf{H}_{\bar{K}}) = \mathrm{rank}([\mathbf{H}_{\bar{K}}|\mathbf{s}^T])$, so that the Rouché-Capelli theorem is always satisfied. Hence, the system admits a unique solution when $\mathrm{rank}(\mathbf{H}_{\bar{K}}) = e$ and multiple solutions when $\mathrm{rank}(\mathbf{H}_{\bar{K}}) < e$ (which is always the case when $e > n - k$). Provided $\mathrm{rank}(\mathbf{H}_{\bar{K}}) = e$ and $\hat{\mathbf{x}}_K$ is the unique solution of the system, we have $\mathbf{x}_K = \hat{\mathbf{x}}_K$ with probability one.

Different decoding algorithms over the BEC attempt to solve the system and find $\hat{\mathbf{x}}_K$ with different approaches, offering a different trade-off between performance and complexity. Among them, ML decoding consists of solving the system by GJE performed on the matrix $\mathbf{H}_{\bar{K}}$. The complexity of GJE decoding is in general cubic with the dimension of the system, so that the overall decoding complexity is $\mathcal{O}(n^3)$.

B. Erasure Decoding over the BEEC with Error Detection

When transmitting over the BEEC ($p > 0$), the relation $\mathrm{rank}(\mathbf{H}_{\bar{K}}) = \mathrm{rank}([\mathbf{H}_{\bar{K}}|\mathbf{s}^T])$, always valid over the BEC, may not hold anymore due to the presence of bit errors affecting $\mathbf{s}$ (through $\mathbf{y}_K$). In this case, (1) admits a unique solution when $\mathrm{rank}(\mathbf{H}_{\bar{K}}) = \mathrm{rank}([\mathbf{H}_{\bar{K}}|\mathbf{s}^T]) = e$. The system admits multiple solutions when $\mathrm{rank}(\mathbf{H}_{\bar{K}}) = \mathrm{rank}([\mathbf{H}_{\bar{K}}|\mathbf{s}^T]) < e$. Finally, the system is impossible when $\mathrm{rank}([\mathbf{H}_{\bar{K}}|\mathbf{s}^T]) = \mathrm{rank}(\mathbf{H}_{\bar{K}}) + 1$.

The event that the linear system (1) is impossible is the key to perform the detection of errors affecting $\mathbf{y}_K$. As depicted in Fig. 2, assuming $e < n - k$ (equivalently $\delta > 0$) and $\mathrm{rank}(\mathbf{H}_{\bar{K}}) = e$, GJE performed on the matrix $\mathbf{H}_{\bar{K}}$ leads to an equivalent linear system $\tilde{\mathbf{y}}_{\bar{K}}\tilde{\mathbf{H}}_{\bar{K}}^T = \tilde{\mathbf{s}}$, where the first e rows of $\tilde{\mathbf{H}}_{\bar{K}}$ form the identity matrix of order e and the last δ rows are all-zero. Here, $\tilde{\mathbf{s}}^T$ and $\tilde{\mathbf{H}}_K$ is obtained by performing on $\mathbf{s}^T$ and $\mathbf{H}_K$ the same row operations leading to $\hat{\mathbf{H}}_{\bar{K}}$, and $\tilde{\mathbf{y}}_{\bar{K}}$ by performing on $\mathbf{y}_{\bar{K}}$ the same column permutations leading to $\tilde{\mathbf{H}}_{\bar{K}}$. Splitting $\tilde{\mathbf{s}}$ as $\tilde{\mathbf{s}} = [\tilde{\mathbf{s}}_U|\tilde{\mathbf{s}}_L]$, where $\tilde{\mathbf{s}}_U$ has length e and $\tilde{\mathbf{s}}_L = \mathbf{y}_K\mathbf{P}^T$ has length δ, detection of errors affecting $\mathbf{y}_K$ may be performed by simply observing that, if $\tilde{\mathbf{s}}_L \neq \mathbf{0}$, then the BEEC must have necessarily introduced errors in $\mathbf{y}_K$.

Next, we derive a tight upper bound on the average failure probability $\bar{P}_{f,\mathcal{R}(n,k)}^{\mathrm{d,BEEC}}$ of the erasure decoder with error detection for the ensemble, denoted by $\mathcal{R}(n,k)$, of random binary linear block codes defined by a parity-check matrix $\mathbf{H}$ with $n - k$ rows and n columns whose entries are i.i.d. Bernoulli random variables with parameter $1/2$.[3] By "failure probability" we mean the probability that either the erasure pattern cannot be recovered due to rank deficiency of $\mathbf{H}_{\bar{K}}$ ($\mathrm{rank}(\mathbf{H}_{\bar{K}}) < E$) or it can be recovered but the error pattern on $\mathbf{y}_K$ is undetected as $\tilde{\mathbf{s}}_L = \mathbf{0}$. Denoting these two disjoint events by A and B, respectively, we have $\bar{P}_{f,\mathcal{R}(n,k)}^{\mathrm{d,BEEC}} = \Pr(A) + \Pr(B) = \sum_{e=1}^n \Pr(A|E = e)\Pr(E = e) + \sum_{e=0}^{n-k} \Pr(B|E = e)\Pr(E = e)$.

