Binary Message Passing Decoding of Product Codes Based on Generalized Minimum Distance Decoding: (Invited Paper)

Downloaded from: https://research.chalmers.se, 2019-08-11 18:32 UTC

Citation for the original published paper (version of record):
Binary Message Passing Decoding of Product Codes Based on Generalized Minimum Distance Decoding: (Invited Paper)
53rd Annual Conference on Information Sciences and Systems, CISS 2019
http://dx.doi.org/10.1109/CISS.2019.8692862

N.B. When citing this work, cite the original published paper.
Binary Message Passing Decoding of Product Codes Based on Generalized Minimum Distance Decoding

Alireza Sheikh§, Alexandre Graell i Amat§, and Gianluigi Liva†
§ Department of Electrical Engineering, Chalmers University of Technology, Sweden
† Institute of Communications and Navigation of the German Aerospace Center (DLR), Germany

(Invited Paper)

Abstract—We propose a binary message passing decoding algorithm for product codes based on generalized minimum distance decoding (GMDD) of the component codes, where the last stage of the GMDD makes a decision based on the Hamming distance metric. The proposed algorithm closes half of the gap between conventional iterative bounded distance decoding (iBDD) and turbo product decoding based on the Chase–Pyndiah algorithm, at the expense of some increase in complexity. Furthermore, the proposed algorithm entails only a limited increase in data flow compared to iBDD.

I. INTRODUCTION

Applications requiring very high throughputs, such as fiber-optic communications and high-speed wireless communications, have recently triggered a significant amount of research on low-complexity decoders. While codes-on-graphs such as low-density parity-check (LDPC) codes and turbo codes have been shown to provide close-to-capacity performance under belief propagation (BP) decoding, scaling their BP decoders to yield throughputs of the order of several Gbps or even 1 Tbps, as required for example for the future optical metro-networks, is a very challenging task. One of the main bottlenecks is the data flow required by the exchange of soft information in the iterative BP decoding. This has spurred a great deal of research in novel low-complexity decoding algorithms.

Several works have attempted to reduce the decoding complexity of BP decoding of LDPC codes, see, e.g., [1]–[4]. For high-throughput applications, an alternative to LDPC codes with (BP) soft decision decoding (SDD) is to consider hard decision decoding (HDD). Product codes (PCs) [5], half-product codes [6], staircase codes [7], braided codes [8], and other product-like code structures [9] with HDD based on bounded distance decoding (BDD) of the component codes (which we refer here to as iterative BDD (iBDD)) yield excellent performance with a significantly reduced data flow, hence achieving very high throughputs. However, this comes at the expense of a performance loss (typically larger than 1 dB) compared to SDD.

To close the performance gap between iBDD of product-like codes and SDD of LDPC codes or product-like codes, yet with throughputs and energy consumption close to that of iBDD, another line of research recently explored is to improve the performance of the conventional iBDD. In [10], an algorithm that exploits conflicts between component codes in order to assess their reliabilities even when no channel reliability information is available, was proposed. The algorithm, dubbed anchor decoding (AD), improves the performance of iBDD at the expense of some increase in decoding complexity. In [11], a decoding algorithm based on marking the least reliable bits was proposed for staircase codes. In [12], we proposed a decoding algorithm based on BDD of the component codes, named iBDD with scaled reliability (iBDD-SR). The algorithm in [12] improves the performance of iBDD by exploiting channel reliabilities as proposed in [13] for LDPC codes, while still only exchanging binary (i.e., hard-decision) messages between component decoders, similar to iBDD. iBDD-SR improves upon iBDD and AD, and achieves the same throughput of iBDD with a slight increase in energy consumption [14]. In [15], we proposed an algorithm based on generalized minimum distance decoding (GMDD) of the component codes. The proposed algorithm closes over 50% of the performance gap between iBDD and turbo product decoding (TPD) based on the Chase–Pyndiah algorithm [16], with lower complexity than TPD. However, the algorithm, which we referred to as iterative GMDD with scaled reliability (iGMDD-SR), requires the exchange of soft information between the component decoders and hence entails a decoder data flow equivalent to that of TPD and significantly higher than that of iBDD.