Concerning the conditional event $\{A|E = e\}$, since $\mathbf{H}_{\bar{K}}$ is a $((n - k) \times e)$ matrix, we have $\Pr(A|E = e) = 1$ for $e > n - k$. Moreover, for $e \leq n - k$ we have $\Pr(A|E = e) < 2^{-\delta}$ from Proposition 1. In conclusion, we may write

$$\Pr(A|E = e) \leq \min\{2^{-\delta}, 1\} \quad (4)$$

with equality if and only if $e > n - k$ and where the compact expression (4) allows δ to assume negative values. Consider now the conditional event $\{B|E = e\}$. Due to independence we have $\Pr(B|E = e) = \Pr(\mathrm{rank}(\mathbf{H}_{\bar{K}}) = e)\Pr(\text{undetected error}|E = e)$. Invoking again Proposition 1, for $e \leq n - k$, $\Pr(\mathrm{rank}(\mathbf{H}_{\bar{K}}) = e)$ can be bounded as

$$1 - 2^{-\delta} < \Pr(\mathrm{rank}(\mathbf{H}_{\bar{K}}) = e) \leq 1 - 2^{-\delta-1}. \quad (5)$$

Moreover, since for $E = e$ the submatrix $\mathbf{P}$ has dimension $((n - k - e) \times (n - e))$ (as depicted in Fig. 2) we have

$$\Pr(\text{undetected error}|E = e)$$
$$= \sum_{l=1}^{n-e} \binom{n-e}{l} 2^{-(n-k-e)} (p^*)^l (1 - p^*)^{n-e-l}$$
$$= 2^{-(n-k-e)} (1 - (1 - p^*)^{n-e}) \quad (6)$$

---

[3]Note that the dimension of the generic code belonging to $\mathcal{R}(n,k)$ is at most equal to k but not necessarily equal to k.

where $p^* = p/(1 - \epsilon)$ as defined in Section II. We obtain

$$\bar{P}_{f,\mathcal{R}(n,k)}^{\mathrm{d,BEEC}} < \sum_{e=1}^{n} \binom{n}{e} \epsilon^e (1-\epsilon)^{n-e} \min\{2^{-(n-k-e)}, 1\}$$

$$+ \sum_{e=0}^{n-k} \binom{n}{e} \epsilon^e (1-\epsilon)^{n-e} (1 - 2^{-(n-k-e+1)})$$

$$\times 2^{-(n-k-e)} (1 - (1-p^*)^{n-e}). \quad (7)$$

The bound is tight due to the tightness of the bounds in (3).

C. SEME Decoding over the BEEC

Besides error detection, correction of errors introduced by the BEEC may be attempted. In the following, we describe a decoding algorithm for the correction of single errors affecting $\mathbf{y}_K$ and of multiple erasures. The algorithm is called SEME decoding algorithm.

After a word $\mathbf{y}$ has been received from the BEEC, let us consider performing GJE on the matrix $\mathbf{H}_{\bar{K}}$, leading to $\tilde{\mathbf{H}}_{\bar{K}}$, and performing in parallel the same row operations on $\mathbf{H}_K$, leading to $\tilde{\mathbf{H}}_K$. As for Section III-A and Section III-B, assuming $e < n-k$ and $\mathrm{rank}(\mathbf{H}_{\bar{K}}) = e$, the linear system (1) is transformed into the equivalent system $\tilde{\mathbf{y}}_{\bar{K}} \tilde{\mathbf{H}}_{\bar{K}}^T = \mathbf{y}_K \tilde{\mathbf{H}}_K^T$, whose right-hand side is denoted again by $\tilde{\mathbf{s}} = [\tilde{\mathbf{s}}_U | \tilde{\mathbf{s}}_L]$ and where $\tilde{\mathbf{H}}_K^T = [\mathbf{Q}^T | \mathbf{P}^T]$ as depicted in Fig. 2.

Let us now focus on the last $n - k - e$ parity-check equations, assuming $\mathrm{rank}(\mathbf{H}_{\bar{K}}) = e$. Due to the presence of an $((n - k - e) \times e)$ all-zero matrix in the last $n - k - e$ rows of $\tilde{\mathbf{H}}_{\bar{K}}$, these parity-check equations may be exploited to correct errors affecting $\mathbf{y}_K$ regardless erasures. In a similar way as error detection described in the previous subsection, error correction may be attempted by exploiting the matrix $\mathbf{P}$. Note in fact that the situation is now equivalent to the transmission over a standard BSC of an $(n - e, k')$ linear block code $\mathcal{C}'$, with $k' \geq k$ and parity-check matrix $\mathbf{P}$. The vector $\mathbf{x}_K$ plays the role of the transmitted codeword, $\mathbf{y}_K$ of the received word, and $\tilde{\mathbf{s}}_L$ of the syndrome. The code $\mathcal{C}'$, and therefore its properties and its error correction (and detection) capability, depend on the number and the positions of bit coordinates erased by the BEEC.

Optimum decoding of $\mathcal{C}'$ may be performed, in principle, via syndrome decoding [25], which requires the construction of a decoding table-lookup. Since $\mathcal{C}'$ is different for different received words $\mathbf{y}$, the table-lookup for $\mathcal{C}'$ should be constructed *on-the-fly* for each received word, after GJE has been performed. However, in a sporadic error regime, performing the correction of only error patterns of Hamming weight 1 may be sufficient: As illustrated in Section VI, it yields a much better performance than that achieved under a simple BEC model, where all elements of $\mathbf{y}_K$ are assumed to be uncorrupted so that all errors are undetected. The key point is that, in the single error correction case, the construction on-the-fly of the table-lookup does not require any extra computation, because the syndrome vectors associated with the weight-1 error patterns are the columns of the $\mathbf{P}$ matrix. Therefore, if there exists a unique column $\mathbf{b}$ of $\mathbf{P}$ such that $\mathbf{b} = \tilde{\mathbf{s}}_L^T$, then decoding consists of setting $\hat{\mathbf{x}}_K = \mathbf{y}_K + \hat{\mathbf{e}}$,

where $\hat{\mathbf{e}}$ is the vector of Hamming weight 1 whose unique bit equal to '1' corresponds to the column $\mathbf{b}$ of $\mathbf{P}$. The vector $\hat{\mathbf{x}}_K$ is then used to recover the vector $\mathbf{x}_{\bar{K}}$ through the first e equations of the equivalent system, i.e., by simply setting $\hat{\mathbf{x}}_{\bar{K}}$ equal to the de-permuted version of $\tilde{\mathbf{y}}_{\bar{K}} = \hat{\mathbf{x}}_K \mathbf{Q}^T$.

Note that, if $\mathbf{P}$ has no all-zero columns and no two columns of $\mathbf{P}$ are equal, then $\mathcal{C}'$ has minimum distance $d_{\min} \geq 3$ and all single error patterns are correctable with probability 1. In this case, an error pattern $\hat{\mathbf{e}}$ is always identified. On the other hand, if $\mathbf{P}$ has no all-zero columns but it has equal columns, then $\mathcal{C}'$ has minimum distance $d_{\min} = 2$. In this case, a unique $\mathbf{b}$ may not exist and the algorithm may be able to only detect some single error patterns. Finally, if $\mathbf{P}$ has all-zero columns then $\mathcal{C}'$ has minimum distance $d_{\min} = 1$ and some error patterns of Hamming weight 1 may be even not detected.

IV. PERFORMANCE BOUND FOR BINARY RANDOM LINEAR BLOCK CODES UNDER SEME DECODING

We now derive a tight upper bound on the average block error probability under SEME decoding for the same ensemble $\mathcal{R}(n, k)$ introduced in Section III-B. Note that by "block error" we denote any instance in which decoding is either not feasible (due to rank deficiency of the matrix $\mathbf{H}_{\bar{K}}$ or due to detectable but uncorrectable errors) or incorrect (due to undetected errors). To proceed with the derivation, we first determine four mutually exclusive block error events, denoted by A, B, C and D, which cover all possible error types. This allows us to write the average block error probability as

$$\bar{P}_{e,\mathcal{R}(n,k)}^{\mathrm{SEME,BEEC}} = \Pr(A) + \Pr(B) + \Pr(C) + \Pr(D).$$

The four error events are defined as follows.

A: $\{\mathrm{rank}(\mathbf{H}_{\bar{K}} < E)\}$.
B: $\{\mathrm{rank}(\mathbf{H}_{\bar{K}}) = E\} \cap \{L > 1\}$.
C: $\{\mathrm{rank}(\mathbf{H}_{\bar{K}}) = E\} \cap \{L = 1\} \cap \{\mathrm{rank}([\mathbf{H}_{\bar{K}} | \mathbf{h}^{\mathrm{err}}]) = E\}$.
D: $\{\mathrm{rank}(\mathbf{H}_{\bar{K}}) = E\} \cap \{L = 1\} \cap \{\mathrm{rank}([\mathbf{H}_{\bar{K}} | \mathbf{h}^{\mathrm{err}}]) = E + 1\} \cap \{\mathbf{b} \text{ is not unique in } \mathbf{P}\}$.

Note that C is the event that a single error on $\mathbf{y}_K$ is undetectable, while D is the event that a single error on $\mathbf{y}_K$ is detectable but not correctable. In the following subsections, we develop the four conditional probabilities $\Pr(A|E = e)$, $\Pr(B|E = e)$, $\Pr(C|E = e)$, $\Pr(D|E = e)$, from which $\bar{P}_{e,\mathcal{R}(n,k)}^{\mathrm{SEME,BEEC}}$ can be obtained as

$$\bar{P}_{e,\mathcal{R}(n,k)}^{\mathrm{SEME,BEEC}} = \sum_{e=1}^{n} \Pr(A|E = e) \Pr(E = e)$$

$$+ \sum_{Z \in \{B,C,D\}} \sum_{e=0}^{n-k} \Pr(Z|E = e) \Pr(E = e). \quad (8)$$

Even though in principle it would be possible to develop exact expressions for the conditional probabilities using (2), we derive upper bounds which exploit again the upper bound in (3). The resulting bound on $\bar{P}_{e,\mathcal{R}(n,k)}^{\mathrm{SEME,BEEC}}$ is tight and much

simpler to implement. As illustrated in Section VI, the bound is useful also to predict the performance of LDPC codes under SEME decoding.

Conditional event $\{A|E = e\}$: The calculation is the same as for the conditional event $\{A|E = e\}$ in Section III-B, yielding again (4).

Conditional event $\{B|E = e\}$: Due to independence, we have

$$\Pr(B|E = e) = \Pr(\text{rank}(\mathbf{H}_{\bar{K}}) = e)\Pr(L > 1|E = e).$$

For $e \leq n - k$, $\Pr(\text{rank}(\mathbf{H}_{\bar{K}}) = e)$ can be bounded again as in (5). Moreover, we have

$$\Pr(L > 1|E = e) = 1 - (1-p^*)^{n-e} - (n-e)p^*(1-p^*)^{n-e-1}$$

where $p^* = p/(1 - \epsilon)$ as from Section II. Hence, we can upper bound $\Pr(B|E = e)$ as

$$\Pr(B|E = e) \leq (1 - 2^{-\delta-1})$$
$$\times [1 - (1-p^*)^{n-e} - (n-e)p^*(1-p^*)^{n-e-1}]. \tag{9}$$