In this paper, we propose a novel binary message passing (BMP) decoding algorithm for product codes based on GMDD of the component codes, which we refer to as BMP-GMDD. The proposed algorithm follows the same principle as the iGMDD-SR algorithm proposed in [15], but a crucial difference is that the Hamming distance metric is used at the final stage of the GMDD of the component codes. In contrast to iGMDD-SR, the resulting algorithm does not require the exchange of soft information, but the exchange of the hard decisions on the code bits (as conventional iBDD) and an ordered list of the \( d_{\text{min}} - 1 \) least reliable code bits for each component code, where \( d_{\text{min}} \) is the minimum Hamming distance of the component code. This list can be represented by a small number of bits. The proposed algorithm yields performance very close to that of iGMDD-SR, closing 50% of

This work was financially supported by the Knut and Alice Wallenberg Foundation, the Swedish Research Council under grant 2016-04253, and the Ericsson Research Foundation.
the performance gap between iBDD and TPD, while entailing only a small increase in data flow compared to iBDD (between 8.5% and 34.3%, depending on the code parameters).

Notation: We use boldface letters to denote vectors and matrices, e.g., \( x \) and \( X = [x_{i,j}] \). The \( i \)-th row and \( j \)-th column of matrix \( X \) is denoted by \( X_{i,:} \) and \( X_{:,j} \), respectively. \(|a|\) denotes the absolute value of \( a \), \( \lfloor a \rfloor \) the largest integer smaller than or equal to \( a \), and \( \lceil a \rceil \) the smallest integer larger than or equal to \( a \). A Gaussian distribution with mean \( \mu \) and variance \( \sigma^2 \) is denoted by \( N(\mu, \sigma^2) \).

II. PRELIMINARIES

Let \( C \) be an \( (n, k, d_{\text{min}}) \) binary linear code, where \( n \), \( k \), and \( d_{\text{min}} \) are the code length, dimension, and minimum distance, respectively. We consider two-dimensional PCs with identical binary Bose–Chaudhuri–Hocquenghem (BCH) component code \( C \) for the row and column codes. Such a PC, of parameters \( (n^2, k^2, d_{\text{min}}^2) \) and rate \( R = k^2/n^2 \), is defined as the set of all \( n \times n \) arrays such that each row and each column of the array is a codeword of \( C \). Thus, a codeword of the PC can be represented by an \( n \times n \) binary matrix \( C = [c_{i,j}] \). Alternatively, a PC can be defined via a Tanner graph with \( 2n \) constraint nodes (CNs), where \( n \) CNs correspond to the row codes and \( n \) CNs correspond to the column codes. The graph has \( n^2 \) variable nodes (VNs) corresponding to the \( n^2 \) code bits. The code array and (simplified) Tanner graph of a two-dimensional PC with \( n = 6 \) is shown in Fig. 1.

We assume transmission over the binary-input additive white Gaussian noise (AWGN) channel. The channel observation corresponding to code bit \( c_{i,j} \) is given by

\[ y_{i,j} = x_{i,j} + z_{i,j}, \]

where \( x_{i,j} = (-1)^{c_{i,j}} \), \( z_{i,j} \sim N(0, (2R E_b/N_0)^{-1}) \), with \( E_b/N_0 \) being the signal to noise ratio. We denote by \( L = [L_{i,j}] \) the matrix of channel log-likelihood ratios (LLRs) and by \( R = [r_{i,j}] \) the matrix of hard decisions at the channel output, where \( r_{i,j} \) is obtained by mapping the sign of \( L_{i,j} \) according to \( 1 \mapsto 0 \) and \( -1 \mapsto 1 \). We denote this mapping by \( B(\cdot) \), i.e., \( r_{i,j} = B(L_{i,j}) \). With some abuse of notation, we also write \( R = B(L) \).