Conditional event $\{C|E = e\}$: We have

$$\Pr(C|E = e) = \Pr(\text{rank}(\mathbf{H}_{\bar{K}}|\mathbf{h}^{\text{err}}) = e|\text{rank}(\mathbf{H}_{\bar{K}} = e))$$
$$\times \Pr(\text{rank}(\mathbf{H}_{\bar{K}} = e))\Pr(L = 1|E = e).$$

For $e \leq n - k$, we can write

$$\Pr(\text{rank}(\mathbf{H}_{\bar{K}}|\mathbf{h}^{\text{err}}) = e|\text{rank}(\mathbf{H}_{\bar{K}} = e)) = 2^{-\delta}$$

and

$$\Pr(\text{rank}(\mathbf{H}_{\bar{K}} = e)) \leq 1 - 2^{-\delta-1}$$

which, combined with $\Pr(L = 1|E = e) = (n-e)p^*(1 - p^*)^{n-e-1}$ yields

$$\Pr(C|E = e) \leq 2^{-\delta}(1 - 2^{-\delta-1})(n-e)p^*(1-p^*)^{n-e-1}. \tag{10}$$

Conditional event $\{D|E = e\}$: Due to independence, we may write

$$\Pr(D|E = e) = \Pr(\text{rank}(\mathbf{H}_{\bar{K}}|\mathbf{h}^{\text{err}}) = e + 1)$$
$$\times \Pr(L = 1|E = e)\Pr(\mathbf{b} \text{ is not unique in } \mathbf{P}|E = e, L = 1).$$

For $e \leq n - k$ we have

$$\Pr(\text{rank}(\mathbf{H}_{\bar{K}}|\mathbf{h}^{\text{err}}) = e + 1) \leq 1 - 2^{-\delta}$$

and

$$\Pr(\mathbf{b} \text{ is not unique in } \mathbf{P}|E = e, L = 1) = 1 - (1 - 2^{-\delta})^{n-e-1}$$

that yield

$$\Pr(D|E = e) \leq (1 - 2^{-\delta})(n-e)p^*(1-p^*)^{n-e-1}$$
$$\times [1 - (1 - 2^{-\delta})^{n-e-1}]. \tag{11}$$

Substituting (4), (9), (10) and (11) into (8), $\bar{P}_{e,\mathcal{R}(n,k)}^{\text{SEME},\text{BEEC}}$ can be upper bounded as

$$\bar{P}_{e,\mathcal{R}(n,k)}^{\text{SEME},\text{BEEC}}$$
$$< \sum_{e=1}^{n} \binom{n}{e}\epsilon^e(1-\epsilon)^{n-e}\min\{2^{-(n-k-e)}, 1\}$$
$$+ \sum_{e=0}^{n-k} \binom{n}{e}\epsilon^e(1-\epsilon)^{n-e}(1 - 2^{-(n-k-e+1)})$$
$$\times [1 - (1-p^*)^{n-e} - (n-e)p^*(1-p^*)^{n-e-1}]$$
$$+ \sum_{e=0}^{n-k} \binom{n}{e}\epsilon^e(1-\epsilon)^{n-e}2^{-(n-k-e)}(1 - 2^{-(n-k-e+1)})$$
$$\times (n-e)p^*(1-p^*)^{n-e-1}$$
$$+ \sum_{e=0}^{n-k} \binom{n}{e}\epsilon^e(1-\epsilon)^{n-e}(1 - 2^{-(n-k-e)})(n-e)$$
$$\times p^*(1-p^*)^{n-e-1}[1 - (1 - 2^{-(n-k-e)})^{n-e-1}]. \tag{12}$$

Due to the tightness of the bounds (5), the bound (12) is also tight. Moreover, it is illustrated that, for sufficiently small values of ϵ, the right-hand side of (12) is dominated by the second summand, i.e. by the upper bound on the probability $P(B)$ that the number of errors on $\mathbf{y}_K$ is larger than one, giving rise to an error floor. The value of this error floor may be easily expressed analytically as the limit of the second summand in (12) when $\epsilon \to 0$. This yields

$$\bar{P}_{e,\mathcal{R}(n,k)}^{\text{SEME},\text{BEEC}} \approx (1 - 2^{-(n-k+1)})[-n\,p\,(1-p)^{n-1}$$
$$+ p\,(1-p)^{n-1} - (1-p)^{n-1} + 1]. \tag{13}$$

Finally note that, for a standard BEC introducing no errors, we have $p^* = 0$ so that only the first summation contributes to the bound. This yields

$$\bar{P}_{e,\mathcal{R}(n,k)}^{\text{ML},\text{BEC}} < \sum_{e=1}^{n} \binom{n}{e}\epsilon^e(1-\epsilon)^{n-e}\min\{2^{-(n-k-e)}, 1\}$$
$$= \sum_{e=1}^{n-k} \binom{n}{e}\epsilon^e(1-\epsilon)^{n-e}2^{-(n-k-e)}$$
$$+ \sum_{e=n-k+1}^{n} \binom{n}{e}\epsilon^e(1-\epsilon)^{n-e} \tag{14}$$

which is a tight upper bound on the average performance of linear random block codes over the BEC [23].[4]

V. EFFICIENT SEME DECODING OF LDPC CODES

Again, let us assume at first that the communication channel is a standard BEC introducing erasures but not errors ($p = 0$). ML decoding of LDPC codes over the BEC can be practically implemented following a reduced complexity approach [8] which exploits the sparseness of the parity-check matrix and which takes its inspiration from a class

[4]It is worthwhile pointing out that the bound (14) also holds for the ensemble of binary nonlinear codes of length n and 2^k codewords [26].

of structured GJE algorithms [27]. The algorithm may be summarized in the following three steps.