A. Generalized Minimum Distance Decoding

Consider the decoding of a BCH component code of length \( n \) and the vector of channel LLRs \( l = (L_1, \ldots, L_n) \) corresponding to the received vector \( r = (r_1, \ldots, r_n) \). GMDD is based on multiple algebraic error-erasure decoding attempts [17]. In particular, the decoder ranks the coded bits in terms of their reliabilities \( |L_1|, \ldots, |L_n| \). Then, the \( m \) least reliable bits in \( r \) are erased, where \( m \in \mathcal{M}_{\text{odd}} \) if \( d_{\text{min}} \) is odd and \( m \in \mathcal{M}_{\text{even}} \) if \( d_{\text{min}} \) is even. For later use, we denote by \( \mathcal{L} \) the ordered list of \( d_{\text{min}} - 1 \) least reliable code bits. It can be readily checked that \( |\mathcal{M}_{\text{odd}}| = |\mathcal{M}_{\text{even}}| = t \), where \( t = \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor \) is the error correcting capability of the code. Together with the received vector \( r \), this gives a list of \( t + 1 \) trial vectors \( \tilde{r}_i, i = 1, \ldots, t + 1 \), out of which \( t \) vectors contain both erasures and (possibly) errors. Finally, algebraic error-erasure decoding [18, Sec. 6.6] is applied to each trial vector \( \tilde{r}_i \), resulting in a set of candidate codewords, of size at most \( t + 1 \), denoted by \( \mathcal{S} \). If decoding fails for all \( t + 1 \) vectors in the list, a failure is declared. Otherwise, the decoder picks among all candidate codewords in \( \mathcal{S} \) the one that minimizes the generalized distance \( d_{\text{GD}}(r, c) \), [17]

\[
\hat{c} = \arg \min_{c \in \mathcal{S}} d_{\text{GD}}(r, c) = \arg \min_{c \in \mathcal{S}} \sum_{i:r_i=c_i} (1 - \alpha_i) + \sum_{i:r_i \neq c_i} (1 + \alpha_i),
\]

where \( \alpha_i = \frac{|L_i|}{\max_{1 \leq j \leq n} |L_j|} \). Note that if all input LLRs \( L_1, \ldots, L_n \) have the same magnitude, we have \( \alpha_i = 1 \) for all \( i = 1, \ldots, n \) and (1) reverts to 2\( d_{\text{h}}(r, \hat{c}) \), where \( d_{\text{h}}(r, \hat{c}) \) is the Hamming distance between \( r \) and \( \hat{c} \).

By introducing erasures and performing multiple error-erasure component decoding attempts, GMDD can decode beyond half the minimum distance of the code.

III. BINARY MESSAGE PASSING DECODING BASED ON GENERALIZED MINIMUM DISTANCE DECODING

In this section, we propose a BMP decoding algorithm for PCs based on GMDD of the component codes. We refer to it as BMP-GMDD. The algorithm follows the same principle as the iGMDD-SR algorithm that we proposed in [15]. However, compared to iGMDD-SR, the proposed BMP-GMDD does not require the exchange of the reliabilities on the code bits between the row and column decoders. To achieve that, rather than considering the generalized distance in (1) to perform the decision at the last stage of GMDD of the row and column decoders as in [15], we perform the decision based on the Hamming distance, i.e., among all candidate codewords in \( \mathcal{S} \) (see Section II-A), the decoder selects the one that minimizes \( d_{\text{h}}(r, c) \), i.e., the decision in (1) is substituted by

\[
\hat{c} = \arg \min_{c \in \mathcal{S}} d_{\text{h}}(r, c). \tag{2}
\]

Making the decision based on the Hamming distance instead of the generalized distance entails a small performance loss, as the decision does not take into consideration the normalized
reliabilities \( \alpha_k \). However, this allows to significantly reduce the decoder data flow, as explained later.

The proposed BMP-GMDD algorithm works as follows. Without loss of generality, assume that the decoding starts with the row codes and let us consider the decoding of the \( i \)-th row code at iteration \( \ell \). Let \( \Psi_i^{c,(\ell-1)} = [\psi_i^{c,(\ell-1)}] \) be the matrix of hard decisions on code bits \( c_{i,j} \) after the decoding of the \( n \) column codes at iteration \( \ell - 1 \). Also, let \( \mathcal{L}_i^{r,(\ell-1)} \) be the ordered list of \( d_{\min} - 1 \) least reliable bits of codeword \( C_{i,:} \) from the decoding of the column codes at iteration \( \ell - 1 \). Note that in the first iteration the list \( \mathcal{L}_i^{r,(\ell-1)} \) is built according to the ordering of the channel reliabilities \( L_{i,:} = (L_{i,1}, \ldots, L_{i,n}) \).