1. *Triangularization.* The sparse matrix $\mathbf{H}_{\bar{K}}$ is transformed into an approximate triangular matrix, as depicted in Fig. 3(b) by row and column permutations only. The obtained matrix is composed of a lower triangular matrix $\mathbf{T}$ and of the three sparse matrices $\mathbf{C}$, $\mathbf{R}_U$, $\mathbf{R}_L$. Some of the columns blocking the triangularization process have been moved to the rightmost part of $\mathbf{H}_{\bar{K}}$ and hence form $[\mathbf{R}_U^T|\mathbf{R}_L^T]^T$. The α unknowns associated with such columns are referred to as the *pivots*.

2. *Sparse row additions.* $\mathbf{T}$ is transformed into an identity matrix by sparse row additions. Moreover, $\mathbf{C}$ is made equal to the zero matrix by sparse row additions, leading to the matrix depicted in Fig. 3(c). Note that, due to the row additions, both $\mathbf{R}_U$ and $\mathbf{R}_L$ may no longer be sparse.

3. *GJE on a dense matrix.* GJE is applied to $\mathbf{R}_L$ to recover the α pivots. The remaining $e - \alpha$ unknowns are solved by simple substitution.

During the triangularization step, the elements of the vector $\mathbf{s}^T = \mathbf{H}_K \mathbf{y}_K^T$ are permuted according to the same row permutations performed on $\mathbf{H}_{\bar{K}}$. Similarly, during the sparse row addition and GJE steps, the elements of $\mathbf{s}^T$ are summed according to the row additions performed on $\mathbf{H}_{\bar{K}}$, leading to $\tilde{\mathbf{s}}^T = [\tilde{\mathbf{s}}_U, \tilde{\mathbf{s}}_L]^T$ as depicted in Fig. 4.

The complexity of the algorithm is dominated by the third step, consisting of performing GJE on a (usually) dense matrix. Therefore, the effectiveness of this approach relies on one's capability to considerably reduce the number of columns of $\mathbf{R}_L$, on which brute-force GJE has to be applied. The number of columns of $\mathbf{R}_L$ at the end of the process depends on the adopted *pivoting* algorithm, i.e. on the procedure to select the pivots during the triangularization step. Having a strong impact on the final number α of pivots, it heavily influences the achievable decoder speed. Effective pivoting algorithms are described in [28, Annex E] and in [12], where a practical software ML erasure decoder implementation has been demonstrated with $(2048, 1024)$ LDPC code, for which decoding rates as high as 1.5 Gbps were achieved.

Over the BEC, a decoding failure may take place only if the rank of $\mathbf{R}_L$ is smaller than α. Over the BEEC, error detection can be performed, as for the general linear block code case, by simply checking whether $\tilde{\mathbf{s}}_L$ is the all-zero vector or not, where $\tilde{\mathbf{s}}_L$ the vector composed by the last $n - k - e$ symbols of $\tilde{\mathbf{s}}$ (see Fig. 4). Moreover, if the row additions/permutations performed on the sparse matrix $\mathbf{H}_{\bar{K}}$ are simultaneously applied to the sparse matrix $\mathbf{H}_K$, single error correction can be attempted by the SEME algorithm as for the general linear block code case. Again, the syndrome vectors of the table look-up used to correct single errors are given by the columns of the $((n-k-e) \times (n-e))$ matrix $\mathbf{P}$ depicted in Fig. 4 and the algorithm sets $\hat{\mathbf{x}}_K = \mathbf{y}_K + \hat{\mathbf{e}}$, where $\hat{\mathbf{e}}$ is the error pattern whose unique '1' bit corresponds
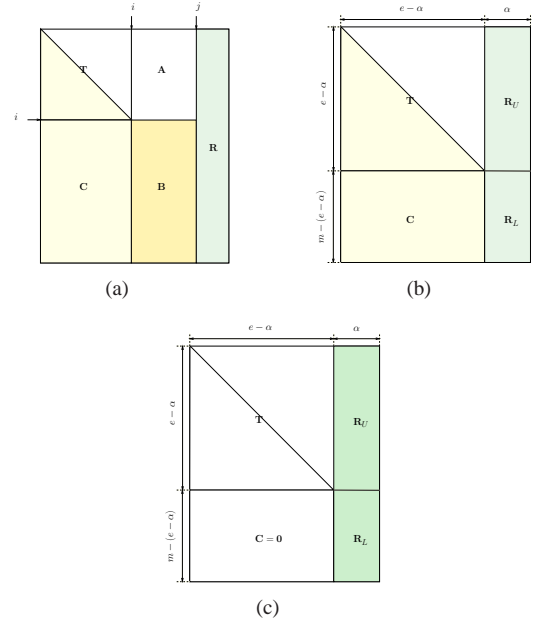

Fig. 3. Efficient Gaussian elimination steps on the $((n - k) \times e)$ matrix $\mathbf{H}_{\bar{K}}$. (a): Structure of $\mathbf{H}_{\bar{K}}$ during the triangularization step. (b): Structure of $\mathbf{H}_{\bar{K}}$ at the end of the triangularization step. (c): Structure of $\mathbf{H}_{\bar{K}}$ at the end of the sparse row addition step. In the figure $m = n - k$.
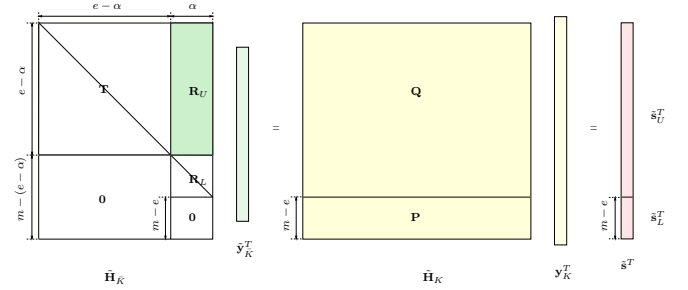

Fig. 4. Structure of the matrices $\tilde{\mathbf{H}}_K, \tilde{\mathbf{H}}_{\bar{K}}$. In the figure $m = n - k$.

to the unique column $\mathbf{b}$ of $\mathbf{P}$ such that $\mathbf{b} = \tilde{\mathbf{s}}_L$, provided such a unique column of $\mathbf{P}$ exists.

VI. PERFORMANCE OF LDPC CODES UNDER SEME DECODING

In Fig. 5, performance bounds for the $(2048, 1024)$ linear random ensemble are depicted, for both the BEC and a BEEC with error probability $p = 10^{-5}$. The performance is given in terms of block error probability, P_e. For the BEC, the upper bound (14) is displayed. For the BEEC, two cases are considered, namely:

- No error correction is attempted. In this case, P_e is simply the probability that the erasure pattern is not recoverable due to rank deficiency of $\mathbf{H}_{\bar{K}}$ plus the probability of the event $\{\text{rank}(\mathbf{H}_{\bar{K}}) = E\} \cap \{L \geq 1\}$.
- The SEME decoding algorithm is applied. In this case, the upper bound (12) is displayed. The contributions to the bound of the events B, C, D defined in Section IV are reported. Note that the contribution to the bound of
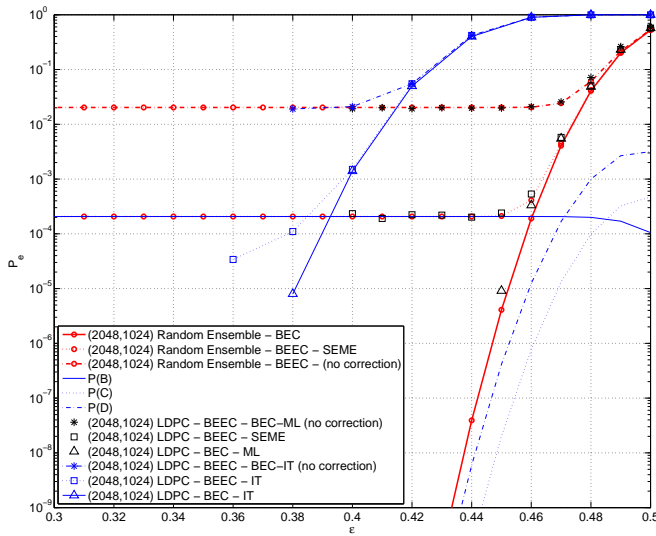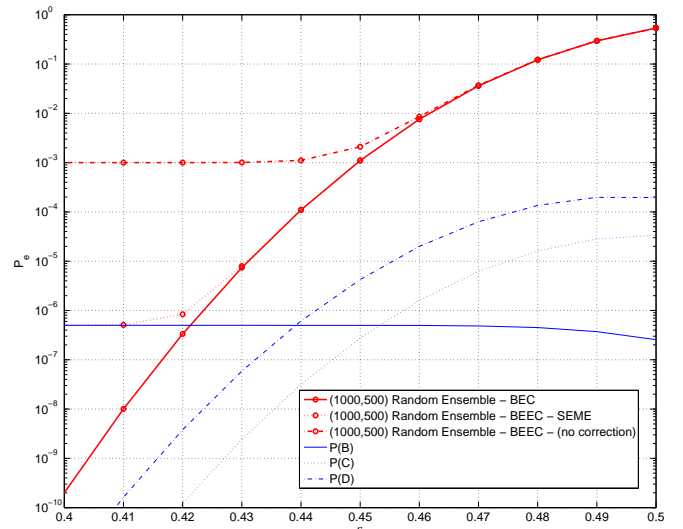
Fig. 5. Block error probability for a $(2048, 1024)$ GeIRA code over the BEC and over a BEEC with error probability $p = 10^{-5}$, under SEME and IT decoding. Comparison with the bounds on the block error probability for the $(2048, 1024)$ binary linear ensemble.

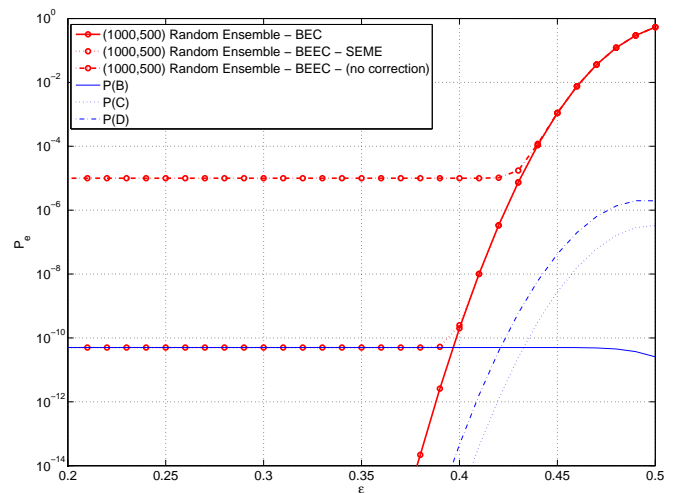the event A is equal to the already displayed right-hand side of (14).