Row decoding of the \( i \)-th row code is then performed based on \( \Psi_i^{c,(\ell-1)} \) and \( \mathcal{L}_i^{r,(\ell-1)} \). First, BMPDD of the \( i \)-th row code based on the Hamming distance is performed based on \( \Psi_i^{c,(\ell-1)} \) and \( \mathcal{L}_i^{r,(\ell-1)} \), as explained in Section II-A (see (2)). Note that GMDD does not provide reliability information about the decoded bits, i.e., it is a soft-input hard-output decoding algorithm. In order to provide the column decoders with the list of \( m \) least reliable bits for each codeword \( C_{:,j} \) after the decoding of the row codes at iteration \( \ell \), we do the following. The output bits of GMDD are mapped according to \( 0 \mapsto +1 \) and \( 1 \mapsto -1 \) if GMDD is successful and mapped to 0 if GMDD fails. Let \( \bar{\mu}_{i,j}^{r,(\ell)} \in \{\pm 1, 0\} \) be the result of this mapping for the decoded bit corresponding to code bit \( c_{i,j} \). The reliability information is then formed according to

\[
\mu_{i,j}^{r,(\ell)} = w_{i}^{r,(\ell)} \cdot \bar{\mu}_{i,j}^{r,(\ell)} + L_{i,j},
\]

where \( w_{i}^{r,(\ell)} > 0 \) is a scaling factor than needs to be optimized. Then, the hard decision on \( c_{i,j} \) made by the \( i \)-th row decoder is formed as

\[
\psi_{i,j}^{r,(\ell)} = B(\mu_{i,j}^{r,(\ell)}).
\]

The hard decision \( \psi_{i,j}^{r,(\ell)} \) is the binary message on code bit \( c_{i,j} \) passed from the \( i \)-th row code to the \( j \)-th column code, i.e., from the \( i \)-th row CN to the \( j \)-th column CN (see Fig. 1). In particular, after applying this procedure to all row codes, the matrix \( \Psi_j^{r,(\ell)} = [\psi_{j}^{r,(\ell)}] \) is formed and used as the input for GMDD-SR of the \( j \)-th column code at iteration \( \ell \). Then, the \( m \) least reliable bits are stored in the list \( \mathcal{L}_j^{c,(\ell)} \), which is passed to the \( j \)-th column decoder.

The decoding of the \( n \) column codes at iteration \( \ell \) is then performed based on the hard decisions \( \Psi_j^{r,(\ell)} \) and the lists of least reliable bits \( \mathcal{L}_1^{r,(\ell)}, \ldots, \mathcal{L}_n^{r,(\ell)} \) as explained for the \( i \)-th row decoder above. After decoding of the \( n \) column codes at decoding iteration \( \ell \), the matrix \( \Psi_j^{c,(\ell)} = [\psi_{j}^{c,(\ell)}] \) of hard decision bits and the lists \( \mathcal{L}_1^{r,(\ell)}, \ldots, \mathcal{L}_n^{r,(\ell)} \) are passed to the \( n \) row decoders for the next decoding iteration. The iterative process continues until a maximum number of iterations is reached. The BMP-GMDD of PCs is schematized in Fig. 2.

Remark: With reference to Fig. 2, the iGMDD-SR algorithm proposed in [15] passes the soft information \( \mu_{i,j}^{r,(\ell)} \) to the \( j \)-th column decoder, which entails a significantly higher decoder data flow compared to BMP-GMDD.

IV. DECODING COMPLEXITY DISCUSSION

A thorough complexity analysis of BMP-GMDD should include, besides pure algorithmic aspects, implementation implications in terms of memory requirements, wiring, and transistor switching activity [14], and is beyond the scope of this paper. We however provide a high-level discussion of the complexity and data flow of BMP-GMDD compared to that of conventional iBDD, AD [10], iBDD-SR [12], and iGMDD-SR [15].

Conventional iBDD, iBDD-SR, and AD are based on BDD of the component codes and are characterized by a similar complexity and data flow. In particular, it was shown in [14] that for the same data throughput (up to 1 Tbps), iBDD-SR provides 0.2–0.25 dB gain with respect to iBDD with only slightly higher energy consumption.

Both GMDD-SR and the proposed BMP-GMDD are based on GMDD of the component codes. In this case, \( t \) error-erasure decoding attempts and one BDD attempt are required. Each error-erasure decoding attempt has a cost close to a run of BDD. Each decoding attempt may result in a candidate codeword that is used to form a list of size up to \( t+1 \), as explained in Section II-A. The minimization of the generalized distance in (1) for GMDD-SR and the Hamming distance in (2) for BMP-GMDD has a negligible cost with respect to the \( t+1 \) decoding attempts. On the other hand, both BMP-GMDD and iGMDD-SR require finding the \( d_{\min} - 1 \) least reliable bits and sorting them according to their reliabilities, which adds some further complexity.

Note that GMDD-SR requires the component decoders to be provided with soft information by the previous decoding iteration. Therefore, its data flow is significantly higher than that of iBDD, iBDD-SR, and AD, and is the same of soft decision TPD. For an \( a \)-bit representation of the soft information, the data flow is roughly \( a \times t \) times that of BDD, iBDD-SR, and AD. In contrast, BMP-GMDD requires only the exchange of the hard decisions and the ordered list of \( d_{\min} - 1 \) least reliable bits for each row and column codeword. For a component code of length \( n \), the index of each code bit can be represented with \( \lceil \log_2(n) \rceil \) bits. Furthermore, for each of the \( d_{\min} - 1 \) least reliable bits we need to provide their ordering in terms of
of reliabilities. Thus, each ordered lists \( L_i^{(t)} \), \( i = 1, \ldots, n \), and \( L_j^{(t)} = j, \ldots, n \), can be represented with

\[
(\lceil \log_2(n) \rceil + \lceil \log_2(d_{\min} - 1) \rceil)(d_{\min} - 1)
\]

bits each. This is the additional data flow (per row and column code decoding) compared to conventional iBDD. For instance, for a component code of code length \( n = 256 \) bits, the data flow of BMP-GDD is 15.625% and 34.375% higher than that of iBDD for \( d_{\min} = 5 \) \((t = 2)\) and \( d_{\min} = 9 \) \((t = 4)\), respectively. For a component code of length \( n = 512 \) bits, the increase in data flow is reduced to 8.593% and 18.75%, respectively. Thus, the increase in data flow of BMP-GMDD compared to iBDD is very limited and is much lower than the data flow of iGMDD-SR and conventional TPD.

V. NUMERICAL RESULTS

In Fig. 3, we give the bit error rate (BER) performance of BMP-GMDD for a PC with double-error-correcting extended BCH (eBCH) codes with parameters \((256, 239, 6)\) as component codes and transmission over the AWGN channel. The resulting PC has rate \( R = 239^2/256^2 \approx 0.8716 \). For comparison purposes, we also plot the performance of conventional iBDD, AD [10], iBDD-SR [12], iGMDD-SR [15], and TPD based on the Chase-Pyndiah decoding [16]. For all algorithms, a maximum of \( \ell_{\text{max}} = 10 \) decoding iterations is performed. As a reference, the Shannon limit for SDD and HDD is also plotted in the figure.

Both BMP-GMDD and iGMDD-SR require a proper choice of the scaling factors \( w_0^{(t)} \). For simplicity, we consider the same scaling factor for all row and column codes, i.e., \( w_0^{(t)} = w_0^{(1)} = w^{(t)} \) for all \( i, j = 1, \ldots, n \), and jointly optimize the vector \( w = (w^{(1)}, \ldots, w^{(\ell_{\text{max}})}) \) by using Monte-Carlo estimates of the BER for a fixed \( E_b/N_0 \) as the optimization criterion. Intuitively, one would expect that the decisions of the component decoders become more reliable with increasing number of iterations, whereas the channel observations become less informative. Therefore, in order to reduce the optimization search space, we only consider vectors \( w \) with monotonically increasing entries. iBDD-SR also requires scaling factors (see [12], [19]). In this case, the scaling factors can be derived using density evolution [13], [19].