The gain due to the single error correction capability of the SEME algorithm is evident in the error floor region. When no error correction is attempted, a high floor at $P_e \simeq n \cdot p \simeq 2 \cdot 10^{-2}$ affects the ensemble average error probability. On the other hand, if single error correction is performed, the floor is lowered by about two orders of magnitude. In this region the error probability for the SEME algorithm is dominated by the probability of the event B, i.e. by the probability that more than one error affects the non-erased bits. Conversely, in the waterfall region, most of the errors are due to rank deficiencies of the matrix $\mathbf{H}_{\bar{K}}$ and the error probability is dominated by the probability of the event A.

In Fig. 5, simulation results are also provided for a $(2048, 1024)$ GeIRA code [29] designed for ML erasure decoding [9]. The code performance has been simulated over the BEC under efficient ML decoding, and over the BEEC both under SEME decoding and without error correction. The simulation results illustrate how LDPC codes can approach the average random code ensemble performance in the three cases, at least down to moderate to low block error probabilities.[5] The performance of the same LDPC code under IT decoding is provided too, for three cases: On the BEC ($p = 0$), on the BEEC with IT erasure decoding (i.e., no error correction), and on the BEEC with input LLRs set according to the channel error/erasure probabilities (as briefly outlined in Section I). The performance under IT decoding on the BEC shows clearly a coding gain loss with respect to the ML counterpart. A block error rate $P_e = 10^{-4}$ is achieved by the IT decoder at $\epsilon \simeq 0.39$, whereas under ML

[5]At low error probabilities, LDPC codes over the BEC under ML decoding exhibit an error floor that is due to their non-ideal minimum distance. Therefore, their performance curve deviates from the bound (14).

(a) $p = 10^{-6}$.

(b) $p = 10^{-8}$.

Fig. 6. Bounds on the block error probability for the $(1000, 500)$ binary linear ensemble over the BEC and BEEC with various error probabilities.

decoding the target is achieved at $\epsilon \simeq 0.46$. On the BEEC channel, the SEME decoder outperforms the IT one down to moderate error rates. As the erasure probability decreases, the performance of the SEME algorithm converges to a block error probability $P_e \simeq 2 \cdot 10^{-4}$, due to the imposed single error correction capability of the algorithm. Since the IT decoder is not limited to correct single errors, at low erasure probabilities it outperforms the SEME algorithm. This effect may be exploited by a hybrid SEME/IT decoder, e.g. the IT decoder might be used whenever multiple errors are detected by the SEME decoder.

Still, in many practical cases, the BEEC error probability may be quite below $p = 10^{-5}$, resulting in a (much) lower error floor for the SEME algorithm, thus reducing the need for an IT decoding stage. In fact, the gain in the error floor due to the single error correction capability of the SEME algorithm is amplified at lower error probabilities

p. In Fig. 6(a) and Fig. 6(b), the bounds for the average random ensemble block error probability are displayed for the case of $n = 1000, k = 500$ and for two BEEC error probabilities, $p = 10^{-6}$ and $p = 10^{-8}$. While in the former case, the floor is reduced by 3 orders of magnitude, in the latter case under SEME decoding the block error probability meets the floor at $P_e < 10^{-10}$, about 5 orders of magnitude lower with respect to the case when no error correction is performed. Note that (13) provides an accurate estimation of the error floor under SEME decoding. For example, for $n = 1000, k = 500, p = 10^{-6}$, the error floor estimated by (13) appears at $\bar{P}_{e,\mathcal{R}(n,k)}^{\text{SEME},\text{BEEC}} \approx 4.99 \cdot 10^{-7}$, while for $n = 1000, k = 500, p = 10^{-8}$ at $\bar{P}_{e,\mathcal{R}(n,k)}^{\text{SEME},\text{BEEC}} \approx 5 \cdot 10^{-11}$. This is in accordance with Figures 6(a) and 6(b).

VII. CONCLUSION

We proposed an efficient single-error multiple-erasures (SEME) decoding algorithm for LDPC codes. The proposed algorithm represents an extension of the efficient ML decoding algorithm for LDPC codes over the BEC of [8], which allows error correction/detection on the BEEC. The block error rate of LDPC codes has been compared to the average block error probability for the random code ensemble over BEECs with sporadic errors, showing that LDPC codes can attain the performance of random codes under SEME decoding. A performance comparison with IT decoding on the BEEC is provided, showing that down to moderate error rates the SEME algorithm brings to a large coding gain with respect to IT decoding. The additional single error correction capability provided by the proposed algorithm allows to reduce the error floors by several orders of magnitude with respect to the case of pure erasure decoding.

Although for complexity reasons the algorithm has been analyzed imposing a single error correction limitation, it may be easily extended to correct multiple errors whenever a higher decoding complexity is affordable by the receiver. To make the algorithm capable of correcting multiple errors, it is sufficient to generate *on-the-fly* a decoding table-lookup up to the desired weight of the error pattern. This usually results in a heavy improvement of the error floor performance. For example, assuming again $p = 10^{-5}$ and letting the algorithm correct single and double errors, the error floor for the LDPC code in Fig. 5 would be lowered to about $\bar{P}_{e,\mathcal{R}(n,k)}^{\text{SEME},\text{BEEC}} \approx 1.4 \cdot 10^{-6}$.

REFERENCES

[1] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: M.I.T. Press, 1963.