The two reference curves are conventional iBDD (red curve with empty triangle markers) and TPD (purple curve with pentagon markers), with the latter performing 1.1 dB better at a BER of \( 10^{-7} \). AD (dark blue curve with filled circle markers) and iBDD-SR (pink curve with filled triangle markers) outperform conventional iBDD by 0.18 dB and 0.27 dB, respectively, at the same BER. As a reference, we also show the performance of ideal iBDD (brown curve with empty circle markers), where a genie prevents miscorrections. Interestingly, at a BER of \( 10^{-7} \) iBDD-SR yields the same performance as ideal iBDD.\(^1\) iGMDD-SR (green curve with diamond markers) outperforms iBDD, iBDD-SR, and AD and closes \( \approx 54\% \) of the gap between iBDD and TPD, at the expense of an increased complexity and data flow.

The performance of the proposed BMP-GMDD is given by the blue curve with square markers. The proposed decoding algorithm yields performance very close to that of iGMDD-SR (a performance degradation compared to iGMDD-SR of only 0.074 dB is observed at a BER of \( 10^{-7} \)), while achieving a significantly lower data flow. BMP-GMDD closes around

\(^1\)We remark that the performance of iBDD-SR in Fig. 3 is improved compared to [15], since in this paper we use the optimized scaling factors based on the density evolution derived in [19], rather than based on Monte-Carlo simulations as in [15].
50% of the performance gap between iBDD and TPD, while requiring only a 21.48% higher data throughput than iBDD.

The coding gain improvements of all considered decoding algorithms over iBDD are summarized in Table I (fifth column). In the table we also indicate whether the algorithms exploit the channel reliabilities or not, the nature of the messages exchanged in the iterative decoding (hard or soft), as well as the gap to capacity for all schemes (sixth column). Note that the performance of iBDD and AD should be compared to the hard decision (HD) capacity, while the performance of iBD-SR, iGMDD-SR, BMP-GMDD, and TPD should be compared to the soft decision (SD) capacity since the channel LLRs are exploited in the decoding. Overall, one can see a clear trade-off between BER performance and decoding complexity for the different algorithms.

We remark that if the channel LLRs are highly reliable but with wrong sign, one can expect that the decoding rule in (3) will be unable to recover from these errors. In this situation, although \( \hat{\mu}_{i,j}^r \) may correspond to a correct decision, it is overridden by the channel channel, i.e., the hard decision on code bit \( c_{i,j} \) made by the \( i \)-th row decoder, \( \psi_{i,j}^r \), becomes\[
\psi_{i,j}^r = B(w_i^r, \mu_{i,j}^r + L_{i,j}) = B(L_{i,j}) \text{ (cf. (3) and (4))},
\]leading to an erroneously decoded bit. Therefore, one needs to be careful when applying BMP-GMDD to avoid the appearance of an error floor. In particular, to avoid such errors and avoid a high error floor, we run BMP-GMDD for some iterations and then we append a few conventional iBDD iterations, where the channel reliabilities are disregarded when making the decision on a given code bit. The appended iBDD iterations increase the chance to correct transmission errors with high channel reliability. By doing so, an error floor is avoided. The same discussion applies to iBDD-SR [12, 19], and iGMDD-SR [15]. For the simulation of BMP-GMDD, iBDD-SR, and iGMDD-SR in Fig. 3 we considered 8 decoding iterations of the algorithms appended with 2 iBDD iterations.

VI. CONCLUSION

We proposed a new message passing decoding algorithm for product codes based on generalized minimum distance decoding, i.e., error and erasure decoding, of the component codes, where the last stage of GMDD is based on the Hamming distance metric. The proposed algorithm, dubbed BMP-GMDD, exploits soft information but requires to exchange only hard decisions and a short ordered list of the least reliable bits between component decoders, hence introducing a limited increase in data flow compared to conventional iterative bounded distance decoding. For the considered scenario based on (256, 239, 6) double-error-correcting \( eBCH \) component codes, the proposed algorithm closes about 50% of the performance gap between iBDD and turbo product decoding and yields performance very close to that of the algorithm iGMDD-SR introduced in [15], with a much lower data flow, only 21.48% higher than that of iBDD. The increase in data flow is even lower for longer component codes. While in this paper we considered PCs, the proposed algorithm can be extended to other classes of product-like codes such as staircase codes. Overall, the proposed BMP-GMDD algorithm provides a very good performance-complexity tradeoff and is appealing for very high-throughput applications such as fiber-optic communications.

ACKNOWLEDGMENT

The authors would like to thank Dr. Christian Häger for providing the simulation results of anchor decoding in Fig. 3.

REFERENCES