[2] N. Alon and M. G. Luby, "A linear time erasure-resilient code with nearly optimal recovery," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1732–1736, Nov. 1996.

[3] M. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 585–598, Feb. 2001.

[4] H. D. Pfister, I. Sason, and R. Urbanke, "Capacity-achieving ensembles for the binary erasure channel with bounded complexity," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2352–2379, Jul. 2005.

[5] C. Di, D. Proietti, I. Telatar, T. Richardson, and R. 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.

[6] H. Pishro-Nik and F. Fekri, "On decoding of low-density parity-check codes over the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 439–454, Mar. 2004.

[7] E. Paolini and M. Chiani, "Construction of near-optimum burst erasure correcting low-density parity-check codes," *IEEE Trans. Commun.*, vol. 57, no. 5, pp. 1320–1328, May 2009.

[8] D. Burshtein and G. Miller, "An efficient maximum likelihood decoding of LDPC codes over the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2837–2844, Nov. 2004.

[9] E. Paolini, G. Liva, B. Matuz, and M. Chiani, "Generalized IRA erasure correcting codes for hybrid iterative / maximum likelihood decoding," *IEEE Commun. Lett.*, vol. 12, no. 6, pp. 450–452, Jun. 2008.

[10] A. Soro, M. Cunche, J. Lacan, and V. Roca, "Erasure codes with a banded structure for hybrid iterative-ML decoding," in *Proc. of 2009 IEEE Global Telecommunications Conf.*, Honolulu, HI, USA, Nov./Dec. 2009, pp. 1–6.

[11] E. R. Berlekamp, *Algerbraic Coding Theory*. McGraw-Hill, 1968.

[12] B. Matuz, G. Liva, E. Paolini, and M. Chiani, "Pivoting algorithms for maximum likelihood decoding of LDPC codes over erasure channels," in *Proc. of 2009 IEEE Global Telecommunications Conf.*, Honolulu, HI, USA, Nov./Dec. 2009, pp. 1–6.

[13] C. Measson, A. Montanari, and R. Urbanke, "Maxwell construction: The hidden bridge between iterative and maximum a posteriori decoding," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5277–5307, Dec. 2008.

[14] L. Rizzo, "Effective erasure codes for reliable computer communication protocols," *ACM Comput. Commun. Rev.*, vol. 27, no. 2, pp. 24–36, Apr. 1997.

[15] J. Massey, "Capacity, cutoff rate, and coding for a direct-detection optical channel," *IEEE Trans. Commun.*, vol. 29, no. 11, pp. 1615–1621, Nov. 1981.

[16] R. McEliece, "Practical codes for photon communication," *IEEE Trans. Inf. Theory*, vol. 27, no. 4, pp. 393–398, Jul. 1981.

[17] J. K. Wolf and R. Blakeney, "An exact evaluation of the probability of undetected error for certain shortened binary CRC codes," in *Proc. of IEEE Military Communications Conf.*, San Diego, CA, USA, Oct. 1988, pp. 287–292.

[18] G. Forney, "Exponential error bounds for erasure, list, and decision feedback schemes," *IEEE Trans. Inf. Theory*, vol. 14, no. 2, pp. 206–220, Mar. 1968.

[19] I. Telatar and R. Gallager, "New exponential upper bounds to error and erasure probabilities," in *Proc. of 1994 IEEE Int. Symp. on Information Theory*, Trondheim, Norway, Jun./Jul. 1994, p. 379.

[20] B. Nakiboğlu and L. Zheng, "Errors-and-erasures decoding for block codes with feedback," in *Proc. of 2008 IEEE Int. Symp. on Information Theory*, Toronto, Canada, Jul. 2008, pp. 712–716.

[21] K. A. Abdel-Ghaffar and J. H. Weber, "Separating erasures from errors for decoding," in *Proc. of 2008 IEEE Int. Symp. on Information Theory*, Toronto, Canada, Jul. 2008, pp. 215–219.

[22] G. Lansberg, "Uber eine anzahlbestimmung und eine damit zusammenhangende reihe," *Journal fur die reine und angewandte Mathematic*, vol. 3, pp. 87–88, 1893.

[23] E. Berlekamp, "The technology of error-correcting codes," *Proc. IEEE*, vol. 68, no. 5, pp. 564–593, May 1980.

[24] G. Liva, E. Paolini, and M. Chiani, "Performance versus overhead for fountain codes over $\mathbb{F}_q$," *IEEE Commun. Lett.*, vol. 14, no. 2, pp. 178–180, Feb. 2010.

[25] S. Lin and D. J. Costello, Jr., *Error Control Coding*. Prentice Hall, Englewood Cliffs, NJ., 2004, second edition.

[26] S. J. MacMullan and O. M. Collins, "A comparison of known codes, random codes, and the best codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 3009–3022, Nov. 1998.

[27] B. LaMacchia and A. Odlyzko, "Solving large sparse linear systems over finite fields," in *Proc. of Advances in Cryptology: CRYPTO'90 (Lecture Notes in Computer Science),* A. Menezes and S. Vanstone, Eds. Berlin, Germany: Springer-Verlag, vol. 537, 1991, pp. 109–133.

[28] 3GPP TS 26.346 V8.0.0, "Technical specification group services and system aspects; multimedia broadcast/multicast service; protocols and codecs," Sep. 2008.

[29] G. Liva, E. Paolini, and M. Chiani, "Simple reconfigurable low-density parity-check codes," *IEEE Commun. Lett.*, vol. 9, no. 3, pp. 258–260, Mar. 2005.